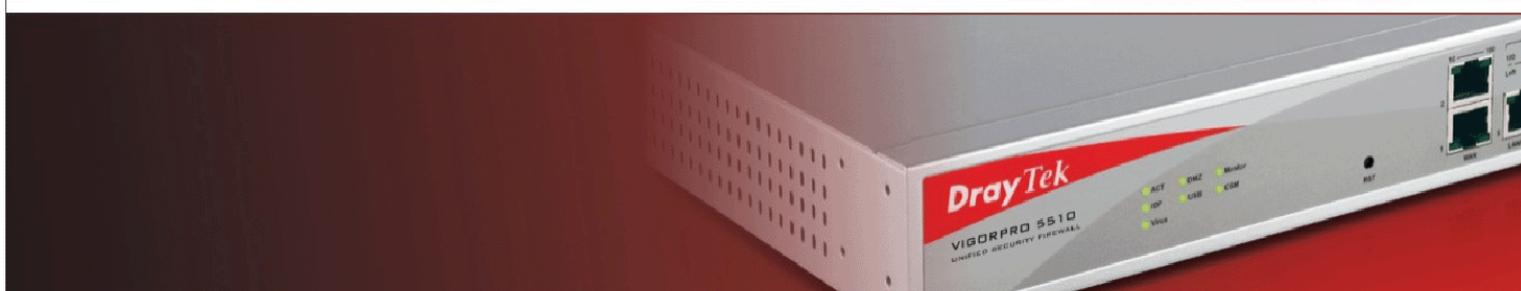


DrayTek

VigorPro 5510 Series

Unified Threat Management



Your reliable networking solutions partner

User's Guide

V2.1

VigorPro 5510 Series Unified Threat Management User's Guide

Version: 2.1

Firmware: V3.3.4

Date: 08/06/2010

Copyright 2010 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, Vista and Explorer are trademarks of Microsoft Corp.

Apple and Mac OS are registered trademarks of Apple Inc.

Other products may be trademarks or registered trademarks of their respective manufacturers.

Safety Instructions and Approval

Safety Instructions

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

Warranty

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

Be a Registered Owner

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

Firmware & Tools Updates

Please consult the DrayTek web site for more information on newest firmware, tools and documents. For more detailed information, please refer to <http://www.draytek.com>



Parts of the anti-virus features are powered by Kaspersky Lab ZAO. For more detailed information, please refer to <http://www.kaspersky.com>.

European Community Declarations

Manufacturer: DrayTek Corp.
Address: No. 26, Fu Shing Road, HuKou Township, HsinChu Industrial Park, Hsin-Chu, Taiwan 303
Product: VigorPro 5510

DrayTek Corp. declares that VigorPro 5510 Series is in compliance with the following essential requirements and other relevant provisions of R&TTE Directive 1999/5/EEC.

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

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

Regulatory Information

Federal Communication Commission Interference Statement

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

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

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

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

Taiwanese BSMI (Bureau of Standards, Metrology and Inspection) A Warning:

Warning: This is a Class A product. In a domestic environment this product may cause radio interference in which case the user may be required to take adequate measures.

Please visit <http://www.draytek.com/user/AboutRegulatory.php>.



This product is designed for the ISDN and 2.4GHz WLAN network throughout the EC region and Switzerland with restrictions in France. Please see the user manual for the applicable networks on your product.

Table of Contents

1

Preface	1
1.1 Web Configuration Buttons Explanation	1
1.2 LED Indicators and Connectors	2
1.2.1 For VigorPro 5510	2
1.2.2 For VigorPro 5510Gi.....	4
1.3 Hardware Installation	6
1.4 Printer Installation	7

2

Configuring Basic Settings	13
2.1 Changing Password.....	13
2.2 Quick Start Wizard	15
2.2.1 PPPoE	16
2.2.2 PPTP.....	18
2.2.3 Static IP.....	19
2.2.4 DHCP.....	20
2.3 Service Activation Wizard.....	21
2.4 Online Status.....	25
2.5 Saving Configuration.....	27

3

Advanced Web Configuration	29
3.1 WAN	29
3.1.1 Basics of Internet Protocol (IP) Network.....	29
3.1.2 Network Connection by 3G USB Modem	30
3.1.3 General Setup.....	30
3.1.4 Internet Access	33
3.1.5 Load-Balance Policy	42
3.2 LAN	45
3.2.1 Basics of LAN	45
3.2.2 General Setup.....	47
3.2.3 Static Route	50
3.2.4 VLAN.....	52
3.2.5 Bind IP to MAC	53
3.3 NAT	55
3.3.1 Port Redirection.....	55
3.3.2 DMZ Host.....	59
3.3.3 Open Ports.....	61
3.3.4 Address Mapping.....	62
3.4 Firewall.....	64

3.4.1 Basics for Firewall.....	64
3.4.2 General Setup.....	66
3.4.3 Filter Setup	71
3.4.4 DoS Defense	78
3.5 Objects Settings	81
3.5.1 IP Object	82
3.5.2 IP Group	84
3.5.3 Service Type Object	85
3.5.4 Service Type Group.....	86
3.5.5 Keyword Object	87
3.5.6 Keyword Group.....	88
3.5.7 File Extension Object.....	89
3.5.8 IM Object	91
3.5.9 P2P Object.....	93
3.5.10 Misc Object	94
3.6 CSM	95
3.6.1 APP Enforcement Profile	97
3.6.2 URL Content Filter Profile.....	97
3.6.3 Web Content Filter Profile.....	101
3.7 Defense Configuration	105
3.7.1 Anti-Intrusion.....	105
3.7.2 Anti-Virus	109
3.7.3 Anti-Spam	116
3.7.4 Activation for Anti-Intrusion/Anti-Virus/Anti-Spam/Web-Filter Service	120
3.7.5 AI/AV Auto Block	122
3.7.6 Signature Upgrade.....	124
3.7.7 Status.....	127
3.8 Bandwidth Management	128
3.8.1 Sessions Limit.....	128
3.8.2 Bandwidth Limit	129
3.8.3 Quality of Service.....	131
3.9 Applications	138
3.9.1 Dynamic DNS	138
3.9.2 Schedule.....	140
3.9.3 RADIUS/LDAP	142
3.9.4 UPnP.....	144
3.9.5 IGMP	146
3.9.6 Wake On LAN.....	146
3.10 VPN and Remote Access.....	148
3.10.1 Remote Access Control.....	148
3.10.2 PPP General Setup	149
3.10.3 IPSec General Setup.....	150
3.10.4 IPSec Peer Identity	151
3.10.5 Remote Dial-in User	153
3.10.6 LAN to LAN.....	158
3.10.7 VPN TRUNK Management.....	167
3.10.8 Connection Management	178
3.11 Certificate Management	179
3.11.1 Local Certificate	179
3.11.2 Trusted CA Certificate	183
3.11.3 Certificate Backup.....	184
3.12 ISDN.....	185

3.12.1 Basic Concept.....	185
3.12.2 General Setup.....	185
3.12.3 Dial to a Single ISP/Dial to Dual ISPs	185
3.12.4 Virtual TA	189
3.12.5 Call Control	192
3.13 Wireless LAN	194
3.13.1 Basic Concepts.....	194
3.13.2 General Setup.....	197
3.13.3 Security.....	199
3.13.4 Access Control.....	201
3.13.5 WDS.....	202
3.13.6 AP Discovery	206
3.13.7 Station List	207
3.13.8 Station Rate Control	208
3.14 VLAN	208
3.14.1 Wired VLAN	209
3.14.2 Wireless VLAN.....	210
3.14.3 VLAN Cross Setup.....	213
3.14.4 Wireless Rate Control.....	215
3.15 SSL VPN	216
3.15.1 General Setup.....	216
3.15.2 SSL Web Proxy	217
3.15.3 SSL Application	218
3.15.4 User Account	220
3.15.5 Online User Status.....	222
3.16 System Maintenance.....	223
3.16.1 System Status.....	223
3.16.2 TR-069 Setting.....	224
3.16.3 Administrator Password.....	226
3.16.4 Configuration Backup	227
3.16.5 Syslog/Mail Alert	228
3.16.6 Time and Date	231
3.16.7 Management.....	232
3.16.8 Reboot System	233
3.16.9 Firmware Upgrade	234
3.17 Diagnostics.....	235
3.17.1 Dial-out Trigger	235
3.17.2 Routing Table	236
3.17.3 ARP Cache Table	236
3.17.4 DHCP Table.....	237
3.17.5 NAT Sessions Table	237
3.17.6 Wireless VLAN Online Station Table.....	238
3.17.7 LAN Security Monitor.....	238
3.17.8 Traffic Graph.....	240
3.17.9 Ping Diagnosis.....	241
3.17.10 Trace Route	242
3.17.11 AV/AI Top 10	243
3.17.12 Web Firewall Syslog	244

4

Registration for the Router245

4.1 Creating and Activating an Account from MyVigor Website.....	245
--	-----

4.2 Creating and Activating an Account from Router Web Configurator.....	249
4.3 Registering Your Vigor Router	254
4.4 Activating Anti-Virus/Anti-Intrusion/Anti-Spam/WCF Service	257
4.4.1 For Anti-Virus and Anti-Intrusion Service	257
4.4.2 For Anti-Spam Service.....	262
4.4.3 For WCF (Web Content Filter) Service.....	266
4.5 Backup and Upgrade Signature for Anti-Intrusion/Anti-Virus	270
4.6 Enabling Anti-Virus/Anti-Intrusion/Anti-Spam/WCF.....	271

5

Application and Examples273

5.1 Create a LAN-to-LAN Connection Between Remote Office and Headquarter	273
5.2 Create a Remote Dial-in User Connection Between the Teleworker and Headquarter.....	280
5.3 QoS Setting Example.....	284
5.4 LAN – Created by Using NAT	287
5.5 Upgrade Firmware for Your Router	289
5.6 Request a certificate from a CA server on Windows CA Server.....	292
5.7 Request a CA Certificate and Set as Trusted on Windows CA Server	297

6

Trouble Shooting299

6.1 Checking If the Hardware Status Is OK or Not.....	299
6.2 Checking If the Network Connection Settings on Your Computer Is OK or Not	299
6.3 Pinging the Router from Your Computer	302
6.4 Checking If the ISP Settings are OK or Not.....	303
6.5 Backing to Factory Default Setting If Necessary	305
6.6 Contacting Your Dealer	306

1

Preface

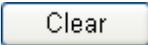
VigorPro 5510 is a UTM router with dual-WAN interface. It provides policy-based load-balance, fail-over and BoD (Bandwidth on Demand), also it integrates IP layer QoS, NAT session/bandwidth management to help users control works well with large bandwidth.

By adopting hardware-based VPN platform, hardware encryption of AES/DES/3DS and hardware key hash of SHA-1/MD5, the router increases the performance of VPN greatly, and offers several protocols (such as IPSec/PPTP/L2TP) with up to 200 VPN tunnels.

The object-originated design used in SPI (Stateful Packet Inspection) firewall allows users to set firewall policy with ease. CSM (Content Security Management) provides users control and management in IM (Instant Messenger), P2P (Peer to Peer), Web Content Filter and URL Content Filter more efficiency than before. By the way, DoS/DDoS prevention and URL/Web content filter strengthen the security outside and control inside.

1.1 Web Configuration Buttons Explanation

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

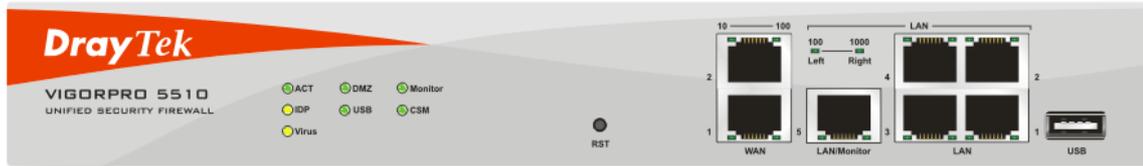
	Save and apply current settings.
	Cancel current settings and recover to the previous saved settings.
	Clear all the selections and parameters settings, including selection from drop-down list. All the values must be reset with factory default settings.
	Add new settings for specified item.
	Edit the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

Note: For the other buttons shown on the web pages, please refer to Chapter 3 for detailed explanation.

1.2 LED Indicators and Connectors

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

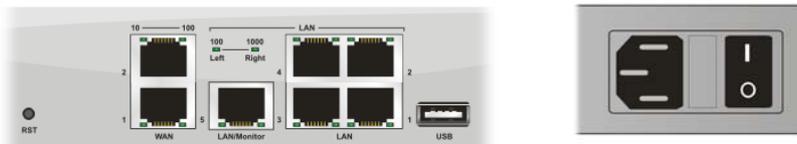
1.2.1 For VigorPro 5510



LED	Status	Explanation
ACT (Activity)	Blinking	The router is powered on and running normally.
	Off	The router is powered off.
IDP (Intrusion Detection and Prevention)	On (Yellow)	The anti-intrusion function is enabled.
Virus	On (Yellow)	The anti-virus function is enabled.
DMZ	On	DMZ Host is specified in certain site.
USB	On	A USB device is connected and active.
	Blinking	The data is transmitting.
Monitor	On	LAN traffic monitor is active.
CSM	On	The profile(s) for IM/P2P, Web Content Filter, and/or URL Content Filter application has been activated. (It is enabled from Firewall >> General Setup).
	Off	No IM/P2P, Web Content Filter, and/or URL Content Filter application has been activated.

LED on Connector

WAN	10 (left LED)	On	The port is connected with 10Mbps.
		Off	The port is disconnected.
		Blinking	The data is transmitting.
	100 (right LED)	On	The port is connected with 100Mbps.
		Off	The port is disconnected.
		Blinking	The data is transmitting.
LAN/Monitor LAN	100 (left LED)	On	The port is connected with 100Mbps.
		Off	The port is disconnected.
		Blinking	The data is transmitting.
	1000 (right LED)	On	The port is connected with 1000Mbps.
		Off	The port is disconnected.
		Blinking	The data is transmitting.



Interface	Description
RST (Factory Reset)	Restore the default settings. Usage: Turn on the router (ACT LED is blinking). Press the hole and keep for more than 5 seconds. When you see the ACT LED begins to blink rapidly than usual, release the button. Then the router will restart with the factory default configuration.

WAN(1/2)	Connector for remote networked devices.
LAN/Monitor	Connector for local networked devices.
LAN (1-4)	Connector for local networked devices.
USB	Connector for a USB device.
	Connector for a power cord with 100-240VAC (inlet).
	Power Switch. "1" is ON; "0" is OFF.

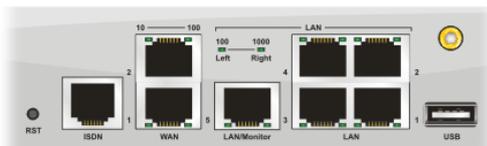
1.2.2 For VigorPro 5510Gi



LED	Status	Explanation
ACT (Activity)	Blinking	The router is powered on and running normally.
	Off	The router is powered off.
IDP (Intrusion Detection and Prevention)	On (Yellow)	The anti-intrusion function is enabled.
Virus	On (Yellow)	The anti-virus function is enabled.
DMZ	On	DMZ Host is specified in certain site.
USB	On	A USB device is connected and active.
	Blinking	The data is transmitting.
WLAN	On	Wireless access point is ready.
	Blinking	Ethernet packets are transmitting over wireless LAN.
	Off	The WLAN function is inactive.
Monitor	On	LAN traffic monitor is active.
CSM	On	The profile(s) for IM/P2P, Web Content Filter, and/or URL Content Filter application has been activated. (It is enabled from Firewall >> General Setup).
	Off	No IM/P2P, Web Content Filter, and/or URL Content Filter application has been activated.
ISDN	On	The ISDN service function is active.
	Blinking	A successful connection on the ISDN BRI B1/B2 channel.

LED on Connector

WAN	10 (left LED)	On	The port is connected with 10Mbps.
		Off	The port is disconnected.
		Blinking	The data is transmitting.
	100 (right LED)	On	The port is connected with 100Mbps.
		Off	The port is disconnected.
		Blinking	The data is transmitting.
LAN/Monitor LAN	100 (left LED)	On	The port is connected with 100Mbps.
		Off	The port is disconnected.
		Blinking	The data is transmitting.
	1000 (right LED)	On	The port is connected with 1000Mbps.
		Off	The port is disconnected.
		Blinking	The data is transmitting.



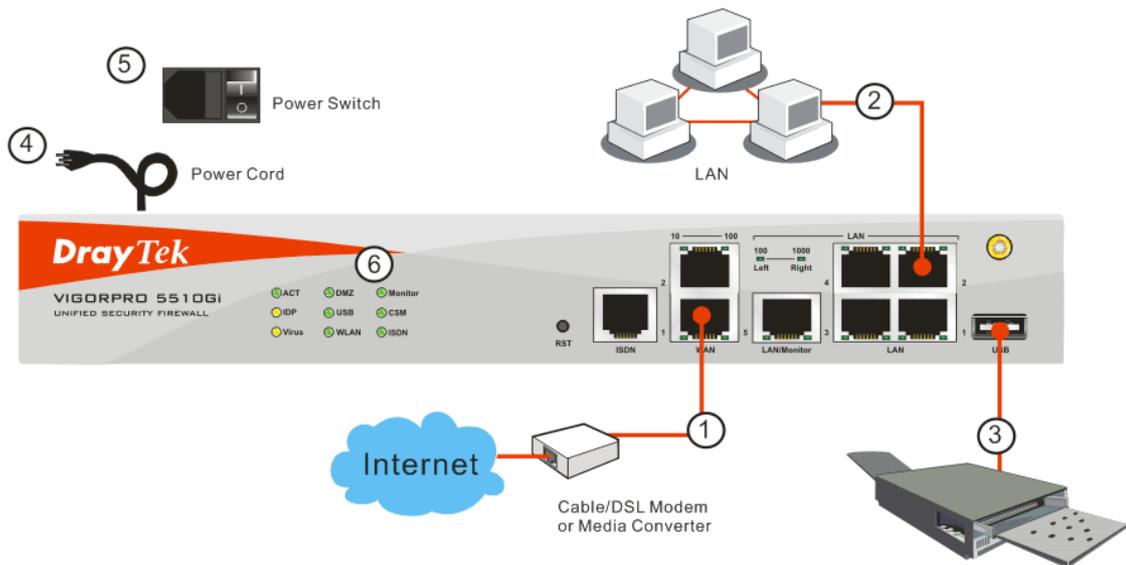
Interface	Description
RST (Factory Reset)	Restore the default settings. Usage: Turn on the router (ACT LED is blinking). Press the hole and keep for more than 5 seconds. When you see the ACT LED begins to blink rapidly than usual, release the button. Then the router will restart with the factory default

	configuration.
ISDN	Connector for ISDN line.
WAN(1/2)	Connector for remote networked devices.
LAN/Monitor	Connector for local networked devices.
LAN (1-4)	Connector for local networked devices.
USB	Connector for a USB device.
	Connector for a power cord with 100-240VAC (inlet).
	Power Switch. "1" is ON; "0" is OFF.

1.3 Hardware Installation

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

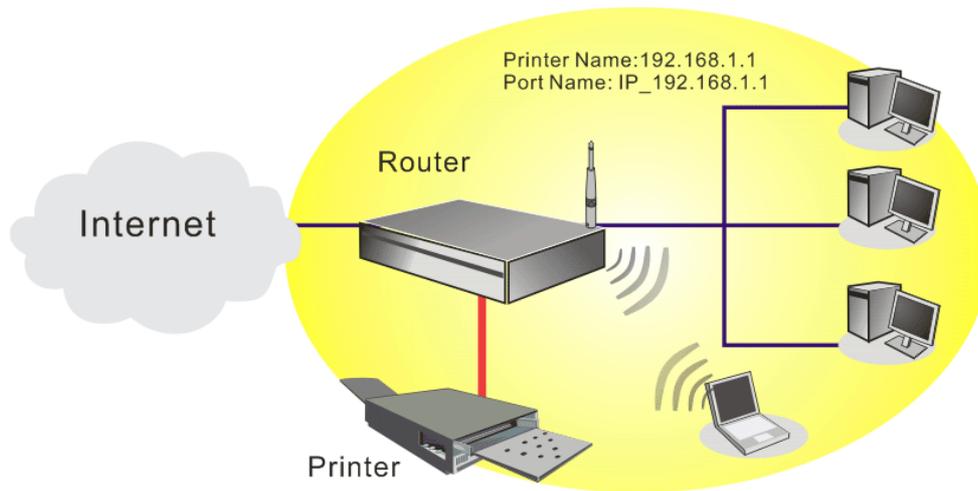
1. Connect a cable Modem/DSL Modem/Media Converter (depends on your requirement) to any WAN port of router with Ethernet cable (RJ-45). The **WAN1/WAN2** LED (Left or Right) will light up according to the speed (100 or 10) of the device that it connected.
2. Connect one end of an Ethernet cable (RJ-45) to one of the **LAN** ports of the router and the other end of the cable (RJ-45) into the Ethernet port on your computer. The **LAN** LED (Left or Right) will light up according to the speed (100 or 10) of the device that it connected.
3. Connect one end of the power adapter to the router's power port on the rear panel, and the other side into a wall outlet.
4. Power on the device by pressing down the power switch on the rear panel.
5. The system starts to initiate. After completing the system test, the **ACT** LED will light up and start blinking.



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

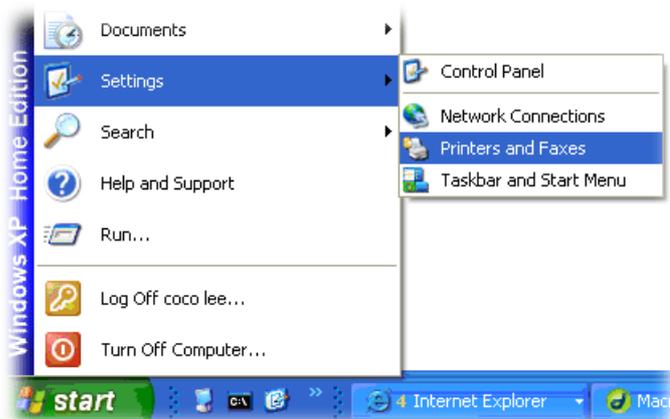
1.4 Printer Installation

You can install a printer onto the router for sharing printing. All the PCs connected this router can print documents via the router. The example provided here is made based on Windows XP/2000. For Windows 98/SE, please visit www.draytek.com.

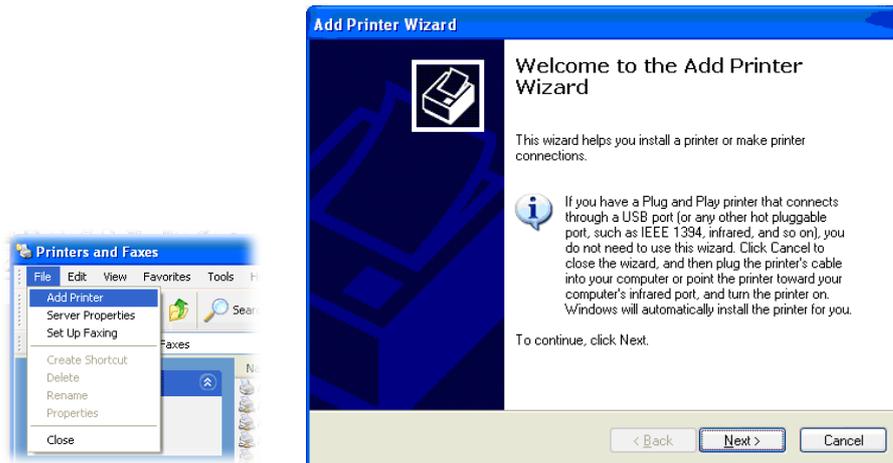


Before using it, please follow the steps below to configure settings for connected computers (or wireless clients).

1. Connect the printer with the router through USB/parallel port.
2. Open **Start->Settings-> Printer and Faxes**.



3. Open **File->Add a New Computer**. A welcome dialog will appear. Please click **Next**.



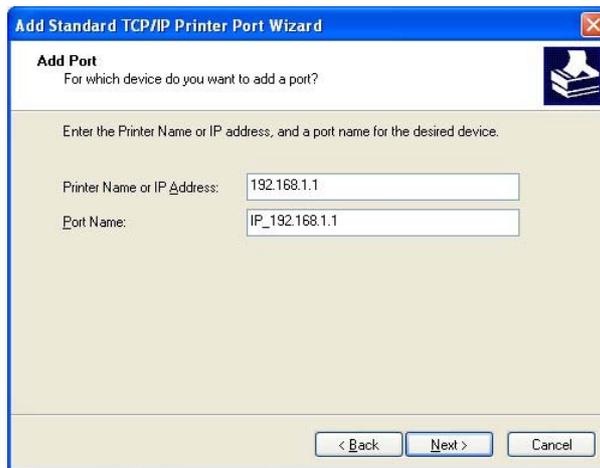
4. Click **Local printer attached to this computer** and click **Next**.



5. In this dialog, choose **Create a new port Type of port** and use the drop down list to select **Standard TCP/IP Port**. Click **Next**.



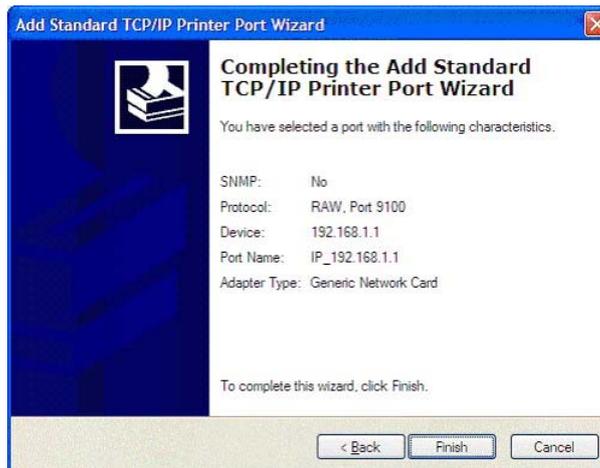
- In the following dialog, type **192.168.1.1** (router's LAN IP) in the field of **Printer Name or IP Address** and type **IP_192.168.1.1** as the port name. Then, click **Next**.



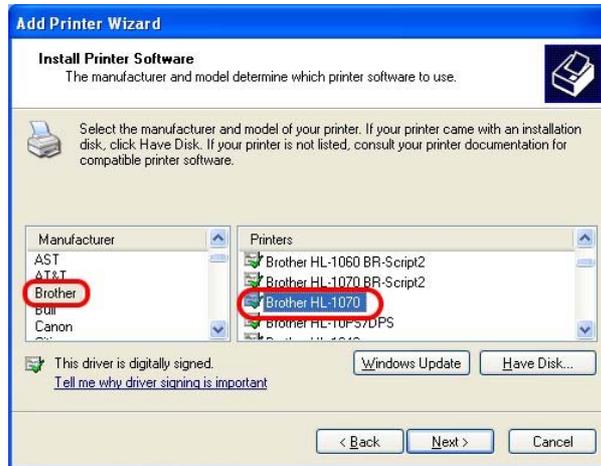
- Click **Standard** and choose **Generic Network Card**.



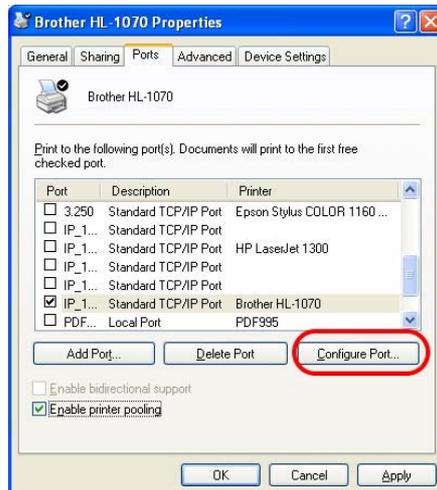
- Then, in the following dialog, click **Finish**.



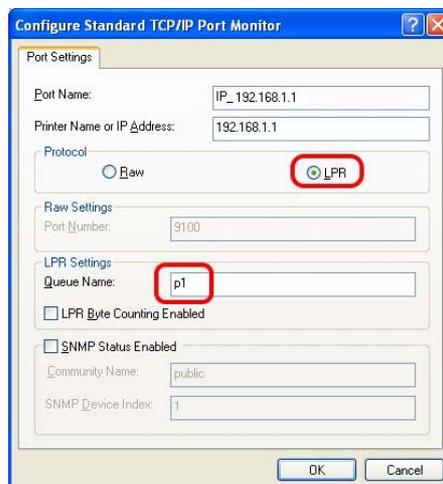
9. Now, your system will ask you to choose right name of the printer that you installed onto the router. Such step can make correct driver loaded onto your PC. When you finish the selection, click **Next**.



10. For the final stage, you need to go back to **Control Panel-> Printers** and edit the property of the new printer you have added.



11. Select "**LPR**" on Protocol, type **p1** (number 1) as Queue Name. Then click **OK**. Next please refer to the red rectangle for choosing the correct protocol and UPR name.



The printer can be used for printing now. Most of the printers with different manufacturers are compatible with vigor router.

Note 1: Some printers with the fax/scanning or other additional functions are not supported. If you do not know whether your printer is supported or not, please visit www.draytek.com to find out the printer list. Open **Support >FAQ**; find out the link of **Printer Server** and click it; then click the **What types of printers are compatible with Vigor router?** link.

Home > Support > **FAQ**

FAQ - Basic

01. What are the differences among these firmware file formats ?
02. How could I get the telnet command for routers ?
03. How can I backup/restore my configuration settings ?
04. How do I reset/clear the router's password ?
05. How to bring back my router to its default value ?
06. How do I tell the type of my Vigor Router is AnnexA or AnnexB? (For ADSL model only)
07. Ways for firmware upgrade.
08. Why is SNMP removed in firmware 2.3.6 and above for Vigor2200 Series routers?
09. I failed to upgrade Vigor Router's firmware from my Mac machine constantly, what should I do?
10. How to upgrade firmware of Vigor Router remotely ?

FAQ

- Basic
- Advanced
- VPN
- DHCP
- Wireless
- VoIP
- QoS
- ISDN
- Firewall / IP Filter
- Printer Server**
- USB/ISDN TA
- USB

FAQ - Printer Server

01. How do I configure LPR printing on Windows2000/XP ?
02. How do I configure LPR printing on Windows98/Me ?
03. How do I configure LPR printing on Linux boxes ?
04. Why there are some strange print-out when I try to print my documents through Vigor210 4P / 2300's print server?
- 05. What types of printers are compatible with Vigor router?**
06. What are the limitations in the USB Printer Port of Vigor Router ?
07. What is the printing buffer size of Vigor Router ?
08. How do I configure LPR printing on Mac OSX ?
09. How do I configure LPR printing on My Windows Vista ?

Note 2: Vigor router supports printing request from computers via LAN ports but not WAN port.

This page is left blank.

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 “admin/admin” as the username/password on the window. Next click **OK** for next screen.

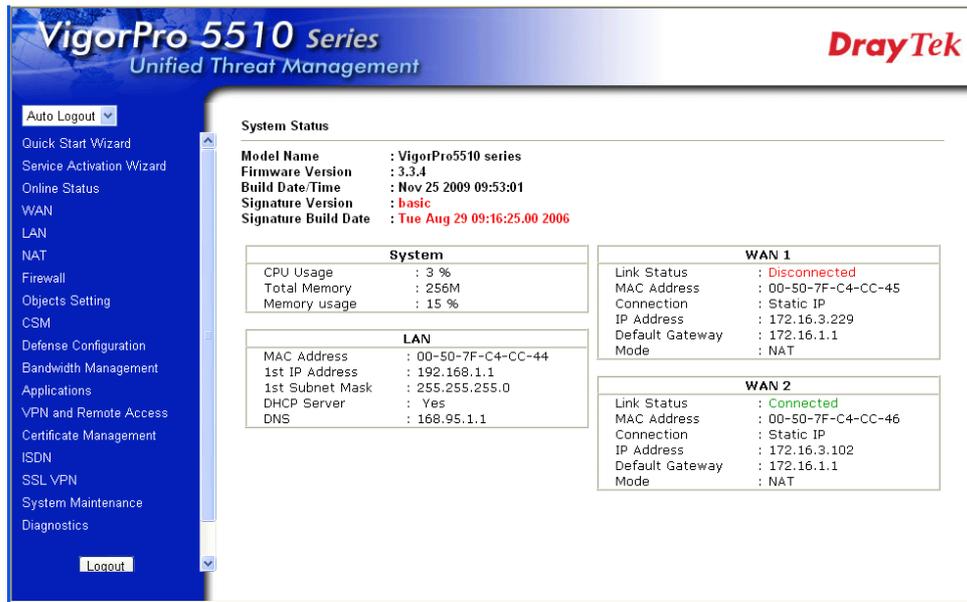
Username

Password

Login

Copyright©, DrayTek Corp. All Rights Reserved. **DrayTek**

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



Note: The home page will change slightly in accordance with the router you have.

- 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"/>
Confirm Password	<input type="text"/>

OK

- 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 **Confirm 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

Enter login password

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

New Password

Confirm Password

On the next page as shown below, please select the WAN interface that you use. Choose **Auto negotiation** as the physical type for your router. Then click **Next** for next step.

Quick Start Wizard

Select WAN Interface

Select WAN Interface:

Display Name:

Physical Mode: Ethernet

Physical Type:

On the next page as shown below, please select the appropriate Internet access type according to the information from your ISP. For example, you should select PPPoE mode if the ISP provides you PPPoE interface. Then click **Next** for next step.

Quick Start Wizard

Connect to Internet

WAN 1
Select one of the following Internet Access types provided by your ISP.

PPPoE
 PPTP
 Static IP
 DHCP

< Back Next > Finish Cancel

In the **Quick Start Wizard**, you can configure the router to access the Internet with different protocol/modes such as **PPPoE**, **PPTP**, **Static IP** or **DHCP**. The router supports the DSL WAN interface for Internet access.

2.2.1 PPPoE

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

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

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

Quick Start Wizard

PPPoE Client Mode

WAN 1
Enter the user name and password provided by your ISP.

User Name
Password
Confirm Password

< Back Next > Finish Cancel

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 for confirmation.

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

Quick Start Wizard

Please confirm your settings:

WAN Interface:	WAN1
Physical Mode:	Ethernet
Physical Type:	Auto negotiation
Internet Access:	PPPoE

Click **Back** to modify changes if necessary. Otherwise, click **Finish** to save the current settings and restart the Vigor router.

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

Quick Start Wizard Setup OK !!!

2.2.2 PPTP

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

Quick Start Wizard

PPTP Client Mode

WAN 1	
Enter the user name, password, WAN IP configuration and PPTP server IP provided by your ISP.	
User Name	<input type="text" value="admin"/>
Password	<input type="password" value="••••"/>
Confirm Password	<input type="password" value="••••"/>
WAN IP Configuration	
<input type="radio"/> Obtain an IP address automatically	
<input checked="" type="radio"/> Specify an IP address	
IP Address	<input type="text" value="172.16.3.229"/>
Subnet Mask	<input type="text" value="255.255.0.0"/>
PPTP Server IP	<input type="text"/>

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

Quick Start Wizard

Please confirm your settings:

WAN Interface:	WAN1
Physical Mode:	Ethernet
Physical Type:	Auto negotiation
Internet Access:	PPTP

Click **Back** to modify changes if necessary. Otherwise, click **Finish** to save the current settings and restart the Vigor router.

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

Quick Start Wizard Setup OK !!!

2.2.3 Static IP

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

Quick Start Wizard

Static IP Client Mode

WAN 1	
Enter the Static IP configuration provided by your ISP.	
WAN IP	<input type="text" value="172.16.3.229"/>
Subnet Mask	<input type="text" value="255.255.0.0"/>
Gateway	<input type="text" value="172.16.1.1"/>
Primary DNS	<input type="text" value="168.95.1.1"/>
Secondary DNS	<input type="text"/> (optional)

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

Quick Start Wizard

Please confirm your settings:

WAN Interface:	WAN1
Physical Mode:	Ethernet
Physical Type:	Auto negotiation
Internet Access:	Static IP

Click **Back** to modify changes if necessary. Otherwise, click **Finish** to save the current settings and restart the Vigor router.

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

Quick Start Wizard Setup OK !!!

2.2.4 DHCP

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

Quick Start Wizard

DHCP Client Mode

WAN 1

If your ISP requires you to enter a specific host name or specific MAC address, please enter it in.

Host Name (optional)

MAC (optional)

< Back

Next >

Finish

Cancel

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

Quick Start Wizard

Please confirm your settings:

WAN Interface: WAN1
Physical Mode: Ethernet
Physical Type: Auto negotiation
Internet Access: DHCP

Click **Back** to modify changes if necessary. Otherwise, click **Finish** to save the current settings and restart the Vigor router.

< Back

Next >

Finish

Cancel

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

Quick Start Wizard Setup OK !!!

2.3 Service Activation Wizard

1. Open Service Activation Wizard.



2. The screen of **Service Activation Wizard** will be shown as follows. Choose the one you need and click **Next**. In this case, we choose to activate free trail edition.

Service Activation Wizard

Select the service type that you want to activate

This wizard is used for activating Anti-Intrusion / Anti-Spam service. Please choose the edition you need.

- Free trial edition for 30 days
 Formal edition with license key

Next >

Finish

Cancel

Free trial edition: if it is the first time that you register the service, please use the option.

Formal edition with license key: you can extend the license valid time manually.

3. In the following page, you can activate the AV/AI, AS and/or Web content filter service at the same time or individually. When you finish the selection, please click **Next**.

Service Activation Wizard

Select the service type that you want to activate

This product provides 30 days of free trial, please choose the item(s) you want to use.

For AI/AV service:

Anti-Intrusion /Anti-Virus (DT-KL) Activation Date : 2010-02-26

Anti-Intrusion /Anti-Virus (DT-DT) Activation Date : 2010-02-26

For WCF service:

Web Content Filter (CT-CF) Activation Date : 2010-02-26

For AS service:

Anti-Spam (CTCH) Activation Date : 2010-02-26

< Back Next > Finish Cancel

4. Setting confirmation page will be displayed as follows, please click **Next**.

Service Activation Wizard

Please confirm your settings

Service Type : Trial version

Service Activated : Anti-Intrusion /Anti-Virus (DT-KL)

 Web Content Filter (CT-CF)

 Anti-Spam (CTCH)

Please click **Back** to re-select service type you to activate.

< Back Next > Finish Cancel

5. Wait for a moment till the following page appears.

Service Activation Wizard

Connection Succeeded!

Please check the following item(s) to enable the AI/AV or WCF or AS services on your router.

Enable Anti-Intrusion / Anti-Virus

Enable Web Content Filter

Enable Anti-Spam

Next > Finish

When such page appears, you can enable or disable these services for your necessity. Then, click **Finish**.

- Now, the web page will display the service(s) with valid time that you have activated according to your selection(s).

Service Activation Wizard

Server Enabled!

DrayTek Service Activation

Service Name	Start Date	Expire Date	Status
Anti-Virus	2010-02-26	2010-03-29	DT-KL
Web Content filter	2010-02-26	2010-03-29	CT-CF
Anti-Spam	2010-02-26	2010-03-29	CTCH

Please check if the license fits with the service provider of your signature. To ensure normal operation for your router, update your signature again is recommended.

Copyright © DrayTek Corp. All Rights Reserved.

- Open **Defense configuration >>Activation** to check the services status.

Defense Configuration >> Activation

Activate via interface : WAN 1

Anti-Intrusion/Anti-Virus License

Activate

[Status:DT-KL] [Start Date:2010-02-26 Expire Date:2010-03-29]

Anti-Spam License

Activate

[Status:CTCH] [Start Date:2010-02-26 Expire Date:2010-03-29]

Web-Filter License

Activate

[Status:CT-CF] [Start Date:2010-02-26 Expire Date:2010-03-29]

Authentication Message

```
WebFilter, Get new license successful, 2010-02-26 01:16:50
Anti-Spam, Get new license successful, 2010-02-26 01:16:50
AV/AI, Get new license successful, 2010-02-26 01:16:50
```

Note: If you want to use email alert or syslog, please configure the [SysLog/Mail Alert Setup](#) page.
If you change the service provider, the configuration of the function will be reset.

If you need to extend the license valid time, you can also use the **Service Activation Wizard** again to reach your goal by clicking the radio button of **Formal edition with license key** and clicking **Next**.

Service Activation Wizard

Select the service type that you want to activate

This wizard is used for activating

- Anti-Intrusion
- Anti-Spam service
- Web Content Filter

Please choose the edition you need.

Free trial edition

Formal edition with license key

Service Activation Wizard

Select the service type that you want to activate

Please choose the item you want to use.

For AI/AV service:

Anti-Intrusion / Anti-Virus (DT-KL) License Agreement Activation Date : 2010-03-30 **select**
Enter your License key:

Anti-Intrusion / Anti-Virus (DT-DT) License Agreement Activation Date : 2010-02-26 **select**
Enter your License key:

For WCF service:

Web Content Filter (CT-CF) License Agreement Activation Date : 2010-03-30 **select**
Enter your License key:

For AS service:

Anti-Spam (CTCH) License Agreement Activation Date : 2010-03-30 **select**
Enter your License key:

I have read and accept the above Agreement.(Please check this box.)

Note :The activation date is brought out by the server automatically and cannot be changed.

2.4 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/PPTP** as the protocol, you will find out a link of **Dial PPPoE/PPPoA** or **Drop PPPoE/PPPoA** in the Online Status web page.

Online status for PPPoE (WAN2)

System Status				System Uptime: 0:0:18		
LAN Status		Primary DNS: 168.95.192.1		Secondary DNS: 168.95.1.1		
IP Address		TX Packets	RX Packets			
192.168.1.1		77	56			
WAN 1 Status						
Enable	Line	Name	Mode	Up Time		
Yes	Ethernet		Static IP	0:00:11		
IP	GW IP	TX Packets	TX Rate	RX Packets	RX Rate	
192.168.5.100	192.168.5.1	3	17	3	42	
WAN 2 Status						>> Drop PPPoE
Enable	Line	Name	Mode	Up Time		
Yes	Ethernet		PPPoE	0:00:11		
IP	GW IP	TX Packets	TX Rate	RX Packets	RX Rate	
61.230.209.207	61.230.192.254	10	16	10	12	

Online status for PPTP (for WAN2)

System Status				System Uptime: 0:0:18		
LAN Status		Primary DNS: 168.95.192.1		Secondary DNS: 168.95.1.1		
IP Address		TX Packets	RX Packets			
192.168.1.1		77	56			
WAN 1 Status						
Enable	Line	Name	Mode	Up Time		
Yes	Ethernet		Static IP	0:00:11		
IP	GW IP	TX Packets	TX Rate	RX Packets	RX Rate	
192.168.5.100	192.168.5.1	3	17	3	42	
WAN 2 Status						>> Drop PPPoE
Enable	Line	Name	Mode	Up Time		
Yes	Ethernet	WAN2	PPTP	0:00:15		
IP	GW IP	TX Packets	TX Rate	RX Packets	RX Rate	
192.168.29.202	192.168.29.1	103	119	14	6	

Online status for Static IP (for WAN1)

System Status				System Uptime: 0:0:18		
LAN Status		Primary DNS: 168.95.192.1		Secondary DNS: 168.95.1.1		
IP Address		TX Packets	RX Packets			
192.168.1.1		77	56			
WAN 1 Status						
Enable	Line	Name	Mode	Up Time		
Yes	Ethernet		Static IP	0:00:11		
IP	GW IP	TX Packets	TX Rate	RX Packets	RX Rate	
192.168.5.100	192.168.5.1	3	17	3	42	
WAN 2 Status						>> Drop PPPoE
Enable	Line	Name	Mode	Up Time		
Yes	Ethernet		PPPoE	0:00:11		
IP	GW IP	TX Packets	TX Rate	RX Packets	RX Rate	
61.230.209.207	61.230.192.254	10	16	10	12	

Online status for DHCP

System Status			System Uptime: 0:6:52		
LAN Status		Primary DNS: 168.95.192.1		Secondary DNS: 168.95.1.1	
IP Address	TX Packets	RX Packets			
192.168.1.1	677	558			
WAN 1 Status					>> Release
Enable	Line	Name	Mode	Up Time	
Yes	Ethernet		DHCP Client	0:06:45	
IP	GW IP	TX Packets	TX Rate	RX Packets	RX Rate
192.168.5.10	192.168.5.1	89	3	68	3
WAN 2 Status					>> Drop PPPoE
Enable	Line	Name	Mode	Up Time	
Yes	Ethernet		PPPoE	0:01:34	
IP	GW IP	TX Packets	TX Rate	RX Packets	RX Rate
61.230.213.66	61.230.192.254	21	7	45	13

Detailed explanation is shown below:

Primary DNS	Displays the IP address of the primary DNS.
Secondary DNS	Displays the IP address of the secondary DNS.
LAN Status	
IP Address	Displays the IP address of the LAN interface.
TX Packets	Displays the total transmitted packets at the LAN interface.
RX Packets	Displays the total number of received packets at the LAN interface.
WAN1/2 Status	
Line	Displays the physical connection (Ethernet) of this interface.
Name	Displays the name set in WAN1/WAN web page.
Mode	Displays the type of WAN connection (e.g., PPPoE).
Up Time	Displays the total uptime of the interface.
IP	Displays the IP address of the WAN interface.
GW IP	Displays the IP address of the default gateway.
TX Packets	Displays the total transmitted packets at the WAN interface.
TX Rate	Displays the speed of transmitted octets at the WAN interface.
RX Packets	Displays the total number of received packets at the WAN interface.
RX Rate	Displays the speed of received octets at the WAN interface.

Note: The words in green mean that the WAN connection of that interface (WAN1/WAN2) is ready for accessing Internet; the words in red mean that the WAN connection of that interface (WAN1/WAN2) is not ready for accessing Internet.

2.5 Saving Configuration

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



Status: Ready

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

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

3 Advanced Web Configuration

After finished basic configuration of the router, you can access Internet with ease. For the people who want to adjust more setting 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 WAN

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

3.1.1 Basics of Internet Protocol (IP) Network

IP means Internet Protocol. Every device in an IP-based Network including 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 the host PCs can share a common Internet connection.

Get Your Public IP Address from ISP

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

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

3.1.2 Network Connection by 3G USB Modem

For 3G mobile communication through Access Point is popular more and more, VigorPro5510 adds the function of 3G network connection for such purpose. By connecting 3G USB Modem to the USB port of VigorPro5510, it can support HSDPA/UMTS/EDGE/GPRS/GSM and the future 3G standard (HSUPA, etc). VigorPro5510 with 3G USB Modem allows you to receive 3G signals at any place such as your car or certain location holding outdoor activity and share the bandwidth for using by more people. Users can use four LAN ports on the router to access Internet. Also, they can access Internet via SuperG wireless function of VigorPro5510G, and enjoy the powerful firewall, bandwidth management and VPN features of VigorPro5510 series.



After connecting into the router, 3G USB Modem will be regarded as the second WAN port. However, the original Ethernet WAN1 still can be used and Load-Balance can be done in the router. Besides, 3G USB Modem in WAN2 also can be used as backup device. Therefore, when WAN1 is not available, the router will use 3.5G for supporting automatically. The supported 3G USB Modem will be listed on Draytek web site. Please visit www.draytek.com for more detailed information.

Below shows the menu items for WAN.



3.1.3 General Setup

This section will introduce some general settings of Internet and explain the connection modes for WAN1 and WAN2 in details.

This router supports dual WAN function. It allows users to access Internet and combine the bandwidth of the dual WAN to speed up the transmission through the network. Each WAN port can connect to different ISPs, Even if the ISPs use different technology to provide telecommunication service (such as DSL, Cable modem, etc.). If any connection problem occurred on one of the ISP connections, all the traffic will be guided and switched to the normal communication port for proper operation. Please configure WAN1 and WAN2 settings.

This webpage allows you to set general setup for WAN1 and WAN respectively.

Note: In default, WAN1 and WAN2 are enabled.

General Setup

WAN1	WAN2
Enable: <input type="checkbox"/> Yes <input checked="" type="checkbox"/> No	Enable: <input type="checkbox"/> Yes <input checked="" type="checkbox"/> No
Display Name: <input type="text"/>	Display Name: <input type="text"/>
Physical Mode: Ethernet	Physical Mode: Ethernet
Physical Type: Auto negotiation	Physical Type: Auto negotiation
Load Balance Mode: Auto Weight	Load Balance Mode: Auto Weight
Line Speed(Kbps): DownLink <input type="text"/>	Line Speed(Kbps): DownLink <input type="text"/>
UpLink <input type="text"/>	UpLink <input type="text"/>
Active Mode: Always On	Active Mode: Always On
Active on demand:	Active on demand:
<input type="radio"/> WAN2 Fail	<input type="radio"/> WAN1 Fail
<input checked="" type="radio"/> WAN2 Upload speed exceed <input type="text"/> Kbps	<input checked="" type="radio"/> WAN1 Upload speed exceed <input type="text"/> Kbps
WAN2 Download speed exceed <input type="text"/> Kbps	WAN1 Download speed exceed <input type="text"/> Kbps

OK

Enable

Choose **Yes** to invoke the settings for this WAN interface. Choose **No** to disable the settings for this WAN interface.

Display Name

Type the description for the WAN1/WAN2 interface.

Physical Mode

For WAN1, the physical connection is done and fixed through Ethernet port; yet the physical connection for WAN2 is done through an Ethernet port (P1) or USB port. You cannot change it.

Physical Mode:

- Ethernet
- 3G USB Modem**

To use 3G network connection through 3G USB Modem, choose **3G USB Modem** as the physical mode in **WAN2**. Next, go to **WAN>> Internet Access**. 3G USB Modem is available for WAN2. You can choose **PPP** as the access mode and click Details Page for further configuration.

Internet Access

Index	Display Name	Physical Mode	Access Mode	
WAN1		Ethernet	Static or Dynamic IP	Details Page
WAN2		3G USB Modem	None	Details Page

- None
- PPP**

Physical Type

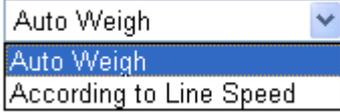
You can change the physical type for WAN2 or choose **Auto negotiation** for determined by the system.

Physical Type:

- Auto negotiation**
- 10M half duplex
- 10M full duplex
- 100M half duplex
- 100M full duplex

Load Balance Mode

If you know the practical bandwidth for your WAN interface, please choose the setting of **According to Line Speed**. Otherwise, please choose **Auto Weigh** to let the router reach the best load balance.

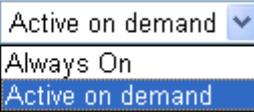
Load Balance Mode: 

Line Speed

If you choose **According to Line Speed** as the **Load Balance Mode**, please type the line speed for downloading and uploading through WAN1/WAN2. The unit is kbps.

Active Mode

Choose **Always On** to make the WAN connection (WAN1/WAN2) being activated always; or choose **Active on demand** to make the WAN connection (WAN1/WAN2) activated if it is necessary.

Active Mode: 

If you choose Active on demand, the Idle Timeout will be available for you to set for PPPoE and PPTP access modes in the Details Page of WAN>>Internet Access. In addition, there are three selections for you to choose for different purposes.

WAN2 Fail – It means the connection for WAN1 will be activated when WAN2 is failed.

WAN2 Upload speed exceed XX kbps – It means the connection for WAN1 will be activated when WAN2 Upload speed exceed certain value that you set in this box for 15 seconds.

WAN2 Download speed exceed XX kbps– It means the connection for WAN1 will be activated when WAN2 Download speed exceed certain value that you set in this box for 15 seconds.

WAN1 Fail – It means the connection for WAN2 will be activated when WAN1 is failed.

WAN1 Upload speed exceed XX kbps – It means the connection for WAN2 will be activated when WAN1 Upload speed exceed certain value that you set in this box for 15 seconds.

WAN1 Download speed exceed XX kbps– It means the connection for WAN2 will be activated when WAN1 Download speed exceed certain value that you set in this box for 15 seconds.

3.1.4 Internet Access

For the router supports dual WAN function, the users can set different WAN settings (for WAN1/WAN2) for Internet Access. Due to different physical mode for WAN1 and WAN2, the Access Mode for these two connections also varies slightly.

WAN >> Internet Access

Internet Access

Index	Display Name	Physical Mode	Access Mode	
WAN1		Ethernet	Static or Dynamic IP	Details Page
WAN2		Ethernet	None	Details Page

None
PPPoE
Static or Dynamic IP
PPTP

WAN >> Internet Access

Internet Access

Index	Display Name	Physical Mode	Access Mode	
WAN1		Ethernet	Static or Dynamic IP	Details Page
WAN2		3G USB Modem	None	Details Page

None
PPP

- Index** It shows the WAN modes that this router supports. WAN1 is the default WAN interface for accessing into the Internet. WAN2 is the optional WAN interface for accessing into the Internet when WAN 1 is inactive for some reason.
- Display Name** It shows the name of the WAN1/WAN2 that entered in general setup.
- Physical Mode** It shows the physical connection for WAN1 (Ethernet) /WAN2 (Ethernet or 3G USB Modem) according to the real network connection.

Internet Access

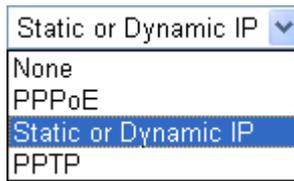
Index	Display Name	Physical Mode
WAN1		Ethernet
WAN2		Ethernet

Internet Access

Index	Display Name	Physical Mode
WAN1		Ethernet
WAN2		3G USB Modem

- Access Mode** Use the drop down list to choose a proper access mode. The details page of that mode will be popped up. If not, click Details Page for

accessing the page to configure the settings.



A dropdown menu with the title "Static or Dynamic IP" and a downward arrow. The menu is open, showing four options: "None", "PPPoE", "Static or Dynamic IP" (which is highlighted in blue), and "PPTP".

There are three access modes provided for PPPoE, Static or Dynamic IP and PPTP.

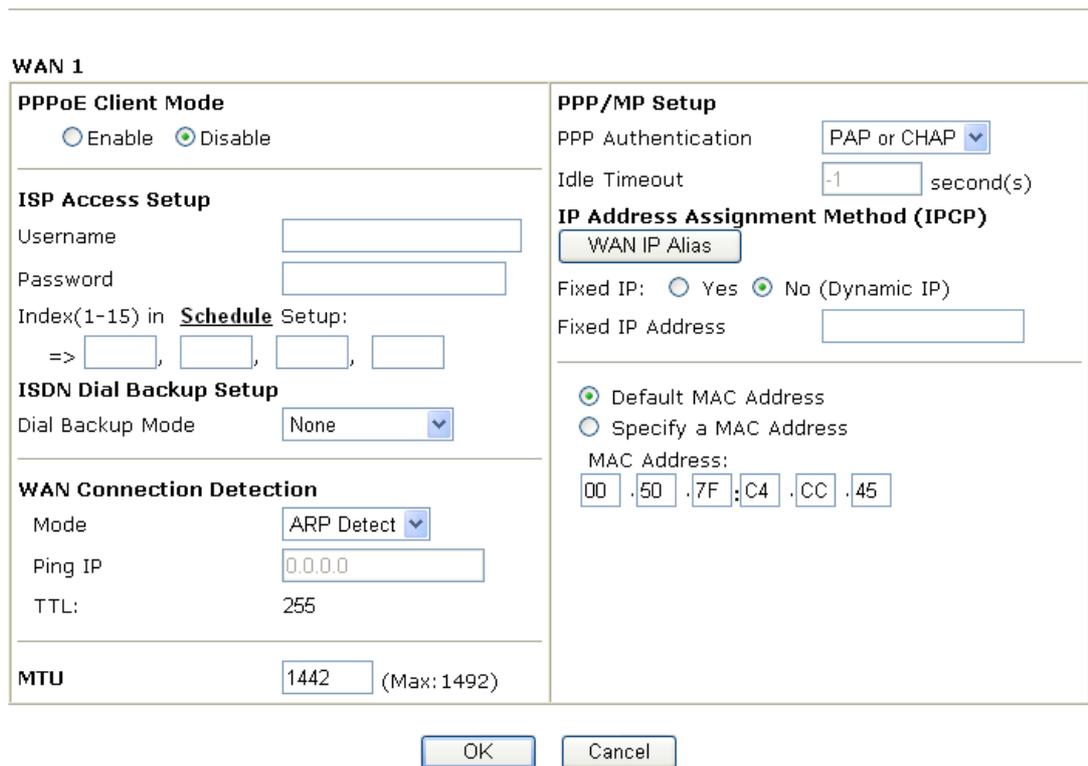
Details Page

This button will open different web page according to the access mode that you choose in WAN1 or WAN2.

Details Page for PPPoE

To use **PPPoE** as the accessing protocol of the internet, please choose **Internet Access** from **WAN** menu. Then, select **PPPoE** mode for WAN. The following web page will be shown.

WAN >> Internet Access



The screenshot shows the "WAN 1" configuration page for PPPoE. It is divided into several sections:

- PPPoE Client Mode:** Radio buttons for "Enable" and "Disable". "Disable" is selected.
- ISP Access Setup:** Fields for "Username", "Password", and "Index(1-15) in Schedule Setup:" with four input boxes.
- ISDN Dial Backup Setup:** "Dial Backup Mode" dropdown menu set to "None".
- WAN Connection Detection:** "Mode" dropdown set to "ARP Detect", "Ping IP" field set to "0.0.0.0", and "TTL:" field set to "255".
- MTU:** Field set to "1442" (Max: 1492).
- PPP/MP Setup:** "PPP Authentication" dropdown set to "PAP or CHAP", "Idle Timeout" field set to "-1" second(s).
- IP Address Assignment Method (IPCP):** "WAN IP Alias" button, "Fixed IP:" radio buttons for "Yes" and "No (Dynamic IP)" (selected), and "Fixed IP Address" field.
- MAC Address:** Radio buttons for "Default MAC Address" (selected) and "Specify a MAC Address". Below is a "MAC Address:" field with six input boxes containing "00", ".50", ".7F", ".C4", ".CC", ".45".

At the bottom, there are "OK" and "Cancel" buttons.

PPPoE Client Mode

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.

ISP Access Setup

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

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

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

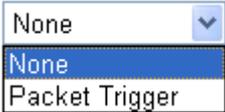
Index (1-15) in Schedule Setup - You can type in four sets of time schedule for your request. All the schedules can be set previously

in **Application >> Schedule** web page and you can use the number that you have set in that web page.

ISDN Dial Backup Setup

This setting is available for the routers supporting ISDN function only. Before utilizing the ISDN dial backup feature, you must create a dial backup profile first. Please click **Internet Access Setup > Dialing to a Single ISP** to enter the backup profile.

Dial Backup Mode



The image shows a dropdown menu for 'Dial Backup Mode'. The current selection is 'None'. The dropdown list is open, showing two options: 'None' (highlighted in blue) and 'Packet Trigger'.

This setting is available for *i* model only.

Due to the absence of the ISDN interface in some models, the ISDN dial backup feature and its associated setup options are not available to them. Please refer to the previous part for further information.

None - Disable the backup function.

Packet Trigger -The backup line is not on until a packet from a local host triggers the router to establish a connection.

WAN Connection Detection

Such function allows you to verify whether network connection is alive or not through ARP Detect or Ping Detect.

Mode – Choose **ARP Detect** or **Ping Detect** for the system to execute for WAN detection.

Ping IP – If you choose Ping Detect as detection mode, you have to type IP address in this field for pinging.

TTL (Time to Live) – Displays value for your reference. TTL value is set by telnet command.

MTU

Mean maximum transmission unit of one packet. The default value is 1442.

PPP/MP Setup

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

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

IP Address Assignment Method (IPCP)

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

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

http://192.168.1.1 - WAN1IP Alias - Microsoft Internet Explorer

WAN1 IP Alias (Multi-NAT)

Index	Enable	Aux. WAN IP	Join NAT IP Pool
1.	<input checked="" type="checkbox"/>	172.16.3.102	<input checked="" type="checkbox"/>
2.	<input type="checkbox"/>	0.0.0.0	<input type="checkbox"/>
3.	<input type="checkbox"/>	0.0.0.0	<input type="checkbox"/>
4.	<input type="checkbox"/>	0.0.0.0	<input type="checkbox"/>
5.	<input type="checkbox"/>	0.0.0.0	<input type="checkbox"/>
6.	<input type="checkbox"/>	0.0.0.0	<input type="checkbox"/>
7.	<input type="checkbox"/>	0.0.0.0	<input type="checkbox"/>
8.	<input type="checkbox"/>	0.0.0.0	<input type="checkbox"/>

<< 1-8 | 9-16 | 17-24 | 25-32 >> Next >>

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

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

Specify a MAC Address – Type the MAC address for the router manually.

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

Details Page for Static or Dynamic IP

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

To use **Static or Dynamic IP** as the accessing protocol of the internet, please choose **Internet Access** from **WAN** menu. Then, select **Static or Dynamic IP** mode for WAN. The following web page will be shown.

WAN 1

<p>Static or Dynamic IP</p> <p><input checked="" type="radio"/> Enable <input type="radio"/> Disable</p>	<p>WAN IP Network Settings WAN IP Alias</p> <p><input type="radio"/> Obtain an IP address automatically (DHCP Client)</p> <p>Router Name <input type="text"/> *</p> <p>Domain Name <input type="text"/> *</p> <p>* : Required for some ISPs</p> <p><input checked="" type="radio"/> Specify an IP address</p> <p>IP Address <input type="text" value="172.16.3.102"/></p> <p>Subnet Mask <input type="text" value="255.255.0.0"/></p> <p>Gateway IP Address <input type="text" value="172.16.1.1"/></p>
<p>ISDN Dial Backup Setup</p> <p>Dial Backup Mode <input type="text" value="None"/></p>	<p>DNS Server IP Address</p> <p>Primary IP Address <input type="text"/></p> <p>Secondary IP Address <input type="text"/></p>
<p>Keep WAN Connection</p> <p><input type="checkbox"/> Enable PING to keep alive</p> <p>PING to the IP <input type="text"/></p> <p>PING Interval <input type="text" value="0"/> minute(s)</p>	<p><input checked="" type="radio"/> Default MAC Address</p> <p><input type="radio"/> Specify a MAC Address</p> <p>MAC Address:</p> <p><input type="text" value="00"/> <input type="text" value="50"/> <input type="text" value="7F"/> <input type="text" value="C4"/> <input type="text" value="CC"/> <input type="text" value="45"/></p>
<p>WAN Connection Detection</p> <p>Mode <input type="text" value="ARP Detect"/></p> <p>Ping IP <input type="text" value="0.0.0.0"/></p> <p>TTL: <input type="text" value="255"/></p>	
<p>MTU <input type="text" value="1442"/> (Max: 1500)</p>	
<p>RIP Protocol</p> <p><input type="checkbox"/> Enable RIP</p>	

Static or Dynamic IP (DHCP 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.

ISDN Dial Backup Setup

This setting is available for the routers supporting ISDN function only. Before utilizing the ISDN dial backup feature, you must create a dial backup profile first. Please click **Internet Access Setup > Dialing to a Single ISP** to enter the backup profile.

- None
- Packet Trigger
- Always On

This setting is available for *i* model only.

Due to the absence of the ISDN interface in some models, the ISDN dial backup feature and its associated setup options are not available to them. Please refer to the previous part for further information.

None - Disable the backup function.

Packet Trigger - The backup line is not on until a packet from a local host triggers the router to establish a connection.

Always On - If the broadband connection is no longer available, the backup line will be activated automatically and always on until the broadband connection is restored. We recommend you to enable this feature if you host a web server for your customers' access.

Keep WAN

Normally, this function is designed for Dynamic IP environments

Connection

because some ISPs will drop connections if there is no traffic within certain periods of time. Check **Enable PING to keep alive** box to activate this function.

PING to the IP - If you enable the PING function, please specify the IP address for the system to PING it for keeping alive.

PING Interval - Enter the interval for the system to execute the PING operation.

WAN Connection Detection

Such function allows you to verify whether network connection is alive or not through ARP Detect or Ping Detect.

Mode – Choose ARP Detect or Ping Detect for the system to execute for WAN detection.

Ping IP – If you choose Ping Detect as detection mode, you have to type IP address in this field for pinging.

TTL (Time to Live) – Displays value for your reference. TTL value is set by telnet command.

MTU

Mean maximum transmission unit of one packet. The default value is 1442.

RIP Protocol

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

WAN IP Network Settings

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

WAN IP Alias - If you have multiple public IP addresses and would like to utilize them on the WAN interface, please use WAN IP Alias. You can set up to 8 public IP addresses other than the current one you are using. Notice that this setting is available for WAN1 only.

Index	Enable	Aux. WAN IP	Join NAT IP Pool
1.	<input checked="" type="checkbox"/>	172.16.3.102	<input checked="" type="checkbox"/>
2.	<input type="checkbox"/>	0.0.0.0	<input type="checkbox"/>
3.	<input type="checkbox"/>	0.0.0.0	<input type="checkbox"/>
4.	<input type="checkbox"/>	0.0.0.0	<input type="checkbox"/>
5.	<input type="checkbox"/>	0.0.0.0	<input type="checkbox"/>
6.	<input type="checkbox"/>	0.0.0.0	<input type="checkbox"/>
7.	<input type="checkbox"/>	0.0.0.0	<input type="checkbox"/>
8.	<input type="checkbox"/>	0.0.0.0	<input type="checkbox"/>

<< 1-8 | 9-16 | 17-24 | 25-32 >> Next >>

OK Clear All Close

Obtain an IP address automatically – Click this button to obtain the IP address automatically if you want to use **Dynamic IP** mode.

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

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

Specify an IP address – Click this radio button to specify some data if you want to use **Static IP** mode.

IP Address: Type the IP address.

Subnet Mask: Type the subnet mask.

Gateway IP Address: Type the gateway IP address.

Default MAC Address: Click this radio button to use default MAC address for the router.

Specify a MAC Address: Some Cable service providers specify a specific MAC address for access authentication. In such cases you need to click the **Specify a MAC Address** and enter the MAC address in the MAC Address field.

DNS Server IP Address

Type in the primary IP address for the router if you want to use **Static IP** mode. If necessary, type in secondary IP address for necessity in the future.

Details Page for PPTP

To use **PPTP** as the accessing protocol of the internet, please choose **Internet Access** from **WAN** menu. Then, select **PPTP** mode for WAN. The following web page will be shown.

WAN >> Internet Access

WAN 1

PPTP Client Mode <input type="radio"/> Enable <input checked="" type="radio"/> Disable PPTP Server <input type="text"/>	PPP Setup PPP Authentication <input type="text" value="PAP or CHAP"/> Idle Timeout <input type="text" value="-1"/> second(s)
ISP Access Setup Username <input type="text"/> Password <input type="text"/> Index(1-15) in Schedule Setup: => <input type="text"/> , <input type="text"/> , <input type="text"/> , <input type="text"/>	IP Address Assignment Method (IPCP) <input type="button" value="WAN IP Alias"/> Fixed IP: <input type="radio"/> Yes <input checked="" type="radio"/> No (Dynamic IP) Fixed IP Address <input type="text"/>
ISDN Dial Backup Setup Dial Backup Mode <input type="text" value="None"/>	WAN IP Network Settings <input type="radio"/> Obtain an IP address automatically <input checked="" type="radio"/> Specify an IP address IP Address <input type="text" value="172.16.3.102"/> Subnet Mask <input type="text" value="255.255.0.0"/>
MTU <input type="text" value="1442"/> (Max: 1460)	

PPTP Setup

PPTP Link - Click **Enable** to enable a PPTP client to establish a tunnel to a DSL modem on the WAN interface.

PPTP Server - Specify the IP address of the PPTP server.

ISP Access Setup

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

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

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.

ISDN Dial Backup Setup

This setting is available for the routers supporting ISDN function only. Before utilizing the ISDN dial backup feature, you must create a dial backup profile first. Please click **Internet Access Setup > Dialing to a Single ISP** to enter the backup profile.

Dial Backup Mode None ▾

None

None

Packet Trigger

This setting is available for *i* model only.

Due to the absence of the ISDN interface in some models, the ISDN dial backup feature and its associated setup options are not available to them. Please refer to the previous part for further information.

None - Disable the backup function.

Packet Trigger -The backup line is not on until a packet from a local host triggers the router to establish a connection.

PPP Setup

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

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

IP Address Assignment Method(IPCP)

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

Fixed IP Address -Type a fixed IP address.

WAN IP Alias - If you have multiple public IP addresses and would like to utilize them on the WAN interface, please use WAN IP Alias. You can set up to 8 public IP addresses other than the current one you are using. Notice that this setting is available for WAN1 only.

http://192.168.1.1 - WAN1IP Alias - Microsoft Internet Explorer

WAN1 IP Alias (Multi-NAT)

Index	Enable	Aux. WAN IP	Join NAT IP Pool
1.	<input checked="" type="checkbox"/>	172.16.3.102	<input checked="" type="checkbox"/>
2.	<input type="checkbox"/>	0.0.0.0	<input type="checkbox"/>
3.	<input type="checkbox"/>	0.0.0.0	<input type="checkbox"/>
4.	<input type="checkbox"/>	0.0.0.0	<input type="checkbox"/>
5.	<input type="checkbox"/>	0.0.0.0	<input type="checkbox"/>
6.	<input type="checkbox"/>	0.0.0.0	<input type="checkbox"/>
7.	<input type="checkbox"/>	0.0.0.0	<input type="checkbox"/>
8.	<input type="checkbox"/>	0.0.0.0	<input type="checkbox"/>

<< 1-8 | 9-16 | 17-24 | 25-32 >> Next >>

Default MAC Address – Click this radio button to use default MAC address for the router.

Specify a MAC Address - Some Cable service providers specify a specific MAC address for access authentication. In such cases you need to click the **Specify a MAC Address** and enter the MAC address in the MAC Address field.

WAN IP Network Settings

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

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

IP Address – Type the IP address.

Subnet Mask – Type the subnet mask.

Details Page for PPP

To use **PPP** (for 3G USB Modem) as the accessing protocol of the internet, please choose **Internet Access** from **WAN** menu. Then, select **PPP** mode for WAN2. The following web page will be shown.

WAN >> Internet Access

WAN 2

PPP Client Mode	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
SIM PIN code	<input type="text"/>
Modem Initial String	<input type="text" value="AT&FE0V1X1&D2&C1S0=0"/> (Default: AT&FE0V1X1&D2&C1S0=0)
APN Name	<input type="text"/> <input type="button" value="Apply"/>
Modem Dial String	<input type="text" value="ATDT*99#"/> (Default: ATDT*99#)
PPP Username	<input type="text"/> (Optional)
PPP Password	<input type="text"/> (Optional)
Index(1-15) in Schedule Setup:	=> <input type="text"/> , <input type="text"/> , <input type="text"/> , <input type="text"/>

PPP Client Mode Click Enable to activate this mode for WAN2.

SIM PIN code Type PIN code of the SIM card that will be used to access Internet.

Modem Initial String Such value is used to initialize USB modem. Please use the default value. If you have any question, please contact to your ISP.

APN Name APN (Access Point Name) is provided by your ISP for identifying different access points. Simply click **Apply** to apply such name. Finally, you have to click **OK** to save the setting.
Apply – Activate the function of identification.

Modem Dial String Such value is used to dial through USB mode. Please use the default value. If you have any question, please contact to your ISP.

PPP Username Type the PPP username (optional).

PPP Password Type the PPP password (optional).

Index (1-15)

Set the PCs on LAN to work at certain time interval only. You may choose up to 4 schedules out of the 15 schedules pre-defined in **Applications >> Schedule** setup. The default setting of this field is blank and the function will always work.

3.1.5 Load-Balance Policy

This router supports the function of load balancing. It can assign traffic with protocol type, IP address for specific host, a subnet of hosts, and port range to be allocated in WAN1 or WAN2 interface. The user can assign traffic category and force it to go to dedicate network interface based on the following web page setup. Twenty policies of load-balance are supported by this router.

Note: Load-Balance Policy is running only when both WAN1 and WAN2 are activated.

WAN >> Load-Balance Policy

Load-Balance Policy

Index	Enable	Protocol	WAN	Src IP Start	Src IP End	Dest IP Start	Dest IP End	Dest Port Start	Dest Port End	Move Up	Move Down
1	<input type="checkbox"/>	any	WAN1								Down
2	<input type="checkbox"/>	any	WAN1							UP	Down
3	<input type="checkbox"/>	any	WAN1							UP	Down
4	<input type="checkbox"/>	any	WAN1							UP	Down
5	<input type="checkbox"/>	any	WAN1							UP	Down
6	<input type="checkbox"/>	any	WAN1							UP	Down
7	<input type="checkbox"/>	any	WAN1							UP	Down
8	<input type="checkbox"/>	any	WAN1							UP	Down
9	<input type="checkbox"/>	any	WAN1							UP	Down
10	<input type="checkbox"/>	any	WAN1							UP	Down

<< 1-10 | 11-20 >>

[Next >>](#)

OK

Index

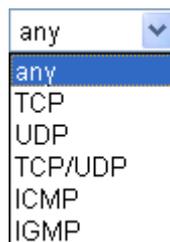
Click the number of index to access into the load-balance policy configuration web page.

Enable

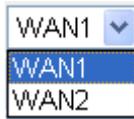
Check this box to enable this policy.

Protocol

Use the drop-down menu to change the protocol for the WAN interface.



WAN Use the drop-down menu to change the WAN interface for such index.



Src IP Start Displays the IP address for the start of the source IP.

Src IP End Displays the IP address for the end of the source IP.

Dest IP Start Displays the IP address for the start of the destination IP.

Dest IP End Displays the IP address for the end of the destination IP.

Dest Port Start Displays the IP address for the start of the destination port.

Dest Port End Displays the IP address for the end of the destination port.

Move UP/Move Down Use **Up** or **Down** link to move the order of the policy.

Click **Index 1** to access into the following page for configuring load-balance policy.

WAN >> Load-Balance Policy

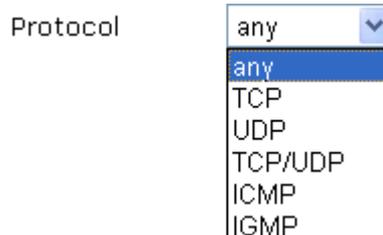
Index: 1

<input checked="" type="checkbox"/> Enable	
Protocol	any
Binding WAN Interface	WAN1 <input checked="" type="checkbox"/> Auto failover to the other WAN
Src IP Start	192.168.1.3
Src IP End	192.168.1.5
Dest IP Start	168.95.0.1
Dest IP End	168.95.0.100
Dest Port Start	80
Dest Port End	100

OK Cancel

Enable Check this box to enable this policy.

Protocol Use the drop-down menu to choose a proper protocol for the WAN interface.



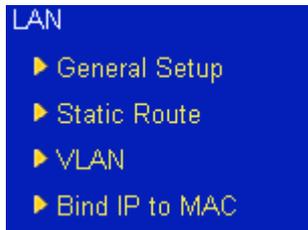
Binding WAN interface Choose the WAN interface (WAN1 or WAN2) for binding.

You can check the box of **Auto failover to other WAN** to make a backup WAN connection if the selected WAN interface fails to connect to Internet.

Src IP Start	Type the source IP start for the specified WAN interface.
Src IP End	Type the source IP end for the specified WAN interface. If this field is blank, it means that all the source IPs inside the LAN will be passed through the WAN interface.
Dest IP Start	Type the destination IP start for the specified WAN interface.
Dest IP End	Type the destination IP end for the specified WAN interface. If this field is blank, it means that all the destination IPs will be passed through the WAN interface.
Dest Port Start	Type the destination port start for the destination IP.
Dest Port End	Type the destination port end for the destination IP. If this field is blank, it means that all the destination ports will be passed through the WAN interface.

3.2 LAN

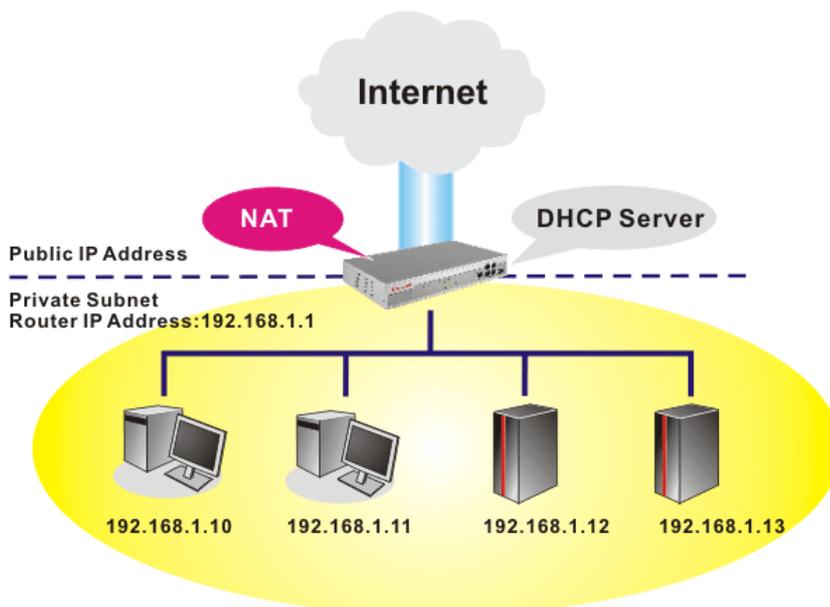
Local Area Network (LAN) is a group of subnets regulated and ruled by router. The design of network structure is related to what type of public IP addresses coming from your ISP.



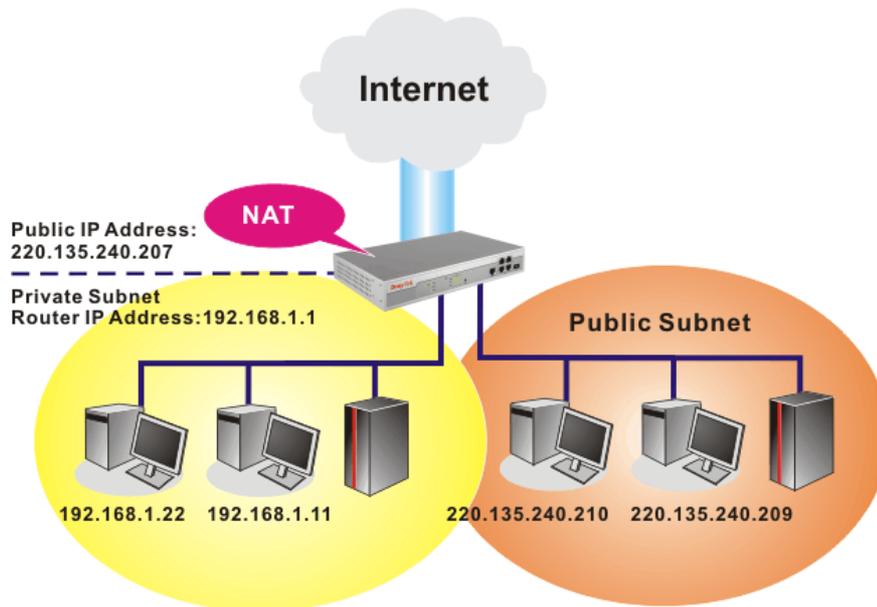
Note: VLAN menu item is only available for VigorPro 5510.

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.



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



What is Routing Information Protocol (RIP)

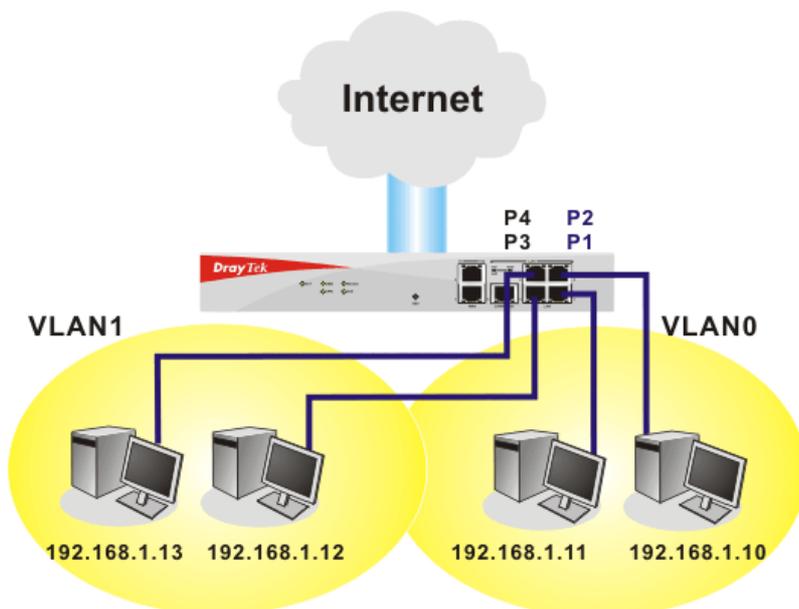
Vigor router will exchange routing information with neighboring routers using the RIP to accomplish IP routing. This allows users to change the information of the router such as IP address and the routers will automatically inform for each other.

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.

What are Virtual LANs and Rate Control

You can group local hosts by physical ports and create up to 4 virtual LANs. To manage the communication between different groups, please set up rules in Virtual LAN (VLAN) function and the rate of each.



3.2.2 General Setup

This page provides you the general settings for LAN.

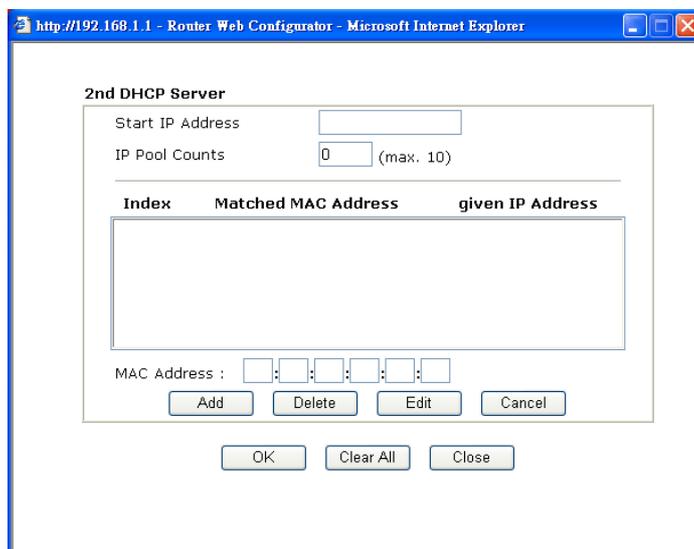
Click **LAN** to open the LAN settings page and choose **General Setup**.

LAN >> General Setup

Ethernet TCP / IP and DHCP Setup

LAN IP Network Configuration		DHCP Server Configuration	
For NAT Usage		<input checked="" type="radio"/> Enable Server <input type="radio"/> Disable Server	
1st IP Address	<input type="text" value="192.168.1.1"/>	Relay Agent:	<input type="radio"/> 1st Subnet <input type="radio"/> 2nd Subnet
1st Subnet Mask	<input type="text" value="255.255.255.0"/>	Start IP Address	<input type="text" value="192.168.1.10"/>
For IP Routing Usage <input type="radio"/> Enable <input checked="" type="radio"/> Disable		IP Pool Counts	<input type="text" value="50"/>
2nd IP Address	<input type="text" value="192.168.2.1"/>	Gateway IP Address	<input type="text" value="192.168.1.1"/>
2nd Subnet Mask	<input type="text" value="255.255.255.0"/>	DHCP Server IP Address for Relay Agent	<input type="text"/>
<input checked="" type="checkbox"/> 2nd Subnet DHCP Server		DNS Server IP Address	
RIP Protocol Control <input type="text" value="Disable"/>		<input type="checkbox"/> Force DNS manual setting	
		Primary IP Address	<input type="text" value="168.95.1.1"/>
		Secondary IP Address	<input type="text"/>

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



Start IP Address: Enter a value of the IP address pool for the DHCP server to start with when issuing IP addresses. If the 2nd IP address of your router is 220.135.240.1, the starting IP address must be 220.135.240.2 or greater, but smaller than 220.135.240.254.

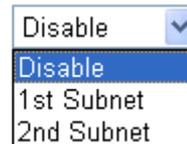
IP Pool Counts: Enter the number of IP addresses in the pool. The maximum is 10. For example, if you type 3 and the 2nd IP address of your router is 220.135.240.1, the range of IP address by the DHCP server will be from 220.135.240.2 to 220.135.240.11.

MAC Address: Enter the MAC Address of the host one by one and click **Add** to create a list of hosts to be assigned, deleted or edited IP address from above pool. Set a list of MAC Address for 2nd DHCP server will help router to assign the correct IP address of the correct subnet to the correct host. So those hosts in 2nd subnet won't get an IP address belonging to 1st subnet.

RIP Protocol Control

Disable deactivates the RIP protocol. It will lead to a stoppage of the exchange of routing information between routers. (Default)

RIP Protocol Control



Disable	▼
Disable	
1st Subnet	
2nd Subnet	

1st Subnet - Select the router to change the RIP information of the 1st subnet with neighboring routers.

2nd Subnet - Select the router to change the RIP information of the 2nd subnet with neighboring routers.

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 the 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 - (1st subnet/2nd subnet) Specify which 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.

DNS Server Configuration

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.

DNS stands for Domain Name System. Every Internet host must have a unique IP address, also they may have a human-friendly, easy to remember name such as www.yahoo.com. The DNS server converts the user-friendly name into its equivalent IP address.

Force DNS manual setting - Force router to use DNS servers in this page instead of DNS servers given by the Internet Access server (PPPoE, PPTP, L2TP or DHCP server).

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

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

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

System Status		System Uptime: 0:53:43	
LAN Status	Primary DNS: 168.95.1.1	Secondary DNS: 168.95.1.1	
IP Address	TX Packets	RX Packets	
192.168.1.1	1878	1739	

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

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

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

3.2.3 Static Route

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

LAN >> Static Route Setup

Static Route Configuration			Set to Factory Default	View Routing Table	
Index	Destination Address	Status	Index	Destination Address	Status
1.	???	?	17.	???	?
2.	???	?	18.	???	?
3.	???	?	19.	???	?
4.	???	?	20.	???	?
5.	???	?	21.	???	?
6.	???	?	22.	???	?
7.	???	?	23.	???	?
8.	???	?	24.	???	?
9.	???	?	25.	???	?
10.	???	?	26.	???	?
11.	???	?	27.	???	?
12.	???	?	28.	???	?
13.	???	?	29.	???	?
14.	???	?	30.	???	?
15.	???	?	31.	???	?
16.	???	?	32.	???	?

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

- Index** The number (1 to 32) under Index allows you to open next page to set up static route.
- Destination Address** Displays the destination address of the static route.
- Status** Displays the status of the static route.
- Viewing Routing Table** Displays the routing table for your reference.

Diagnostics >> View Routing Table

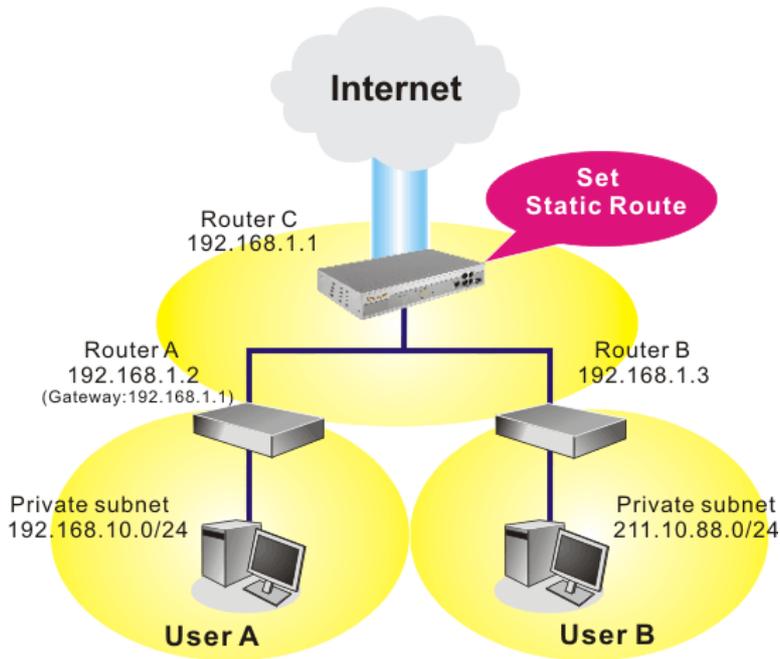
Current Running Routing Table		Refresh
Key: C - connected, S - static, R - RIP, * - default, ~ - private		
* 0.0.0.0/	0.0.0.0 via 172.16.3.1,	WAN1
C~ 192.168.1.0/	255.255.255.0 is directly connected,	LAN
C 172.16.3.0/	255.255.255.0 is directly connected,	WAN1

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.



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.

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

LAN >> Static Route Setup

Index No. 1

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

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

LAN >> Static Route Setup

Index No. 1

Enable

Destination IP Address: 211.100.88.0

Subnet Mask: 255.255.255.0

Gateway IP Address: 192.168.1.3

Network Interface: LAN

OK Cancel

- 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
*   0.0.0.0/      0.0.0.0 via 172.16.3.1,  WAN1
S~  192.168.10.0/ 255.255.255.0 via 192.168.1.2,  LAN
C~  192.168.1.0/   255.255.255.0 is directly connected,  LAN
C   172.16.3.0/   255.255.255.0 is directly connected,  WAN1
S~  211.100.88.0/  255.255.255.0 via 192.168.1.3,  LAN
  
```

3.2.4 VLAN

Virtual LAN function provides you a very convenient way to manage hosts by grouping them based on the physical port. You can also manage the in/out rate of each port. Go to **LAN** page and select **VLAN**. The following page will appear. Click **Enable** to invoke VLAN function.

Note: VLAN menu item is only available for VigorPro 5510.

LAN >> VLAN Configuration

VLAN Configuration

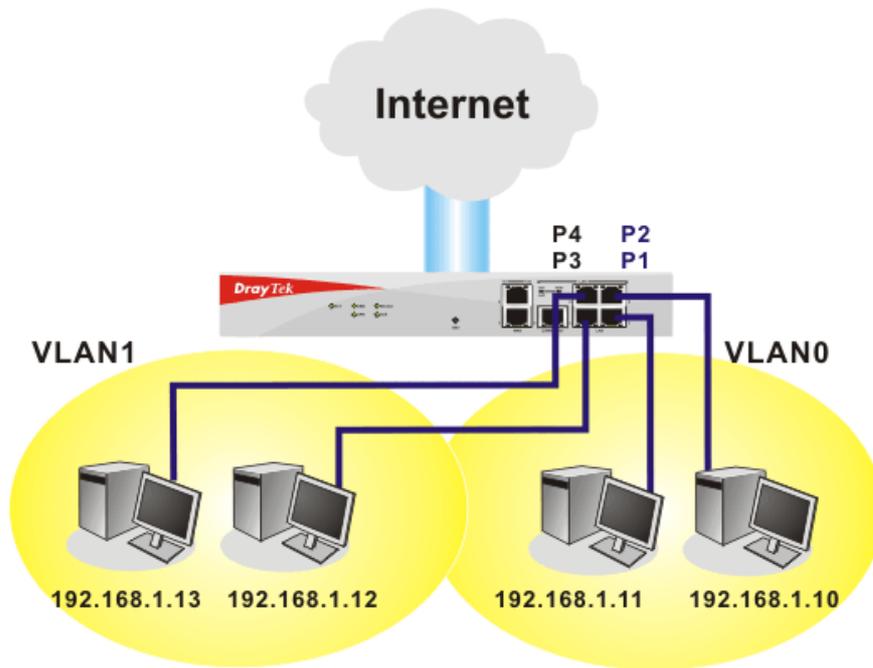
Enable

	P1	P2	P3	P4
VLAN0	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
VLAN1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
VLAN2	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
VLAN3	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

OK Clear Cancel

To add or remove a VLAN, please refer to the following example.

- If, VLAN 0 is consisted of hosts linked to P1 and P2 and VLAN 1 is consisted of hosts linked to P3 and P4.



2. After checking the box to enable VLAN function, you will check the table according to the needs as shown below.

LAN >> VLAN Configuration

VLAN Configuration

	P1	P2	P3	P4
<input checked="" type="checkbox"/> Enable				
VLAN0	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
VLAN1	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
VLAN2	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
VLAN3	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

OK Clear Cancel

To remove VLAN, uncheck the needed box and click **OK** to save the results.

3.2.5 Bind IP to MAC

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

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

Bind IP to MAC

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

Enable
 Disable
 Strict Bind

ARP Table | [Select All](#) | [Sort](#) | [Refresh](#) |
 IP Bind List | [Select All](#) | [Sort](#)

IP Address	Mac Address	Index	IP Address	Mac Address
192.168.1.10	00-0E-A6-2A-D5-A1			
192.168.1.100	00-08-A1-36-97-5D			
192.168.1.11	00-13-D4-A4-99-92			
192.168.1.12	00-0B-CD-55-CB-45			
192.168.1.10	00-13-D4-A4-99-92			
192.168.1.123	00-08-A1-01-53-BB			

Add and Edit

IP Address

Mac Address

- Enable** Click this radio button to invoke this function. However, IP/MAC which is not listed in IP Bind List also can connect to Internet.
- Disable** Click this radio button to disable this function. All the settings on this page will be invalid.
- Strict Bind** Click this radio button to block the connection of the IP/MAC which is not listed in IP Bind List.
- ARP Table** This table is the LAN ARP table of this router. The information for IP and MAC will be displayed in this field. Each pair of IP and MAC address listed in ARP table can be selected and added to IP Bind List by clicking **Add** below.
- Add and Edit**

IP Address – Type the IP address that will be used for the specified MAC address.

Mac Address – Type the MAC address that is used to bind with the assigned IP address.
- Refresh** It is used to refresh the ARP table. When there is one new PC added to the LAN, you can click this link to obtain the newly ARP table information.
- IP Bind List** It displays a list for the IP bind to MAC information.
- Add** It allows you to add the one you choose from the ARP table or the IP/MAC address typed in **Add and Edit** to the table of **IP Bind List**.
- Edit** It allows you to edit and modify the selected IP address and MAC address that you create before.
- Delete** You can remove any item listed in **IP Bind List**. Simply click and select the one, and click **Delete**. The selected item will be removed from the **IP Bind List**.

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

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.

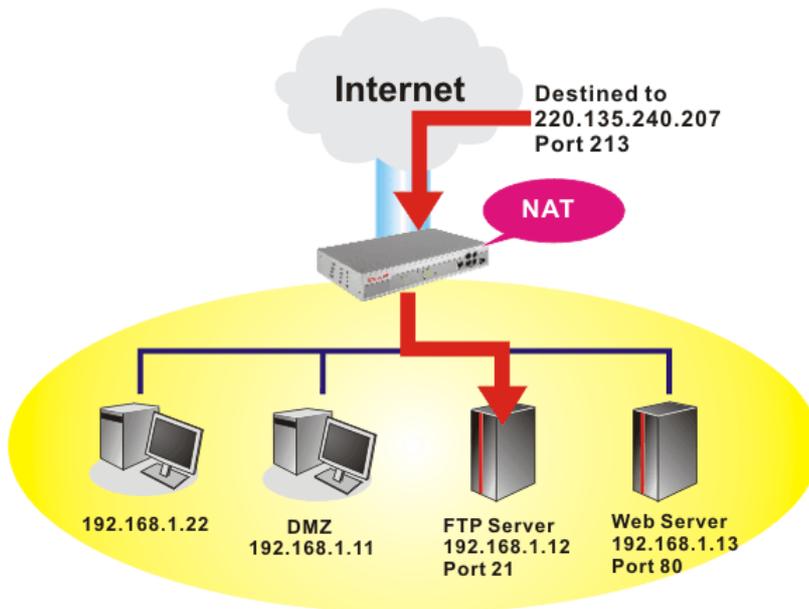
Note: On NAT page, you will see the private IP address defined in RFC-1918. Usually we use the 192.168.1.0/24 subnet for the router. As stated before, the NAT facility can map one or more IP addresses and/or service ports into different specified services. In other words, the NAT function can be achieved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

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

NAT >> Port Redirection

Port Redirection

[Set to Factory Default](#)

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

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

[Next](#) >>

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

Index No. 1

<input checked="" type="checkbox"/> Enable	
Mode	Range
Service Name	learning
Protocol	TCP
WAN Interface	ALL
Public Port	82 - 100
Private IP	192.168.1.55 - 73
Private Port	0

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

OK Clear Cancel

Enable

Check this box to enable such port redirection setting.

Mode

Two options (Single and Range) are provided here for you to choose. To set a range for the specific service, select **Range**. In Range mode, if the public port (start port and end port) and the starting IP of private IP had been entered, the system will calculate and display the ending IP of private IP automatically.

Service Name

Enter the description of the specific network service.

Protocol

Select the transport layer protocol (TCP or UDP).

WAN Interface

Chose the WAN interface for applying port redirection. The default setting is **All** which means all the incoming data from any port will be redirected to WAN1 and WAN2 at the same time.

Public Port

Specify which port can be redirected to the specified **Private IP and Port** of the internal host. If you choose **Range** as the port redirection mode, you will see two boxes on this field. Simply type the required numbers on these two boxes.

Private IP

Specify the private IP address of the internal host providing the service. If you choose **Range** as the port redirection mode, you will see two boxes on this field. Simply type the IP address in the first box (as the starting point). The second one is assigned automatically after you type the private port number below.

Private Port

Specify the private port number of the service offered by the internal host. After you enter the proper number in this box, the second box of Private IP address will be assigned accordingly.

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 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

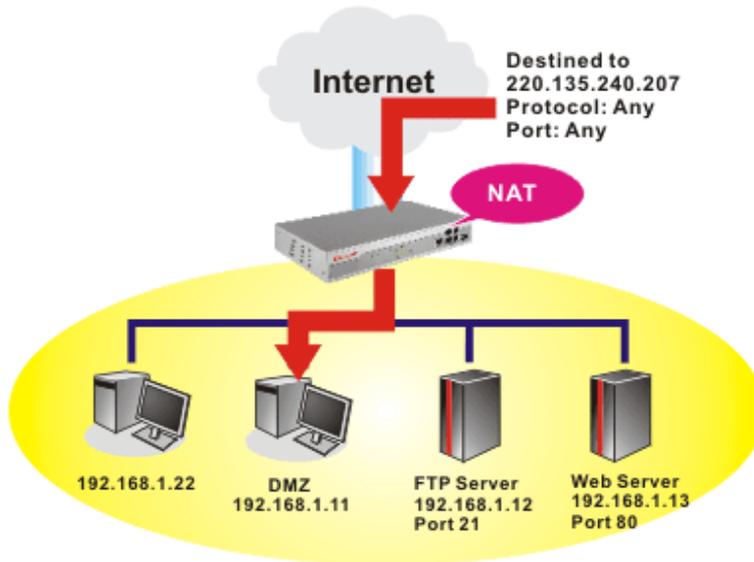
Management Setup

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

OK

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

WAN1 WAN2

WAN 1

None

Private IP

MAC Address of the True IP DMZ Host

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

WAN1

NAT >> DMZ Host Setup

DMZ Host Setup

WAN1 WAN2

WAN 2

Enable

Private IP

WAN2

WAN1 This page allows you to configure **Private IP** or **Active True IP** as DMZ host.

WAN2 This page allows you to configure **Private IP** as DMZ host.

Private IP If you choose **Private IP** as DMZ host, you can type a private IP in this box or use Choose PC button to choose the one you want.

MAC Address of the True.... If you choose **Active True IP** as DMZ host, please type the MAC address of the one you want.

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

NAT >> DMZ Host Setup

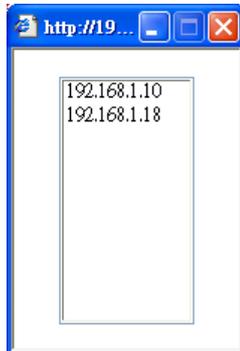
DMZ Host Setup

WAN1		WAN2	
WAN 1			
Index	Enable	Aux. WAN IP	Private IP
1.	<input type="checkbox"/>	172.16.3.102	<input type="text" value="0.0.0.0"/> <input type="button" value="Choose PC"/>
2.	<input type="checkbox"/>	172.16.3.55	<input type="text" value="0.0.0.0"/> <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

WAN1		WAN2	
WAN 1			
Index	Enable	Aux. WAN IP	Private IP
1.	<input checked="" type="checkbox"/>	172.16.3.102	<input type="text" value="192.168.1.10"/> <input type="button" value="Choose PC"/>
2.	<input type="checkbox"/>	172.16.3.55	<input type="text" value="0.0.0.0"/> <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

Open Ports Setup				Set to Factory Default
Index	Comment	WAN Interface	Local IP Address	Status
1.				X
2.				X
3.				X
4.				X
5.				X
6.				X
7.				X
8.				X
9.				X
10.				X

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

- Index** Indicate the relative number for the particular entry that you want to offer service in a local host. You should click the appropriate index number to edit or clear the corresponding entry.
- Comment** Specify the name for the defined network service.
- WAN Interface** Display the WAN interface for the entry.
- 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.

Index No. 1

<input checked="" type="checkbox"/> Enable Open Ports							
Comment		P2P					
WAN Interface		WAN1					
Local Computer		192.168.1.10			Choose PC		
	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

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

3.3.4 Address Mapping

This page is used to map specific private IP to specific WAN IP alias.

If you have "a group of IP Addresses" and want to apply to the router, please use WAN IP alias function to record these IPs first. Then, use address mapping function to map specific private IP to specific WAN IP alias.

For example, you have IP addresses ranging from 86.123.123.1 ~ 86.123.123.8. However, your router uses 86.123.123.1, and the rest of the IPs are recorded in WAN IP alias. You want that private IP 192.168.1.10 can use 86.123.123.2 as source IP when it sends packet out to Internet. You can use address mapping function to achieve this demand. Simply type 192.168.1.10 as the Private IP; and type 86.123.123.2 as the WAN IP.

NAT >> Address Mapping

Address Mapping Setup					Set to Factory Default
Index	Protocol	Public IP	Private IP	Mask	Status
1.	ALL	172.16.3.102		/32	x
2.	ALL	172.16.3.102		/32	x
3.	ALL	172.16.3.102		/32	x
4.	ALL	172.16.3.102		/32	x
5.	ALL	172.16.3.102		/32	x
6.	ALL	172.16.3.102		/32	x
7.	ALL	172.16.3.102		/32	x
8.	ALL	172.16.3.102		/32	x
9.	ALL	172.16.3.102		/32	x
10.	ALL	172.16.3.102		/32	x

- Protocol** Display the protocol used for this address mapping.
- Public IP** Display the public IP address selected for this entry, e.g., 172.16.3.102.
- Private IP** Display the private IP set for this address mapping, e.g., 192.168.1.10
- Mask** Display the subnet mask selected for this address mapping.
- Status** Display the status for the entry, enable or disable.

Click the index number link to open the configuration page.

NAT >> Address Mapping

Index No. 1

Enable

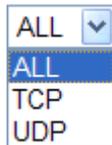
Protocol: ALL ▾

Public IP: 1.WAN IP Alias[1]172.16.3.102 ▾

Private IP: 192.168.1.10

Subnet Mask: /32 ▾

- Enable** Check to enable this entry.
- Protocol** Specify the transport layer protocol. It could be **TCP**, **UDP**, or **ALL** for selection.



- WAN IP** Select an IP address (the selections provided here are set in **IP Alias List** of **Network >>WAN** interface). Local host can use this IP to connect to Internet.
If you want to choose any one of the Public IP settings, you must specify some IP addresses in the IP Alias List of the Static/DHCP Configuration page first. If you did not type in any IP address in

the IP Alias List, the Public IP setting will be empty in this field. When you click **Apply**, a message will appear to inform you.

Private IP

Assign an IP address (e.g., 192.168.1.10) or a subnet to be compared with the Public IP address for incoming packets.

Subnet Mask

Select a value of subnet mask for private IP address.

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.

Firewall Facilities

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

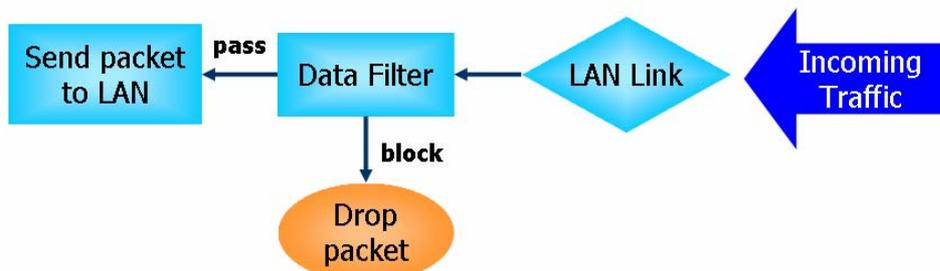
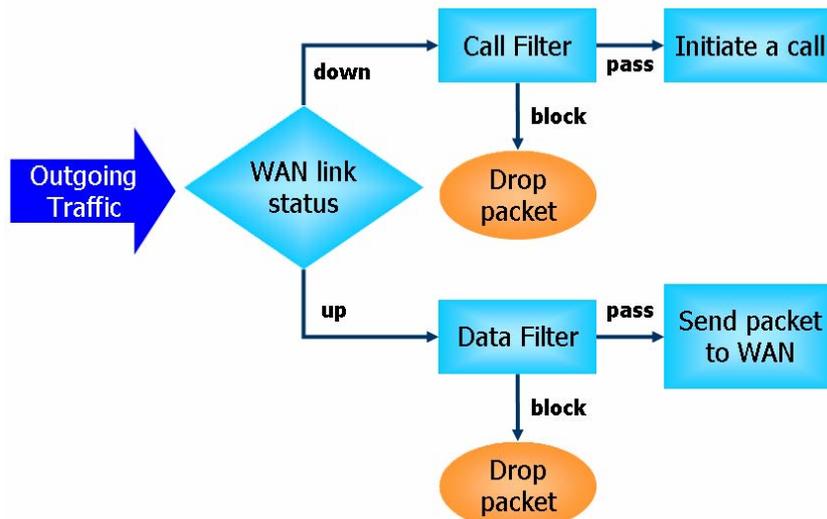
- User-configurable IP filter (Call Filter/ Data Filter).
- Stateful Packet Inspection (SPI): tracks packets and denies unsolicited incoming data
- Selectable Denial of Service (DoS) /Distributed DoS (DDoS) attacks protection
- URL Content Filter

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.

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.

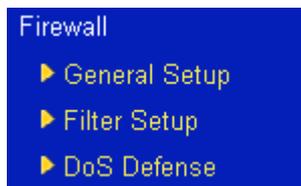
The below shows the attack types that DoS/DDoS defense function can detect:

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

Anti-Virus and Anti-Intrusion

Users might have much more confidence about the security in the network for data transmission if the functions of anti-virus and anti-intrusion are activated. The VigorPro router offers the mechanism of anti-virus and anti-intrusion. What you have to do is to set the proper profiles and invoke them. The anti-virus profile and anti-intrusion configuration can be set in Anti-Virus menu (refer to section 3.7) and Anti-Intrusion menu (refer to section 3.6). However, the mechanism must be enabled either in **Firewall>>General Setup** or **Firewall>>Filter Setup** web page. After you choose proper Anti-Virus profile and check Anti-Intrusion box, the Anti-Virus and Anti-Intrusion LEDs on the front panel will light up.

Below shows the menu items for Firewall.



3.4.2 General Setup

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

Important: When some packet does not fit the rule configured in **Filter Setup** web page, the filtering action configured in general setup web page will apply to that packet.

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

General Setup

Call Filter Enable Start Filter Set Set#1 Disable

Data Filter Enable Start Filter Set Set#2 Disable

Actions for default rule:

Application	Action/Profile	Syslog
Filter	Pass <input type="button" value="v"/>	<input type="checkbox"/>
IM/P2P Filter	None <input type="button" value="v"/>	<input type="checkbox"/>
URL Content Filter	None <input type="button" value="v"/>	<input type="checkbox"/>
Web Content Filter	None <input type="button" value="v"/>	<input type="checkbox"/>
Anti-Virus	None <input type="button" value="v"/>	<input type="checkbox"/>
Anti-Intrusion	<input type="checkbox"/> Enable	<input type="checkbox"/>
Anti-Spam	None <input type="button" value="v"/>	<input type="checkbox"/>

Advance Setting

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

Enable Transparent mode

[Strict Security Checking](#)

Anti-Virus Anti-Spam In-Sequence

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

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

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



IM/P2P Filter Select an IM/P2P profile for global IM/P2P application blocking. All the hosts in LAN must follow the standard configured in the IM/P2P profile selected here. For detailed information, refer to the section of IM/P2P profile setup. For troubleshooting needs, you can specify to record information for IM/P2P by checking the Log box. It will be sent to Syslog server. Please refer to section 3.13.4 Syslog/Mail Alert for more detailed information.

URL Content Filter Select one of the **URL Content Filter** profile settings (created in **CSM>> URL Content Filter**) for applying with this router. Please set at least one profile for choosing in **CSM>> URL Content Filter** web page first. For troubleshooting needs, you can specify to record information for **URL Content Filter** by checking the Log box. It will be sent to Syslog server. Please refer to section 3.13.4 Syslog/Mail Alert for more detailed information.

Web Content Filter Select one of the **Web Content Filter** profile settings (created in **CSM>> Web Content Filter**) for applying with this router. Please set at least one profile for anti-virus in **CSM>> Web Content**

Filter web page first. For troubleshooting needs, you can specify to record information for **Web Content Filter** by checking the Log box. It will be sent to Syslog server. Please refer to section 3.13.4 Syslog/Mail Alert for more detailed information.

Anti-Virus

Select one of the anti-virus profile settings (created in **Anti-Virus>>Profile Setting**) for applying with this router. Please set at least one profile for anti-virus in **Anti-Virus-> Profile Setting** web page first. For troubleshooting needs, you can specify to record information for **Anti-Virus** by checking the Log box. It will be sent to Syslog server. Please refer to section 3.13.4 Syslog/Mail Alert for more detailed information.

Anti-Intrusion

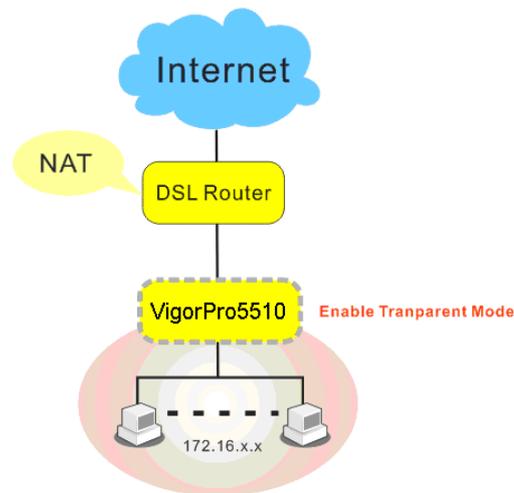
Check the **Enable** box to invoke anti-intrusion filter function. For troubleshooting needs, you can specify to record information for **Anti-Intrusion** by checking the Log box. It will be sent to Syslog server. Please refer to section 3.13.4 Syslog/Mail Alert for more detailed information.

Accept large incoming...

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

Enable Transparent Mode

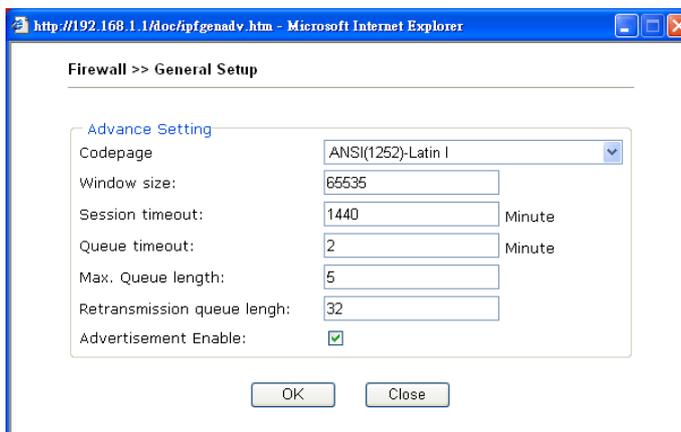
Check this box to enable transparent function for such router. It is not necessary for users to re-organize the network or configure the subnet settings for each PC connected under such router. However, the configured Anti-Virus and Anti-Intrusion profiles can be applied to PCs connected behind vigor router to have the best security. The following picture explains the basic structure for using transparent mode for vigor router.



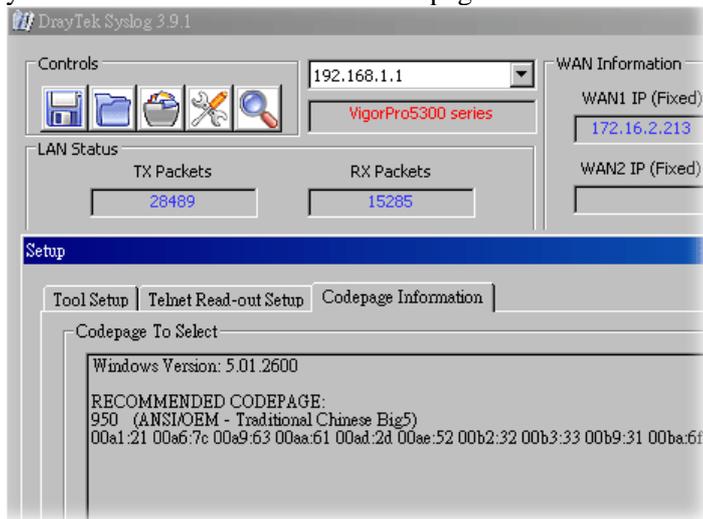
PCs with subnet “172.16.x.x” connected under VigorPro 5510 will be protected by security settings enabled and configured on the web pages of Vigor router. When the transparent mode has been checked, hackers from Internet do not sense the existence of vigor router, therefore they cannot attack the router.

Advance Setting

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



Codepage - This function is used to compare the characters among different languages. Choose correct codepage can help the system obtaining correct ASCII after decoding data from URL and enhance the correctness of URL Content Filter. The default value for this setting is ANSI 1252 Latin I. If you do not choose any codepage, no decoding job of URL will be processed. Please use the drop-down list to choose a codepage. If you do not have any idea of choosing suitable codepage, please open Syslog. From Codepage Information of Setup dialog, you will see the recommended codepage listed on the dialog box.



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

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

Max. Queue length - When the network connection is not stable, you can set large number for this setting to get better performance. Yet large value will consume large resource.

Retransmission queue length – Type the number here as a base

for the router to verify if the retransmitted data is the same as the old one.

Advertisement Enable – Check this box to display the words – [Powered by Draytek] on the unreachable web page



Strict Security Checking

For the sake of security, you might want the router executing strict security checking for data transmission. The router performance will be affected if you invoke strict security checking.

Anti-Virus – Check this box to execute the critical checking for virus.

Anti-Spam – Check this box to execute the critical checking for e-mails.

In sequence – Check this box to execute the critical checking for all the files in sequence.

3.4.3 Filter Setup

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

Firewall >> Filter Setup

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

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

Firewall >> Filter Setup >> Edit Filter Set

Filter Set 1

Comments :

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

Next Filter Set

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

Active Enable or disable the filter rule.

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

Move Up/Down Use **Up** or **Down** link to move the order of the filter rules.

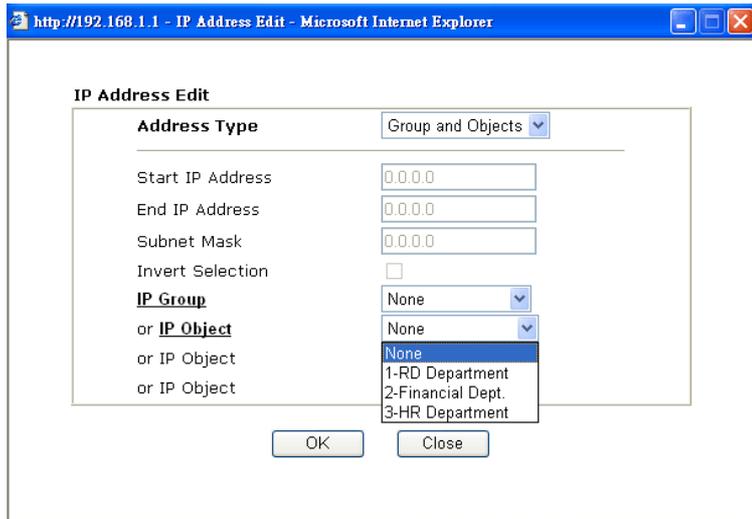
Next Filter Set Set the link to the next filter set to be executed after the current filter run. Do not make a loop with many filter sets.

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

Filter Set 1 Rule 1

<input checked="" type="checkbox"/> Check to enable the Filter Rule		
Comments:	Block NetBios	
Index(1-15) in Schedule Setup:	, , ,	
<hr/>		
Direction:	LAN -> WAN	
Source IP:	Any	<input type="button" value="Edit"/>
Destination IP:	Any	<input type="button" value="Edit"/>
Service Type:	TCP/UDP, Port: from 137~139 to undefined	<input type="button" value="Edit"/>
Fragments:	Don't Care	
<hr/>		
Application	Action/Profile	Syslog
Filter:	Block Immediately	<input type="checkbox"/>
Branch to Other Filter Set:	None	
IM/P2P Filter:	None	<input type="checkbox"/>
URL Content Filter	None	<input type="checkbox"/>
Web Content Filter	None	<input type="checkbox"/>
Anti-Virus:	None	<input type="checkbox"/>
Anti-Intrusion:	<input type="checkbox"/> Enable	<input type="checkbox"/>
Anti-Spam:	None	<input type="checkbox"/>
<hr/>		
Advance Setting	<input type="button" value="Edit"/>	

- Check to enable the Filter Rule** Check this box to enable the filter rule.
- Comments** Enter filter set comments/description. Maximum length is 14-character long.
- Index (1-15)** Set PCs on LAN to work at certain time interval only. You may choose up to 4 schedules out of the 15 schedules pre-defined in **Applications >> Schedule** setup. The default setting of this field is blank and the function will always work.
- Direction** Set the direction of packet flow (LAN->WAN/WAN->LAN). It is for **Data Filter** only. For the **Call Filter**, this setting is not available since **Call Filter** is only applied to outgoing traffic.
- Source/Destination IP** Click **Edit** to access into the following dialog to choose the source/destination IP or IP ranges.



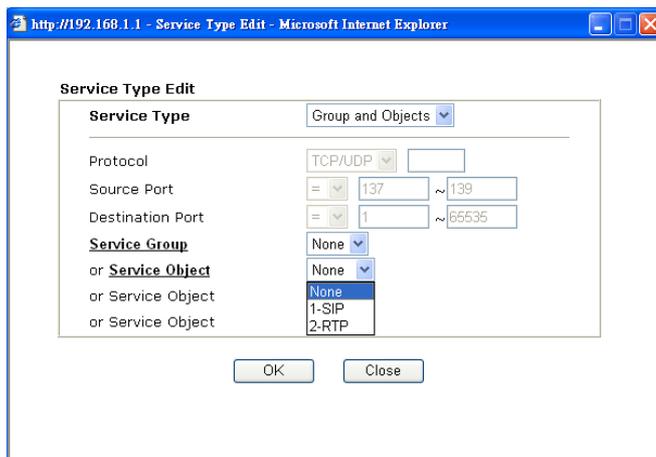
To set the IP address manually, please choose **Any Address/Single Address/Range Address/Subnet Address** as the Address Type and type them in this dialog. In addition, if you want to use the IP range from defined groups or objects, please choose **Group and Objects** as the Address Type.



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

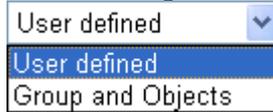
Service Type

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



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

choose **Group and Objects** as the Service Type.



Protocol - Specify the protocol(s) which this filter rule will apply to.

Source/Destination Port -

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

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

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

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

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

Fragments

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

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

Unfragmented -Apply the rule to unfragmented packets.

Fragmented - Apply the rule to fragmented packets.

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

Filter

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

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

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

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

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

Branch to other Filter Set

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

IM/P2P Filter

Select a IM/P2P profile for global IM/P2P application blocking. All the hosts in LAN must follow the standard configured in the IM/P2P profile selected here. For detailed information, refer to the section of IM/P2P profile setup. For troubleshooting needs, you can specify to record information for IM/P2P by checking the Log box. It will be sent to Syslog server. Please refer to section Syslog/Mail Alert for more detailed information.

URL Content Filter

Select one of the **URL Content Filter** profile settings (created in **CSM>> URL Content Filter Profile**) for applying with this router. Please set at least one profile for choosing in **CSM>> URL Content Filter Profile** web page first. For troubleshooting needs, you can specify to record information for **URL Content**

Filter by checking the Log box. It will be sent to Syslog server. Please refer to section **Syslog/Mail Alert** for more detailed information.

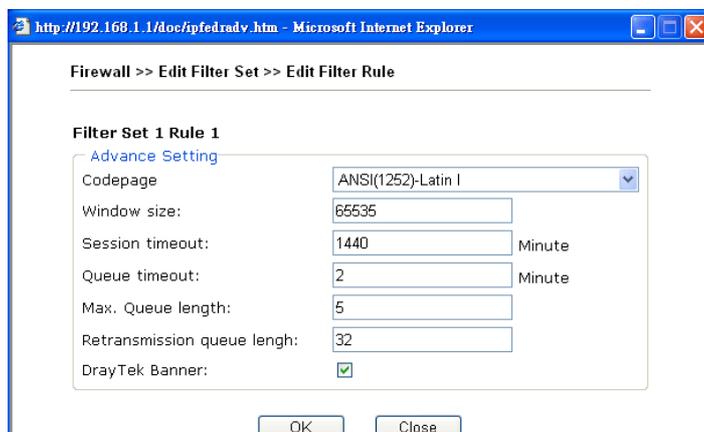
Web Content Filter Select one of the **Web Content Filter** profile settings (created in **CSM>> Web Content Filter Profile**) for applying with this router. Please set at least one profile for anti-virus in **CSM>> Web Content Filter Profile** web page first. For troubleshooting needs, you can specify to record information for **Web Content Filter** by checking the Log box. It will be sent to Syslog server. Please refer to section **Syslog/Mail Alert** for more detailed information.

Anti-Virus Select one of the anti-virus profile settings (created in **Defense Configuration>>Anti-Virus>>Profile Setting**) for applying with this router. Please set at least one profile for anti-virus in **Defense Configuration>>Anti-Virus-> Profile Setting** web page first. For troubleshooting needs, you can specify to record information for **Anti-Virus** by checking the Log box. It will be sent to Syslog server. Please refer to section **Syslog/Mail Alert** for more detailed information.

Anti-Intrusion Check the **Enable** box to invoke anti-intrusion filter function. For troubleshooting needs, you can specify to record information for **Anti-Intrusion** by checking the Log box. It will be sent to Syslog server. Please refer to section **Syslog/Mail Alert** for more detailed information.

Anti-Spam Select one of the anti-spam profile settings (created in **Defense Configuration>>Anti-Spam>>Profile Setting**) for applying with this router. Please set at least one profile for anti-spam in **Defense Configuration>>Anti-Spam>>Profile Setting** web page first. For troubleshooting needs, you can specify to record information for **Anti-Spam** by checking the Log box. It will be sent to Syslog server. Please refer to section **Syslog/Mail Alert** for more detailed information.

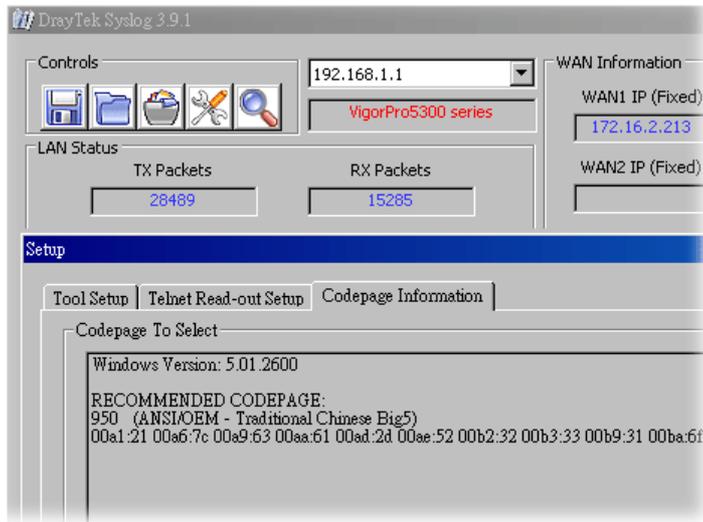
Advance Setting Click **Edit** to open the following window. Click **Edit** to open the following window. However, it is **strongly recommended** to use the default settings here.



Codepage - This function is used to compare the characters among different languages. Choose correct codepage can help the system obtaining correct ASCII after decoding data from URL and enhance the correctness of URL Content Filter. The

default value for this setting is ANSI 1252 Latin I. If you do not choose any codepage, no decoding job of URL will be processed. Please use the drop-down list to choose a codepage.

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



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 Start Filter Set: Set#1
 Disable

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

Actions for default rule:

Application	Action/Profile	Syslog
Filter	Pass	<input type="checkbox"/>
IM/P2P Filter	None	<input type="checkbox"/>
URL Content Filter	None	<input type="checkbox"/>
Web Content Filter	None	<input type="checkbox"/>
Anti-Virus	None	<input type="checkbox"/>
Anti-Intrusion	<input type="checkbox"/> Enable	<input type="checkbox"/>
Anti-Spam	None	<input type="checkbox"/>

Advance Setting:

Accept large incoming fragmented UDP or ICMP packets (for some games,)
 Enable Transparent mode
 Strict Security Checking:
 Anti-Virus Anti-Spam In-Sequence

Firewall >> Filter Setup

Filter Setup | Set to Factory Default |

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

Firewall >> Filter Setup >> Edit Filter Set

Filter Set 1
 Comments: Default Call Filter

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

Next Filter:

Firewall >> Edit Filter Set >> Edit Filter Rule

Filter Set 1 Rule 1

Check to enable the Filter Rule
 Comments: Block NetBios
 Index(1-15) in Schedule Setup: [] [] [] []

Direction: LAN -> WAN
 Source IP: Any [Edit]
 Destination IP: Any [Edit]
 Service Type: TCP/UDP, Port: from 137-139 to undefined [Edit]
 Fragments: Don't Care

Application	Action/Profile	Syslog
Filter	Block Immediately	<input type="checkbox"/>
Branch to Other Filter Set:	None	
IM/P2P Filter	None	<input type="checkbox"/>
URL Content Filter	None	<input type="checkbox"/>
Web Content Filter	None	<input type="checkbox"/>
Anti-Virus	None	<input type="checkbox"/>
Anti-Intrusion	<input type="checkbox"/> Enable	<input type="checkbox"/>
Anti-Spam	None	<input type="checkbox"/>

Advance Setting:

3.4.4 DoS Defense

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

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

Firewall >> DoS defense Setup

DoS defense Setup

Enable DoS Defense Select All

<input type="checkbox"/> Enable SYN flood defense	Threshold	<input type="text" value="50"/>	packets / sec
	Timeout	<input type="text" value="10"/>	sec
<input type="checkbox"/> Enable UDP flood defense	Threshold	<input type="text" value="150"/>	packets / sec
	Timeout	<input type="text" value="10"/>	sec
<input type="checkbox"/> Enable ICMP flood defense	Threshold	<input type="text" value="50"/>	packets / sec
	Timeout	<input type="text" value="10"/>	sec
<input type="checkbox"/> Enable Port Scan detection	Threshold	<input type="text" value="150"/>	packets / sec
<input type="checkbox"/> Block IP options	<input type="checkbox"/> Block TCP flag scan		
<input type="checkbox"/> Block Land	<input type="checkbox"/> Block Tear Drop		
<input type="checkbox"/> Block Smurf	<input type="checkbox"/> Block Ping of Death		
<input type="checkbox"/> Block trace route	<input type="checkbox"/> Block ICMP fragment		
<input type="checkbox"/> Block SYN fragment	<input type="checkbox"/> Block UnknownProtocol		
<input type="checkbox"/> Block Fraggle Attack			

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

OK Clear All Cancel

Enable Dos Defense

Check the box to activate the DoS Defense Functionality.

Enable SYN flood defense

Check the box to activate the SYN flood defense function. Once detecting the Threshold of the TCP SYN packets from the Internet has exceeded the defined value, the Vigor 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 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

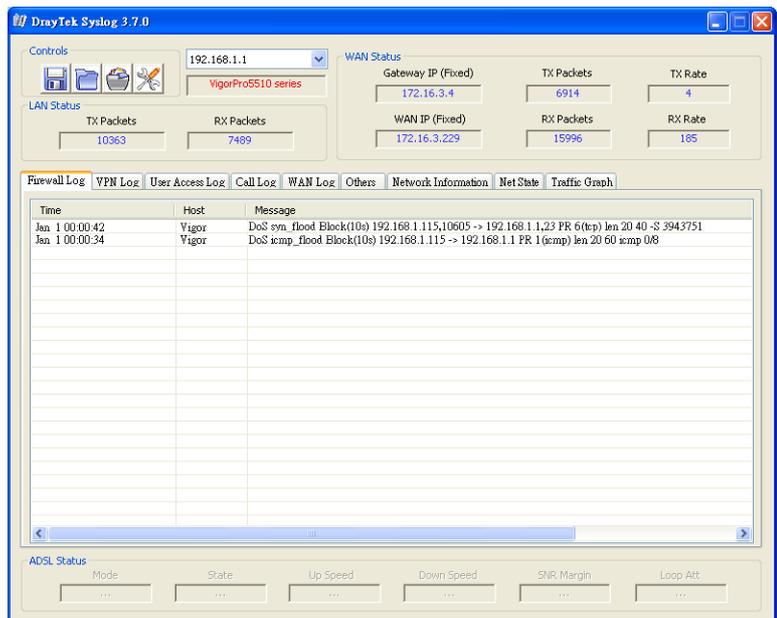
We provide Syslog function for user to retrieve message from Vigor router. The user, as a Syslog Server, shall receive the report sending from Vigor router which is a Syslog Client.

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

<p>SysLog Access Setup</p> <p><input checked="" type="checkbox"/> Enable</p> <p>Router Name <input type="text"/></p> <p>Server IP Address <input type="text"/></p> <p>Destination Port <input type="text" value="514"/></p> <p>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>AI/AV AlertLog Setup</p> <p><input type="checkbox"/> Enable</p> <p>AlertLog Port <input type="text" value="514"/></p> <p><input checked="" type="checkbox"/> AI/AV Attack Log</p> <p><input checked="" type="checkbox"/> Access Block Log</p>	<p>Mail Alert Setup</p> <p><input type="checkbox"/> Enable Send a test e-mail</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> <p>Enable E-Mail Alert:</p> <p><input checked="" type="checkbox"/> DoS Attack</p> <p><input checked="" type="checkbox"/> IM-P2P</p> <p><input checked="" type="checkbox"/> Anti-Intrusion</p> <p><input checked="" type="checkbox"/> Anti-Virus</p>
---	---



3.5 Objects Settings

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

- 
- ▶ Objects Setting
 - ▶ IP Object
 - ▶ IP Group
 - ▶ Service Type Object
 - ▶ Service Type Group
 - ▶ Keyword Object
 - ▶ Keyword Group
 - ▶ File Extension Object

3.5.1 IP Object

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

Objects Setting >> IP Object

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

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

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

Set to Factory Default Clear all profiles.

Click the number under Index column for settings in detail.

Objects Setting >> IP Object

Profile Index : 1

Name:	<input type="text" value="RD Department"/>
Interface:	<input style="border: none; background-color: #e0e0e0; padding: 2px 5px;" type="button" value="Any"/> ▾
Address Type:	<input style="border: none; background-color: #e0e0e0; padding: 2px 5px;" type="button" value="Range Address"/> ▾
Mac Address:	<input type="text" value="00 : 00 : 00 : 00 : 00 : 00"/>
Start IP Address:	<input type="text" value="192.168.1.64"/>
End IP Address:	<input type="text" value="192.168.1.75"/>
Subnet Mask:	<input type="text" value="0.0.0.0"/>
Invert Selection:	<input type="checkbox"/>

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

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

Interface: ▾

Any

LAN

WAN

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

Address Type	Determine the address type for the IP address. Select Single Address if this object contains one IP address only. Select Range Address if this object contains several IPs within a range. Select Subnet Address if this object contains one subnet for IP address. Select Any Address if this object contains any IP address.
Start IP Address	Type the start IP address for Single Address type.
End IP Address	Type the end IP address if the Range Address type is selected.
Subnet Mask	Type the subnet mask if the Subnet Address type is selected.
Invert Selection	If it is checked, all the IP addresses except the ones listed above will be applied later while it is chosen.

Below is an example of IP objects settings.

Objects Setting >> IP Object

IP Object Profiles:

Index	Name
<u>1.</u>	RD Department
<u>2.</u>	Financial Dept.
<u>3.</u>	HR Department
<u>4.</u>	
<u>5.</u>	

3.5.2 IP Group

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

Objects Setting >> IP Group

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

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

Set to Factory Default Clear all profiles.

Click the number under Index column for settings in detail.

Objects Setting >> IP Group

Profile Index : 1

Name:

Interface: ▾

Available IP Objects

1-RD Department
 2-Financial Dept.
 3-HR Department

Selected IP Objects

(Empty)

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

Interface Choose WAN, LAN or Any to display all the available IP objects with the specified interface.

Available IP Objects All the available IP objects (created in IP Object web page) with the specified interface chosen above will be shown in this box.

Selected IP Objects Click button to add the selected IP objects in this box.

3.5.3 Service Type Object

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

Objects Setting >> Service Type Object

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

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

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

Set to Factory Default Clear all profiles.

Click the number under Index column for settings in detail.

Objects Setting >> Service Type Object Setup

Profile Index : 1

Name	<input type="text" value="SIP"/>		
Protocol	TCP	<input type="text" value="6"/>	
Source Port	=	<input type="text" value="1"/>	~ <input type="text" value="65535"/>
Destination Port	=	<input type="text" value="80"/>	~ <input type="text" value="80"/>

Name Type a name for this profile.

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

TCP	<input type="text" value="6"/>
Any	
ICMP	
TCP	
UDP	
TCP/UDP	
Other	

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

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

(!=) – when the first and last value are the same, it indicates

all the ports except the port defined here; when the first and last values are different, it indicates that all the ports except the range defined here are available for this service type.

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

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

Below is an example of service type objects settings.

Service Type Object Profiles:

Index	Name
<u>1.</u>	SIP
<u>2.</u>	RTP
<u>3.</u>	
<u>4.</u>	

3.5.4 Service Type Group

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

Objects Setting >> Service Type Group

Service Type Group Table:

[Set to Factory Default](#)

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

Set to Factory Default Clear all profiles.

Click the number under Index column for setting in detail.

Profile Index : 1

Name:

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

- Name** Type a name for this profile.
- Available Service Type Objects** You can add IP objects from IP Object page. All the available IP objects will be shown in this box.
- Selected Service Type Objects** Click button to add the selected IP objects in this box.

3.5.5 Keyword Object

You can set 200 keyword object profiles for choosing as black /white list in **Anti-Spam >>Profile Setting.**

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

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

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

- Set to Factory Default** Clear all profiles.
- Click the number under Index column for setting in detail.

Profile Index : 1

Name	<input type="text"/>
Contents	<input type="text"/>
<p>Limit of Contents: Max 3 Words and 63 Characters. Each word should be separated by a single space.</p> <p>You can replace a character with %HEX. Example: Contents: backdoo%72 virus keep%20out</p> <p>Result: 1. backdoor 2. virus 3. keep out</p>	

OK Clear Cancel

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

3.5.6 Keyword Group

This page allows you to bind several keyword objects into one group. The keyword groups set here will be chosen as black /white list in **Anti-Spam >>Profile Setting**.

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

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

- Set to Factory Default** Clear all profiles.
- Click the number under Index column for setting in detail.

Profile Index : 1

Name:

Available Keyword Objects

>>

<<

Selected Keyword Objects(Max 16 Objects)

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

3.5.7 File Extension Object

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

Profile 1 with name of “default” is the default profile, some files with the file extensions specified in this profile will be ignored and not be scanned by Vigor router.

File Extension Object Profiles: | **Set to Factory Default** |

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

- Set to Factory Default** Clear all profiles.
- Click the number under Profile column for configuration in details.

Objects Setting >> File Extension Object Setup

Profile Index: 1 Profile Name:

Categories	File Extensions
Image <input type="button" value="Select All"/> <input type="button" value="Clear All"/>	<input checked="" type="checkbox"/> .bmp <input checked="" type="checkbox"/> .dib <input checked="" type="checkbox"/> .gif <input checked="" type="checkbox"/> .jpeg <input checked="" type="checkbox"/> .jpg <input checked="" type="checkbox"/> .jpg2 <input checked="" type="checkbox"/> .jp2 <input checked="" type="checkbox"/> .pct <input checked="" type="checkbox"/> .pcx <input checked="" type="checkbox"/> .pic <input checked="" type="checkbox"/> .pict <input checked="" type="checkbox"/> .png <input checked="" type="checkbox"/> .tif <input checked="" type="checkbox"/> .tiff
Video <input type="button" value="Select All"/> <input type="button" value="Clear All"/>	<input checked="" type="checkbox"/> .asf <input checked="" type="checkbox"/> .avi <input checked="" type="checkbox"/> .mov <input checked="" type="checkbox"/> .mpe <input checked="" type="checkbox"/> .mpeg <input checked="" type="checkbox"/> .mpg <input checked="" type="checkbox"/> .mp4 <input checked="" type="checkbox"/> .qt <input checked="" type="checkbox"/> .rm <input checked="" type="checkbox"/> .wmv <input checked="" type="checkbox"/> .3gp <input checked="" type="checkbox"/> .3gpp <input checked="" type="checkbox"/> .3gpp2 <input checked="" type="checkbox"/> .3g2
Audio <input type="button" value="Select All"/> <input type="button" value="Clear All"/>	<input checked="" type="checkbox"/> .aac <input checked="" type="checkbox"/> .aiff <input checked="" type="checkbox"/> .au <input checked="" type="checkbox"/> .mp3 <input checked="" type="checkbox"/> .m4a <input checked="" type="checkbox"/> .m4p <input checked="" type="checkbox"/> .ogg <input checked="" type="checkbox"/> .ra <input checked="" type="checkbox"/> .ram <input checked="" type="checkbox"/> .vox <input checked="" type="checkbox"/> .wav <input checked="" type="checkbox"/> .wma
Java <input type="button" value="Select All"/> <input type="button" value="Clear All"/>	<input type="checkbox"/> .class <input type="checkbox"/> .jad <input type="checkbox"/> .jar <input type="checkbox"/> .jav <input type="checkbox"/> .java <input type="checkbox"/> .jcm <input type="checkbox"/> .js <input type="checkbox"/> .jse <input type="checkbox"/> .jsp <input type="checkbox"/> .jtk
ActiveX <input type="button" value="Select All"/> <input type="button" value="Clear All"/>	<input type="checkbox"/> .alx <input type="checkbox"/> .apb <input type="checkbox"/> .axs <input type="checkbox"/> .ocx <input type="checkbox"/> .olb <input type="checkbox"/> .ole <input type="checkbox"/> .tlb <input type="checkbox"/> .viv <input type="checkbox"/> .vrm
Compression <input type="button" value="Select All"/> <input type="button" value="Clear All"/>	<input type="checkbox"/> .ace <input type="checkbox"/> .arj <input type="checkbox"/> .bzip2 <input type="checkbox"/> .bz2 <input type="checkbox"/> .cab <input type="checkbox"/> .gz <input type="checkbox"/> .gzip <input type="checkbox"/> .rar <input type="checkbox"/> .sit <input type="checkbox"/> .zip
Execution <input type="button" value="Select All"/> <input type="button" value="Clear All"/>	<input type="checkbox"/> .bas <input type="checkbox"/> .bat <input type="checkbox"/> .com <input type="checkbox"/> .exe <input type="checkbox"/> .inf <input type="checkbox"/> .pif <input type="checkbox"/> .reg <input type="checkbox"/> .scr

Profile Name Type a name for this profile.

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

3.5.8 IM Object

This page allows you to set 32 profiles for Instant Messenger. These profiles will be applied in **Firewall>>IM/P2P Filter Profile** for filtering.

Objects Setting >> IM Object Profile

IM Profile Table: | [Set to Factory Default](#) |

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

Set to Factory Default Clear all profiles.

Click the number under Profile column for configuration in details. There are several types of Instant Messenger (IM) provided here for you to choose to disallow people using. Simple check the box (es) and then click **OK**. Later, in the **CSM>>IM/P2P Filter Profile** page, you can use **IM Object** drop down list to choose the proper profile configured here as the standard for the host(s) to follow.

Objects Setting >> IM Object Profile

Profile Index: 1

Profile Name:

Check for Disallow:

Advanced Management				
Activity / Application	MSN	YahooIM	AIM(<=5.9)	ICQ
Login	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Message	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
File Transfer	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Game	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Video	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Voice	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Conference	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Other Activities	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Other IM Application				VoIP
<input type="checkbox"/> AIM6	<input type="checkbox"/> QQ	<input type="checkbox"/> iChat	<input type="checkbox"/> Jabber/GoogleTalk	<input type="checkbox"/> Skype
<input type="checkbox"/> GoogleChat	<input type="checkbox"/> XFire	<input type="checkbox"/> GaduGadu	<input type="checkbox"/> Paltalk	<input type="checkbox"/> SIP
<input type="checkbox"/> Qnext	<input type="checkbox"/> Meetro	<input type="checkbox"/> POCO/PP365	<input type="checkbox"/> AresChat	

Web IM (* = more than one address)					
<input type="checkbox"/> WebIM URLs	<u>eMessenger</u>	<u>WebMSN</u>	<u>meebo*</u>	<u>eBuddy</u>	<u>ILoveIM*</u>
	<u>ICQ Java*</u>	<u>ICQ Flash*</u>	<u>goowy*</u>	<u>IMhaha*</u>	<u>getMessenger</u>
	<u>IMUnitive*</u>	<u>WabJet*</u>	<u>mabber*</u>	<u>MSN2GO*</u>	<u>KoolIM</u>
	<u>MessengerFX*</u>	<u>MessengerAdictos</u>	<u>WebYahooIM</u>		

Profile Name Type a name for this profile.

Type a name for such profile and check all the items that not allowed to be used in the host. Finally, click **OK** to save this profile.

3.5.9 P2P Object

This page allows you to set 32 profiles for peer-to-peer application. These profiles will be applied in **Firewall>>IM/P2P Filter Profile** for filtering.

Objects Setting >> P2P Object Profile

P2P Profile Table: | [Set to Factory Default](#) |

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

Set to Factory Default Clear all profiles.

Click the number under Profile column for configuration in details. There are several items for P2P protocols provided here for you to choose to disallow people using. Simple check the box (es) and then click **OK**. Later, in the **CSM>>IM/P2P Filter Profile** page, you can use **P2P Object** drop down list to choose the proper profile configured here as the standard for the host(s) to follow.

Objects Setting >> P2P Object Profile

Profile Index: 1

Profile Name:

Check for Disallow:

Protocol	Applications
<input type="checkbox"/> SoulSeek	SoulSeek
<input type="checkbox"/> eDonkey	eDonkey, eMule, Shareaza
<input type="checkbox"/> FastTrack	KazaA, BearShare, iMesh
<input type="checkbox"/> OpenFT	KCeasy, FilePipe
<input type="checkbox"/> Gnutella	BearShare, Limewire, Shareaza, Foxy
<input type="checkbox"/> OpenNap	Lopster, XNap, WinLop
<input type="checkbox"/> BitTorrent	BitTorrent, BitSpirit, BitComet
<input type="checkbox"/> Winny	Winny, WinMX, Share

Other P2P Applications			
<input type="checkbox"/> Xunlei	<input type="checkbox"/> Vagaa	<input type="checkbox"/> PP365	<input type="checkbox"/> POCO
<input type="checkbox"/> Clubbox	<input type="checkbox"/> Ares	<input type="checkbox"/> ezPeer	

Profile Name Type a name for this profile.

Type a name for such profile and check all the protocols that not allowed to be used in the host. Finally, click **OK** to save this profile.

3.5.10 Misc Object

This page allows you to set 32 profiles for miscellaneous applications. These profiles will be applied in **Firewall>>IM/P2P Filter Profile** for filtering.

Objects Setting >> Misc Object Profile

Misc Profile Table: | [Set to Factory Default](#) |

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

Set to Factory Default Clear all profiles.

Click the number under Profile column for configuration in details. Applications for tunneling and streaming are listed in the page for you to choose to disallow people using. Simple check the box (es) and then click **OK**. Later, in the **CSM>>IM/P2P Filter Profile** page, you can use **Misc Object** drop down list to choose the proper profile configured here as the standard for the host(s) to follow.

Profile Index: 16

Profile Name:

Check for Disallow:

Tunneling				
<input type="checkbox"/> Socks4/5	<input type="checkbox"/> PGPNet	<input type="checkbox"/> HTTP Proxy	<input type="checkbox"/> TOR	<input type="checkbox"/> VNN
<input type="checkbox"/> SoftEther	<input type="checkbox"/> FolderShare	<input type="checkbox"/> MS TEREDO	<input type="checkbox"/> Wujie/UltraSurf	<input type="checkbox"/> Hamachi
<input type="checkbox"/> HTTP Tunnel	<input type="checkbox"/> Ping Tunnel	<input type="checkbox"/> TinyVPN		

Streaming			
<input type="checkbox"/> MMS	<input type="checkbox"/> RTSP	<input type="checkbox"/> TVAnts	<input type="checkbox"/> PPSstream
<input type="checkbox"/> PPlive	<input type="checkbox"/> FeiDian	<input type="checkbox"/> UUSee	<input type="checkbox"/> NSPlayer
<input type="checkbox"/> PCAST	<input type="checkbox"/> TVKoo	<input type="checkbox"/> SopCast	<input type="checkbox"/> UDLiveX
<input type="checkbox"/> TVUPlayer	<input type="checkbox"/> MySee	<input type="checkbox"/> Joost	<input type="checkbox"/> FlashVideo

Remote Control			
<input type="checkbox"/> VNC	<input type="checkbox"/> Radmin	<input type="checkbox"/> SpyAnywhere	<input type="checkbox"/> ShowMyPC
<input type="checkbox"/> LogMeIn	<input type="checkbox"/> TeamViewer	<input type="checkbox"/> Gogrok	<input type="checkbox"/> RemoteControlPro
<input type="checkbox"/> CrossLoop	<input type="checkbox"/> WindowsRDP	<input type="checkbox"/> pcAnywhere	

Profile Name Type a name for this profile.

Type a name for such profile and check all the protocols that not allowed to be used in the host. Finally, click **OK** to save this profile.

3.6 CSM

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

IM/P2P Filtering

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.

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.

Web Filtering

We all know that the content on the Internet just like other types of media may be inappropriate sometimes. As a responsible parent or employer, you should protect those in your trust against the hazards. With Web filtering service of the Vigor router, you can protect your business from common primary threats, such as productivity, legal liability, network and security threats. For parents, you can protect your children from viewing adult websites or chat rooms.

Once you have activated your Web Filtering service in Vigor router and chosen the categories of website you wish to restrict, each URL address requested (e.g. www.bbc.co.uk) will be checked against our server database. This database is updated as frequent as daily by a global team of Internet researchers. The server will look up the URL and return a category to your router. Your Vigor router will then decide whether to allow access to this site according to the categories you have selected. Please note that this action will not introduce any delay in your Web surfing because each of multiple load balanced database servers can handle millions of requests for categorization.

Note: The priority of URL Content Filter is higher than Web Content Filter.



3.6.1 APP Enforcement Profile

You can define policy profiles for IM (Instant Messenger)/P2P (Peer to Peer)/Protocol application. This page allows you to set 32 profiles for different requirements. The APP Enforcement Profile will be applied in **Default Rule of Firewall>>General Setup** for filtering.

CSM >> APP Enforcement Profile

APP Enforcement Profile Table: | [Set to Factory Default](#) |

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

Set to Factory Default

Clear all profiles.

Profile

Display the number of the profile which allows you to click to set different policy.

Name

Display the name of the APP Enforcement Profile.

Click the number under Index column for settings in detail.

CSM >> APP Enforcement Profile

Profile Index: 1

Profile Name:

IM Object	None <input type="button" value="v"/>
P2P Object	None <input type="button" value="v"/>
Protocol Object	None <input type="button" value="v"/>
Misc Object	None <input type="button" value="v"/>

Profile Name

Type a name for the CSM profile.

Each profile can contain three objects settings, IM Object, P2P Object and Misc Object. Such profile can be applied in the **Firewall>>General Setup** and **Firewall>>Filter Setup** pages as the standard for the host(s) to follow.

3.6.2 URL Content Filter Profile

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

CSM >> URL Content Filter Profile

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

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

Administration Message (Max 255 characters)

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

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

CSM >> URL Content Filter Profile

Profile Index: 1

Profile Name:

Priority: **Log:**

1.URL Access Control

Enable URL Access Control Prevent web access from IP address

Action: Group/Object Selections:

2.Web Feature

Enable Restrict Web Feature

Action: Cookie Proxy Upload **File Extension Profile:**

Profile Name Type the name for such profile.

Priority It determines the action that this router will apply.
Both: Pass – The router will let all the packages that match with the conditions specified in URL Access Control and Web Feature below passing through. When you choose this setting, both

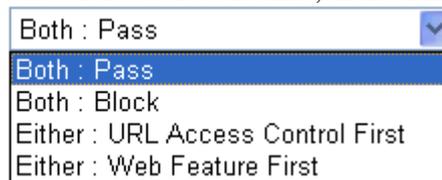
configuration set in this page for URL Access Control and Web Feature will be inactive.

Both:Block –The router will block all the packages that match with the conditions specified in URL Access Control and Web Feature below. When you choose this setting, both configuration set in this page for URL Access Control and Web Feature will be inactive.

Either: URL Access Control First – When all the packages matching with the conditions specified in URL Access Control and Web Feature below, such function can determine the priority for the actions executed. For this one, the router will process the packages with the conditions set below for URL first, then Web feature second.

Either: Web Feature First –When all the packages matching with the conditions specified in URL Access Control and Web Feature below, such function can determine the priority for the actions executed. For this one, the router will process the packages with the conditions set below for web feature first, then URL second.

Priority:



A dropdown menu for the 'Priority' setting. The current selection is 'Both : Pass'. The menu is open, showing the following options: 'Both : Pass', 'Both : Block', 'Either : URL Access Control First', and 'Either : Web Feature First'.

Log

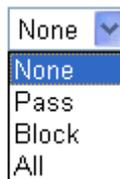
None – There is no log file will be recorded for this profile.

Pass – Only the log about Pass will be recorded in Syslog.

Block – Only the log about Block will be recorded in Syslog.

All – All the actions (Pass and Block) will be recorded in Syslog.

Log:



A dropdown menu for the 'Log' setting. The current selection is 'None'. The menu is open, showing the following options: 'None', 'Pass', 'Block', and 'All'.

URL Access Control

Enable URL Access Control - Check the box to activate URL Access Control. Note that the priority for **URL Access Control** is higher than **Restrict Web Feature**. If the web content match the setting set in URL Access Control, the router will execute the action specified in this field and ignore the action specified under Restrict Web Feature.

Prevent web access from IP address - Check the box to deny any web surfing activity using IP address, such as http://202.6.3.2. The reason for this is to prevent someone dodges the URL Access Control. You must clear your browser cache first so that the URL content filtering facility operates properly on a web page that you visited before.

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

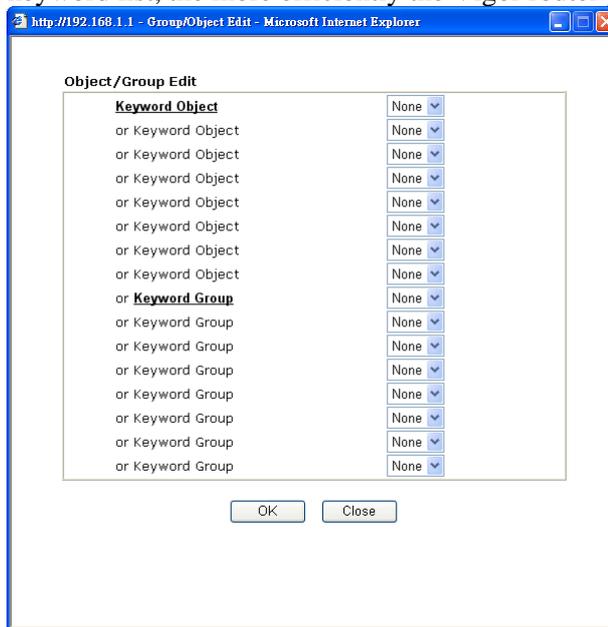
Block - Restrict accessing into the corresponding webpage with the keywords listed on the box below.

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

Action:

Block	▼
Pass	
Block	

Group/Object Selections – The Vigor router provides several frames for users to define keywords and each frame supports multiple keywords. The keyword could be a noun, a partial noun, or a complete URL string. Multiple keywords within a frame are separated by space, comma, or semicolon. In addition, the maximal length of each frame is 32-character long. After specifying keywords, the Vigor 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.



Web Feature

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

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

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

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

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

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

Proxy - Check the box to reject any proxy transmission. To control efficiently the limited-bandwidth usage, it will be of great value to

provide the blocking mechanism that filters out the multimedia files downloading from web pages.

Upload – Check the box to reject any file upload job.

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

File Extension Profile:

None	▼
None	
1-default	

3.6.3 Web Content Filter Profile

There are three ways to activate WCF on vigor router, using **Service Activation Wizard**, by means of **CSM>>Web Content Filter Profile** or via **System Maintenance>>Activation**.

Service Activation Wizard allows you to use trial version or update the license of WCF directly without accessing into the server (**MyVigor**) located on <http://myvigor.draytek.com>.

However, if you use the **Web Content Filter Profile** page to activate WCF feature, it is necessary for you to access into the server (**MyVigor**) located on <http://myvigor.draytek.com>. Therefore, you need to register an account on <http://myvigor.draytek.com> for using corresponding service. Please refer to section 4.1 for more information of creating MyVigor account.

Note: If you have used **Service Activation Wizard** to activate WCF service, you can skip this section.

WCF adopts the mechanism developed and offered by certain service provider (e.g., DrayTek). No matter activating WCF feature or getting a new license for web content filter, you have to click **Activate** to satisfy your request. Be aware that service provider matching with VigorPro5510 currently offers a period of time for trial version for users to experiment. If you want to purchase a formal edition, simply contact with the channel partner or your dealer.

Click **CSM** and click **Web Content Filter Profile** to open the profile setting page. The default setting for Setup Query Server /Setup Test Server is **auto-selected**. You can choose another server for your necessity by clicking **Find more** to open <http://myvigor.draytek.com> for searching another qualified and suitable one. Next, click the link of **Test a site to verify whether it is categorized** to do the verification.

Web-Filter License [Activate](#)
 [Status: Not Activated]

Setup Query Server	auto-selected	Find more
Setup Test Server	auto-selected	Find more

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

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

Administration Message (Max 255 characters) Cache : [L1 + L2 Cache](#)

```
<body><center><br><br><br><p>The requested Web page <br> from %SIP% <br>to %URL%
<br>that is categorized with %CL% <br>has been blocked by %RNAME% Web Content
Filter.<p>Please contact your system administrator for further
information.</center></body>
```

OK

- Activate** Click it to access into MyVigor for activating WCF service.
- Setup Query Server** It is recommend for you to use the default setting, auto-selected. You need to specify a server for categorize searching when you type URL in browser based on the web content filter profile.
- Setup Test Server** It is recommend for you to use the default setting, auto-selected. By the way, you can click the link of **Test a site to verify whether it is categorized** to access into the test server selected.
- Find more** Click it to open <http://myvigor.draytek.com> for searching another qualified and suitable server.
- Set to Factory Default** Click this link to retrieve the factory settings.
- Cache**
 - None** – the router will check the URL that the user wants to access via WCF precisely, however, the processing rate is normal. Such item can provide the most accurate URL matching.
 - L1** – the router will check the URL that the user wants to access via WCF. If the URL has been accessed previously, it will be stored for a short time (about 1 second) in the router to be accessed quickly if required. Such item can provide accurate URL matching with faster rate.
 - L2** – the router will check the URL that the user wants to access via WCF. If the data has been accessed previously, the IP addresses of source and destination IDs will be memorized for a short time (about 1 second) in the router. When the user tries to access the same destination ID, the router will check it by comparing the record stored. If it matches, the page will be retrieved quickly. Such item can provide URL matching with the fastest rate.
 - L1+L2 Cache** – the router will check the URL with fast

processing rate combining the feature of L1 and L2.

Eight profiles are provided here as Web content filters. Simply click the index number under Profile to open the following web page. The items listed in Categories will be changed according to the different service providers. If you have and activate another web content filter license, the items will be changed simultaneously. All of the configuration made for web content filter will be deleted automatically. Therefore, please backup your data before you change the web content filter license.

CSM >> Web Content Filter Profile

Profile Index: 1

Profile Name:

Log:

Black/White List

Enable

Action: Group/Object Selections

Action:

Groups	Categories		
Child Protection <input type="button" value="Select All"/> <input type="button" value="Clear All"/>	<input checked="" type="checkbox"/> Alcohol & Tobacco <input checked="" type="checkbox"/> Hate & Intolerance <input checked="" type="checkbox"/> Porn & Sexually <input checked="" type="checkbox"/> School Cheating <input checked="" type="checkbox"/> Child Abuse Images	<input checked="" type="checkbox"/> Criminal Activity <input checked="" type="checkbox"/> Illegal Drug <input checked="" type="checkbox"/> Violence <input checked="" type="checkbox"/> Sex Education	<input type="checkbox"/> Gambling <input checked="" type="checkbox"/> Nudity <input checked="" type="checkbox"/> Weapons <input checked="" type="checkbox"/> Tasteless
Leisure <input type="button" value="Select All"/> <input type="button" value="Clear All"/>	<input type="checkbox"/> Entertainment <input type="checkbox"/> Travel	<input type="checkbox"/> Games <input type="checkbox"/> Leisure & Recreation	<input type="checkbox"/> Sports <input type="checkbox"/> Fashion & Beauty
Business <input type="button" value="Select All"/> <input type="button" value="Clear All"/>	<input type="checkbox"/> Business	<input type="checkbox"/> Job Search	<input type="checkbox"/> Web-based Mail
Chating <input type="button" value="Select All"/> <input type="button" value="Clear All"/>	<input type="checkbox"/> Chat	<input type="checkbox"/> Instant Messaging	
Computer-Internet <input type="button" value="Select All"/> <input type="button" value="Clear All"/>	<input type="checkbox"/> Anonymizers <input type="checkbox"/> Download Sites <input type="checkbox"/> Search Engine,Portals <input type="checkbox"/> Malware <input type="checkbox"/> Illegal Software	<input type="checkbox"/> Forums & Newsgroups <input type="checkbox"/> Streaming, Downloads <input type="checkbox"/> Social Networking <input type="checkbox"/> Botnets <input type="checkbox"/> Information Security	<input type="checkbox"/> Computers <input type="checkbox"/> Phishing & Fraud <input type="checkbox"/> Spam Sites <input type="checkbox"/> Hacking <input type="checkbox"/> Peer-to-Peer
Other <input type="button" value="Select All"/> <input type="button" value="Clear All"/>	<input type="checkbox"/> Adv & Pop-Ups <input type="checkbox"/> Compromised <input type="checkbox"/> Finance <input type="checkbox"/> News <input type="checkbox"/> Politics <input type="checkbox"/> Restaurants & Dining <input type="checkbox"/> General <input type="checkbox"/> Image Sharing <input type="checkbox"/> Private IP Addresses	<input type="checkbox"/> Arts <input type="checkbox"/> Dating & Personals <input type="checkbox"/> Government <input type="checkbox"/> Non-profits & NGOs <input type="checkbox"/> Real Estate <input type="checkbox"/> Shopping <input type="checkbox"/> Cults <input type="checkbox"/> Network Errors <input type="checkbox"/> Uncategorized Sites	<input type="checkbox"/> Transportation <input type="checkbox"/> Education <input type="checkbox"/> Health & Medicine <input type="checkbox"/> Personal Sites <input type="checkbox"/> Religion <input type="checkbox"/> Translators <input type="checkbox"/> Greeting cards <input type="checkbox"/> Parked Domains

Profile Name

Type a name for such profile.

Log

None – There is no log file will be recorded for this profile.

Pass – Only the log about Pass will be recorded in Syslog.

Block – Only the log about Block will be recorded in Syslog.

All – All the actions (Pass and Block) will be recorded in Syslog.



White/Black List

Enable – Activate white/black list function for such profile.

Group/Object Selections – Click **Edit** to choose the group or object profile as the content of white/black list.

Pass - allow accessing into the corresponding webpage with the characters listed on **Group/Object Selections**. If the web pages do not match with the specified feature set here, they will be processed with the categories listed on the box below.

Block - restrict accessing into the corresponding webpage with the characters listed on **Group/Object Selections**.

If the web pages do not match with the specified feature set here, they will be processed with the categories listed on the box below.

Action

Pass - allow accessing into the corresponding webpage with the categories listed on the box below.

Block - restrict accessing into the corresponding webpage with the categories listed on the box below.

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

3.7 Defense Configuration

This menu allows you to set profiles for, activate and upgrade the service of Anti-Intrusion/Anti-Virus in your system.

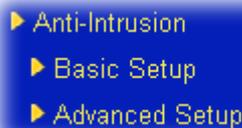


3.7.1 Anti-Intrusion

Anti-Intrusion allows you to prevent the intrusion from hackers while accessing into Internet. It can detect the intrusion and execute basic defense.

There are more than 200 basic rules for anti-intrusion and anti-virus for this router. To acquire more rules for anti-intrusion, it is suggested for you to register your router by entering www.vigorpro.com. When you finished the registration, you can get and activate a wide range of anti-intrusion rules from the website. In addition, you will be allowed to download/update new rules (if they are released) from the websites lately (during the valid time of the license key you purchased) after completing the registration.

You are allowed to use trial version with anti-intrusion and anti-virus features for 30 days after you register for the router. And you will be noticed with an e-mail while it is going to expire.



3.7.1.1 Basic Setup

Basic Setup page lets you to enable the anti-intrusion service and choose the suitable level for the detection.

Anti-Intrusion Control Setup [Signature Version : **basic**]

Enable Anti-Intrusion Service: Intrusion detection of the hacker is made effective

Sensitiveness of intrusion detection:

High Security: Matching all rules

Medium Security: Matching high and medium severity rules

Low Security: Matching high severity rules

Action's "default" processing at time of intrusion detection:

Enable Pass processing

Enable Disallow processing

Enable Reset processing

Note : If you want to email alert or syslog, please setup on the [SysLog/Mail Alert Setup](#) page. If you need more information, please enter [Advanced Setup](#)

Anti-Intrusion Control Setup

This field will display the signature version of this router. The default signature version is “**basic**”. In this version, you can modify the settings for Anti-Intrusion rules in **Defense Configuration>>Anti-Intrusion >>Advanced Setup** page. However, if you restart/reset the router, all the modified configurations for the rules will not be available and return to the default settings. Except “**basic**”, the modified configurations for other signature versions are available all the time after you saved them in **Defense Configuration>>Anti-Intrusion >>Advanced Setup** page.

Enable Anti-Intrusion Service

Check this box to enable the anti-intrusion function.

High Security

Click this radio button to activate the anti-intrusion service with overall detecting conditions. That is, the router will detect and block the incoming/outgoing packets which match all the severity rules, including high, medium and low. The degree of severity for each rule is defined in Advance Setup.

Medium Security

Click this radio button to activate the anti-intrusion service with medium detecting conditions. That is, the router will detect and block the incoming/outgoing packets which match the highest and medium severity rules. The degree of severity for each rule is defined in Advance Setup.

Low Security

Click this radio button to activate the anti-intrusion service with minimum detecting conditions. That is, the router will detect and block the incoming/outgoing packets which match the highest severity rules. The degree of severity for each rule is defined in **Advanced Setup**.

Enable Pass processing

Click this radio button to detect if there is any intrusion occurrence for your reference. The system will not do any advanced action for such condition.

Enable Disallow processing

Click this radio button to block the incoming/outgoing packets with possible intrusion actions transmitting through the router.

Enable Reset procession Click this radio button to break down the communication between your computer and specific link which might have intrusion actions.

3.7.1.2 Advanced Setup

This page lists all the available types and allows you to adjust the rule setting for each type. The rules will be applied by the options chosen in the page of **Defense Configuration>>Anti-Intrusion>>Basic Setup** for Anti-Intrusion.

Defense Configuration >> Anti-Intrusion >> Advanced Setup

Anti-Intrusion Type Setup		SID/NAME:	<input type="text"/>	<input type="button" value="Search"/>
BO (55)	Web-Client (58)			
DDoS/DoS (61)	Web-IDS (145)			
Exploit (290)	Web-Misc (438)			
ICMP (42)	Web-PHP (463)			
I-Worm (42)	Latest (0)			
IRC (15)				
Malware (591)				
Misc (239)				
RPC (57)				
Scan (105)				
SQL-Inject (26)				
Web-CGI (82)				

SID/Name To find the specific type of anti-intrusion, you can type its SID number or name in this field if you know, and then click **Search**. The system will locate that type for you.

Search It can help the user to find out specific anti-intrusion rule quickly.

Type links Click any anti-intrusion type link to access into next page for configuring the rules settings. Here we provide several rules for each type. The factory types and rules for anti-intrusion are shown in this page. If you want to acquire more types and rules, please go to www.vigorpro.com and finish the registration work. Later, the wide range of anti-intrusion types will be added into this page.

After you click any one of type links, you can access into the rules setup page for activating rules. We take the type of BO as an example. Below is the rules setup page for BO type.

For the detailed information about the full name, meaning of each rule and/or type, you can click the name link list on the Anti-Intrusion Rules Setup page to connect VigorPro webpage for viewing.

Anti-Intrusion Rules Setup Page: 1 / 7

Enable	Name	SID	Severity	Log	Action			
					Pass	Disallow	Reset	Default
<input checked="" type="checkbox"/>	AJ Web Server DoS	1585	M	<input checked="" type="checkbox"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
<input checked="" type="checkbox"/>	Active Webcam WebServer DoS	1518	M	<input checked="" type="checkbox"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
<input checked="" type="checkbox"/>	Allaire JRUN DoS attempt	1121	M	<input checked="" type="checkbox"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
<input checked="" type="checkbox"/>	Annex Terminal DoS attempt	1172	M	<input checked="" type="checkbox"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
<input checked="" type="checkbox"/>	Appian Enterprise BS DoS	3784	M	<input checked="" type="checkbox"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
<input checked="" type="checkbox"/>	Apple MAC OSX VPN DoS	3749	M	<input checked="" type="checkbox"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
<input checked="" type="checkbox"/>	Arescom NetDSL Telnet DoS	2370	M	<input checked="" type="checkbox"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
<input checked="" type="checkbox"/>	Ascend Route	77	M	<input checked="" type="checkbox"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
<input checked="" type="checkbox"/>	Bot channel DDoS command2	4684	M	<input checked="" type="checkbox"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
<input checked="" type="checkbox"/>	CISCO VoIP DoS attempt	1216	M	<input checked="" type="checkbox"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>

- Enable** Check to enable this rule. If you uncheck this box, the corresponding settings for the rule will not be executed.
- SID** The number for each anti-intrusion rule is displayed in this field.
- Name** A brief description name for the anti-intrusion rule is shown in this field. Click the name link to access into VigorPro website for checking the detailed information for the specified anti-intrusion.
- Severity** It means the degree of the influence for this type to the computer, machine, network and environment.
 H: representing that this type will cause severest effect which must crash/destroy your computer.
 M: representing that this type will cause severer effect which might crash your computer.
 L: representing that this type will cause small effect which might not crash your computer.
- Log** In order to show the detection log with such rule on the window of Draytek Syslog, you have to check the log box here and enable the **SysLog Access Setup** from **System Maintenance >> Syslog/Mail Alert**.
- Action**
Pass - Click this radio button to detect if there is any intrusion occurrence for your reference. The system will not do any advanced action for such condition.
Disallow - Click this radio button to block the incoming/outgoing packets with possible intrusion actions transmitting through the router.
Reset - Click this radio button to break down the communication between your computer and specific link which might have intrusion actions.
Default - Click this radio button to execute the anti-intrusion detection according to the setting that you set in Basic Setup.

Page

Type the page number in this field (if there is more than one page of anti-virus detail view displayed on this page). Then click **Go** to the specified page. Or you can click **/>**, **>>**, **<<** or **</** button on the right side of the **Go** button to access to the home/previous/next/end page.

3.7.2 Anti-Virus

Vigor router can offer basic virus scanning, destroying and cut off the connection between questionable link and your computer for the files transmitted through specified protocol. In addition, several types of compressed file formats such as .zip, .gzip, .bzip2 are supported and can be scanned with this router. There is no limitation in the file size for the transmitted (incoming or outgoing) file. With this feature, all the files processed with the protocol specified in Anti-Virus web page will be scanned for finding out virus while passing through the router.



Note: Files with three-layer compression (the files are compressed with three times) also can be scanned by this router.

3.7.2.1 Profile Setting

This page allows you to set eight profiles for anti-virus scanning. These profiles can be invoked through firewall configuration. It is recommended to build one profile at least. Thus you will have selectable anti-virus profile setting in **Firewall->General Setup**.

Defense Configuration >> Anti-Virus >> Profile Setting

Anti-Virus Profile Table [Signature Version: **basic**] | [Set to Factory Default](#) |

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

Administration Message (Max 255 characters)

Email scanned by DrayTek VigorPro UTM.

Note: If you want to use email alert or syslog, please configure the [SysLog/Mail Alert Setup](#) page. For more information, please visit the [Virus List](#) page.

OK

The Administration Message box allows you to fill in important notification directly for SMTP and POP3 protocols. It will be saved as a file. While receiving an e-mail, the user will receive an attached file with the content listed in this box.

To edit a profile setting, please click the number link under Profile. You can see the following screen. You can check the boxes listed below for different operation respectively. If you uncheck this box, the corresponding settings for the protocol will not be performed.

Profile Index : 1 Profile Name:

Operation/Protocol	SMTP	POP3	IMAP	HTTP	FTP
Action	Pass	Pass	Pass	Pass	Pass
Enable Virus Scan	<input checked="" type="checkbox"/>				
Enable Log	<input checked="" type="checkbox"/>				
Detect Macro Attachment	<input type="checkbox"/>				
Detect Encrypted Zipped Files	<input type="checkbox"/>				
Detect Suspicious Compression	<input type="checkbox"/>				
Compression Ratio Threshold	1:400	1:400	1:400	1:400	1:400
Append Message	<input type="checkbox"/>	<input type="checkbox"/>			
File Filter	1-default	1-default	1-default	1-default	1-default
Block Fragmented Mail	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		
Block Multiple Sessions Download				<input type="checkbox"/>	

Note: If the document file is generated by Microsoft Office 2003 or earlier version, we advise you to enable **Detect Macro Attachment** function.

- Profile Name** Type a name for the profile.
- Protocol** Currently, only the files transmitted through the protocols listed in this page including **SMTP**, **POP3**, **IMAP**, **HTTP** and **FTP** will be scanned by this router.
- Action** Choose the action that you want to apply to the protocols of each operation.

Action	Pass
	Pass
	Destroy
	Reset

 - Pass** - Detect if there is any virus for your reference. The system will not do any advanced action for such condition.
 - Destroy**- Destroy the infected file found by the router system. However, the file will be downloaded still.
 - Reset** - Break down the communication between your computer and specific link which might have virus included.
- Enable Virus Scan** Check this box to enable the general virus scan procedure for different protocols.
- Enable Log** In order to show the virus detection log on the window of Draytek Syslog, you have to check the log box here and enable the **SysLog Access Setup** from **System Maintenance >> Syslog/Mail Alert**.

SysLog / Mail Alert Setup

SysLog Access Setup

Enable

Server IP Address

Destination Port

Enable syslog message:

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

- Detect Macro Attachment** The file with macro attachment will be passed/destroyed/reset under different protocols. The system will detect it automatically if you set corresponding configuration here.
- Detect Encrypted Zipped Files** The file zipped with encryption will be detected and then be passed/destroyed/reset according to the configuration set here.
- Detect Suspicious Compression** The file with suspicious or non-support compression format will be detected and then be passed/destroyed/reset according to the configuration set here.
- Compression Ratio Threshold** Choose one of the compression ration selections as the threshold for the system to block or pass the file compressed with the ratio specified here.
- Append Message** This function is available for SMTP and POP3 protocols. If you check it, the message typed under the box of Administration Message will be sent out with e-mail.
- File Filter** Click this link to open **Defense Configuration>>Anti-Virus >>File Pattern List** for viewing current settings.
- Block Fragmented Mail** The file with fragmentations will be passed/destroyed/reset under different protocols. The router cannot execute the scanning job for some mail fragmentation if you check the boxes here.
- Block Multiple Sessions Download** The file with multiple sessions which are created by **HTTP** will be detected and then be passed/destroyed/reset according to the configuration set here.

3.7.2.2 Virus List

This page displays the virus list ordered by digits (0-9) and letters (A-Z). Each number after the letter link indicates the total types of the virus collected.

Anti-Virus List Overview

SID/NAME:

0 - 9 (0)	M - N (231)
A - B (537)	O - P (269)
C - D (3)	Q - R (5)
E - F (229)	S - T (1055)
G - H (2)	U - V (33)
I - J (21)	W - X (244)
K - L (0)	Y - Z (0)

SID/NAME

To find the specific type of anti-virus, you can type its SID number or name in this field if you know, and then click **Search**. The system will locate that rule for you.

Search

Click this button to find out all the virus rules related to the SID/NAME that you entered. The page of the searching result will be shown as the following picture.

Anti-Virus Search Result < << >> >

Name	SID
Bagle.AC	21593
Bagle.AF	22361
Bagle.AG	22417
Bagle.BL	34196
Bagle.BY-2	35493
Bagle.BZ-1	35496
Bagle.BZ-2	35497
Bagle.CB	35682
Bagle.CD-1	35686
Bagle.CD-2	35687

Click each name link to check the detailed information of the anti-virus rule.

Detailed View for Anti-Virus

From the fourteen types of anti-virus list, click any one of them to access into next page. The detailed view list for anti-virus rule will be shown as below.

Anti-Virus Detail View

Page: / 23

NAME	SID	NAME	SID
Bkdr.Agent.afci	31032	Bkdr.Agent.la	4483
Bkdr.Agent.agkm	30566	Bkdr.Agent.ms	2736
Bkdr.Agent.ahe	7706	Bkdr.Agent.nf	2222
Bkdr.Agent.alnt	35565	Bkdr.Agent.nx	2754
Bkdr.Agent.alnv	35566	Bkdr.Agent.uek	32450
Bkdr.Agent.aly	10163	Bkdr.Agobot.adb	6029
Bkdr.Agent.amhs	36411	Bkdr.Agobot.adg	5424
Bkdr.Agent.amms	37687	Bkdr.Agobot.afk	5427
Bkdr.Agent.amrc	37670	Bkdr.Agobot.gen	6275
Bkdr.Agent.anef	37194	Bkdr.Agobot.gen*1	6224
Bkdr.Agent.aou	12567	Bkdr.Agobot.gen*10	5403
Bkdr.Agent.ddm	15135	Bkdr.Agobot.gen*11	5401

NAME A brief description name for the anti-virus rule is shown in this field. Click the name link to access into VigorPro website for checking the detailed information for the specified anti-virus.

SID The number for each anti-virus rule is displayed in this field.

Page Type the page number in this field (if there is more than one page of anti-virus detail view displayed on this page). Then click **Go** to the specified page. Or you can click **/>**, **>>**, **<<** or **>/** button on the right side of the Go button to access to the home/previous/next/end page.

3.7.2.3 File Filter Profile

To avoid confidential file being leaked out by someone else through network and cause severe consequence, you can specify the file name in this page and determine to destroy or scan or pass it while the file passes through the router.

Before activating the File Filter Profile, you have to set one Anti-Virus profile on **Defense Configuration>>Anti-Virus>>Profile Setting**. Also you can specify file names without virus appended to be ignored by anti-virus server to improve the performance.

This page allows you to set 32 entries (rules) of file names to be filtered by the router. In such case, the file format is ignored. The router will destroy, scan or non-scan the specified filename according to the configuration that you set here.

File Filter Profile Table

[Set to Factory Default](#)

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

Click any number link to open the configuration page. Below is the page of **File Filter Profile**. The priority of each entry is determined by the index number. That is, the entry of Index 1 has the highest priority in file name filtering; the entry of Index 32 has the lowest priority in filtering.

Defense Configuration >> Anti-Virus >> File Filter Profile >> Profile Setting

Profile Index: 1 Profile Name: default

Priority: File Extension First Default Action: Scan

Keyword

	Action	Group/Object Selections	
1.	Scan		Edit
2.	Scan		Edit
3.	Scan		Edit

File Extension

Action: Non-Scan Profile: 1-default

Destroy the file if the file name is over length (Max 76 characters).

Syslog/Mail Alert: Non-Match Only

OK Clear Cancel

Profile Name

Type a name for such profile.

Priority

Such item determines which profile will be executed first. If you choose File Extension First, Vigor router will filter the virus based on the file extension profile selected first, next filter the virus based on the keyword later; vice versa.

Priority: File Extension First

- File Extension First
- Keyword First

Default Action

Choose one of the actions (Scan, Non-Scan, Destroy) as the default action if the file does not meet the conditions configured below.

Keyword

You can set three sets of keywords for this profile.

Action -

Choose the action that you want to apply to the selected keyword.

Destroy- Destroy the file with name specified here which is found by the router system.

Non-Scan –The file will not be scanned and will not be processed by using general rules set in Anti-Virus profile.

Scan – Just scan the file with name specified here which is found by the router system, and be processed by using general rules set in Anti-Virus profile.

Group/Object Selections - Click **Edit** to choose the preset keyword groups and/or objects.

File Extension

Determine the filtering condition for downloading files.

Action -

Choose the action that you want to apply to the selected file extension profile.

Destroy- Destroy the file with name specified here which is

found by the router system.

Non-Scan –The file will not be scanned and will not be processed by using general rules set in Anti-Virus profile.

Scan – Just scan the file with name specified here which is found by the router system, and be processed by using general rules set in Anti-Virus profile.

Profile – Use the drop down list to specify one profile to be executed as filtering condition.

Destroy the file if the file name is over length

Check this box to destroy the file with filename over 76 characters.

Syslog/Mail Alert

Specify the condition for the system to send Syslog/Mail Alert for the default action.

Syslog/Mail Alert: 

None
Match Only
Non-Match Only
Both

None – No action will be recorded in Syslog.

Match Only- Only the log that matching with the above condition will be recorded in Syslog.

No-Match Only – Only the log that not matching with the above condition will be recorded in Syslog.

Both – All the actions will be recorded in Syslog.

Click **OK** to finish the page configuration.

3.7.3 Anti-Spam

Many people suffer with unwanted mails coming from everywhere. Such device offers a mechanism, named Anti-Spam, to do basic scanning for filtering unnecessary mails and sorting the mails.

To activate function of Anti-Spam, you **have to configure profile(s) for your computer first.**



3.7.3.1 Profile Setting

Open **Defense Configuration>>Anti- Spam>>Profile Setting** menu to access into the following page. There are sixteen profiles provided by this system for you to define.

Defense Configuration >> Anti-Spam >> Profile Setting

Anti-Spam Profile Table		Set to Factory Default	
Profile	Name	Profile	Name
1.	Default	9.	
2.		10.	
3.		11.	
4.		12.	
5.		13.	
6.		14.	
7.		15.	
8.		16.	

Profile (1 ~16)

There are sixteen profiles provided for you to define. Simply click the number link under Profile, the setting page for that number will be open for you to configure.

Name List the name for the profile setting.

Simply click number under Profile item. The detailed page will be shown right away. The following graphic is the web page for the profile marked with number 1.

Profile Index : 1 Profile Name:

Choose Protocol to Scan Spam Log All Mail Events

SMTP POP3

Priority	Anti-Spam Function												
1.	<input type="checkbox"/> Enable SPAM Grey List Defense	<input type="checkbox"/> Log Grey List Events											
2.	<input type="checkbox"/> Enable Black/White List	<input type="checkbox"/> Log Matched Events											
	Priority Selection	<input type="text" value="Pass First"/>											
	<table border="1"> <thead> <tr> <th>Category</th> <th>Action</th> <th>Group/Object Selections</th> </tr> </thead> <tbody> <tr> <td>Sender</td> <td><input type="text" value="Pass"/></td> <td><input type="text"/> <input type="button" value="Edit"/></td> </tr> <tr> <td>Receiver</td> <td><input type="text" value="Pass"/></td> <td><input type="text"/> <input type="button" value="Edit"/></td> </tr> <tr> <td>Subject</td> <td><input type="text" value="Pass"/></td> <td><input type="text"/> <input type="button" value="Edit"/></td> </tr> </tbody> </table>		Category	Action	Group/Object Selections	Sender	<input type="text" value="Pass"/>	<input type="text"/> <input type="button" value="Edit"/>	Receiver	<input type="text" value="Pass"/>	<input type="text"/> <input type="button" value="Edit"/>	Subject	<input type="text" value="Pass"/>
Category	Action	Group/Object Selections											
Sender	<input type="text" value="Pass"/>	<input type="text"/> <input type="button" value="Edit"/>											
Receiver	<input type="text" value="Pass"/>	<input type="text"/> <input type="button" value="Edit"/>											
Subject	<input type="text" value="Pass"/>	<input type="text"/> <input type="button" value="Edit"/>											
Destroy Tag Message(Max 30 characters)		<input type="text"/>											
3.	<input checked="" type="checkbox"/> Enable Anti-Spam Server Query (Need license)												
	Select an Action for Each Category												
	Category	Action Log Message(Max 30 characters)											
	Spam	<input type="text" value="Tag"/> <input checked="" type="checkbox"/> <input type="text" value="***VigorPro SPAM***"/>											
Bulk	<input type="text" value="Tag"/> <input checked="" type="checkbox"/> <input type="text" value="***VigorPro BULK***"/>												
Time Out	<input type="text" value="Pass"/> <input type="checkbox"/> <input type="text"/>												

Profile Name

Type a name for such profile setting.

Choose Protocol to Scan Spam

Spam files usually come with protocol of SMTP or POP3. Please check the box that you want to avoid. It would be better to check both protocols. In addition, you can check **Log All Mail Events** to send record of all mail events to syslog.

Enable SPAM Grey List Defense

Grey List is a method for e-mail against spam. A mail transfer agent (MTA) using grey list will "temporarily reject" any email from a sender it does not recognize. If the mail is legal, the server will check it again and the email will be accepted. If the mail is from a spammer, it will probably not be retried since a spammer goes through thousands of email addresses and can not afford the time delay to retry.

Check this button to enable SPAM grey list defense function.

In addition, you can check **Log Grey List Events** to send record of events to syslog.

Enable Black/White List

Check this box to enable black and white list settings.

Priority Selection – Choose **Pass First** for passing the mails matching with **Black and White List** first, or choose **Destroy First** for destroying the content of mail matching with **Black and White List** first.

Priority Selection

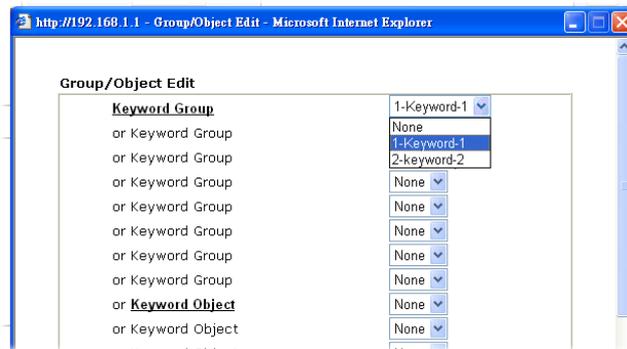
Log Matched Events - Check this box to record all the matched events of mails on Syslog.

Action – Determines the action (**Pass** or **Destroy**) for the

emails coming from the sender, or for the emails sending out from the receiver, or for the subject with the keyword selected here.

Action	
Sender	Destroy
Receiver	Pass Destroy
Subject	Pass

Group/Object Selections - Choose a suitable group or object for passing or blocking. Click **Edit** to open the following dialog. The keyword/group that you have set on **Object Settings>>Keyword Object/ Object Settings>>Keyword Group** will be displayed here for you to choose.



Destroy Tag Message (Max 30 characters) - Type the character(s) as a tag for destroying.

Enable Anti-Spam Server Query (Need license)

Mails would be judged and categorized into Spam, Bulk or normal mails. For the one that is confirmed as spam will be processed with the rule of **Spam**; and the one that is probably spam will be processed with the rule of **Bulk**. Please set different process action for Spam and Bulk respectively.

Action - When the system fails due to system timeout or network problem, you can specify specific action (Pass or Tag) for the system to execute immediately. Choose the action (**Pass**, **Tag** or **Reset**) for the spam, bulk and time out emails.

Category	Action
Spam	Tag
Bulk	Pass Tag
Time Out	Reset

Pass - Choose this action to make all mails passing through.

Tag - Choose this action to make all mails be tagged with certain words for you to identify easily. For example, type "SPAM" on the box of **Message**. If the subject of some mail is "license page" and it is judged as spam, then it will be

shown as “***SPAM*** license page” in your mail box. Such tag can help users to identify which mail is useful or useless quickly.

Reset – Choose this action to disconnect the network. It is mainly applied on SMTP server.

Log - Check the box to have the process record stated on Syslog.

Message - Type words which will be placed before the subject of mail and help you to identify.

Clear

Delete the settings configured above and reset to default settings.

Cancel

Delete the settings configured above and return to previous page.

Click **OK** to finish the page configuration.

3.7.3.2 Grey List Detail Setting

Grey List is a method for e-mail against spam. A mail transfer agent (MTA) using grey list will "temporarily reject" any email from a sender it does not recognize. If the mail is legal, the server will check it again and the email will be accepted. If the mail is from a spammer, it will probably not be retried since a spammer goes through thousands of email addresses and can not afford the time delay to retry.

This page allows user to set conditions to block mails coming from outside. Basically, the incoming mails will be regarded as malice and must be blocked. However, mails sent out by the host will be regarded as normal and no limitation will be set for them.

Defense Configuration >> Anti-Spam >> Grey List Setting

Grey List Entry Table (Add)
Page: / 1000

State	Sender	Receiver	Sender_IP	Action Result
N/A	perry@hotmail.com	carrie_ni@draytek.com	192.168.1.12	Success

Grey List Entry Setting:

Grey List System Setting:

Initial Delay Time(sec)

White List Accept Time(sec)

White List Timeout(sec)

Sender E-Mail Address Type the e-mail address of the sender.

Receiver E-Mail Address Type the e-mail address of the receiver.

Sender IP Specify the sender’s IP for blocking with grey list.

Initial Delay Time Type the time of initial delay for mail checking.

White List Accept Time Type the time for mail tracing with white list.

White List Timeout (sec) Type the timeout for mail checking with white list.

Set Click to save and invoke the timer setting.

3.7.4 Activation for Anti-Intrusion/Anti-Virus/Anti-Spam/Web-Filter Service

After you have finished the profile settings, it is the time to activate the mechanism for your computer. Click **Defense Configuration>>Activation** to open the following page for accessing <http://myvigor.draytek.com>.

Defense Configuration >> Activation Activate via interface : WAN 1

Anti-Intrusion/Anti-Virus License [Status:Not Activated]	Activate
Anti-Spam License [Status:Not Activated]	Activate
Web-Filter License [Status:Not Activated]	Activate

Authentication Message

Note: If you want to use email alert or syslog, please configure the [SysLog/Mail Alert Setup](#) page.
If you change the service provider, the configuration of the function will be reset.

Activate via interface Choose WAN interface used by such device for activating Web Content Filter.

Activate via interface :

WAN 1	▼
WAN 1	
WAN 2	

Activate The **Activate** link brings you accessing into www.vigorpro.com to finish the activation of the account and the router.

Authentication Message As for authentication information of **web filter, Anti-Intrusion/Anti-Virus/Anti-Spam**, the process of authenticating will be displayed on this field for your reference.

Below shows the successful activation of AI/AV/AS/Web Content Filter:

Anti-Intrusion/Anti-Virus License[Activate](#)

[Status:DT-KL] [Start Date:2010-02-26 Expire Date:2010-03-29]

Anti-Spam License[Activate](#)

[Status:CTCH] [Start Date:2010-02-26 Expire Date:2010-03-29]

Web-Filter License[Activate](#)

[Status:CT-CF] [Start Date:2010-02-26 Expire Date:2010-03-29]

```
Authentication Message
WebFilter, Authenticate successful, 2010-03-25 03:30:07
Anti-Spam, Authenticate successful, 2010-03-24 15:37:15
AV/AI, Authenticate successful, 2010-03-25 05:28:47
```

Note: If you want to use email alert or syslog, please configure the [SysLog/Mail Alert Setup](#) page.

If you change the service provider, the configuration of the function will be reset.

OK

Cancel

3.7.5 AI/AV Auto Block

This page can determine the block standard for data transmission based on the AI/AV auto block setting. In another word, when the host is attacked over the count number set here, the system will block the data transmission from the source IP automatically for security.

Limitation List displays the specific limitations that you set in this web page.

Defense Configuration >> AI/AV Auto Block

AI/AV Auto Block

Enable Disable Action: Block ▾ Syslog Enable

General Setup

AI Count: Severity: Medium ▾ AV Count: Time Interval: seconds

Limitation List

Index	Start IP	End IP	AI Counts	AV Counts	Time Interval

Specific Limitation

Start IP: End IP:
 AI Count: AV Count: Time Interval: seconds

Time Schedule

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

Note: Action and Idle Timeout settings will be ignored.

Enable/Disable

Click **Enable** to activate AI/AV Count Setting. The AI/AV auto block setting result will be seen in **Diagnostics>>LAN Security Monitor**. Default setting is **Disable**.

Diagnostics >> LAN Security Monitor

LAN Security Monitor

Refresh Seconds: Page: Refresh

Index	IP Address	Tx rate(Kbps)	Rx rate(Kbps)	Sessions	AI Count	AV Count	Action

General Setup

Settings configured here will be applied for most of the defense events (intrusion/virus) except settings configured in Specific Limitation.

AI Count – type the number for the system to block the connection of the source IP for AI events.

Severity – choose **Low**, **Medium** or **High** for the system to block the connection of the source IP for AI and AV events.

AV Count – type the number for the system to block the connection of the source IP for AV events.

Time Interval – type the time for the system to wait and execute the action of blocking,

Limitation List

This field displays the information for specific limitation.

Specific Limitation

Users can specify clients on LAN and let the router count AI/AV event in certain range by specifying start IP, end IP, AI count, AV count, time interval and etc.

Start IP/End IP – Specify the range for specific limitation (starting IP and ending IP).

AI Count – type the number for the system to block the connection of the source IP (within the range of specific limitation) for AI events.

AV Count – type the number for the system to block the connection of the source IP (within the range of specific limitation) for AV events.

Time Interval – type the time for the system to wait and execute the action of blocking,

Add – Click this button to add one new condition for AI/AV count to the list above.

Edit – Click this button to modify selected item listed on Limitation List.

Delete – Click this button to delete the selected item listed on Limitation List.

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.

3.7.6 Signature Upgrade

You can get the most updated signature from DrayTek's server if the license key of anti-virus/anti-intrusion for the VigorPro 5510 is not expired. Before you upgrade the signature, please check the validation information either from WEB user interface of VigorPro 5510 or account information from www.vigorpro.com.

Defense Configuration >> Signature Upgrade

Signature Upgrade Setting

Signature Version : **basic**
 Signature Build Date : **Tue Aug 29 09:16:25.00 2006**
 Upgrade via interface : WAN 1

Setup download server	<input type="text" value="auto-selected"/>	find more
Setup query server	<input type="text" value="auto-selected"/>	find more
Signature authentication/download message: <input type="text"/>		

Upgrade Manually

Upgrade Automatically

Scheduled Update

Every: (hour) (minutes after the hour)

Daily: (hour) (minute)

Weekly: (day) (hour) (minute)

Signature Upgrade Setting

It displays the signature version for your reference. There are three levels for the signature:

basic – If you did not register and activate your account, you can just own the default 200 (or more) anti-intrusion and anti-virus rules for your router.

DT-DT/DT-KL_XXXXXX – If you have registered and activated your AI/AV account, and downloaded the newest rules from www.vigorpro.com, you can see DT-DT/DT-KL in this field that means you have obtained the latest signature information.

Upgrade via Interface

Choose WAN interface used by such device for upgrading signature.

Setup download server/Setup query server

The default setting is auto-selected. You can change the setting if it is required to be. Click the **find more** link to get more information.

Please choose a download server / query server of the continent that your router is located.

Zone	Service	Provider	Download Server	Query Server
Africa	AI-AV	DT-DT	85.236.48.68	85.236.48.68
Africa	AI-AV	DT-KL	85.236.48.68	85.236.48.68
Africa	WCF	CT-CF	ctwsd1.ctmail.com	www.vigorpro.com
Africa	AS	CTCH	resolver1.ctmail.com	www.vigorpro.com
Africa	ACS	DT-ACS	myvigor.draytek.com	myvigor.draytek.com
America	WCF	CT-CF	ctwsd1.ctmail.com	www.vigorpro.com
America	AS	CTCH	resolver1.ctmail.com	www.vigorpro.com
America	ACS	DT-ACS	myvigor.draytek.com	myvigor.draytek.com
America	AI-AV	DT-DT	85.236.48.68	www.vigorpro.com
America	AI-AV	DT-KL	85.236.48.68	www.vigorpro.com
Asia	AS	CTCH	resolver1.ctmail.com	www.vigorpro.com

Signature authentication/download message

It displays the message of signature authentication or download procedure.

Upgrade Manually

The buttons in this field are only available when you finished the registration and activation for new account and your router. If not, these buttons do not have any effect even if you click them.

Import – You can import a saved file to manually upgrade the signature. Click **Browse** to choose the right file with **.sig** file format. Next, click **Upgrade**.

System Maintenance >> Signature Upgrade

Signature Upgrade Manually [Signature Version : basic]

Upgrade Signature

Select a signature file.

Click Upgrade to upload the file.

Backup - You can backup current signature information with the filename vigorpro.sig.

Download Now!!! – This button will download newly update anti-intrusion and anti-virus from VigorPro website. While downloading the file, a progress bar will be shown as follows.

Signature Upgrade Setting

Signature Version : **basic**
 Signature Build Date : **Tue Aug 29 09:16:25.00 2006**

Setup download server auto-selected

Setup query server auto-selected

Signature download progress: **24%** 

Signature authentication/download message:

Upgrade Manually

After downloading is finished, the signature version will be upgraded and displayed on the web page.

Signature Upgrade Setting

Signature Version :	DT-KL_2_46.0.0
Signature Build Date :	Wed Jan 13 10:02:36.00 2010
Upgrade via interface :	WAN 1

Setup download server	auto-selected	find more
Setup query server	auto-selected	find more

Upgrade Automatically

Specify certain time for executing the upgrade automatically. Remember to check the **Scheduled Update** box to activate the time settings.

Every – It means the downloading procedure will be executed automatically whenever passing through the time (hours and minutes) that you set here.

Daily - It means the downloading procedure will be automatically executed every day at the time (hours and minutes) that you set here.

Weekly - It means the downloading procedure will be automatically executed at the time (hours and minutes) that you set here every week.

Upgrade Automatically			
<input checked="" type="checkbox"/> Scheduled Update			
<input checked="" type="radio"/> Every:	1 (hour)	00 (minutes after the hour)	
<input type="radio"/> Daily:	0 (hour)	00 (minute)	
<input type="radio"/> Weekly:	Sunday (day)	0 (hour)	00 (minute)
		<input type="button" value="OK"/>	<input type="button" value="Cancel"/>

Below shows an example with DT-KL signature used.

Defense Configuration >> Signature Upgrade

Signature Upgrade Setting

Signature Version : DT-KL_2_46.0.0
Signature Build Date : Wed Jan 13 10:02:36.00 2010
Upgrade via interface : WAN 1

Setup download server	auto-selected	find more
Setup query server	auto-selected	find more
Signature authentication/download message: <div style="border: 1px solid gray; height: 40px;"></div>		

Upgrade Manually

Upgrade Automatically

Scheduled Update

Every: 1 (hour) 00 (minutes after the hour)

Daily: 0 (hour) 00 (minute)

Weekly: Sunday (day) 0 (hour) 00 (minute)

3.7.7 Status

This field will show the status for the license, start date and expire date for Anti-Intrusion/Anti-Virus service. If your account or router is still not activated, the word **Not Activated** will be displayed here to inform you.

Defense Configuration >> Status

Anti-Intrusion/Anti-Virus License

[Status: **Not Activated**]

Signature Version : basic	Signature Build Date : Tue Aug 29 09:16:25.00 2006
Current Download Server : auto-selected	Current Query Server : auto-selected
Signature Authentication/Download Message for Anti-Intrusion/Anti-Virus: <div style="border: 1px solid gray; height: 20px;"></div>	

Anti-Spam License

[Status: **Not Activated**]

Authentication Message for Anti-Spam <div style="border: 1px solid gray; height: 20px;"></div>

Web-Filter License

[Status: **Not Activated**]

Authentication Message for Web-Filter License <div style="border: 1px solid gray; height: 20px;"></div>
--

Below is a sample page with valid license.

Defense Configuration >> Status

Anti-Intrusion/Anti-Virus License

[Status:DT-KL] [Start Date:2010-02-26 Expire Date:2010-03-29]

Signature Version : DT-KL_2_46.0.0 Signature Build Date : Wed Jan 13 10:02:36.00 2010
Current Download Server : auto-selected Current Query Server : auto-selected
Signature Authentication/Download Message for Anti-Intrusion/Anti-Virus:

Anti-Spam License

[Status:CTCH] [Start Date:2010-02-26 Expire Date:2010-03-29]

Authentication Message for Anti-Spam

Anti-Spam, Authenticate successful, 2010-03-24 15:37:15

Web-Filter License

[Status:CT-CF] [Start Date:2010-02-26 Expire Date:2010-03-29]

Authentication Message for Web-Filter License

WebFilter, Authenticate successful, 2010-03-25 03:30:07

3.8 Bandwidth Management

Below shows the menu items for Bandwidth Management.



3.8.1 Sessions Limit

A PC with private IP address can access to the Internet via NAT router. The router will generate the records of NAT sessions for such connection. The P2P (Peer to Peer) applications (e.g., BitTorrent) always need many sessions for procession and also they will occupy over resources which might result in important accesses impacted. To solve the problem, you can use limit session to limit the session procession for specified Hosts.

In the **Bandwidth Management** menu, click **Sessions Limit** to open the web page.

Sessions Limit

Enable
 Disable

Default Max Sessions:

Limitation List

Index	Start IP	End IP	Max Sessions

Specific Limitation

Start IP: End IP:

Maximum Sessions:

Time Schedule

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

Note: Action and Idle Timeout settings will be ignored.

To activate the function of limit session, simply click **Enable** and set the default session limit.

Enable	Click this button to activate the function of limit session.
Disable	Click this button to close the function of limit session.
Default session limit	Defines the default session number used for each computer in LAN.
Limitation List	Displays a list of specific limitations that you set on this web page.
Start IP	Defines the start IP address for limit session.
End IP	Defines the end IP address for limit session.
Maximum Number	Defines the available session number for each host in the specific range of IP addresses. If you do not set the session number in this field, the system will use the default session limit for the specific limitation you set for each index.
Add	Adds the specific session limitation onto the list above.
Edit	Allows you to edit the settings for the selected limitation.
Delete	Delete the selected settings existing on the limitation list.
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.

3.8.2 Bandwidth Limit

The downstream or upstream from FTP, HTTP or some P2P applications will occupy large of bandwidth and affect the applications for other programs. Please use Limit Bandwidth to make the bandwidth usage more efficient.

	limit and RX limit.
TX limit	Define the limitation for the speed of the upstream. If you do not set the limit in this field, the system will use the default speed for the specific limitation you set for each index.
RX limit	Define the limitation for the speed of the downstream. If you do not set the limit in this field, the system will use the default speed for the specific limitation you set for each index.
Add	Add the specific speed limitation onto the list above.
Edit	Allow you to edit the settings for the selected limitation.
Delete	Delete the selected settings existing on the limitation list.
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.

3.8.3 Quality of Service

Deploying QoS (Quality of Service) management to guarantee that all applications receive the service levels required and sufficient bandwidth to meet performance expectations is indeed one important aspect of modern enterprise network.

One reason for QoS is that numerous TCP-based applications tend to continually increase their transmission rate and consume all available bandwidth, which is called TCP slow start. If other applications are not protected by QoS, it will detract much from their performance in the overcrowded network. This is especially essential to those are low tolerant of loss, delay or jitter (delay variation).

Another reason is due to congestions at network intersections where speeds of interconnected circuits mismatch or traffic aggregates, packets will queue up and traffic can be throttled back to a lower speed. If there's no defined priority to specify which packets should be discarded (or in another term "dropped") from an overflowing queue, packets of sensitive applications mentioned above might be the ones to drop off. How this will affect application performance?

There are two components within Primary configuration of QoS deployment:

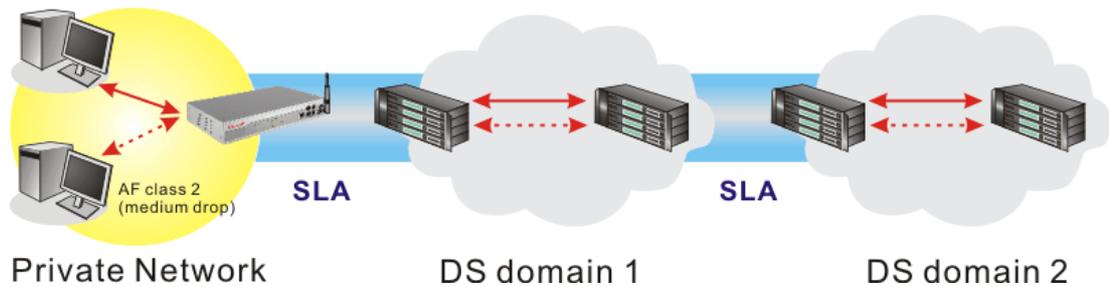
- **Classification:** Identifying low-latency or crucial applications and marking them for high-priority service level enforcement throughout the network.
- **Scheduling:** Based on classification of service level to assign packets to queues and associated service types

The basic QoS implementation in Vigor routers is to classify and schedule packets based on the service type information in the IP header. For instance, to ensure the connection with the headquarter, a teleworker may enforce an index of QoS Control to reserve bandwidth for HTTPS connection while using lots of application at the same time.

One more larger-scale implementation of QoS network is to apply DSCP (Differentiated Service Code Point) and IP Precedence disciplines at Layer 3. Compared with legacy IP Precedence that uses Type of Service (ToS) field in the IP header to define 8 service classes, DSCP is a successor creating 64 classes possible with backward IP Precedence compatibility. In a QoS-enabled network, or Differentiated Service (DiffServ or DS) framework, a DS domain owner should sign a Service License Agreement (SLA) with other DS domain owners to define the service level provided toward traffic from different domains. Then each

DS node in these domains will perform the priority treatment. This is called per-hop-behavior (PHB). The definition of PHB includes Expedited Forwarding (EF), Assured Forwarding (AF), and Best Effort (BE). AF defines the four classes of delivery (or forwarding) classes and three levels of drop precedence in each class.

Vigor routers as edge routers of DS domain shall check the marked DSCP value in the IP header of bypassing traffic, thus to allocate certain amount of resource execute appropriate policing, classification or scheduling. The core routers in the backbone will do the same checking before executing treatments in order to ensure service-level consistency throughout the whole QoS-enabled network.



However, each node may take different attitude toward packets with high priority marking since it may bind with the business deal of SLA among different DS domain owners. It's not easy to achieve deterministic and consistent high-priority QoS traffic throughout the whole network with merely Vigor router's effort.

In the **Bandwidth Management** menu, click **Quality of Service** to open the web page.

Bandwidth Management >> Quality of Service

General Setup

Index	Status	Bandwidth	Directon	Class 1	Class 2	Class 3	Others	UDP Bandwidth Control	
WAN1	Disable	10000Kbps/10000Kbps		25%	25%	25%	25%	Inactive	Setup
WAN2	Disable	10000Kbps/10000Kbps		25%	25%	25%	25%	Inactive	Setup

Class Rule

Index	Name	Rule	Service Type
Class 1		Edit	Edit
Class 2		Edit	
Class 3		Edit	

This page displays the QoS settings result of the WAN interface. Click the **Setup** link to access into next page for the general setup of WAN (1/2) interface. As to class rule, simply click the **Edit** link to access into next for configuration.

You can configure general setup for the WAN interface, edit the Class Rule, and edit the Service Type for the Class Rule for your request.

General Setup for WAN Interface

When you click **Setup**, you can configure the bandwidth ratio for QoS of the WAN interface. There are four queues allowed for QoS control. The first three (Class 1 to Class 3) class rules can be adjusted for your necessity. Yet, the last one is reserved for the packets which are not suitable for the user-defined class rules.

WAN1 General Setup

Enable the QoS Control OUT

WAN Inbound Bandwidth Kbps

WAN Outbound Bandwidth Kbps

Index	Class Name	Reserved Bandwidth Ratio
Class 1		<input type="text" value="25"/> %
Class 2		<input type="text" value="25"/> %
Class 3		<input type="text" value="25"/> %
	Others	<input type="text" value="25"/> %

Enable UDP Bandwidth Control Limited Bandwidth Ratio %

Outbound TCP ACK Prioritize

Enable the QoS Control

The factory default for this setting is checked.

Please also define which traffic the QoS Control settings will apply to.

IN- apply to incoming traffic only.

OUT- apply to outgoing traffic only.

BOTH- apply to both incoming and outgoing traffic.

Check this box and click **OK**, then click **Setup** link again.

You will see the **Online Statistics** link appearing on this page.

WAN Inbound Bandwidth

It allows you to set the connecting rate of data input for WAN. For example, if your ADSL supports 1M of downstream and 256K upstream, please set 1000kbps for this box. The default value is 10000kbps.

WAN Outbound Bandwidth

It allows you to set the connecting rate of data output for WAN. For example, if your ADSL supports 1M of downstream and 256K upstream, please set 256kbps for this box. The default value is 10000kbps.

Note: The rate of outbound/inbound must be smaller than the real bandwidth to ensure correct calculation of QoS. It is suggested to set the bandwidth value for inbound/outbound as 80% - 85% of physical network speed provided by ISP to maximize the QoS performance.

Reserved Bandwidth Ratio

It is reserved for the group index in the form of ratio of **reserved bandwidth to upstream speed** and **reserved bandwidth to downstream speed**.

Enable UDP Bandwidth Control

Check this and set the limited bandwidth ratio on the right field. This is a protection of TCP application traffic since UDP application traffic such as streaming video will exhaust lots of bandwidth.

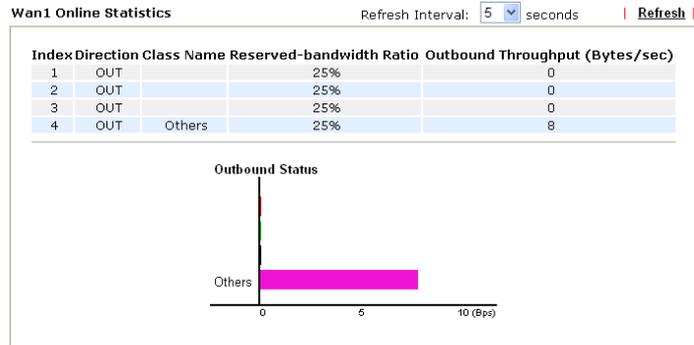
Outbound TCP ACK Prioritize

The difference in bandwidth between download and upload are great in ADSL2+ environment. For the download speed might be impacted by the uploading TCP ACK, you can check this box to push ACK of upload faster to speed the network traffic.

Limited_bandwidth Ratio The ratio typed here is reserved for limited bandwidth of UDP application.

Online Statistics Display an online statistics for quality of service for your reference. This link will be seen only if you click **OK** in WAN1/WAN2 General Setup web page and click Setup again (for WAN1/WAN2) on the **Bandwidth Management>>Quality of Service**.

Bandwidth Management >> Quality of Service



Edit the Class Rule for QoS

The first three (Class 1 to Class 3) class rules can be adjusted for your necessity. To add, edit or delete the class rule, please click the **Edit** link of that one.

Bandwidth Management >> Quality of Service

General Setup

Index	Status	Bandwidth	Directon	Class 1	Class 2	Class 3	Others	UDP Bandwidth Control	
WAN1	Disable	10000Kbps/10000Kbps		25%	25%	25%	25%	Inactive	Setup
WAN2	Disable	10000Kbps/10000Kbps		25%	25%	25%	25%	Inactive	Setup

Class Rule

Index	Name	Rule	Service Type
Class 1		Edit	Edit
Class 2		Edit	
Class 3		Edit	

After you click the **Edit** link, you will see the following page. Now you can define the name for that Class. In this case, “Test” is used as the name of Class Index #1.

Bandwidth Management >> Quality of Service

Class Index #1

Name

NO	Status	Local Address	Remote Address	DiffServ CodePoint	Service Type
1	Empty	-	-	-	-

For adding a new rule, click **Add** to open the following page.

Bandwidth Management >> Quality of Service

Rule Edit

ACT

Local Address

Remote Address

DiffServ CodePoint

Service Type

Note: Please choose/setup the **Service Type** first.

ACT

Check this box to invoke these settings.

Local Address

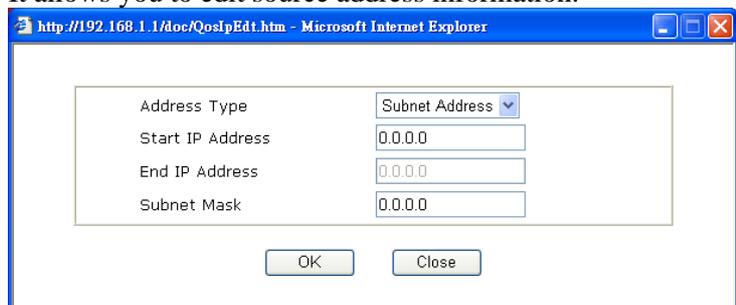
Click the **Edit** button to set the local IP address (on LAN) for the rule.

Remote Address

Click the **Edit** button to set the remote IP address (on LAN/WAN) for the rule.

Edit

It allows you to edit source address information.



Address Type – Determine the address type for the source address.

For **Single Address**, you have to fill in Start IP address.

For **Range Address**, you have to fill in Start IP address and End IP address.

For **Subnet Address**, you have to fill in Start IP address and Subnet Mask.

DiffServ CodePoint

All the packets of data will be divided with different levels and will be processed according to the level type by the system. Please assign one of the level of the data for processing with QoS control.

Service Type

It determines the service type of the data for processing with QoS control. It can also be edited. You can choose the predefined service type from the Service Type drop down list. Those types are predefined in factory. Simply choose the one that you want for using by current QoS.

By the way, you can set up to 20 rules for one Class. If you want to edit an existed rule, please select the radio button of that one and click **Edit** to open the rule edit page for modification.

Class Index # 1

Name

NO	Status	Local Address	Remote Address	DiffServ CodePoint	Service Type
1 <input type="radio"/>	Active	Any	Any	IP precedence 2	ANY
2 <input type="radio"/>	Active	192.168.1.66	Any	ANY	TFTP(UDP:69)

Edit the Service Type for Class Rule

To add a new service type, edit or delete an existed service type, please click the Edit link under Service Type field.

General Setup

Index	Status	Bandwidth	Directon	Class 1	Class 2	Class 3	Others	UDP Bandwidth Control	
WAN1	Disable	10000Kbps/10000Kbps		25%	25%	25%	25%	Inactive	Setup
WAN2	Disable	10000Kbps/10000Kbps		25%	25%	25%	25%	Inactive	Setup

Class Rule

Index	Name	Rule	Service Type
Class 1		Edit	Edit
Class 2		Edit	
Class 3		Edit	

After you click the **Edit** link, you will see the following page.

User Defined Service Type

NO	Name	Protocol	Port
1	Empty	-	-

For adding a new service type, click **Add** to open the following page.

Bandwidth Management >> Quality of Service

Service Type Edit

Service Name	<input type="text" value="Game"/>
Service Type	<input type="text" value="TCP"/> <input type="text" value="6"/>
Port Configuration	
Type	<input checked="" type="radio"/> Single <input type="radio"/> Range
Port Number	<input type="text" value="88"/> - <input type="text" value="0"/>

Service Name

Type in a new service for your request.

Service Type

Choose the type (TCP, UDP or TCP/UDP) for the new service.

Port Configuration

Click **Single** or **Range**. If you select Range, you have to type in the starting port number and the end porting number on the boxes below.

Port Number – Type in the starting port number and the end porting number here if you choose Range as the type.

By the way, you can set up to 40 service types. If you want to edit/delete an existed service type, please select the radio button of that one and click **Edit/Edit** for modification.

3.9 Applications

Below shows the menu items for Applications.



3.9.1 Dynamic DNS

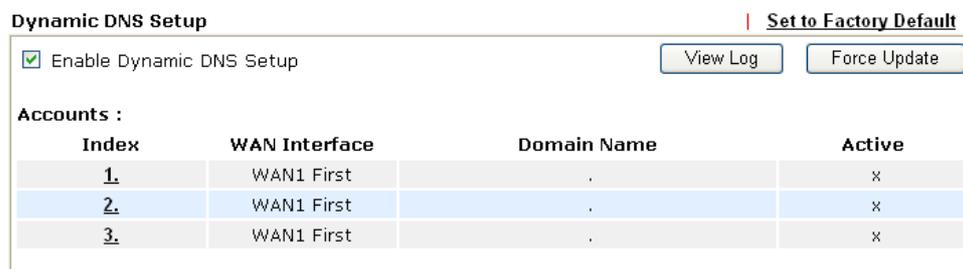
The ISP often provides you with a dynamic IP address when you connect to the Internet via your ISP. It means that the public IP address assigned to your router changes each time you access the Internet. The Dynamic DNS feature lets you assign a domain name to a dynamic WAN IP address. It allows the router 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



The screenshot shows the "Dynamic DNS Setup" configuration page. At the top right, there is a link "Set to Factory Default". Below the title, there is a checkbox labeled "Enable Dynamic DNS Setup" which is checked. To the right of the checkbox are two buttons: "View Log" and "Force Update". Below this is a section titled "Accounts:" containing a table with four columns: "Index", "WAN Interface", "Domain Name", and "Active".

Index	WAN Interface	Domain Name	Active
<u>1.</u>	WAN1 First	.	x
<u>2.</u>	WAN1 First	.	x
<u>3.</u>	WAN1 First	.	x

OK Clear All

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).

WAN Interface Display current WAN interface used for accessing Internet.

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

WAN Interface:

Service Provider:

Service Type:

Domain Name: .

Login Name: (max. 23 characters)

Password: (max. 23 characters)

Wildcards

Backup MX

Mail Extender:

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).
WAN Interface	Select the WAN interface order to apply settings here.
Service Provider	Select the service provider for the DDNS account.
Service Type	Select a service type (Dynamic, Custom, Static). If you choose Custom, you can modify the domain that is chosen in the Domain Name field.
Domain Name	Type in the domain name that you applied previously. Use the drop down list to choose the desired domain.
Login Name	Type in the login name that you set for applying domain.
Password	Type in the password that you set for applying domain.
Wildcards	It is not supported for all Dynamic DNS providers. Please get more detailed information from its website.
Backup MX	It is not supported for all Dynamic DNS providers. Please get more detailed information from its website.
Mail Extender	It allows you to control the delivery of mails for a given <i>domain</i> or <i>subdomain</i> . The entry you type here can be specified as a secondary mail exchanger. It means that delivery will be attempted to your host first, and then to the host you specify here if that fails.

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.

3.9.2 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 and Date** menu, press **Inquire Time** button to set the Vigor router's clock to current time of your PC. The clock will reset once if you power down or reset the 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: | [Set to Factory Default](#) |

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

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

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

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

Status Display if this schedule setting is active or inactive.

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

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

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).



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.

3.9.3 RADIUS/LDAP

Remote Authentication Dial-In User Service (RADIUS) is a security authentication client/server protocol that supports authentication, authorization and accounting, which is widely used by Internet service providers. It is the most common method of authenticating and authorizing dial-up and tunneled network users.

The built-in RADIUS client feature enables the router to assist the remote dial-in user or a wireless station and the RADIUS server in performing mutual authentication. It enables centralized remote access authentication for network management.

Lightweight Directory Access Protocol (LDAP) is a communication protocol for using in TCP/IP network. It defines the methods to access distributing directory server by clients, work on directory and share the information in the directory by clients. The LDAP standard is established by the work team of Internet Engineering Task Force (IETF).

As the name described, LDAP is designed as an effect way to access directory service without the complexity of other directory service protocols. For LDAP is defined to perform, inquire and modify the information within the directory, and acquire the data in the directory securely, therefore users can apply LDAP to search or list the directory object, inquire or manage the active directory.

Applications >> RADIUS / LDAP

RADIUS / LDAP Setup

RADIUS Setup	
<input type="checkbox"/> Enable	
Server IP Address	<input type="text"/>
Destination Port	<input type="text" value="1812"/>
Shared Secret	<input type="text"/>
Confirm Shared Secret	<input type="text"/>
LDAP Setup	
<input type="checkbox"/> Enable	
Server IP Address	<input type="text"/>
Destination Port	<input type="text" value="389"/>
Common Name Identifier	<input type="text"/>
Distinguished Name	<input type="text"/>

OK Clear Cancel

- | | |
|--------------------------|--|
| Enable | Check to enable RADIUS client feature |
| Server IP Address | Enter the IP address of RADIUS server. |
| Destination Port | The UDP port number that the RADIUS server is using. The default value is 1812, based on RFC 2138. |

Shared Secret	The RADIUS server and client share a secret that is used to authenticate the messages sent between them. Both sides must be configured to use the same shared secret.
Confirm Shared Secret	Re-type the Shared Secret for confirmation.
Common Name Identifier	Type or edit the common name identifier for the LDAP server. The common name identifier for most LDAP server is cn.
Distinguished Name	Type or edit the distinguished name used to look up entries on the LDAP server.

3.9.4 UPnP

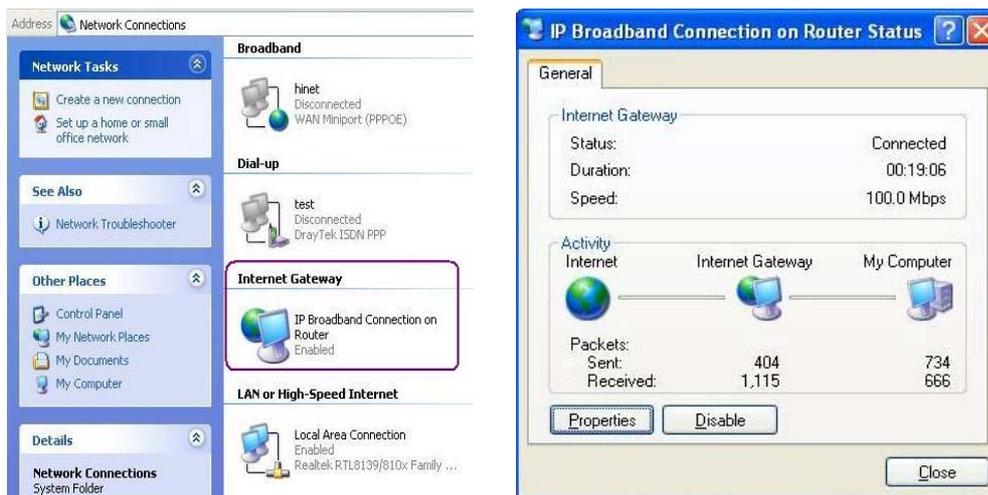
The **UPnP** (Universal Plug and Play) protocol is supported to bring to network connected devices the ease of installation and configuration which is already available for directly connected PC peripherals with the existing Windows 'Plug and Play' system. For NAT routers, the major feature of UPnP on 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

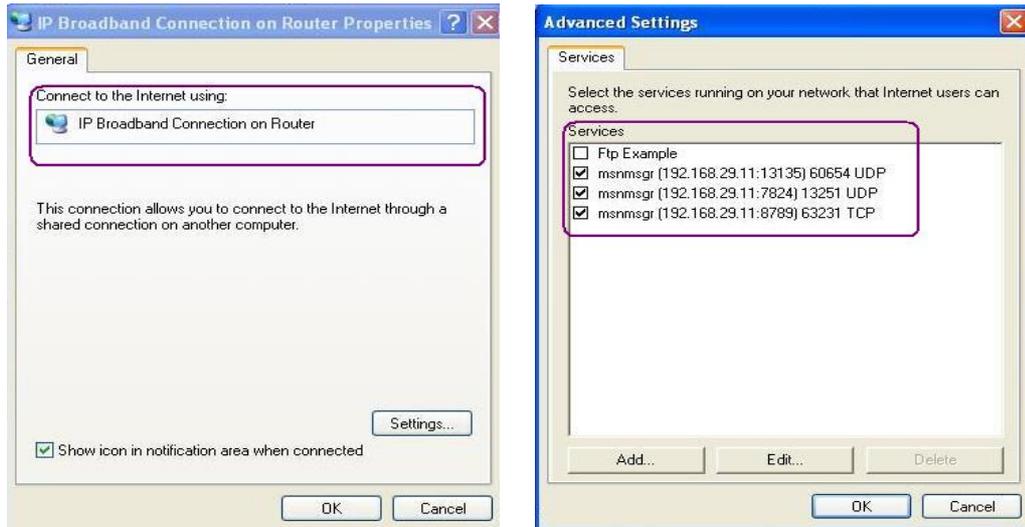


Enable UPnP Service Accordingly, you can enable either the **Connection Control Service** or **Connection Status Service**.

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.

3.9.5 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

IGMP

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

OK Cancel

| Refresh |

Working Multicast Groups					
Index	Group ID	P1	P2	P3	P4

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

Enable IGMP Snooping Check this box to enable this function. The application of multicast will be executed for the clients in LAN.

Group ID This field displays the ID port for the multicast group. The available range for IGMP starts from 224.0.0.0 to 239.255.255.254.

P1 to P4 It indicates the LAN port used for the multicast group.

Refresh Click this link to renew the working multicast group status.

If you check Enable IGMP Proxy, you will get the following page. All the multicast groups will be listed and all the LAN ports (P1 to P4) are available for use.

Applications >> IGMP

IGMP

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

OK Cancel

| Refresh |

Working Multicast Groups					
Index	Group ID	P1	P2	P3	P4
1.	224.0.0.9	v	v	v	v

3.9.6 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

Note: Wake on LAN integrates with **Bind IP to MAC** function, only binded PCs can wake up through IP.

Wake by:

IP Address:

MAC Address: : : : : :

Result

Wake by

Two types provide for you to wake up the binded IP. If you choose Wake by MAC Address, you have to type the correct MAC address of the host in MAC Address boxes. If you choose Wake by IP Address, you have to choose the correct IP address.

Wake by:

IP Address

The IP addresses that have been configured in LAN>>Bind IP to MAC will be shown in this drop down list. Choose the IP address from the drop down list that you want to wake up.

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.

Application >> Wake on LAN

Wake on LAN

Note: Wake on LAN integrates with **Bind IP to MAC** function, only binded PCs can wake up through IP.

Wake by:

IP Address:

MAC Address: : : : : :

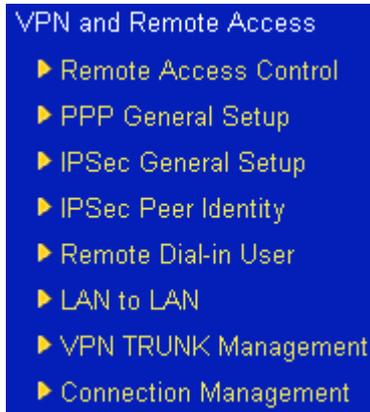
Result

Send command to client done.

3.10 VPN and Remote Access

A Virtual Private Network (VPN) is the extension of a private network that encompasses links across shared or public networks like the Internet. In short, by VPN technology, you can send data between two computers across a shared or public network in a manner that emulates the properties of a point-to-point private link.

Below shows the menu items for VPN and Remote Access.



3.10.1 Remote Access Control

Enable the necessary VPN service as you need. If you intend to run a VPN server inside your LAN, you should disable the VPN service of Vigor Router to allow VPN tunnel pass through, as well as the appropriate NAT settings, such as DMZ or open port.

VPN and Remote Access >> Remote Access Control Setup

Remote Access Control Setup

<input checked="" type="checkbox"/>	Enable PPTP VPN Service
<input checked="" type="checkbox"/>	Enable IPSec VPN Service
<input checked="" type="checkbox"/>	Enable L2TP VPN Service
<input checked="" type="checkbox"/>	Enable SSL VPN Service
<input type="checkbox"/>	Enable ISDN Dial-In

Note: If you intend running a VPN server inside your LAN, you should uncheck the appropriate protocol above to allow pass-through, as well as the appropriate NAT settings.

OK Clear Cancel

The Vigor router will not accept the ISDN dial-in connection if the box of **Enable ISDN Dial-in** is not checked.

3.10.2 PPP General Setup

This submenu only applies to PPP-related VPN connections, such as PPTP, L2TP, L2TP over IPsec.

VPN and Remote Access >> PPP General Setup

PPP General Setup

PPP/MP Protocol		IP Address Assignment for Dial-In Users (When DHCP Disable set)	
Dial-In PPP Authentication	PAP or CHAP	Assigned IP range	192.168.1.200
Dial-In PPP Encryption (MPPE)	Optional MPPE		
Mutual Authentication (PAP)	<input type="radio"/> Yes <input checked="" type="radio"/> No		
Username	<input type="text"/>		
Password	<input type="text"/>		

OK

Dial-In PPP Authentication PAP Only

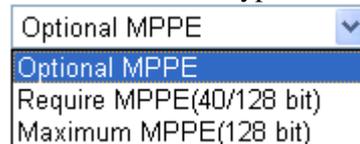
Select this option to force the router to authenticate dial-in users with the PAP protocol.

PAP or CHAP

Selecting this option means the router will attempt to authenticate dial-in users with the CHAP protocol first. If the dial-in user does not support this protocol, it will fall back to use the PAP protocol for authentication.

Dial-In PPP Encryption (MPPE Optional MPPE)

This option represents that the MPPE encryption method will be optionally employed in the router for the remote dial-in user. If the remote dial-in user does not support the MPPE encryption algorithm, the router will transmit “no MPPE encrypted packets”. Otherwise, the MPPE encryption scheme will be used to encrypt the data.



Require MPPE (40/128bits) - Selecting this option will force the router to encrypt packets by using the MPPE encryption algorithm. In addition, the remote dial-in user will use 40-bit to perform encryption prior to using 128-bit for encryption. In other words, if 128-bit MPPE encryption method is not available, then 40-bit encryption scheme will be applied to encrypt the data.

Maximum MPPE - This option indicates that the router will use the MPPE encryption scheme with maximum bits (128-bit) to encrypt the data.

Mutual Authentication (PAP)

The Mutual Authentication function is mainly used to communicate with other routers or clients who need bi-directional authentication in order to provide stronger security, for example, Cisco routers. So you should enable this function when your peer router requires mutual authentication. You should further specify the **User Name** and **Password** of the mutual authentication peer.

Assigned IP Address

Enter an IP address for the dial-in PPP connection. You

should choose an IP address from the local private network. For example, if the local private network is 192.168.1.0/255.255.255.0, you could choose 192.168.1.200 as the Start IP Address. But, you have to notice that the first two IP addresses of 192.168.1.200 and 192.168.1.201 are reserved for ISDN remote dial-in user.

3.10.3 IPSec General Setup

In **IPSec General Setup**, there are two major parts of configuration.

There are two phases of IPSec.

- Phase 1: negotiation of IKE parameters including encryption, hash, Diffie-Hellman parameter values, and lifetime to protect the following IKE exchange, authentication of both peers using either a Pre-Shared Key or Digital Signature (x.509). The peer that starts the negotiation proposes all its policies to the remote peer and then remote peer tries to find a highest-priority match with its policies. Eventually to set up a secure tunnel for IKE Phase 2.
- Phase 2: negotiation IPSec security methods including Authentication Header (AH) or Encapsulating Security Payload (ESP) for the following IKE exchange and mutual examination of the secure tunnel establishment.

There are two encapsulation methods used in IPSec, **Transport** and **Tunnel**. The **Transport** mode will add the AH/ESP payload and use original IP header to encapsulate the data payload only. It can just apply to local packet, e.g., L2TP over IPSec. The **Tunnel** mode will not only add the AH/ESP payload but also use a new IP header (Tunneled IP header) to encapsulate the whole original IP packet.

Authentication Header (AH) provides data authentication and integrity for IP packets passed between VPN peers. This is achieved by a keyed one-way hash function to the packet to create a message digest. This digest will be put in the AH and transmitted along with packets. On the receiving side, the peer will perform the same one-way hash on the packet and compare the value with the one in the AH it receives.

Encapsulating Security Payload (ESP) is a security protocol that provides data confidentiality and protection with optional authentication and replay detection service.

VPN and Remote Access >> IPSec General Setup

VPN IKE/IPSec General Setup

Dial-in Set up for Remote Dial-in users and Dynamic IP Client (LAN to LAN).

IKE Authentication Method

Certificate for Dial-in None ▾

Pre-Shared Key

Pre-Shared Key

Confirm Pre-Shared Key

IPSec Security Method

Medium (AH)
Data will be authentic, but will not be encrypted.

High (ESP) DES 3DES AES
Data will be encrypted and authentic.

OK

Cancel

IKE Authentication Method

This usually applies to those are remote dial-in user or node (LAN-to-LAN) which uses dynamic IP address and IPSec-related VPN connections such as L2TP over IPSec and IPSec tunnel.

Certificate for Dial-in – Choose the local certificate that generated or imported on **Certificate Management>>Local Certificate**.

Pre-Shared Key -Currently only support Pre-Shared Key authentication.

Pre-Shared Key- Specify a key for IKE authentication.

Confirm Pre-Shared Key-Confirm the pre-shared key.

IPSec Security Method

Medium - Authentication Header (AH) means data will be authenticated, but not be encrypted. By default, this option is active.

High - Encapsulating Security Payload (ESP) means payload (data) will be encrypted and authenticated. You may select encryption algorithm from Data Encryption Standard (DES), Triple DES (3DES), and AES.

3.10.4 IPSec Peer Identity

To use digital certificate for peer authentication in either LAN-to-LAN connection or Remote User Dial-In connection, here you may edit a table of peer certificate for selection. As shown below, the router provides **200** entries of digital certificates for peer dial-in users.

VPN and Remote Access >> IPSec Peer Identity

X509 Peer ID Accounts: [Set to Factory Default](#)

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

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

Set to Factory Default

Click it to clear all indexes.

Index

Click the number below Index to access into the setting page of IPSec Peer Identity.

Name

Display the profile name of that index.

Click each index to edit one peer digital certificate. There are three security levels of digital signature authentication: Fill each necessary field to authenticate the remote peer. The following explanation will guide you to fill all the necessary fields.

VPN and Remote Access >> IPSec Peer Identity

Profile Index : 1

Profile Name

Enable this account

Accept Any Peer ID

Accept Subject Alternative Name

Type

IP

Accept Subject Name

Country (C)

State (ST)

Location (L)

Organization (O)

Organization Unit (OU)

Common Name (CN)

Email (E)

Profile Name

Type in a name in this file.

Accept Any Peer ID

Click to accept any peer regardless of its identity.

Accept Subject Alternative Name

Click to check one specific field of digital signature to accept the peer with matching value. The field can be **IP Address**, **Domain**, or **E-mail** address. The box under the Type will appear according to the type you select and ask you to fill in corresponding setting.

Accept Subject Name

Click to check the specific fields of digital signature to accept the peer with matching value. The field includes **Country (C)**, **State (ST)**, **Location (L)**, **Organization (O)**, **Organization Unit (OU)**, **Common Name (CN)**, and **Email (E)**.

3.10.5 Remote Dial-in User

You can manage remote access by maintaining a table of remote user profile, so that users can be authenticated to dial-in via ISDN or build the VPN connection. You may set parameters including specified connection peer ID, connection type (VPN connection - including PPTP, IPsec Tunnel, and L2TP by itself or over IPsec) and corresponding security methods, etc.

The router provides **200** access accounts for dial-in users. Besides, you can extend the user accounts to the RADIUS server through the built-in RADIUS client function. The following figure shows the summary table.

VPN and Remote Access >> Remote Dial-in User

Remote Access User Accounts:			Set to Factory Default		
Index	User	Status	Index	User	Status
1.	???	X	17.	???	X
2.	???	X	18.	???	X
3.	???	X	19.	???	X
4.	???	X	20.	???	X
5.	???	X	21.	???	X
6.	???	X	22.	???	X
7.	???	X	23.	???	X
8.	???	X	24.	???	X
9.	???	X	25.	???	X
10.	???	X	26.	???	X
11.	???	X	27.	???	X
12.	???	X	28.	???	X
13.	???	X	29.	???	X
14.	???	X	30.	???	X
15.	???	X	31.	???	X
16.	???	X	32.	???	X

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

Set to Factory Default

Click to clear all indexes.

Index

Click the number below Index to access into the setting page of Remote Dial-in User.

User

Display the username for the specific dial-in user of the LAN-to-LAN profile. The symbol ??? represents that the profile is empty.

Status

Display the access state of the specific dial-in user. The symbol V and X represent the specific dial-in user to be active and inactive, respectively.

Click each index to edit one remote user profile. **Each Dial-In Type requires you to fill the different corresponding fields on the right.** If the fields gray out, it means you may leave it untouched. The following explanation will guide you to fill all the necessary fields.

Index No. 1

User account and Authentication <input type="checkbox"/> Enable this account Idle Timeout <input type="text" value="300"/> second(s)	
Allowed Dial-In Type <input checked="" type="checkbox"/> ISDN <input checked="" type="checkbox"/> PPTP <input checked="" type="checkbox"/> IPsec Tunnel <input checked="" type="checkbox"/> L2TP with IPsec Policy <input type="text" value="None"/> <input checked="" type="checkbox"/> SSL Tunnel <input type="checkbox"/> Specify Remote Node Remote Client IP or Peer ISDN Number <input type="text"/> or Peer ID <input type="text"/> Netbios Naming Packet <input checked="" type="radio"/> Pass <input type="radio"/> Block	
SSL VPN Set SSL Web Proxy Set SSL Application	
Username <input type="text" value="???"/> Password <input type="text"/> Authentication Type <input type="text" value="Local User Database"/> <input type="checkbox"/> Enable Mobile One-Time Passwords(mOTP) PIN Code <input type="text"/> Secret <input type="text"/>	IKE Authentication Method <input checked="" type="checkbox"/> Pre-Shared Key IKE Pre-Shared Key <input type="text"/> <input type="checkbox"/> Digital Signature (X.509) <input type="text" value="None"/>
IPsec Security Method <input checked="" type="checkbox"/> Medium (AH) <input type="checkbox"/> High (ESP) <input checked="" type="checkbox"/> DES <input checked="" type="checkbox"/> 3DES <input checked="" type="checkbox"/> AES Local ID <input type="text"/> (optional)	
Callback Function <input type="checkbox"/> Check to enable Callback function <input type="checkbox"/> Specify the callback number Callback Number <input type="text"/> <input checked="" type="checkbox"/> Check to enable Callback Budget Control Callback Budget <input type="text" value="30"/> minute(s)	

OK Clear Cancel

Enable this account

Check the box to enable this function.

ISDN

Idle Timeout- If the dial-in user is idle over the limitation of the timer, the router will drop this connection. By default, the Idle Timeout is set to 300 seconds.

Allow the remote ISDN dial-in connection. You can further set up Callback function below. You should set the User Name and Password of remote dial-in user below. This feature is for *i* model only.

PPTP

Allow the remote dial-in user to make a PPTP VPN connection through the Internet. You should set the User Name and Password of remote dial-in user below.

IPsec Tunnel

Allow the remote dial-in user to make an IPsec VPN connection through Internet.

L2TP

Allow the remote dial-in user to make a L2TP VPN connection through the Internet. You can select to use L2TP alone or with IPsec. Select from below:

None - Do not apply the IPsec policy. Accordingly, the VPN connection employed the L2TP without IPsec policy can be viewed as one pure L2TP connection.

Nice to Have - Apply the IPSec policy first, if it is applicable during negotiation. Otherwise, the dial-in VPN connection becomes one pure L2TP connection.

Must -Specify the IPSec policy to be definitely applied on the L2TP connection.

SSL Tunnel

It allows the remote dial-in user to make an SSL VPN Tunnel connection through Internet, suitable for the application through network accessing (e.g., PPTP/L2TP/IPSec)

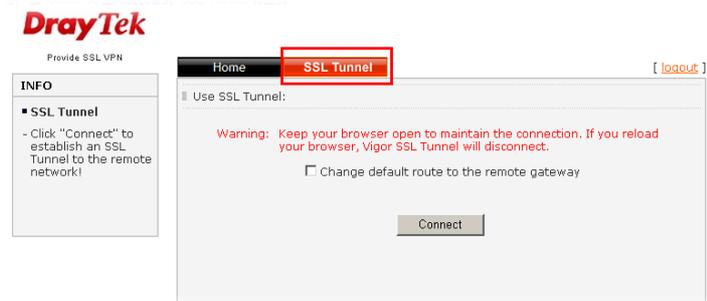
If you check this box, the function of SSL Tunnel for this account will be activated immediately.

VPN and Remote Access >> Remote Dial-in User

Index No. 1

User account and Authentication <input type="checkbox"/> Enable this account Idle Timeout: <input type="text" value="300"/> second(s)		Username: <input type="text" value="???"/> Password: <input type="password"/>
Allowed Dial-In Type <input checked="" type="checkbox"/> ISDN <input checked="" type="checkbox"/> PPTP <input checked="" type="checkbox"/> IPSec Tunnel <input checked="" type="checkbox"/> L2TP with IPSec Policy: <input type="text" value="None"/> <input checked="" type="checkbox"/> SSL Tunnel <input type="checkbox"/> Specify Remote Node Remote Client IP or Peer ISDN Number: <input type="text"/> or Peer ID: <input type="text"/>		IKE Authentication Method <input checked="" type="checkbox"/> Pre-Shared Key IKE Pre-Shared Key: <input type="text"/> <input type="checkbox"/> Digital Signature (X.509) <input type="text" value="None"/>
		IPSec Security Method <input checked="" type="checkbox"/> Medium (AH) <input checked="" type="checkbox"/> High (ESP) <input checked="" type="checkbox"/> DES <input checked="" type="checkbox"/> 3DES <input checked="" type="checkbox"/> AES Local ID: <input type="text"/> (optional)

To check if SSL Tunnel is activated or not, please open Draytek SSL VPN portal interface. From the web page, you will see the message to indicate the SSL Tunnel is activated.



Specify Remote Node

Check the checkbox-You can specify the IP address of the remote dial-in user, ISDN number or peer ID (used in IKE aggressive mode).

Uncheck the checkbox-This means the connection type you select above will apply the authentication methods and security methods in the **general settings**.

Netbios Naming Packet

Pass – click it to have an inquiry for data transmission between the hosts located on both sides of VPN Tunnel while connecting.

Block – When there is conflict occurred between the hosts on both sides of VPN Tunnel in connecting, such function can block data transmission of Netbios Naming Packet inside the tunnel.

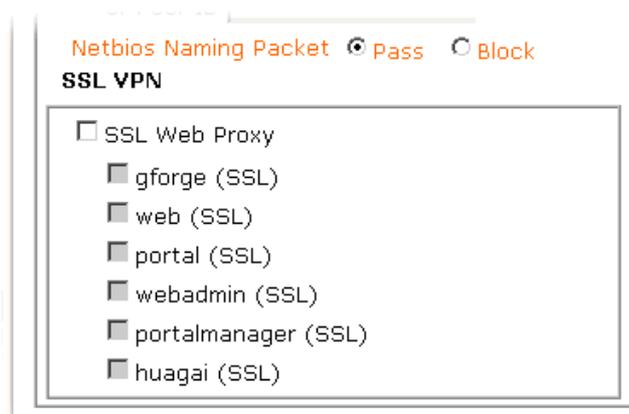
SSL VPN

Set SSL Web Proxy - It allows the remote dial-in user to access internal web over SSL VPN, suitable for the application through web only (e.g., HTTP). Click **SSL VPN>> SSL Web Proxy** to set profiles.

If you haven't set any SSL VPN web proxy profiles, you will see a link here. Click this link to access into the configuration page of SSL VPN.

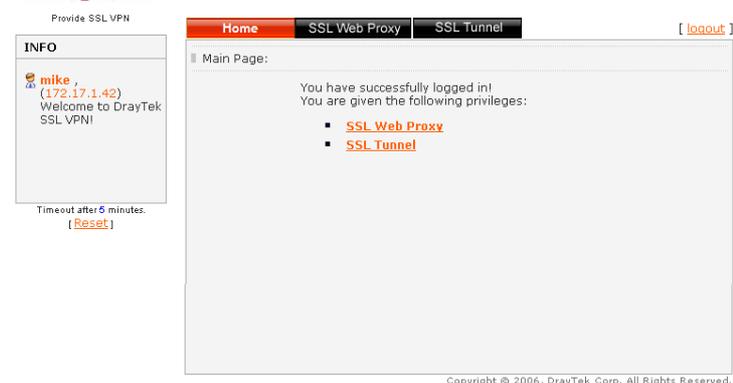
Note: SSL VPN can be applied in browser (e.g., IE) which supports ActivateX only.

If you have set several profiles beforehand, you can check SSL Web Proxy and choose the one(s) you need as SSL VPN.



To check if SSL Web Proxy is activated or not, please open Draytek SSL VPN portal interface. From the web page, you will see the message to indicate that you have the privilege for the SSL Web Proxy.

DrayTek



Set SSL Application - If you've already set up SSL application profiles, you'll see some check boxes here. Please check the profiles that you want to enable for this account. If you haven't set any SSL application yet, you'll see a hyperlink here. Click the link, the system will lead you to access **SSL VPN > SSL Application** for advanced configuration.

User Name

This field is applicable when you select ISDN, PPTP or L2TP with or without IPSec policy above.

Password

This field is applicable when you select ISDN, PPTP or L2TP

with or without IPSec policy above.

IKE Authentication Method

This group of fields is applicable for IPSec Tunnels and L2TP with IPSec Policy when you specify the IP address of the remote node. The only exception is Digital Signature (X.509) can be set when you select IPSec tunnel either with or without specify the IP address of the remote node.

Pre-Shared Key - Check the box of Pre-Shared Key to invoke this function and type in the required characters (1-63) as the pre-shared key.

Digital Signature (X.509) – Check the box of Digital Signature to invoke this function and Select one predefined Profiles set in the **VPN and Remote Access >>IPSec Peer Identity**.

IPSec Security Method

This group of fields is a must for IPSec Tunnels and L2TP with IPSec Policy when you specify the remote node. Check the Medium, DES, 3DES or AES box as the security method. **Medium - Authentication Header (AH)** means data will be authenticated, but not be encrypted. By default, this option is invoked. You can uncheck it to disable it.

High-Encapsulating Security Payload (ESP) means payload (data) will be encrypted and authenticated. You may select encryption algorithm from Data Encryption Standard (DES), Triple DES (3DES), and AES.

Local ID - Specify a local ID to be used for Dial-in setting in the LAN-to-LAN Profile setup. This item is optional and can be used only in IKE aggressive mode.

Callback Function

The callback function provides a callback service only for the ISDN dial-in user (for *i* model only). The remote user will be charged the connection fee by the telecom.

Check to enable Callback function-Enables the callback function.

Specify the callback number-The option is for extra security. Once enabled, the router will ONLY call back to the specified Callback Number.

Check to enable callback budget control-By default, the callback function has a time restriction. Once the callback budget has been exhausted, the callback mechanism will be disabled automatically.

Callback Budget (Unit: minutes)- Specify the time budget for the dial-in user. The budget will be decreased automatically per callback connection.

3.10.6 LAN to LAN

Here you can manage LAN-to-LAN connections by maintaining a table of connection profiles. You may set parameters including specified connection direction (dial-in or dial-out), connection peer ID, connection type (VPN connection - including PPTP, IPsec Tunnel, and L2TP by itself or over IPsec) and corresponding security methods, etc.

The router provides up to **200** profiles, which also means supporting **200** VPN tunnels simultaneously. The following figure shows the summary table.

VPN and Remote Access >> LAN to LAN

LAN-to-LAN Profiles: | [Set to Factory Default](#) |

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

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

Set to Factory Default Click to clear all indexes.

Name Indicate the name of the LAN-to-LAN profile. The symbol ??? represents that the profile is empty.

Status Indicate the status of individual profiles. The symbol V and X represent the profile to be active and inactive, respectively.

Click each index to edit each profile and you will get the following page. Each LAN-to-LAN profile includes 4 subgroups. If the fields gray out, it means you may leave it untouched. The following explanations will guide you to fill all the necessary fields.

For the web page is too long, we divide the page into several sections for explanation.

Profile Index : 1

1. Common Settings

Profile Name <input type="text" value="???"/> <input type="checkbox"/> Enable this profile	Call Direction <input checked="" type="radio"/> Both <input type="radio"/> Dial-Out <input type="radio"/> Dial-In <input type="checkbox"/> Always on Idle Timeout <input type="text" value="300"/> second(s) <input type="checkbox"/> Enable PING to keep alive PING to the IP <input type="text"/>
VPN Dial-Out Through: <input type="text" value="WAN1 First"/> Netbios Naming Packet <input checked="" type="radio"/> Pass <input type="radio"/> Block	

2. Dial-Out Settings

<p>Type of Server I am calling</p> <input type="radio"/> ISDN <input type="radio"/> PPTP <input type="radio"/> IPsec Tunnel <input checked="" type="radio"/> L2TP with IPsec Policy <input type="text" value="None"/>	Link Type <input type="text" value="64k bps"/> Username <input type="text" value="???"/> Password <input type="text"/> PPP Authentication <input type="text" value="PAP/CHAP"/> VJ Compression <input checked="" type="radio"/> On <input type="radio"/> Off
Dial Number for ISDN or Server IP/Host Name for VPN. (such as 5551234, draytek.com or 123.45.67.89) <input type="text"/>	<p>IKE Authentication Method</p> <input checked="" type="radio"/> Pre-Shared Key <input type="text" value="IKE Pre-Shared Key"/> <input type="radio"/> Digital Signature(X.509) Peer ID <input type="text" value="None"/> Local ID <input checked="" type="radio"/> Alternative Subject Name First <input type="radio"/> Subject Name First Local Certificate <input type="text" value="None"/>
	<p>IPsec Security Method</p> <input checked="" type="radio"/> Medium(AH) <input type="radio"/> High(ESP) <input type="text" value="DES without Authentication"/> <input type="button" value="Advanced"/>
	Index(1-15) in Schedule Setup: <input type="text"/> , <input type="text"/> , <input type="text"/> , <input type="text"/>
	<p>Callback Function (CBCP)</p> <input type="checkbox"/> Require Remote to Callback <input type="checkbox"/> Provide ISDN Number to Remote

Profile Name Specify a name for the profile of the LAN-to-LAN connection.

Enable this profile Check here to activate this profile.

VPN Connection Through Use the drop down menu to choose a proper WAN interface for this profile. This setting is useful for dial-out only.

VPN Connection Through:

WAN1 First

WAN1 Only

WAN2 First

WAN2 Only

WAN1 First - While connecting, the router will use WAN1

as the first channel for VPN connection. If WAN1 fails, the router will use another WAN interface instead.

WAN1 Only - While connecting, the router will use WAN1 as the only channel for VPN connection.

WAN2 First - While connecting, the router will use WAN2 as the first channel for VPN connection. If WAN2 fails, the router will use another WAN interface instead.

WAN2 Only - While connecting, the router will use WAN2 as the only channel for VPN connection.

Netbios Naming Packet

Pass – click it to have an inquiry for data transmission between the hosts located on both sides of VPN Tunnel while connecting.

Block – When there is conflict occurred between the hosts on both sides of VPN Tunnel in connecting, such function can block data transmission of Netbios Naming Packet inside the tunnel.

Call Direction

Specify the allowed call direction of this LAN-to-LAN profile.

Both:-initiator/responder

Dial-Out- initiator only

Dial-In- responder only.

Always On or Idle Timeout

Always On-Check to enable router always keep VPN connection.

Idle Timeout: The default value is 300 seconds. If the connection has been idled over the value, the router will drop the connection.

Enable PING to keep alive

This function is to help the router to determine the status of IPSec VPN connection, especially useful in the case of abnormal VPN IPSec tunnel disruption. For details, please refer to the note below. Check to enable the transmission of PING packets to a specified IP address.

PING to the IP

Enter the IP address of the remote host that located at the other-end of the VPN tunnel.

Enable PING to Keep Alive is used to handle abnormal IPSec VPN connection disruption. It will help to provide the state of a VPN connection for router's judgment of redial.

Normally, if any one of VPN peers wants to disconnect the connection, it should follow a serial of packet exchange procedure to inform each other. However, if the remote peer disconnect without notice, Vigor router will by no where to know this situation. To resolve this dilemma, by continuously sending PING packets to the remote host, the Vigor router can know the true existence of this VPN connection and react accordingly. This is independent of DPD (dead peer detection).

ISDN

Build ISDN LAN-to-LAN connection to remote network.

You should set up Link Type and identity like User Name and Password for the authentication of remote server. You can further set up Callback (CBCP) function below. This feature is useful for *i* model only.

PPTP

Build a PPTP VPN connection to the server through the Internet. You should set the identity like User Name and Password below for the authentication of remote server.

IPSec Tunnel

Build an IPSec VPN connection to the server through Internet.

L2TP with IPSec Policy

Build a L2TP VPN connection through the Internet. You can select to use L2TP alone or with IPSec. Select from below:

None: Do not apply the IPSec policy. Accordingly, the VPN connection employed the L2TP without IPSec policy can be viewed as one pure L2TP connection.

Nice to Have: Apply the IPSec policy first, if it is applicable during negotiation. Otherwise, the dial-out VPN connection becomes one pure L2TP connection.

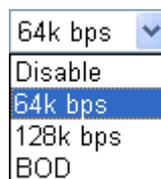
Must: Specify the IPSec policy to be definitely applied on the L2TP connection.

Dial Number for ISDN or Server IP/Host Name for.

You can specify the IP address of the remote dial-out user.

Link Type

Link Type – There are three link types provided here for different purpose. **Disable** disables the ISDN connection function. **64Kbps** allows you to use one ISDN channel for Internet access. **128Kbps** allows you to use both ISDN B channels for Internet access. **BOD** stands for bandwidth-on-demand. The router will use only one B channel in low traffic situations. Once the single B channel bandwidth is fully used, the other B channel will be activated automatically through the dialup. For more detailed BOD parameter settings, please refer to the section of **Call Control**.



User Name

This field is applicable when you select ISDN, PPTP or L2TP with or without IPSec policy above.

Password

This field is applicable when you select ISDN, PPTP or L2TP with or without IPSec policy above.

PPP Authentication

This field is applicable when you select ISDN, PPTP or L2TP with or without IPSec policy above. PAP/CHAP is the most common selection due to wild compatibility.

VJ compression

This field is applicable when you select ISDN, PPTP or L2TP with or without IPSec policy above. VJ Compression is used for TCP/IP protocol header compression. Normally

IKE Authentication Method

set to **Yes** to improve bandwidth utilization.

This group of fields is applicable for IPSec Tunnels and L2TP with IPSec Policy.

Pre-Shared Key-Input 1-63 characters as pre-shared key.

Digital Signature (X.509) – This setting will be available when IPSec Tunnel is selected. Click this radio button to invoke this function and select one predefined profile in the Peer ID (set from **VPN and Remote Access>>IPSec Peer Identity**).

Peer ID – Display the IPSec Peer Identity profiles. Use the drop down menu to choose any one desired.

Local ID – There are two selections offered here. Choose **Alternative Subject Name First** or choose **Subject Name First** based on the local certificate selected below.

Local Certificate - When the router (served as the client) executes LAN to LAN dial out with IPSec mode, it will transfer the certificate to the server based on the setting selected here. Please use the drop down list to choose one of the certificates configured in **Certificate Management>>Local Certificate**.

IPSec Security Method

This group of fields is a must for IPSec Tunnels and L2TP with IPSec Policy.

Medium (AH - Authentication Header) means data will be authenticated, but not be encrypted. By default, this option is active.

High (ESP-Encapsulating Security Payload)- means payload (data) will be encrypted and authenticated. Select from below:

DES without Authentication -Use DES encryption algorithm and not apply any authentication scheme.

DES with Authentication-Use DES encryption algorithm and apply MD5 or SHA-1 authentication algorithm.

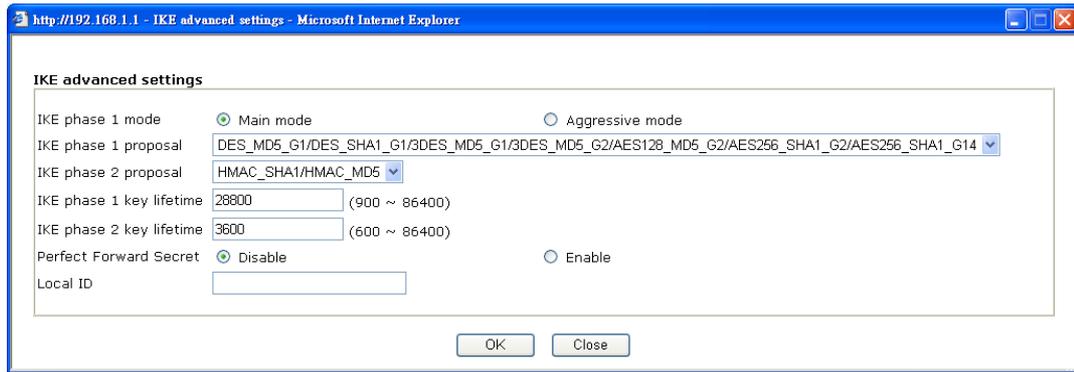
3DES without Authentication-Use triple DES encryption algorithm and not apply any authentication scheme.

3DES with Authentication-Use triple DES encryption algorithm and apply MD5 or SHA-1 authentication algorithm.

AES without Authentication-Use AES encryption algorithm and not apply any authentication scheme.

AES with Authentication-Use AES encryption algorithm and apply MD5 or SHA-1 authentication algorithm.

Advanced - Specify mode, proposal and key life of each IKE phase, Gateway etc. The window of advance setup is shown as below:



IKE phase 1 mode -Select from **Main** mode and **Aggressive** mode. The ultimate outcome is to exchange security proposals to create a protected secure channel. **Main** mode is more secure than **Aggressive** mode since more exchanges are done in a secure channel to set up the IPSec session. However, the **Aggressive** mode is faster. The default value in Vigor router is Main mode.

IKE phase 1 proposal-To propose the local available authentication schemes and encryption algorithms to the VPN peers, and get its feedback to find a match. Two combinations are available for Aggressive mode and nine for **Main** mode. We suggest you select the combination that covers the most schemes.

IKE phase 2 proposal-To propose the local available algorithms to the VPN peers, and get its feedback to find a match. Three combinations are available for both modes. We suggest you select the combination that covers the most algorithms.

IKE phase 1 key lifetime-For security reason, the lifetime of key should be defined. The default value is 28800 seconds. You may specify a value in between 900 and 86400 seconds.

IKE phase 2 key lifetime-For security reason, the lifetime of key should be defined. The default value is 3600 seconds. You may specify a value in between 600 and 86400 seconds.

Perfect Forward Secret (PFS)-The IKE Phase 1 key will be reused to avoid the computation complexity in phase 2. The default value is inactive this function.

Local ID - In **Aggressive** mode, Local ID is on behalf of the IP address while identity authenticating with remote VPN server. The length of the ID is limited to 47 characters.

Callback Function (for *i* models only)

The callback function provides a callback service as a part of PPP suite only for the ISDN dial-in user. The router owner will be charged the connection fee by the telecom.

Require Remote to Callback-Enable this to let the router to require the remote peer to callback for the connection afterwards.

Provide ISDN Number to Remote-In the case that the

remote peer requires the Vigor router to callback, the local ISDN number will be provided to the remote peer. Check here to allow the Vigor router to send the ISDN number to the remote router. This feature is useful for *i* model only.

3. Dial-In Settings

<p>Allowed Dial-In Type</p> <p><input checked="" type="checkbox"/> ISDN</p> <p><input checked="" type="checkbox"/> PPTP</p> <p><input checked="" type="checkbox"/> IPsec Tunnel</p> <p><input checked="" type="checkbox"/> L2TP with IPsec Policy None</p> <p><input type="checkbox"/> Specify ISDN CLID or Remote VPN Gateway Peer ISDN Number or Peer VPN Server IP</p> <p><input type="text"/></p> <p>or Peer ID <input type="text"/></p>	<p>Username <input style="width: 100px;" type="text" value="???"/></p> <p>Password <input style="width: 100px;" type="password"/></p> <p>VJ Compression <input checked="" type="radio"/> On <input type="radio"/> Off</p> <hr/> <p>IKE Authentication Method</p> <p><input checked="" type="checkbox"/> Pre-Shared Key</p> <p style="margin-left: 20px;">IKE Pre-Shared Key <input style="width: 100px;" type="text"/></p> <p><input type="checkbox"/> Digital Signature(X.509)</p> <p style="margin-left: 20px;">Peer ID None</p> <p style="margin-left: 20px;">Local ID</p> <p style="margin-left: 40px;"><input checked="" type="radio"/> Alternative Subject Name First</p> <p style="margin-left: 40px;"><input type="radio"/> Subject Name First</p> <hr/> <p>IPsec Security Method</p> <p><input checked="" type="checkbox"/> Medium (AH)</p> <p>High (ESP)</p> <p style="margin-left: 40px;"><input checked="" type="checkbox"/> DES <input checked="" type="checkbox"/> 3DES <input checked="" type="checkbox"/> AES</p> <hr/> <p>Callback Function (CBCP)</p> <p><input type="checkbox"/> Enable Callback Function</p> <p><input type="checkbox"/> Use the Following Number to Callback</p> <p style="margin-left: 20px;">Callback Number <input style="width: 100px;" type="text"/></p> <p>Callback Budget <input type="text" value="0"/> minute(s)</p>
---	---

4. GRE over IPsec Settings

<input type="checkbox"/> Enable IPsec Dial-Out function GRE over IPsec	
<input type="checkbox"/> Logical Traffic	My GRE IP <input style="width: 100px;" type="text"/> Peer GRE IP <input style="width: 100px;" type="text"/>

5. TCP/IP Network Settings

<p>My WAN IP <input style="width: 100px;" type="text" value="0.0.0.0"/></p> <p>Remote Gateway IP <input style="width: 100px;" type="text" value="0.0.0.0"/></p> <p>Remote Network IP <input style="width: 100px;" type="text" value="0.0.0.0"/></p> <p>Remote Network Mask <input style="width: 100px;" type="text" value="255.255.255.0"/></p> <p style="text-align: center;"><input type="button" value="More"/></p>	<p>RIP Direction Disable</p> <p>From first subnet to remote network, you have to do</p> <p style="text-align: center;">Route</p> <hr/> <p><input type="checkbox"/> Change default route to this VPN tunnel (Only single WAN supports this)</p>
--	--

Allowed Dial-In Type

Determine the dial-in connection with different types.

ISDN

Allow the remote ISDN LAN-to-LAN connection. You should set the User Name and Password of remote dial-in user below. This feature is useful for *i* model only. In addition, you can further set up Callback function below.

PPTP

Allow the remote dial-in user to make a PPTP VPN connection through the Internet. You should set the User Name and Password of remote dial-in user below.

IPSec Tunnel	Allow the remote dial-in user to trigger an IPSec VPN connection through Internet.
L2TP	<p>Allow the remote dial-in user to make a L2TP VPN connection through the Internet. You can select to use L2TP alone or with IPSec. Select from below:</p> <p>None- Do not apply the IPSec policy. Accordingly, the VPN connection employed the L2TP without IPSec policy can be viewed as one pure L2TP connection.</p> <p>Nice to Have- Apply the IPSec policy first, if it is applicable during negotiation. Otherwise, the dial-in VPN connection becomes one pure L2TP connection.</p> <p>Must- Specify the IPSec policy to be definitely applied on the L2TP connection.</p>
Specify CLID or Remote VPN Gateway	<p>You can specify the IP address of the remote dial-in user or peer ID (should be the same with the ID setting in dial-in type) by checking the box. Enter Peer ISDN number if you select ISDN above (This feature is useful for <i>i</i> model only.). Also, you should further specify the corresponding security methods on the right side.</p> <p>If you uncheck the checkbox, the connection type you select above will apply the authentication methods and security methods in the general settings.</p>
User Name	This field is applicable when you select ISDN, PPTP or L2TP with or without IPSec policy above.
Password	This field is applicable when you select ISDN, PPTP or L2TP with or without IPSec policy above.
VJ Compression	VJ Compression is used for TCP/IP protocol header compression. This field is applicable when you select ISDN, PPTP or L2TP with or without IPSec policy above.
IKE Authentication Method	<p>This group of fields is applicable for IPSec Tunnels and L2TP with IPSec Policy.</p> <p>Pre-Shared Key-Input 1-63 characters as pre-shared key.</p> <p>Digital Signature (X.509) – This setting will be available when IPSec Tunnel is selected. Click this radio button to invoke this function and select one predefined profile in the Peer ID (set from VPN and Remote Access>>IPSec Peer Identity).</p> <p>Peer ID – Display the IPSec Peer Identity profiles. Use the drop down menu to choose any one desired.</p> <p>Local ID – There are two selections offered here. Choose Alternative Subject Name First or choose Subject Name First based on the local certificate selected below.</p>
IPSec Security Method	<p>This group of fields is a must for IPSec Tunnels and L2TP with IPSec Policy when you specify the remote node.</p> <p>Medium- Authentication Header (AH) means data will be authenticated, but not be encrypted. By default, this option is active.</p>

High- Encapsulating Security Payload (ESP) means payload (data) will be encrypted and authenticated. You may select encryption algorithm from Data Encryption Standard (DES), Triple DES (3DES), and AES.

Callback Function

The callback function provides a callback service only for the ISDN LAN-to-LAN connection (this feature is useful for *i* model only). The remote user will be charged the connection fee by the telecom.

Enable Callback function-Enables the callback function.

Use the Following Number to Callback – Check this box to use the number typed below for callback.

Callback Number -The option is for extra security. Once enabled, the router will ONLY call back to the specified Callback Number.

Callback Budget (Unit: minutes)- By default, the callback function has limitation of callback period. Once the callback budget is exhausted, the function will be disabled automatically. Specify the time budget for the dial-in user. The budget will be decreased automatically per callback connection. The default value 0 means no limitation of callback period.

GRE over IPSec Settings

Enable IPSec Dial-Out function GRE over IPSec: Check this box to verify data and transmit data in encryption with GRE over IPSec packet after configuring IPSec Dial-Out setting. Both ends must match for each other by setting same virtual IP address for communication.

Logical Traffic: Such technique comes from RFC2890. Define logical traffic for data transmission between both sides of VPN tunnel by using the characteristic of GRE. Even hacker can decipher IPSec encryption, he/she still cannot ask LAN site to do data transmission with any information. Such function can ensure the data transmitted on VPN tunnel is really sent out from both sides. This is an optional function. However, if one side wants to use it, the peer must enable it, too.

My GRE IP: Type the virtual IP for router itself for verified by peer.

Peer GRE IP: Type the virtual IP of peer host for verified by router.

My WAN IP

This field is only applicable when you select ISDN, PPTP or L2TP with or without IPSec policy above. The default value is 0.0.0.0, which means the Vigor router will get a PPP IP address from the remote router during the IPCP negotiation phase. If the PPP IP address is fixed by remote side, specify the fixed IP address here. Do not change the default value if you do not select ISDN, PPTP or L2TP.

Remote Gateway IP

This field is only applicable when you select ISDN, PPTP or L2TP with or without IPSec policy above. The default value is 0.0.0.0, which means the Vigor router will get a remote

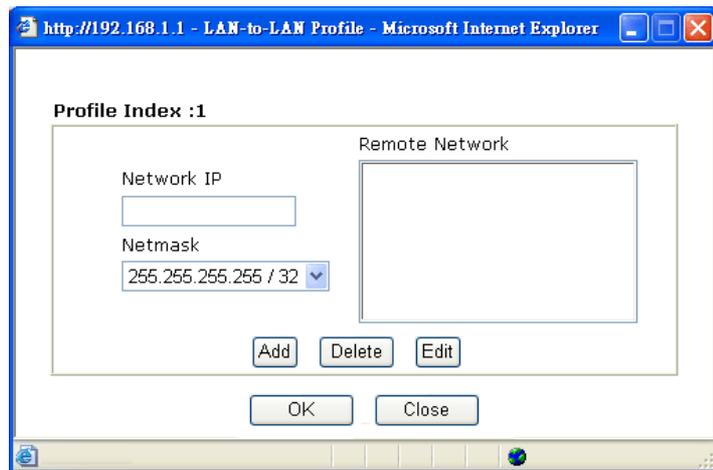
Gateway PPP IP address from the remote router during the IPCP negotiation phase. If the PPP IP address is fixed by remote side, specify the fixed IP address here. Do not change the default value if you do not select ISDN, PPTP or L2TP.

**Remote Network IP/
Remote Network Mask**

Add a static route to direct all traffic destined to this Remote Network IP Address/Remote Network Mask through the VPN connection. For IPsec, this is the destination clients IDs of phase 2 quick mode.

More

Add a static route to direct all traffic destined to more Remote Network IP Addresses/ Remote Network Mask through the VPN connection. This is usually used when you find there are several subnets behind the remote VPN router.



RIP Direction

The option specifies the direction of RIP (Routing Information Protocol) packets. You can enable/disable one of direction here. Herein, we provide four options: TX/RX Both, TX Only, RX Only, and Disable.

From first subnet to remote network, you have to do

If the remote network only allows you to dial in with single IP, please choose **NAT**, otherwise choose **Route**.

Change default route to this VPN tunnel (Only single WAN supports this)

Check this box to change the default route with this VPN tunnel. Be aware that this setting is available only for one WAN interface is enabled. It is not available when both WAN interfaces are enabled.

3.10.7 VPN TRUNK Management

VPN trunk includes four features - VPN Backup, VPN load balance, GRE over IPsec, and Binding tunnel policy.

Features of VPN TRUNK – VPN Backup Mechanism

VPN TRUNK Management is a backup mechanism which can set multiple VPN tunnels as backup tunnel. It can assure the network connection not to be cut off due to network environment blocked by any reason.

- VPN TRUNK-VPN Backup mechanism can judge abnormal situation for the environment of VPN server and correct it to complete the backup of VPN Tunnel in real-time.

- VPN TRUNK-VPN Backup mechanism is compliant with all WAN modes (single/multi)
- Dial-out connection types contain IPSec, PPTP, L2TP, L2TP over IPSec and ISDN (depends on hardware specification)
- The web page is simple to understand and easy to configure
- Fully compliant with VPN Server LAN Side Single/Multi Network
- Mail Alert support, please refer to **System Maintenance >> SysLog / Mail Alert** for detailed configuration
- Syslog support, please refer to **System Maintenance >> SysLog / Mail Alert** for detailed configuration
- Specific ERD (Environment Recovery Detection) mechanism which can be operated by using Telnet command

VPN TRUNK-VPN Backup mechanism profile will be activated when initial connection of single VPN tunnel is off-line. Before setting VPN TRUNK -VPN Backup mechanism backup profile, please configure at least two sets of LAN-to-LAN profiles (with fully configured dial-out settings) first, otherwise you will not have selections for grouping Member1 and Member2.

Features of VPN TRUNK – VPN Load Balance Mechanism

VPN Load Balance Mechanism can set multiple VPN tunnels for using as traffic load balance tunnel. It can assist users to do effective load sharing for multiple VPN tunnels according to real line bandwidth. Moreover, it offers three types of algorithms for load balancing and binding tunnel policy mechanism to let the administrator manage the network more flexibly.

- Three types of load sharing algorithm offered, Round Robin, Weighted Round Robin and Fastest
- Binding Tunnel Policy mechanism allows users to encrypt the data in transmission or specified service function in transmission and define specified VPN Tunnel for having effective bandwidth management.
- Dial-out connection types contain IPSec, PPTP, L2TP, L2TP over IPSec and GRE over IPSec
- The web page is simple to understand and easy to configure
- The TCP Session transmitted by using VPN TRUNK-VPN Load Balance mechanism will not be lost due to one of VPN Tunnels disconnected. Users do not need to reconnect with setting TCP/UDP Service Port again. The VPN Load Balance function can keep the transmission for internal data on tunnel stably.

Backup profile list | [Set to Factory Default](#) |

Note: [Active:NO] The LAN-to-LAN Profile is disable or under Dial-In(Call Direction) at present.

No.	Status	Name	Member1(Active)Type	Member2(Active)Type

Advanced

Load Balance Profile List | [Set to Factory Default](#) |

Note: [Active:NO] The LAN-to-LAN Profile is disable or under Dial-In(Call Direction) at present.

No.	Status	Name	Member1(Active)Type	Member2(Active)Type

Advanced

General Setup

Status Enable Disable

Profile Name

Member1

Member2

Attribute Mode Backup Load Balance

Backup Profile List

Set to Factory Default - Click to clear all VPN TRUNK-VPN Backup mechanism profile.

No-The order of VPN TRUNK-VPN Backup mechanism profile.

Status (on Backup Profile field) - “v” means such profile is enabled; ”x” means such profile is disabled.

Name (on Backup Profile field) - Display the name of VPN TRUNK-VPN Backup mechanism profile.

Member1 (on Backup Profile field) - Display the dial-out profile selected from the Member1 drop down list below.

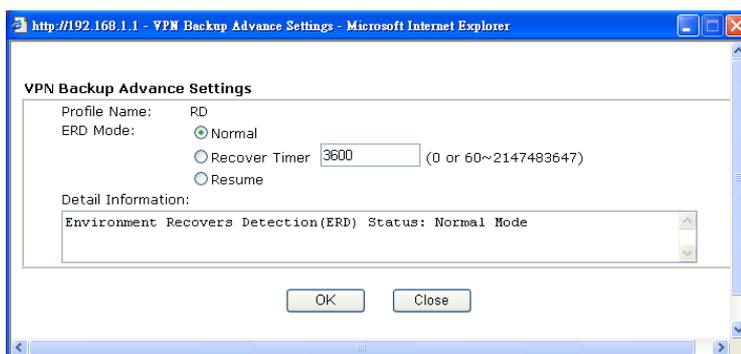
Active (on Backup Profile field) - “Yes” means normal condition. ”No” means the state might be disabled or that profile currently is set with Dial-in mode (for call direction) in LAN-to-LAN.

Type (on Backup Profile field) - Display the connection type for that profile, such as IPSec, PPTP, L2TP, L2TP over IPSec (NICE), L2TP over IPSec(MUST) and so on.

Member2 (on Backup Profile field) - Display the dial-out profile selected from the Member2 drop down list below.

Advanced – This button is only available when there is one

profile (or more) created in this page



Detailed information for this dialog, see later section - **Advanced Load Balance and Backup.**

Load Balance Profile List

Set to Factory Default - Click to clear all VPN TRUNK-VPN Load Balance mechanism profile.

No - The order of VPN TRUNK-VPN Load Balance mechanism profile.

Status - “v” means such profile is enabled; ”x” means such profile is disabled.

Name - Display the name of VPN TRUNK-VPN Load Balance mechanism profile.

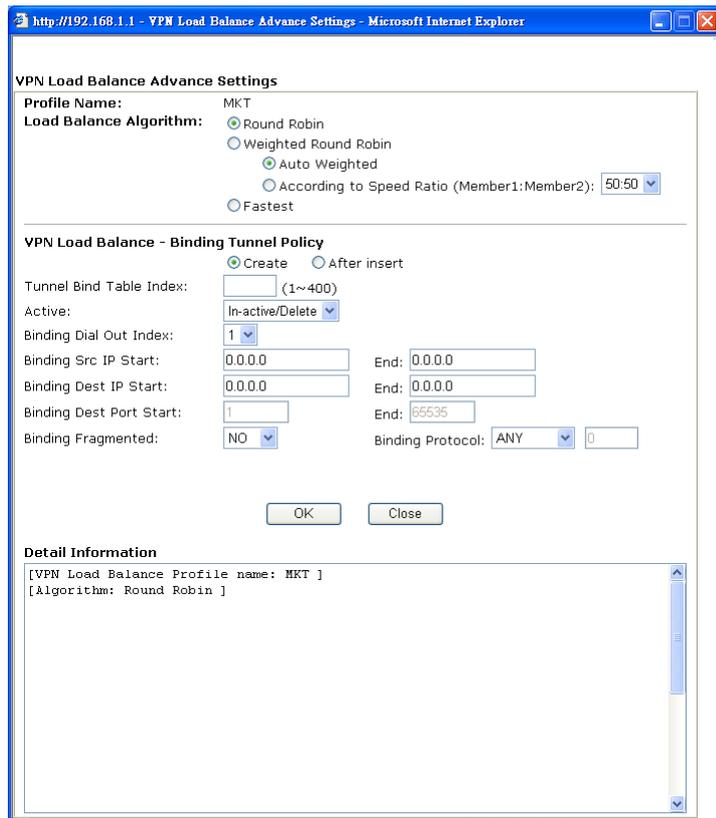
Member1 - Display the dial-out profile selected from the Member1 drop down list below.

Active - “Yes” means normal condition. ”No” means the state might be disabled or that profile currently is set with Dial-in mode (for call direction) in LAN-to-LAN.

Type - Display the connection type for that profile, such as IPSec, PPTP, L2TP, L2TP over IPSec (NICE), L2TP over IPSec(MUST) and so on.

Member2 - Display the dial-out profile selected from the Member2 drop down list below.

Advanced – This button is only available when there is one or more profiles created in this page.



Detailed information for this dialog, see later section - **Advanced Load Balance and Backup.**

General Setup

Status- After choosing one of the profile listed above, please click **Enable** to activate this profile. If you click **Disable**, the selected or current used VPN TRUNK-Backup/Load Balance mechanism profile will not have any effect for VPN tunnel.

Profile Name- Type a name for VPN TRUNK profile. Each profile can group two VPN connections set in LAN-to-LAN. The saved VPN profiles in LAN-to-LAN will be shown on Member1 and Member2 fields.

Member 1/Member2 - Display the selection for LAN-to-LAN dial-out profiles (configured in **VPN and Remote Access >> LAN-to-LAN**) for you to choose for grouping under certain VPN TRUNK-VPN Backup/Load Balance mechanism profile.
No - Index number of LAN-to-LAN dial-out profile.

Name - Profile name of LAN-to-LAN dial-out profile.

Connection Type - Connection type of LAN-to-LAN dial-out profile.

VPN ServerIP (Private Network) - VPN Server IP of LAN-to-LAN dial-out profiles.

Attribute Mode - Display available mode for you to choose. Choose **Backup** or **Load Balance** for your router.

Add

Add and save new profile to the backup profile list. The corresponding members (LAN-to-LAN profiles) grouped in such new VPN TRUNK – VPN Backup mechanism profile will be locked. The profiles in LAN-to-LAN will be displayed

in red. VPN TRUNK – VPN Load Balance mechanism profile will be locked. The profiles in LAN-to-LAN will be displayed in blue.

Edit	Click this button to save the changes to the Status (Enable or Disable), profile name, member1 or member2.
Delete	Click this button to delete the selected VPN TRUNK profile. The corresponding members (LAN-to-LAN profiles) grouped in the deleted VPN TRUNK profile will be released and that profiles in LAN-to-LAN will be displayed in black.

Time for activating VPN TRUNK – VPN Backup mechanism profile

VPN TRUNK – VPN Backup mechanism will be activated automatically after the initial connection of single VPN Tunnel off-line. The content in Member1/2 within VPN TRUNK – VPN Backup mechanism backup profile is similar to dial-out profile configured in LAN-to-LAN web page. VPN TRUNK – VPN Backup mechanism backup profile will process and handle everything unless it is off-line once it is activated.

Time for activating VPN TRUNK – VPN Load Balance mechanism profile

After finishing the connection for one tunnel, the other tunnel will dial out automatically within two seconds. Therefore, you can choose any one of members under VPN Load Balance for dialing out.

Time for activating VPN TRUNK –Dial-out when VPN Load Balance Disconnected

For there is one Tunnel created and connected successfully, to keep the load balance effect between two tunnels, auto-dial will be executed within two seconds.

To close two tunnels of load balance after connecting, please click **Disable** for **Status** in **General Setup** field.

How can you set a VPN TRUNK-VPN Backup/Load Balance mechanism profile?

1. First of all, go to **VPN and Remote Access>>LAN-to-LAN**. Set two or more LAN-to-LAN profiles first that will be used for Member1 and Member2. If you do not set enough LAN-to-LAN profiles, you cannot operate VPN TRUNK – VPN Backup /Load Balance mechanism profile management well.
2. Access into **VPN and Remote Access>>VPN TRUNK Management**.
3. Set one group of VPN TRUNK – VPN Backup/Load Balance mechanism backup profile by choosing **Enable** radio button; type a name for such profile (e.g., 071023); choose one of the LAN-to-LAN profiles from Member1 drop down list; choose one of the LAN-to-LAN profiles from Member2 drop down list; and click **Add** at last.

General Setup

Status Enable Disable

Profile Name

Member1

Member2

No.	<Name>	<Connection-Type>	<VPN ServerIP(Private Network)>
1	V1	PPTP	(0.0.0.0)
2	V2	ISDN	(0.0.0.0)

- Take a look for LAN-to-LAN profiles. Index 1 is chosen as Member1; index 2 is chosen as Member2. For such reason, LAN-to-LAN profiles of 1 and 2 will be expressed in red to indicate that they are fixed. If you delete the VPN TRUNK – VPN Backup/Load Balance mechanism profile, the selected LAN-to-LAN profiles will be released and expressed in black.

VPN and Remote Access >> LAN to LAN

LAN-to-LAN Profiles:

Index	Name	Status
<u>1.</u>	To-A place	√
<u>2.</u>	To-B site	√
<u>3.</u>	To-C place	√
<u>4.</u>	To-D site	√

How can you set a GRE over IPSec profile?

- Please go to LAN to LAN to set a profile with IPSec.
- If the router will be used as the VPN Server (i.e., with virtual address 192.168.50.200). Please type 192.168.50.200 in the field of My GRE IP. Type IP address (192.168.50.100) of the client in the field of Peer GRE IP. See the following graphic for an example.

4. GRE over IPSec Settings

Enable IPSec Dial-Out function GRE over IPSec

Logical Traffic

My GRE IP Peer GRE IP

5. TCP/IP Network Settings

My WAN IP

Remote Gateway IP

Remote Network IP

Remote Network Mask

RIP Direction

From first subnet to remote network, you have to do

Change default route to this VPN tunnel (Only single WAN supports this)

- Later, on peer side (as VPN Client): please type 192.168.50.100 in the field of My GRE IP and type IP address of the server (192.168.50.200) in the field of Peer GRE IP.

4. GRE over IPsec Settings

<input checked="" type="checkbox"/> Enable IPsec Dial-Out function GRE over IPsec
<input type="checkbox"/> Logical Traffic
My GRE IP <input type="text" value="192.168.50.100"/> Peer GRE IP <input type="text" value="192.168.50.200"/>

5. TCP/IP Network Settings

My WAN IP <input type="text" value="0.0.0.0"/>	RIP Direction <input type="text" value="TX/RX Both"/>
Remote Gateway IP <input type="text" value="0.0.0.0"/>	From first subnet to remote network, you have to do
Remote Network IP <input type="text" value="192.168.1.0"/>	<input type="text" value="Route"/>
Remote Network Mask <input type="text" value="255.255.255.0"/>	
<input type="button" value="More"/>	<input type="checkbox"/> Change default route to this VPN tunnel (Only single WAN supports this)

Advanced Load Balance and Backup

After setting profiles for load balance, you can choose any one of them and click Advance for more detailed configuration. The windows for advanced load balance and backup are different. Refer to the following explanation:

Advanced Load Balance

Profile Name

List the load balance profile name.

Load Balance Algorithm

Round Robin – Based on packet base, both tunnels will send the packet alternatively. Such method can reach the balance of packet transmission with fixed rate.

Weighted Round Robin –Such method can reach the

VPN Load Balance – Binding Tunnel Policy

balance of packet transmission with flexible rate. It can be divided into Auto Weighted and According to Speed Ratio. **Auto Weighted** can detect the device speed (10Mbps/100Mbps) and switch with fixed value ratio (3:7) for packet transmission. If the transmission rate for packets on both sides of the tunnels is the same, the value of Auto Weighted should be 5.5. **According to Speed Ratio** allows user to adjust suitable rate manually. There are 100 groups of rate ratio for Member1:Member2 (range from 1:99 to 99:1).

Fastest – Based on available bandwidth that integrated and considered by DrayOS system, the system can adjust dynamically for bandwidth of both VPN tunnels. In most cases, VPN Tunnel with high rate will use the WAN interface which has more available bandwidth.

Below shows the algorithm for Load Balance.

Create – Click this radio button for assign a blank table for configuring Binding Tunnel.

After insert – Click this radio button to adding a new binding tunnel table.

Tunnel Bind Table Index- 400 binding tunnel tables are provided by this device. Choose any one of them for such Load Balance profile.

Active – In-active/Delete can delete this binding tunnel table. Active can activate this binding tunnel table.

Binding Dial Out Index – Specify connection type for transmission by choosing the index (LAN to LAN Profile Index) for such binding tunnel table.

Binding Set IP Start /End– Specify source IP addresses as starting point and ending point.

Binding Dest IP Start/End – Specify destination IP addresses as starting point and ending point.

Binding Dest Port Start /End– Specify destination service port as starting point and ending point.

Binding Fragmented – Non fragmented packets will be bound with such tunnel table if you choose **No**. Fragmented packets will be bound with such tunnel table if you choose **Yes**.

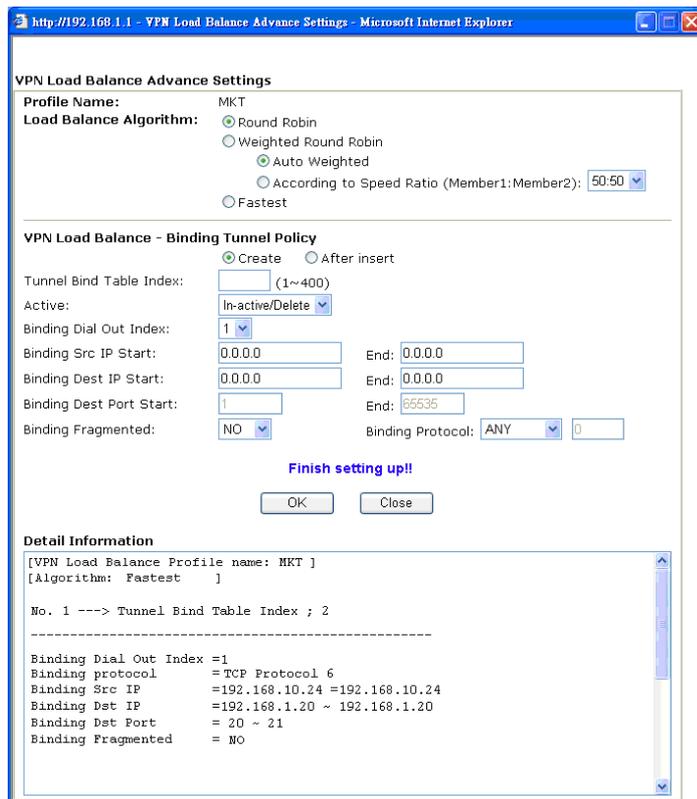
Binding Protocol – **Any** means when the source IP, destination IP, destination port and fragment conditions match with the settings specified here, such binding tunnel table can be established for TCP Service Port/UDP Service Port/ICMP/IGMP specified here.

TCP means when the source IP, destination IP, destination port and fragment conditions match with the settings specified here and TCP Service Port also fits the number here, such binding tunnel table can be established. **UDP** means when the source IP, destination IP, destination port and fragment conditions match with the settings specified here and UDP Service Port also fits the number here, such

binding tunnel table can be established. **TCP/UPD** means when the source IP, destination IP, destination port and fragment conditions match with the settings specified here and TCP/UDP Service Port also fits the number here, such binding tunnel table can be established. **ICMP** means when the source IP, destination IP, destination port and fragment conditions match with the settings specified here and ICMP Service Port also fits the number here, such binding tunnel table can be established. **IGMP** means when the source IP, destination IP, destination port and fragment conditions match with the settings specified here and IGMP Service Port also fits the number here, such binding tunnel table can be established. **Other** means when the source IP, destination IP, destination port and fragment conditions match with the settings specified here with different TCP Service Port/UDP Service Port/ICMP/IGMP, such binding tunnel table can be established.

Detail Information

This field will display detailed information for Binding Tunnel Policy. Below shows a successful binding tunnel policy for load balance:

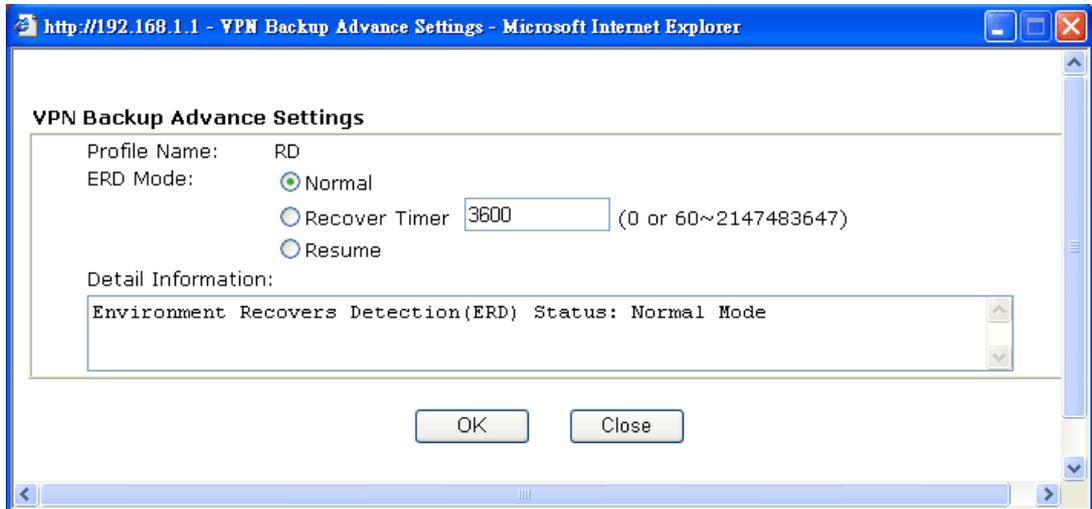


Note : To configure a successful binding tunnel, you have to:

- Type Binding Src IP range (Start and End) and Binding Des IP range (Start and End) Choose YES or NO for Binding Fragmented. If you choose YES for Binding Fragmented, you don't need to choose Binding Protocol.
- Type Binding Src IP range (Start and End) and Binding Des IP range (Start and End). Choose YES or

NO for Binding Fragmented. If you choose **NO** for Binding Fragmented, please choose TCP/UDP, IGMP/ICMP or Other as Binding Protocol.

Advanced Backup



Profile Name

List the backup profile name.

ERD Mode

ERD means “Environment Recovers Detection”.

Normal – choose this mode to make all dial-out VPN TRUNK backup profiles being activated alternatively.

Recover Timer – choose this mode to detect VPN connection periodically and type the value for it (the unit is second). If VPN server for Member 1 has completed the network connection, current VPN Tunnel backup connection will be off.

Resume – when VPN connection breaks down or disconnects, Member 1 will be the top priority for the system to do VPN connection.

Detail Information

This field will display detailed information for Environment Recovers Detection.

3.10.8 Connection Management

You can find the summary table of all VPN connections. You may disconnect any VPN connection by clicking **Drop** button. You may also aggressively Dial-out by using Dial-out Tool and clicking **Dial** button.

VPN and Remote Access >> Connection Management

Dial-out Tool Refresh Seconds : 10

General Mode: <input type="button" value="v"/>	<input type="button" value="Dial"/>
Backup Mode: <input type="button" value="v"/>	<input type="button" value="Dial"/>
Load Balance Mode: <input type="button" value="v"/>	<input type="button" value="Dial"/>

VPN Connection Status

Current Page: 1 Page No.

VPN	Type	Remote IP	Virtual Network	Tx Pkts	Tx Rate (Bps)	Rx Pkts	Rx Rate (Bps)	UpTime
xxxxxxxx : Data is encrypted. xxxxxxxx : Data isn't encrypted.								

Dial Click this button to execute dial out function with general mode, backup mode or load balance mode.

Refresh Seconds Choose the time for refresh the dial information among 5, 10, and 30.

Refresh Click this button to refresh the whole connection status.

3.11 Certificate Management

A digital certificate works as an electronic ID, which is issued by a certification authority (CA). It contains information such as your name, a serial number, expiration dates etc., and the digital signature of the certificate-issuing authority so that a recipient can verify that the certificate is real. Here Vigor router support digital certificates conforming to standard X.509.

Any entity wants to utilize digital certificates should first request a certificate issued by a CA server. It should also retrieve certificates of other trusted CA servers so it can authenticate the peer with certificates issued by those trusted CA servers.

Here you can manage generate and manage the local digital certificates, and set trusted CA certificates. Remember to adjust the time of Vigor router before using the certificate so that you can get the correct valid period of certificate.

Below shows the menu items for Certificate Management.



3.11.1 Local Certificate

This page allows users to adopt single certificate or multiple certificates for certification through generating or importing. Users can generate up to three local certificates or they can import the third-party certificate(s) to fit different requests.

Certificate Management >> Local Certificate

X509 Local Certificate Configuration

Name	Subject	Status	Modify	
---	---	---	<input type="button" value="View"/>	<input type="button" value="Delete"/>
---	---	---	<input type="button" value="View"/>	<input type="button" value="Delete"/>
---	---	---	<input type="button" value="View"/>	<input type="button" value="Delete"/>

GENERATE

Click this button to open **Generate Certificate Signing Request** window. Type in all the information that the window request such as certificate name (used for identifying different certificate), subject alternative name type and relational settings for subject name. Then click **GENERATE** again.

Generate Certificate Signing Request

Certificate Name	<input type="text"/>
Subject Alternative Name	
Type	IP Address <input type="button" value="v"/>
IP	<input type="text"/>
Subject Name	
Country (C)	<input type="text"/>
State (ST)	<input type="text"/>
Location (L)	<input type="text"/>
Organization (O)	<input type="text"/>
Organization Unit (OU)	<input type="text"/>
Common Name (CN)	<input type="text"/>
Email (E)	<input type="text"/>
Key Type	RSA <input type="button" value="v"/>
Key Size	1024 Bit <input type="button" value="v"/>

Note: Please be noted that “Common Name” must be configured with rotuer’s WAN IP or domain name.

After clicking **GENERATE**, the generated information will be displayed on the window below:

X509 Local Certificate Configuration

Name	Subject	Status	Modify	
server	/C=TW/ST=Hsinchu/L=Hsinchu/O...	Requesting	<input type="button" value="View"/>	<input type="button" value="Delete"/>
---	---	---	<input type="button" value="View"/>	<input type="button" value="Delete"/>
---	---	---	<input type="button" value="View"/>	<input type="button" value="Delete"/>

IMPORT

Vigor router allows you to generate a certificate request and submit it the CA server, then import it as “Local Certificate”. If you have already gotten a certificate from a third party, you may import it directly. The supported types are PKCS12 Certificate and Certificate with a private key.

Click this button to import a saved file as the certification information. There are three types of local certificate supported by Vigor router.

Import X509 Local Certificate

Upload Local Certificate
Select a local certificate file.
Certificate file:
Click [Import](#) to upload the local certificate.

Upload PKCS12 Certificate
Select a PKCS12 file.
PKCS12 file:
Password:
Click [Import](#) to upload the PKCS12 file.

Upload Certificate and Private Key
Select a certificate file and a matchable Private Key.
Certificate file:
Key file:
Password:
Click [Import](#) to upload the local certificate and private key.

Upload Local Certificate It allows users to import the certificate which is generated by vigor router and signed by CA server.

If you have done well in certificate generation, the Status of the certificate will be shown as “**OK**”.

Upload PKCS12 Certificate

It allows users to import the certificate whose extensions are usually .pfx or .p12. And these certificates usually need passwords.

Note: PKCS12 is a standard for storing private keys and certificates securely. It is used in (among other things) Netscape and Microsoft Internet Explorer with their import and export options.

Upload Certificate and Private Key

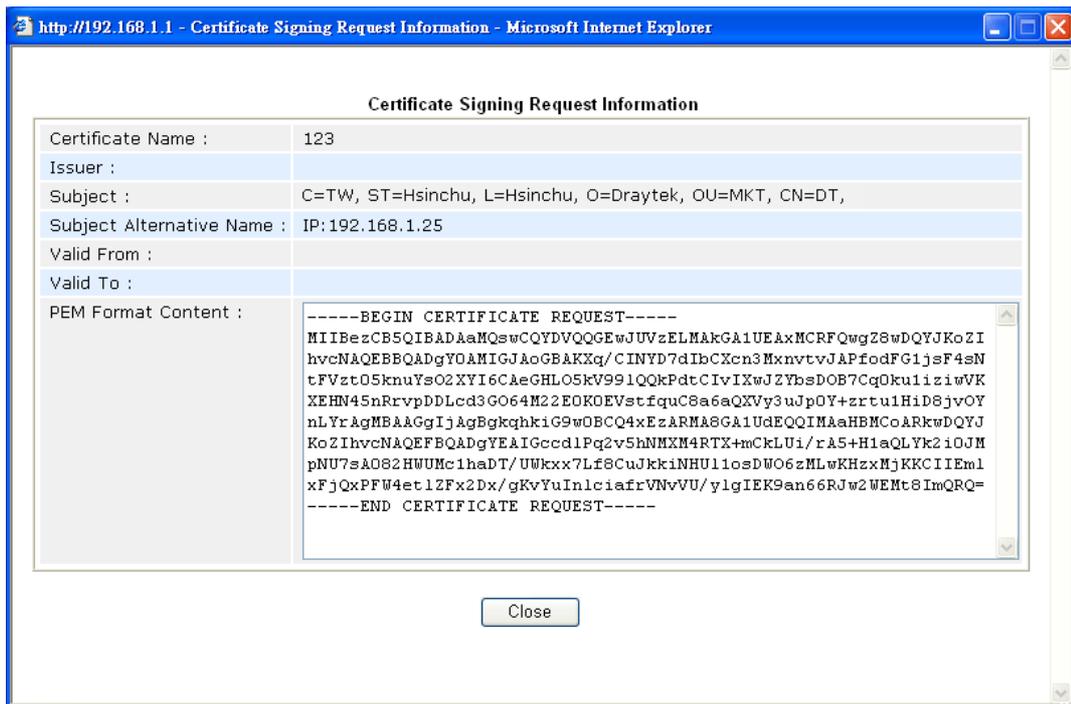
It is useful when users have separated certificates and private keys. And the password is needed if the private key is encrypted.

REFRESH

Click this button to refresh the information listed below.

View

Click this button to view the detailed settings for certificate request.



Note: You have to copy the certificate request information from above window. Next, access your CA server and enter the page of certificate request, copy the information into it and submit a request. A new certificate will be issued to you by the CA server. You can save it.

3.11.2 Trusted CA Certificate

Trusted CA certificate lists three sets of trusted CA certificate.

Certificate Management >> Trusted CA Certificate

X509 Trusted CA Certificate Configuration

Name	Subject	Status	Modify	
Trusted CA-1	---	---	<input type="button" value="View"/>	<input type="button" value="Delete"/>
Trusted CA-2	---	---	<input type="button" value="View"/>	<input type="button" value="Delete"/>
Trusted CA-3	---	---	<input type="button" value="View"/>	<input type="button" value="Delete"/>

To import a pre-saved trusted CA certificate, please click **IMPORT** to open the following window. Use **Browse...** to find out the saved text file. Then click Import. The one you imported will be listed on the Trusted CA Certificate window. Then click **Import** to use the pre-saved file.

Certificate Management >> Trusted CA Certificate

Import X509 Trusted CA Certificate

Select a trusted CA certificate file.

Click [Import](#) to upload the certification.

For viewing each trusted CA certificate, click **View** to open the certificate detail information window. If you want to delete a CA certificate, choose the one and click **Delete** to remove all the certificate information.



3.11.3 Certificate Backup

Local certificate and Trusted CA certificate for this router can be saved within one file. Please click **Backup** on the following screen to save them. If you want to set encryption password for these certificates, please type characters in both fields of **Encrypt password** and **Retype password**.

Also, you can use **Restore** to retrieve these two settings to the router whenever you want.

Certificate Management >> Certificate Backup

Certificate Backup / Restoration

Backup

Encrypt password:

Retype password:

Click to download certificates to your local PC as a file.

Restoration

Select a backup file to restore.

Decrypt password:

Click to upload the file.

3.12 ISDN

3.12.1 Basic Concept

ISDN means integrated services digital network that is an international communications standard for sending voice, video, and data over digital telephone lines or normal telephone wires.

Below shows the menu items for ISDN.



3.12.2 General Setup

This web page allows you to enable ISDN function.

ISDN >> General Setup

ISDN Setup

Country Code	International	▼
D-Channel Mode		
ISDN1	<input type="radio"/> Point-to-Point	<input type="radio"/> Point-to-Multipoint
ISDN2	<input type="radio"/> Point-to-Point	<input type="radio"/> Point-to-Multipoint

OK Cancel

Country Code

For proper operation on your local ISDN network, you should choose the correct country code.



D-Channel Mode

It allows you to configure ISDN layer2 protocol as:
Point-to-Point - Configure ISDN port to use static TEI (Terminal Endpoint Identifier).

Point-to-Multipoint - Configure ISDN port to use Dynamic TEI.

3.12.3 Dial to a Single ISP/Dial to Dual ISPs

Select **Dialing to a Single ISP** if you access the Internet via a single ISP.

Single ISP	
<p>ISP Access Setup</p> <p>ISP Name <input type="text"/></p> <p>Dial Number <input type="text"/></p> <p>Username <input type="text"/></p> <p>Password <input type="text"/></p> <p><input type="checkbox"/> Require ISP callback (CBCP)</p> <p>Index(1-15) in Schedule Setup: => <input type="text"/>, <input type="text"/>, <input type="text"/>, <input type="text"/></p>	<p>PPP/MP Setup</p> <p>Link Type <input type="text" value="Dialup BOD"/></p> <p>PPP Authentication <input type="text" value="PAP or CHAP"/></p> <p>Idle Timeout <input type="text" value="180"/> second(s)</p> <p>IP Address Assignment Method (IPCP)</p> <p>Fixed IP <input type="radio"/> Yes <input checked="" type="radio"/> No (Dynamic IP)</p> <p>Fixed IP Address <input type="text"/></p>
<input type="button" value="OK"/>	

ISP Access Setup

ISP Name - Enter your ISP name such as Seednet, Hinet and so on.

Dial Number - Enter the ISDN access number provided by your ISP.

Username - Enter the username provided by your ISP.

Password - Enter the password provided by your ISP.

Require ISP Callback (CBCP) - If your ISP supports the callback function, check this box to activate the Callback Control Protocol during the PPP negotiation.

Scheduler (1-15) - Enter the index of schedule profiles to control the Internet access according to the preconfigured schedules. Refer to section **3.9.2 Schedule** for detailed configuration.

PPP/MP Setup

Link Type - There are three link types provided here for different purpose. **Link Disable** disables the ISDN dial-out function. **Dialup 64Kbps** allows you to use one ISDN B channel for Internet access. **Dialup 128Kbps** allows you to use both ISDN B channels for Internet access. **Dialup BOD** stands for bandwidth-on-demand. The router will use only one B channel in low traffic situations. Once the single B channel bandwidth is fully used, the other B channel will be activated automatically through the dialup. For more detailed BOD parameter settings, please refer to the section of **Call Control**.

PPP Authentication - PAP only allows you to configure the PPP session to use the PAP protocol to negotiate the username and password with the ISP. **PAP or CHAP** is to configure the PPP session to use the PAP or CHAP protocols to negotiate the username and password with the ISP.

Idle Timeout - Idle timeout means the router will be disconnect after being idle for a preset amount of time. The default is 180 seconds. If you set the time to 0, the ISDN connection to the ISP will always remain on.

IP Address Assignment

In most environments, you should not change these settings as

Method (IPCP)

most ISPs provide a dynamic IP address for the router when it connects to the ISP. If your ISP provides a fixed IP address, check **Yes** and enter the IP address in the field of **Fixed IP Address**.

Select **Dialing to Dual ISPs** if you have more than one ISP. You will be able to dial to both ISPs at the same time. This is mainly for those ISPs that do not support Multiple-Link PPP (ML-PPP). In such cases, dialing to two ISPs can increase the bandwidth utilization of the ISDN channels to 128kbps data speed.

ISDN >> Dialing to Dual ISPs

Dual ISP	
Common Settings 1. <input type="checkbox"/> Enable Dual ISPs Function 2. <input type="checkbox"/> Require ISP callback (CBCP)	PPP/MP Setup Link Type <input type="text" value="Dialup BOD"/> PPP Authentication <input type="text" value="PAP or CHAP"/> Idle Timeout <input type="text" value="180"/> second(s)
Primary ISP Setup ISP Name <input type="text"/> Dial Number <input type="text"/> Username <input type="text"/> Password <input type="text"/> IP Address Assignment Method (IPCP) Fixed IP <input type="radio"/> Yes <input checked="" type="radio"/> No (Dynamic IP) Fixed IP Address <input type="text"/>	Secondary ISP Setup ISP Name <input type="text"/> Dial Number <input type="text"/> Username <input type="text" value="84005755@hinet.net"/> Password <input type="text" value="....."/> IP Address Assignment Method (IPCP) Fixed IP <input type="radio"/> Yes <input checked="" type="radio"/> No (Dynamic IP) Fixed IP Address <input type="text"/>
<input type="button" value="OK"/>	

Common Settings

Enable Dual ISPs Function - Check to enable the Dual ISPs function. **Require ISP Callback (CBCP)** -If your ISP supports the callback function, check this box to activate the Callback Control Protocol during the PPP negotiation.

PPP/MP Setup

Link Type – There are three link types provided here for different purpose. **Link Disable** disables the ISDN dial-out function. **Dialup 128Kbps** allows you to use both ISDN B channels for Internet access. **Dialup BOD** (for detailed information of configuration, please refer to section 3.10.5) stands for bandwidth-on-demand. The router will use only one B channel in low traffic situations. Once the single B channel bandwidth is fully used, the other B channel will be activated automatically through the dialup.

PPP Authentication - PAP only allows you to configure the PPP session to use the PAP protocol to negotiate the username and password with the ISP. **PAP or CHAP** can configure the PPP session to use the PAP or CHAP protocols to negotiate the username and password with the ISP.

Idle Timeout - Idle timeout means the router will be disconnect after being idle for a preset amount of time. The default is 180 seconds. If you set the time to 0, the ISDN connection to the ISP will always remain on.

Primary ISP Setup

ISP Name - Enter your ISP name.

Dial Number - Enter the ISDN access number provided by your ISP.

Username - Enter the username provided by your ISP.

Password - Enter the password provided by your ISP.

IP Address Assignment Method (IPCP) for primary ISP setup

In most environments, you should not change these settings as most ISPs provide a dynamic IP address for the router when it connects to the ISP. If your ISP provides a fixed IP address, check **Yes** and enter the IP address in the field of **Fixed IP Address**.

Secondary ISP Setup

ISP Name - Enter the secondary ISP name.

Dial Number - Enter the ISDN access number provided by the ISP.

Username - Enter the username provided by your ISP.

Password - Enter the password provided by your ISP.

IP Address Assignment Method (IPCP) for secondary ISP setup

In most environments, you should not change these settings as most ISPs provide a dynamic IP address for the router when it connects to the ISP. If your ISP provides a fixed IP address, check **Yes** and enter the IP address in the field of **Fixed IP Address**.

After entering the necessary settings and clicking **OK**, you will see **Goto ISDN Diagnostic** link appears on the bottom of the webpage. To have an ISDN connection, please click this link.

[ISDN >> Dialing to a Single ISP](#)

Active Configuration

ISP Access Setup ISP Name <input type="text"/> Dial Number <input type="text" value="30"/> Username <input type="text" value="vivian"/> Password <input type="password" value="••••••"/> <input type="checkbox"/> Require ISP callback Index(1-15) in Schedule Setup: => <input type="text"/> , <input type="text"/> , <input type="text"/> , <input type="text"/> >> Goto ISDN Diagnostic	PPP/MP Setup Link Type <input type="text" value="Dialup BOD"/> PPP Authentication <input type="text" value="PAP or CHAP"/> Idle Timeout 180 second(s) IP Address Assignment Method (IPCP) Fixed IP <input type="radio"/> Yes <input checked="" type="radio"/> No (Dynamic IP) Fixed IP Address
---	--

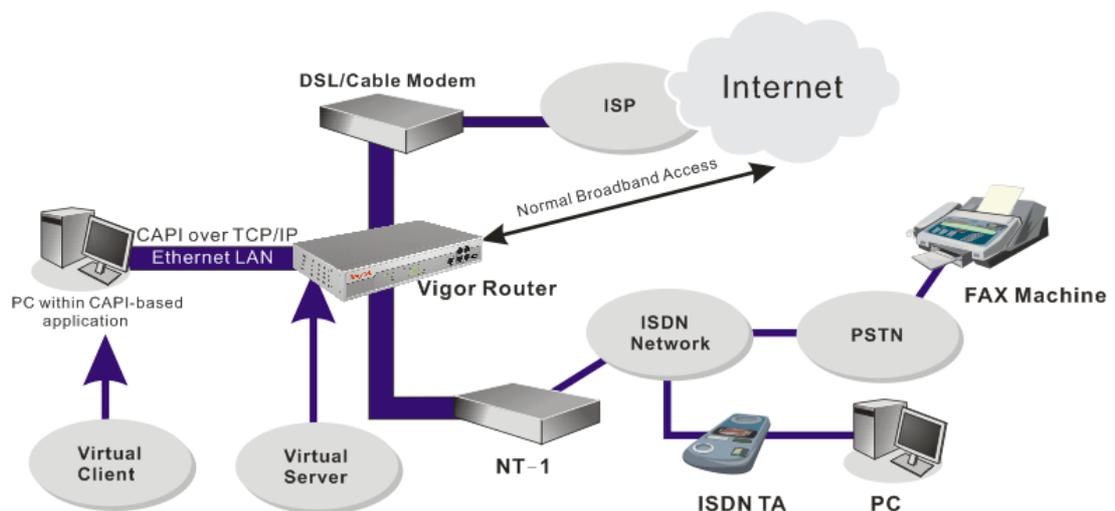
Now, the system will guide you to click **Dial ISDN**. Wait for a moment after clicking the dial link. Then, a successful ISDN connection will be shown as the following.

Online Status

System Status				System Uptime: 2:33:16			
LAN Status		Primary DNS: 194.109.6.66		Secondary DNS: 168.95.1.1			
IP Address		TX Packets		RX Packets			
192.168.1.1		12160		10217			
WAN 1 Status							
Enable	Line	Name	Mode	Up Time			
Yes	Ethernet		Static IP	2:33:06			
IP	GW IP	TX Packets	TX Rate(Bps)	RX Packets	RX Rate(Bps)		
172.16.3.229	172.16.3.4	8694	27	18977	499		
WAN 2 Status							
Enable	Line	Name	Mode	Up Time			
Yes	Ethernet		---	00:00:00			
IP	GW IP	TX Packets	TX Rate(Bps)	RX Packets	RX Rate(Bps)		
---	---	0	0	0	0		
ISDN Status							
				>> Dial ISDN	>> Drop B1	>> Drop B2	
Channel	Active Connection	TX Pkts	TX Rate (Bps)	RX Pkts	RX Rate (Bps)	Up Time	AOC
ISDN1-B1	[192.168.225.200]	19	4	18	4	0:0:46	0
ISDN1-B2	[192.168.225.200]	13	3	14	3	0:0:43	0

3.12.4 Virtual TA

Virtual TA means the local hosts or PCs in the network that uses popular CAPI-based software such as RVS-COM or BVRP to access the router as a local ISDN TA for sending or receiving FAX messages over the ISDN line. Basically, it is a client/server network model. The built-in Virtual TA server handles the establishment and release of connections. The Virtual TA client, which is installed on the local hosts or PCs, creates a CAPI-based driver to relay all CAPI messages between the applications and the router CAPI module. Before describing the configuration of **Virtual TA** in the Vigor routers, please notice the following limitations.



As depicted in the above application scenario, the Virtual TA client can make an outgoing call or accept an incoming call to/from a peer FAX machine or ISDN TA, etc. Click the **Virtual TA(Remote CAPI) Setup** tab in the **Quick Setup** field to configure the Virtual TA features.

Before describing the configuration of Virtual TA in the Vigor routers, please heed the following limitations.

- The Virtual TA client only supports Microsoft™ Windows 98/SE/2000/XP platforms.
- The Virtual TA client only supports the CAPI 2.0 protocol and has no built-in FAX engine.
- One ISDN BRI interface has two B channels. The maximum number of active clients is also 2.

Before you configure the Virtual TA, you must set the correct country code in **ISDN Setup**.

ISDN >> Virtual TA

Virtual TA Setup

Virtual TA Server : Enable Disable

Virtual TA Users Profiles						
	Username	Password	MSN1	MSN2	MSN3	Active
1.	<input type="text"/>	<input type="checkbox"/>				
2.	<input type="text"/>	<input type="checkbox"/>				
3.	<input type="text"/>	<input type="checkbox"/>				
4.	<input type="text"/>	<input type="checkbox"/>				
5.	<input type="text"/>	<input type="checkbox"/>				

Virtual TA Server

Enable - Select it to activate the server.

Disable - Select it to deactivate the server. All Virtual TA applications will be terminated.

Virtual TA User Profiles

Username - Enter the username of a specific client.

Password - Enter the password of a specific client.

MSN 1/2/3 - MSN stands for Multiple Subscriber Number. It means you can apply to more than one ISDN lines number over a single subscribed line. Note that the service must be acquired from your telecom. Specify the MSN numbers for a specific client. If you have no MSN services, leave this field blank.

Active - Check it to enable the client to access the server.

Install a Virtual TA Client

1. Insert the CD-ROM bundled with your Vigor router. Find **VTA Client** tool in the Utility menu and click on the Install button.
2. Follow the on-screen instructions of the installer. The last step will ask you to restart your computer. Click **OK** to restart your computer.
3. After the computer restarts, you will see a VT icon in the taskbar (usually in the bottom-right of the screen, near the clock) as shown below.

When the icon text is GREEN, the Virtual TA client is connected to the Virtual TA server and you can launch your CAPI-based software to use the client to access the router. If the icon

text is RED, it means the client has lost the connection to the server. This time, please check the physical Ethernet connection.



Configure a Virtual TA Client/ Server

Since the Virtual TA application is a client/server network model, you must configure it on both ends to run properly your Virtual TA application.

By default, the Virtual TA server is enabled and the Username/Password fields are left blank. Any Virtual TA client may login to the server. Once a single Username/Password field has been filled in, the Virtual TA server will only allow clients with a valid Username/Password to login. The screen of Virtual TA configuration is presented below.

User Profile

Note that creating a single user access account will limit the access to the Virtual TA server to only the specified account holders.

Assume you did not acquire any MSN service from your ISDN network provider.

On the server - Click **Virtual TA (Remote CAPI) Setup** link, and fill in the Username and Password fields. Check the **Active** box to enable the account.

ISDN >> Virtual TA

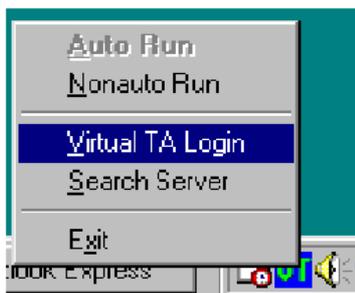
Virtual TA Setup

Virtual TA Server : Enable Disable

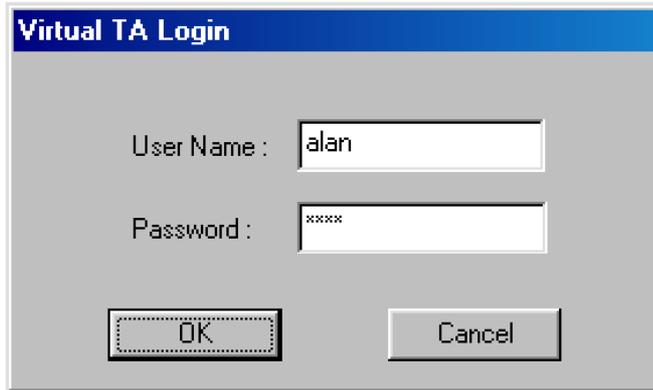
Virtual TA Users Profiles

	Username	Password	MSN1	MSN2	MSN3	Active
1.	alan	••••				<input checked="" type="checkbox"/>

On the client - Right-click the mouse on the VT icon. The following pop-up menu will be shown.



Click the **Virtual TA Login** tab to launch the login box.



The image shows a 'Virtual TA Login' dialog box with a blue title bar. It contains two text input fields: 'User Name' with the value 'alan' and 'Password' with the value 'xxxx'. Below the fields are two buttons: 'OK' and 'Cancel'.

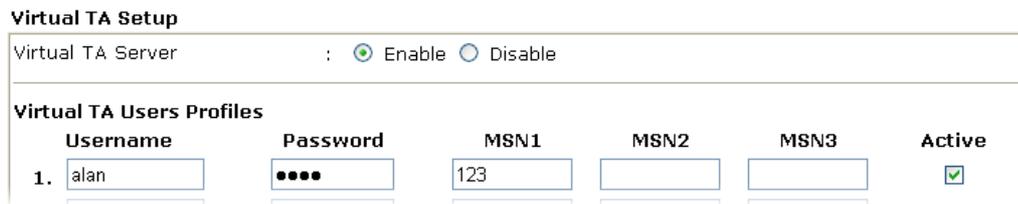
Enter the Username/Password and then click **OK**. After a short time, the VT icon text will turn green.

MSN Configuration

If you have applied to an MSN number service, the Virtual TA server can assign which client has the specified MSN number. When an incoming call arrives, the server will inform the appropriate client. Now we set an example to describe the configuration of the MSN number.

Suppose that you could assign the MSN number **123** to the client "alan".

ISDN >> Virtual TA



The image shows the 'Virtual TA Setup' configuration screen. At the top, there is a section for 'Virtual TA Server' with radio buttons for 'Enable' (selected) and 'Disable'. Below this is a table titled 'Virtual TA Users Profiles' with columns for Username, Password, MSN1, MSN2, MSN3, and Active. The first row shows a profile for 'alan' with a password of 'xxxx', MSN1 of '123', and the 'Active' checkbox checked.

	Username	Password	MSN1	MSN2	MSN3	Active
1.	alan	xxxx	123			<input checked="" type="checkbox"/>

Type the specified MSN number in the CAPI-based software. When the Virtual TA server sends an alert signal to the specified Virtual TA client, the CAPI-based software will also receive the action, the software will not accept the incoming call.

3.12.5 Call Control

Some applications require that the router (only for the ISDN models) be remotely activated, or be able to dial up to the ISP via the ISDN interface. Vigor routers provide this feature by allowing user to make a phone call to the router and then ask it to dial up to the ISP.

Accordingly, a teleworker can access the remote network to retrieve resources. Of course, a fixed IP address is required for WAN connection and some internal network resource has to be exposed for remote users, such as FTP, WWW.

Call Control Setup			
Dial Retry	<input type="text" value="0"/>	times	Remote Activation <input type="text"/>
Dial Delay Interval	<input type="text" value="0"/>	second(s)	

PPP/MP Dial-Out Setup			
Basic Setup		Bandwidth On Demand (BOD) Setup	
Link Type	<input type="text" value="Dialup BOD"/>	High Water Mark	<input type="text" value="7000"/> cps
PPP Authentication	<input type="text" value="PAP or CHAP"/>	High Water Time	<input type="text" value="30"/> second(s)
TCP Header Compression	<input type="text" value="None"/>	Low Water Mark	<input type="text" value="6000"/> cps
Idle Timeout	<input type="text" value="180"/> second(s)	Low Water Time	<input type="text" value="30"/> second(s)

Call Control Setup

Dial Retry - It specifies the dial retry counts per triggered packet. A triggered packet is the packet whose destination is outside the local network. The default setting is no dial retry. If set to 5, for each triggered packet, the router will dial 5 times until it is connected to the ISP or remote access router.

Dial Delay Interval - It specifies the interval between dialup retries. By default, the interval is 0 second.

Remote Activation – It can help users who would like to access the server which is off the Internet in the head office. To remotely make the server to be available on the Internet, i.e. make the router in the head office activating its Internet access either by dialing-up or starting broadband connection, users can make a regular phone call (the number is set in the Remote Activation field) to the router as signaling it for activation. The phone call will be soon disconnected once the router is on line.

Note that **Dialing to a Single ISP** should be pre-configured properly.

Basic Setup

Link Type - Because ISDN has two B channels (64Kbps/per channel), you can specify whether you would like to have single B channel, two B channels or BOD (Bandwidth on Demand). Four options are available: Link Disable, Dialup 64Kbps, Dialup 128Kbps, Dialup BOD.

Link Type

Dialup BOD ▾

Link Disable

Dialup 64Kbps

Dialup 128Kbps

Dialup BOD

PPP Authentication - It specifies the PPP authentication method for PPP/MP connections. Normally you can set it to PAP/CHAP for better compatibility.

TCP Header Compression - VJ Compression: It is used for TCP/IP protocol header compression. Normally it is set to Yes to improve bandwidth utilization.

Bandwidth-On-Demand (BOD) Setup

Idle Timeout - Because our ISDN link type is **Dial On Demand**, the connection will be initiated only when needed.

Bandwidth-On-Demand is for Multiple-Link PPP (ML-PPP or MP). The parameters are only applied when you set the **Link Type** to **Dialup BOD**. The ISDN usually use one B channel to access the Internet or remote network when you choose the Dialup BOD link type. The router will use the parameters here to decide on when you activate/drop the additional B channel. Note that **cps** (characters-per-second) measures the total link utilization.

High Water Mark and High Water Time - These parameters specify the situation in which the second channel will be activated. With the first connected channel, if its utilization exceeds the High Water Mark and such a channel is being used over the High Water Time, the additional channel will be activated. Thus, the total link speed will be 128kbps (two B channels).

Low Water Mark and Low Water Time - These parameters specify the situation in which the second channel will be dropped. In terms of the two B channels, if their utilization is under the Low Water Mark and these two channels are being used over the High Water Time, the additional channel will be dropped. As a result, the total link speed will be 64kbps (one B channel).

3.13 Wireless LAN

This function is used for G models only.

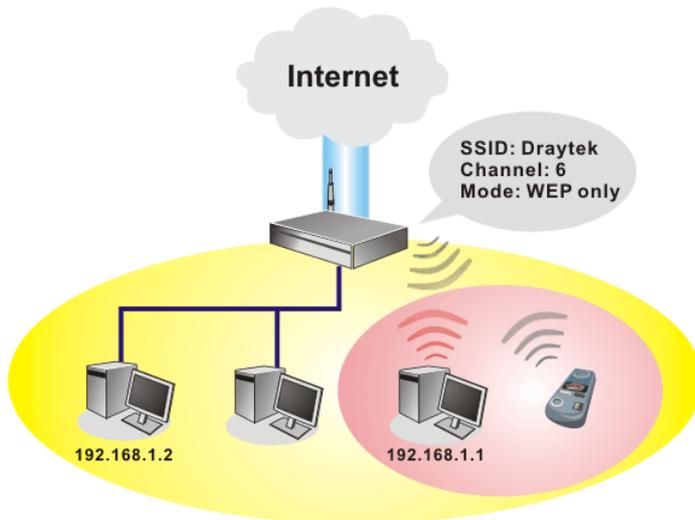
3.13.1 Basic Concepts

Over recent years, the market for wireless communications has enjoyed tremendous growth. Wireless technology now reaches or is capable of reaching virtually every location on the surface of the earth. Hundreds of millions of people exchange information every day via wireless communication products. The Vigor G model, a.k.a. Vigor wireless router, is designed for maximum flexibility and efficiency of a small office/home. Any authorized staff can bring a built-in WLAN client PDA or notebook into a meeting room for conference without laying a clot of LAN cable or drilling holes everywhere. Wireless LAN enables high mobility so WLAN users can simultaneously access all LAN facilities just like on a wired LAN as well as Internet access.

The Vigor wireless routers are equipped with a wireless LAN interface compliant with the standard IEEE 802.11g protocol. To boost its performance further, the Vigor Router is also loaded with advanced wireless technology Super G™ to lift up data rate up to 108 Mbps*. Hence, you can finally smoothly enjoy stream music and video.

Note: * The actual data throughput will vary according to the network conditions and environmental factors, including volume of network traffic, network overhead and building materials.

In an Infrastructure Mode of wireless network, Vigor wireless router plays a role as an Access Point (AP) connecting to lots of wireless clients or Stations (STA). All the STAs will share the same Internet connection via Vigor wireless router. The **General Settings** will set up the information of this wireless network, including its SSID as identification, located channel etc.



Security Overview

Real-time Hardware Encryption: Vigor Router is equipped with a hardware AES encryption engine so it can apply the highest protection to your data without influencing user experience.

Complete Security Standard Selection: To ensure the security and privacy of your wireless communication, we provide several prevailing standards on market.

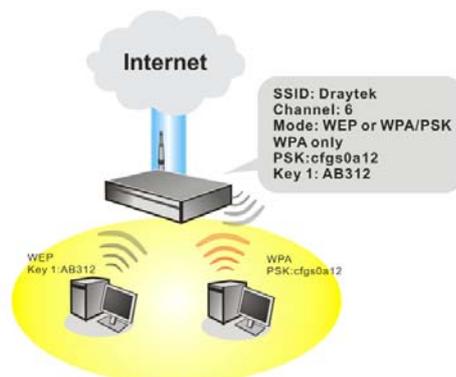
WEP (Wired Equivalent Privacy) is a legacy method to encrypt each frame transmitted via radio using either a 64-bit or 128-bit key. Usually access point will preset a set of four keys and it will communicate with each station using only one out of the four keys.

WPA(Wi-Fi Protected Access), the most dominating security mechanism in industry, is separated into two categories: WPA-personal or called WPA Pre-Share Key (WPA/PSK), and WPA-Enterprise or called WPA/802.1x.

In WPA-Personal, a pre-defined key is used for encryption during data transmission. WPA applies Temporal Key Integrity Protocol (TKIP) for data encryption while WPA2 applies AES. The WPA-Enterprise combines not only encryption but also authentication.

Since WEP has been proved vulnerable, you may consider using WPA for the most secure connection. You should select the appropriate security mechanism according to your needs. No matter which security suite you select, they all will enhance the over-the-air data protection and /or privacy on your wireless network. The Vigor wireless router is very flexible and can support multiple secure connections with both WEP and WPA at the same time.

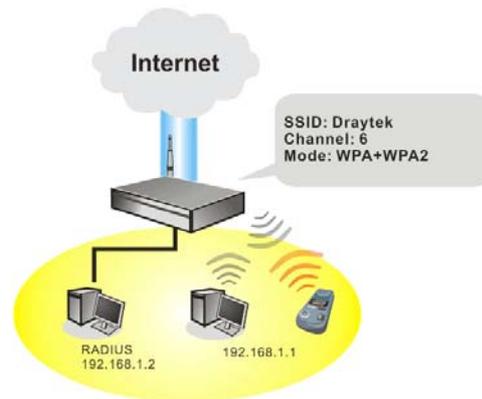
Example 1



Example 2



Example 3



Separate the Wireless and the Wired LAN- WLAN Isolation enables you to isolate your wireless LAN from wired LAN for either quarantine or limit access reasons. To isolate means neither of the parties can access each other. To elaborate an example for business use, you may set up a wireless LAN for visitors only so they can connect to Internet without hassle of the confidential information leakage. For a more flexible deployment, you may add filters of MAC addresses to isolate users' access from wired LAN.

Manage Wireless Stations - Station List will display all the station in your wireless network and the status of their connection.

Below shows the menu items for Wireless LAN.

- Wireless LAN
 - ▶ General Setup
 - ▶ Security
 - ▶ Access Control
 - ▶ WDS
 - ▶ AP Discovery
 - ▶ Station List
 - ▶ Station Rate Control

3.13.2 General Setup

By clicking the **General Settings**, a new web page will appear so that you could configure the SSID and the wireless channel. Please refer to the following figure for more information.

Wireless LAN >> General Setup

General Setting (IEEE 802.11)

Enable Wireless LAN

Mode:

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

SSID:

Channel :

Note: If SuperG mode is enabled, channel is fixed at 6.

Hide SSID

Long Preamble

Hide SSID: prevent SSID from being scanned.
Long Preamble: necessary for some older 802.11b devices only (lowers performance).

Enable Wireless LAN

Check the box to enable wireless function.

Mode

Select an appropriate wireless mode.

Mixed (11b+11g+SuperG) - The radio can support IEEE802.11b, IEEE802.11g and SuperG protocols simultaneously.

Mixed (11b+11g) - The radio can support both IEEE802.11b and IEEE802.11g protocols simultaneously.

SuperG - The radio only supports SuperG.

11g only - The radio only supports IEEE802.11g.

11b only - The radio only supports IEEE802.11b.

Mode :

Mixed(11b+11g)	▼
Mixed(11b+11g+SuperG)	
Mixed(11b+11g)	
SuperG Only	
11g Only	
11b Only	

Index(1-15)

Set the wireless LAN to work at certain time interval only. You may choose up to 4 schedules out of the 15 schedules pre-defined in **Applications >> Schedule** setup. The default setting of this field is blank and the function will always work.

SSID

The default SSID is "default". We suggest you change it to a particular name. It is the identification of the wireless LAN. SSID can be any text numbers or various special characters.

Channel

The channel of frequency of the wireless LAN. The default channel is 6. You may switch channel if the

selected channel is under serious interference.

Channel :

Channel 6, 2437MHz	▼
Channel 1, 2412MHz	
Channel 2, 2417MHz	
Channel 3, 2422MHz	
Channel 4, 2427MHz	
Channel 5, 2432MHz	
Channel 6, 2437MHz	
Channel 7, 2442MHz	
Channel 8, 2447MHz	
Channel 9, 2452MHz	
Channel 10, 2457MHz	
Channel 11, 2462MHz	
Channel 12, 2467MHz	
Channel 13, 2472MHz	

Hide SSID

Check it to prevent from wireless sniffing and make it harder for unauthorized clients or STAs to join your wireless LAN. Depending on the wireless utility, the user may only see the information except SSID or just cannot see any thing about Vigor wireless router while site surveying.

Long Preamble This option is to define the length of the sync field in an 802.11 packet. Most modern wireless network uses short preamble with 56 bit sync field instead of long preamble with 128 bit sync field. However, some original 11b wireless network devices only support long preamble. Check it to use **Long Preamble** if needed to communicate with this kind of devices.

3.13.3 Security

By clicking the **Security Settings**, a new web page will appear so that you could configure the settings of WEP and WPA.

Wireless LAN >> Security Settings

Security Settings

Mode :

Set up **RADIUS Server** if 802.1x is enabled.

WPA:
 Type: Mixed(WPA+WPA2) WPA2 Only
 Pre-Shared Key(PSK)

Type 8~63 ASCII character or 64 Hexadecimal digits leading by "0x", for example "cfigs01a2..." or "0x655abcd....".

WEP:
 Encryption Mode:
 Use WEP Key

Key 1 :
 Key 2 :
 Key 3 :
 Key 4 :

For 64 bit WEP key
 Type 5 ASCII character or 10 Hexadecimal digits leading by "0x", for example "AB312" or "0x4142333132".

For 128 bit WEP key
 Type 13 ASCII character or 26 Hexadecimal digits leading by "0x", for example "0123456789abc" or "0x30313233343536373839414243".

Mode

There are several modes provided for you to choose.

Mode :

- WEP Only
- Disable
- WEP Only
- WEP/802.1x Only
- WEP or WPA/PSK
- WEP/802.1x or WPA/802.1x
- WPA/PSK Only
- WPA/802.1x Only

Disable - Turn off the encryption mechanism.

WEP Only - Accepts only WEP clients and the encryption key should be entered in WEP Key.

WEP/802.1x Only - Accept WEP clients with 802.1x authentication. Since the key will be auto-negotiated during authentication, the field of key setting below will be not available for input.

WEP or WPA/PSK - Accepts WEP and WPA clients with legal key accordingly. Only Mixed (WPA+WPA2) is applicable if you select WPA/PSK.

WEP/802.1x or WPA/802.1x - Accept WEP or WPA clients with 802.1x authentication. Only Mixed(WPA+WPA2) is applicable if you select WPA/PSK. Since the key will be auto-negotiated during authentication, the field of key setting below will be not available for input.

WPA/PSK Only - Accepts WPA clients and the encryption key should be entered in PSK. Remember to select WPA type to define either Mixed or WPA2 only in the field below.

WPA/802.1x Only - Accept WPA clients with 802.1x authentication. Remember to select WPA type to define either Mixed or WPA2 only in the field below. Since the key will be auto-negotiated during authentication, the field of key setting below will be not available for input.

WPA

The WPA encrypts each frame transmitted from the radio using the key, which either PSK entered manually in this field below or automatically negotiated via 802.1x authentication.

Type - Select from Mixed (WPA+WPA2) or WPA2 only.

Pre-Shared Key (PSK) - Either **8~63** ASCII characters, such as 012345678..(or 64 Hexadecimal digits leading by 0x, such as "0x321253abcde...").

WEP

64-Bit - For 64 bits WEP key, either **5** ASCII characters, such as 12345 (or 10 hexadecimal digitals leading by 0x, such as 0x4142434445.)

128-Bit - For 128 bits WEP key, either **13** ASCII characters, such as ABCDEFGHIJKLM (or 26 hexadecimal digits leading by 0x, such as 0x4142434445464748494A4B4C4D).

Encryption Mode:



A dropdown menu with a blue border. The top part shows '64-Bit' with a downward arrow. Below it, a list is open showing '64-Bit' (highlighted in blue) and '128-Bit'.

All wireless devices must support the same WEP encryption bit size and have the same key. Four keys can be entered here, but only one key can be selected at a time. The keys can be entered in ASCII or Hexadecimal. Check the key you wish to use.

3.13.4 Access Control

For additional security of wireless access, the **Access Control** facility allows you to restrict the network access right by controlling the wireless LAN MAC address of client. Only the valid MAC address that has been configured can access the wireless LAN interface. By clicking the **Access Control**, a new web page will appear, as depicted below, so that you could edit the clients' MAC addresses to control their access rights.

Wireless LAN >> Access Control

OK Clear All

Enable Access Control

Select to enable the MAC Address access control feature.

Policy

Select to enable any one of the following policy. Choose **Activate MAC address filter** to type in the MAC addresses for other clients in the network manually. Choose **Isolate WLAN from LAN** will separate all the WLAN stations from LAN based on the MAC Address list. Choose **Blocked MAC address filter** will block all the WLAN stations from LAN based on the MAC Address list.

Policy :

MAC Address Filter

Display all MAC addresses that are edited before. Four buttons (Add, Remove, **Client's MAC Address** - Manually enter the MAC address of wireless client.

Attribute

s - select to isolate the wireless connection of the wireless client of the MAC address from LAN.

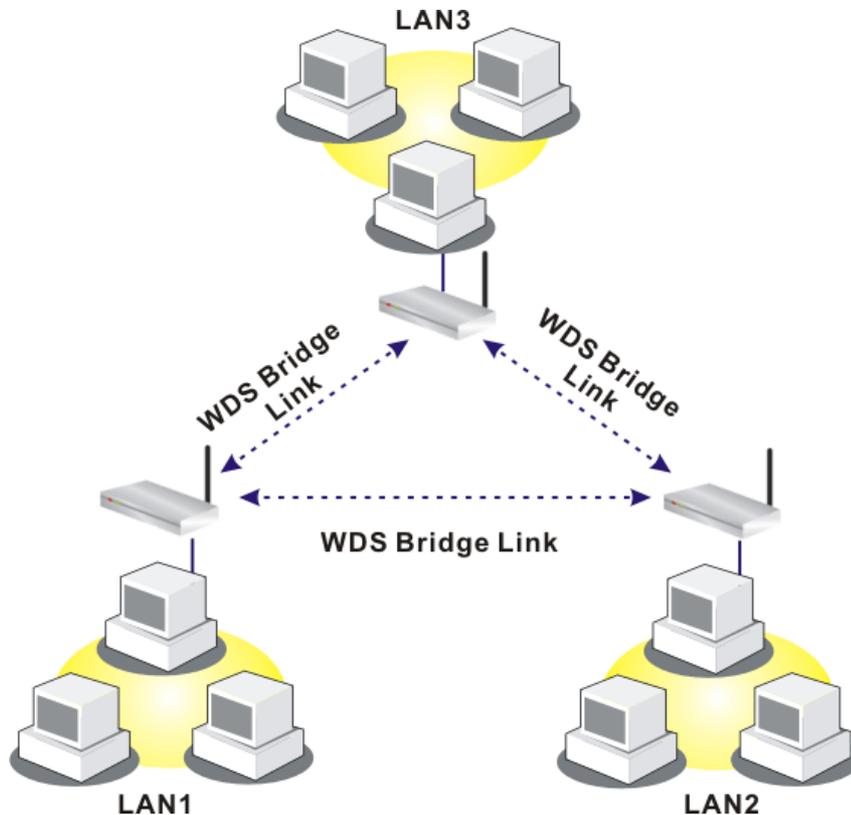
Add	Add a new MAC address into the list.
Delete	Delete the selected MAC address in the list.
Edit	Edit the selected MAC address in the list.
Cancel	Give up the access control set up.
OK	Click it to save the access control list.
Clear All	Clean all entries in the MAC address list.

3.13.5 WDS

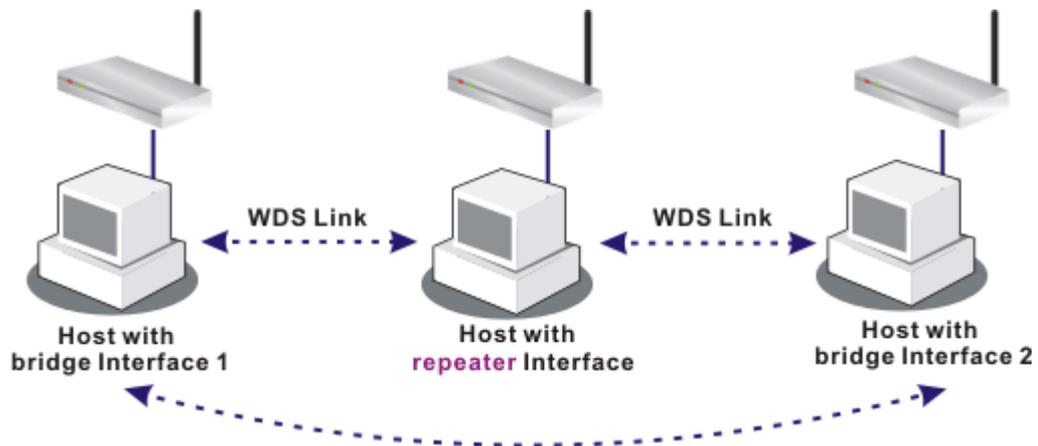
WDS means Wireless Distribution System. It is a protocol for connecting two access points (AP) wirelessly. Usually, it can be used for the following application:

- Provide bridge traffic between two LANs through the air.
- Extend the coverage range of a WLAN.

To meet the above requirement, two WDS modes are implemented in Vigor router. One is **Bridge**, the other is **Repeater**. Below shows the function of WDS-bridge interface:

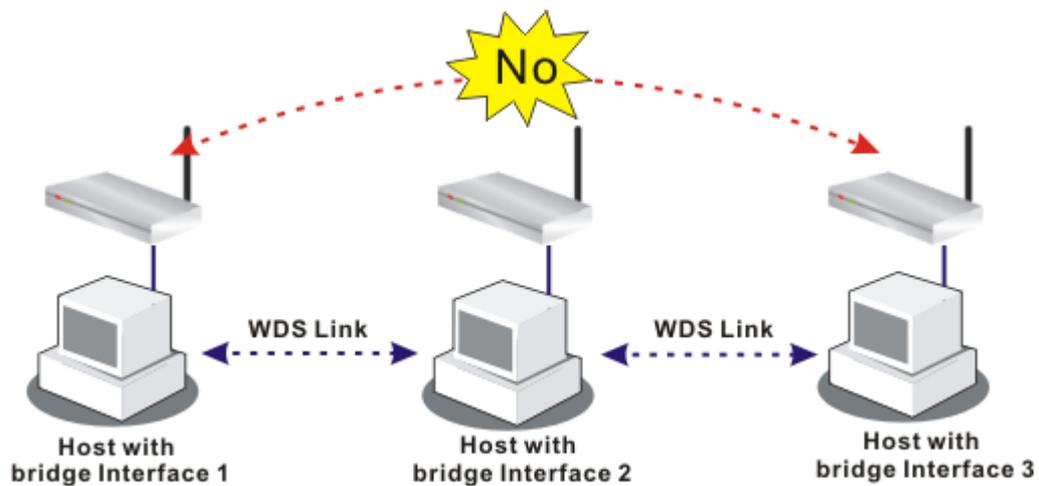


The application for the WDS-Repeater mode is depicted as below:



The major difference between these two modes is that: while in **Repeater** mode, the packets received from one peer AP can be repeated to another peer AP through WDS links. Yet in **Bridge** mode, packets received from a WDS link will only be forwarded to local wired or wireless hosts. In other words, only Repeater mode can do WDS-to-WDS packet forwarding.

In the following examples, hosts connected to Bridge 1 or 3 can communicate with hosts connected to Bridge 2 through WDS links. However, hosts connected to Bridge 1 CANNOT communicate with hosts connected to Bridge 3 through Bridge 2.



Click **WDS** from **Wireless LAN** menu. The following page will be shown.

WDS Settings
| [Set to Factory Default](#) |

Mode: Repeater ▾

Security:

Disable WEP Pre-shared Key

WEP:

Use the same WEP key set in **Security Settings**.

Encryption Mode: 64-bit ▾

Key index: 1 ▾

The key index is fixed if the security mode is not "WEP Only".

Key:

The key format is the same as the one used in **Security Settings**.

Pre-shared Key:

Type: TKIP

Key:

Type 8~63 ASCII characters or 64 hexadecimal digits leading by "0x", for example "cfgs01a2..." or "0x655abcd....".

Bridge

Enable	Peer MAC Address
<input type="checkbox"/>	<input type="text" value=": : : : :"/>
<input type="checkbox"/>	<input type="text" value=": : : : :"/>
<input type="checkbox"/>	<input type="text" value=": : : : :"/>
<input type="checkbox"/>	<input type="text" value=": : : : :"/>
<input type="checkbox"/>	<input type="text" value=": : : : :"/>
<input type="checkbox"/>	<input type="text" value=": : : : :"/>

Note: Disable unused links to get better performance.

Repeater

Enable	Peer MAC Address
<input type="checkbox"/>	<input type="text" value=": : : : :"/>
<input type="checkbox"/>	<input type="text" value=": : : : :"/>

Access Point Function:

Enable Disable

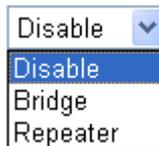
Status:

Send "Hello" message to peers.

Note: The status is valid only when the peer also supports this function.

Mode

Choose the mode for WDS setting. **Disable** mode will not invoke any WDS setting. **Bridge** mode is designed to fulfill the first type of application. **Repeater** mode is for the second one.



Security

There are three types for security, **Disable**, **WEP** and **Pre-shared key**. The setting you choose here will make the following WEP or Pre-shared key field valid or not. Choose one of the types for the router.

WEP

Check this box to use the same key set in **Security Settings** page. If you did not set any key in **Security Settings** page, this check box will be dimmed.

Settings

Encryption Mode - If you checked the box of **Use the same WEP key ...**, you do not need to choose 64-bit or 128-bit as the Encryption Mode. If you do not check that box, you can set the WEP key now in this page.

Key Index - Choose the key that you want to use after selecting the proper encryption mode.

Key - Type the content for the key.

Pre-shared Key	Type 8 ~ 63 ASCII characters or 64 hexadecimal digits leading by “0x”.
Bridge	If you choose Bridge as the connecting mode, please type in the peer MAC address in these fields. Six peer MAC addresses are allowed to be entered in this page at one time. Yet please disable the unused link to get better performance. If you want to invoke the peer MAC address, remember to check Enable box in the front of the MAC address after typing.
Repeater	If you choose Repeater as the connecting mode, please type in the peer MAC address in these fields. Two peer MAC addresses are allowed to be entered in this page at one time. Similarly, if you want to invoke the peer MAC address, remember to check Enable box in the front of the MAC address after typing.
Access Point Function	Click Enable to make this router serving as an access point; click Disable to cancel this function.
Status	It allows user to send “hello” message to peers. Yet, it is valid only when the peer also supports this function.

3.13.6 AP Discovery

Vigor router can scan all regulatory channels and find working APs in the neighborhood. Based on the scanning result, users will know which channel is clean for usage. Also, it can be used to facilitate finding an AP for a WDS link. Notice that during the scanning process (about 5 seconds), no client is allowed to connect to Vigor.

This page is used to scan the existence of the APs on the wireless LAN. Yet, only the AP which is in the same channel of this router can be found. Please click **Scan** to discover all the connected APs.

Wireless LAN >> Access Point Discovery

Access Point List

BSSID	Channel	SSID

See [Statistics](#).

Note: During the scanning process (~5 seconds), no station is allowed to connect with the router.

Add to WDS Settings :

AP's MAC address : : : : :

Bridge Repeater

If you want the found AP applying the WDS settings, please type in the AP's MAC address on the bottom of the page and click Bridge or Repeater. Next, click **Add to**. Later, the MAC address of the AP will be added to Bridge or Repeater field of WDS settings page.

3.13.7 Station List

Station List provides the knowledge of connecting wireless clients now along with its status code. There is a code summary below for explanation. For convenient **Access Control**, you can select a WLAN station and click **Add to Access Control** below.

Wireless LAN >> Station List

Station List

Status	MAC Address	Associated with

Status Codes :
C: Connected, No encryption.
E: Connected, WEP.
P: Connected, WPA.
A: Connected, WPA2.
B: Blocked by Access Control.
N: Connecting.
F: Fail to pass WPA/PSK authentication.

Note: After a station connects to the router successfully, it may be turned off without notice. In that case, it will still be on the list until the connection expires.

Add to Access Control :

Client's MAC address : : : : :

Refresh

Click this button to refresh the status of station list.

Add

Click this button to add current selected MAC address into **Access Control**.

3.13.8 Station Rate Control

This page allows you to control the upload and download rate of each wireless client (station) and SSID1-4. Please check the box of **Enable** to invoke this setting. The range for the rate is between 100 ~ 100,000 kbps.

Wireless LAN >> Station Rate Control

Station Rate Control

Enable

Upload Rate : 00 Kbps
Download Rate : 00 Kbps

Note:
1. Range: 100~100,000 Kbps, Increment: 100 Kbps.
2. The specified rates are applied to each associated wireless client.

SSID rate control controls the data transmission rate through wireless connection.

Enable Check **Enable** for typing upload and download rate.

Upload Type the transmitting rate for data upload. Default value is 1,000 kbps.

Download Type the transmitting rate for data download. Default value is 1,000 kbps.

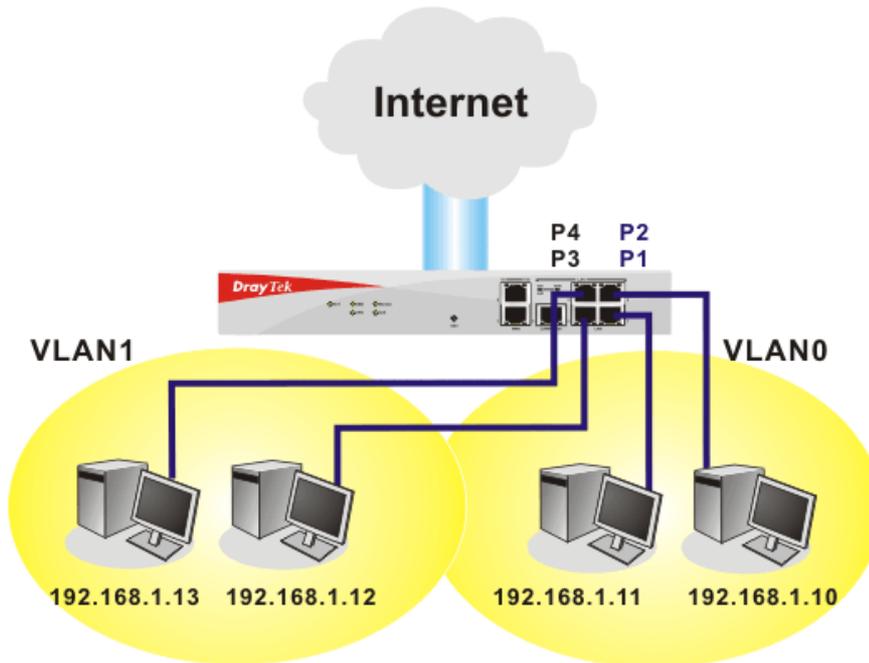
3.14 VLAN

Virtual LAN function provides you a very convenient way to manage hosts by grouping them based on the physical port. Such menu is available for Vigor5510Gi only.



3.14.1 Wired VLAN

PCs connected to Ethernet ports of the router can be divided into different groups and formed VLAN. PCs under the same groups can share each other information through the router and will not be peeked by other groups.



The **VLAN >> Wired VLAN** allows you to configure VLAN settings through wired connection to achieve the above intention. Simply check P1 and P2 boxes on the line of VLAN0; and check P3 and P4 boxes on the line of VLAN1.

VLAN >> Wired VLAN Configuration

Wired VLAN Configuration

<input type="checkbox"/> Enable					
	P1	P2	P3	P4	
VLAN0	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
VLAN1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
VLAN2	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
VLAN3	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	

OK Clear Cancel

Enable

Check this box to enable this function (for VLAN Configuration).

P1 – P4

Check the box to make the computer connecting to the port being grouped in specified VLAN. Be aware that each port can be grouped in different VLAN at the same time only if you check the box. For example, if you check the boxes of VLAN0-P1 and VLAN1-P1, you can make P1 to be grouped under VLAN0 and VLAN1 simultaneously.

VLAN0-3

This router allows you to set 4 groups of virtual LAN.

Wired VLAN Configuration

Enable

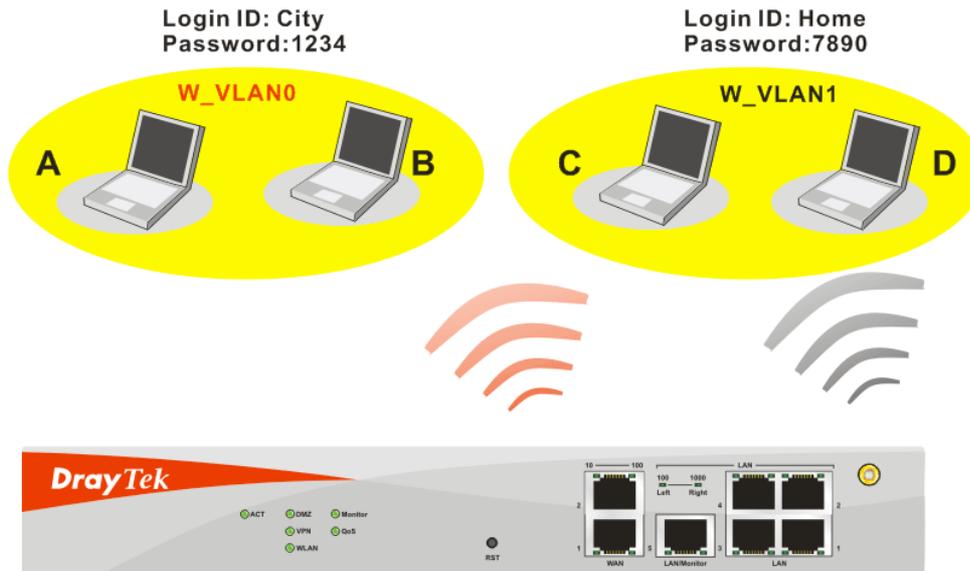
	P1	P2	P3	P4
VLAN0	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
VLAN1	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
VLAN2	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
VLAN3	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

OK Clear Cancel

3.14.2 Wireless VLAN

PCs (equipped with wireless network cards) connected to the router through wireless interface can be divided into different groups and formed W_VLAN. PCs under the same groups can share each other information through the router and will not be peeked by other groups.

PCs under the same groups can use same Login ID and password to access into Internet. For example, see the following graphic. Both A and B use the same login ID (City) and password (1234). Therefore, they are grouped in the same W_VLAN.



The VLAN >> Wireless VLAN allows you to configure Wireless VLAN settings through wireless connection to achieve the above intention. Simply type Login ID and password with **City** and **1234** in the boxes of W_VLAN0. And type Login ID and password with **Home** and **7890** in the boxes of W_VLAN1. Users can configure fifteen groups of wireless VLAN in this page.

Wireless VLAN Configuration

Enable View [Online Station Table](#)

W_VLAN	Login ID	Password	Attributes	W_VLAN	Login ID	Password	Attributes
0	city	1234	Details	8			Details
1	home	7890	Details	9			Details
2			Details	10			Details
3			Details	11			Details
4			Details	12			Details
5			Details	13			Details
6			Details	14			Details
7			Details	15			Details

Disable broadcast and multicast traffic.

Notes:
 1. Login ID: 1~11 characters, Password: 1~11 characters.
 2. Disable broadcast and multicast traffic to maximize wireless VLAN security; however, the WLAN throughput will be reduced.
 3. Login URL for wireless clients:
<http://www.draytek.vlan/login.htm> or [http://\(Vigor IP Address\)/login.htm](http://(Vigor IP Address)/login.htm)

Enable

Check this box to invoke wireless VLAN function.

Login ID

Type Login ID for different groups of W_VLAN with 1 to 11 characters.

Password

Type password for different groups of W_VLAN with 1 to 11 characters.

Details

Click this button to set additional attributes settings for W_VLAN.

VLAN >> Wireless VLAN Setup

W_VLAN Attributes

Activated Date: 2000 -1 -1

Expired Date: 2020 -12 -31

Connect all WDS links with this VLAN group.

Isolate each member in this VLAN group.

Activated Date – Use the drop down lists to set the activated date for the wireless VLAN. The wireless VLAN function will be available when the time is arrival.

Expired Date – Use the drop down lists to set the expired date for the wireless VALN. This function will be invalid when the time is arrival.

Connect all WDS links with this VALN group – Check this box to activate this connection.

Isolate each member in this VLAN group – Check this box to isolate all the members in this VLAN group and not allow the information sharing among them.

Disable broadcast and multicast traffic

Check this box to prevent broadcast and multicast traffic forwarding to all W_VLAN.

How can you (wireless client) access into Internet?

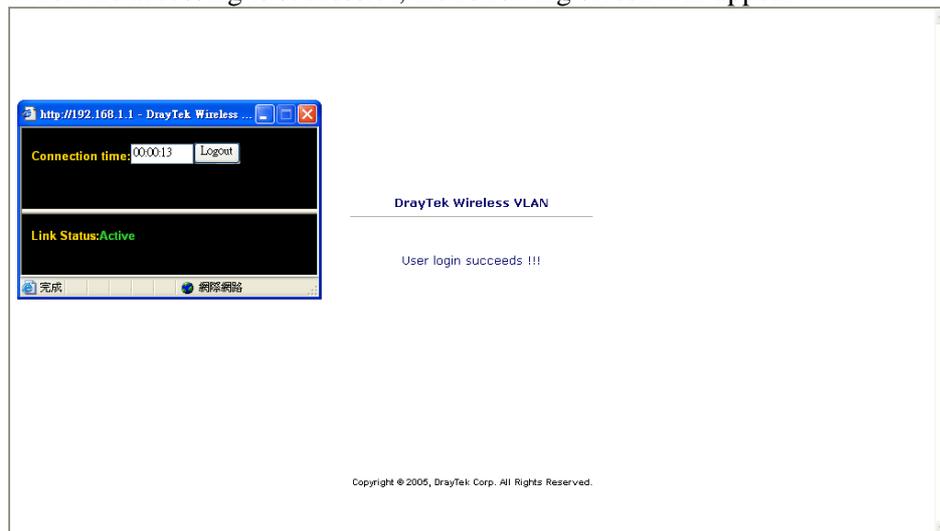
After finishing the configuration of wireless VLAN, the wireless clients connecting to this router must do the following steps to access into Internet.

1. Open a browser and type `http://www.draytek.vlan/login.htm` or `http://(vigor router's IP address)/login.htm` on the address line.
2. The following screen will appear.

DrayTek Wireless VLAN

Login ID	<input type="text" value="City"/>
Password	<input type="password" value="••••"/>

3. Type in Login ID and Password that was configured in Wireless VLAN Setup page. In this case, we choose the configuration set in first group of W_VLAN (City and 1234).
4. When the accessing is successful, the following screen will appear.



Note: The floating window with connection time will be shown on the screen till you logout.

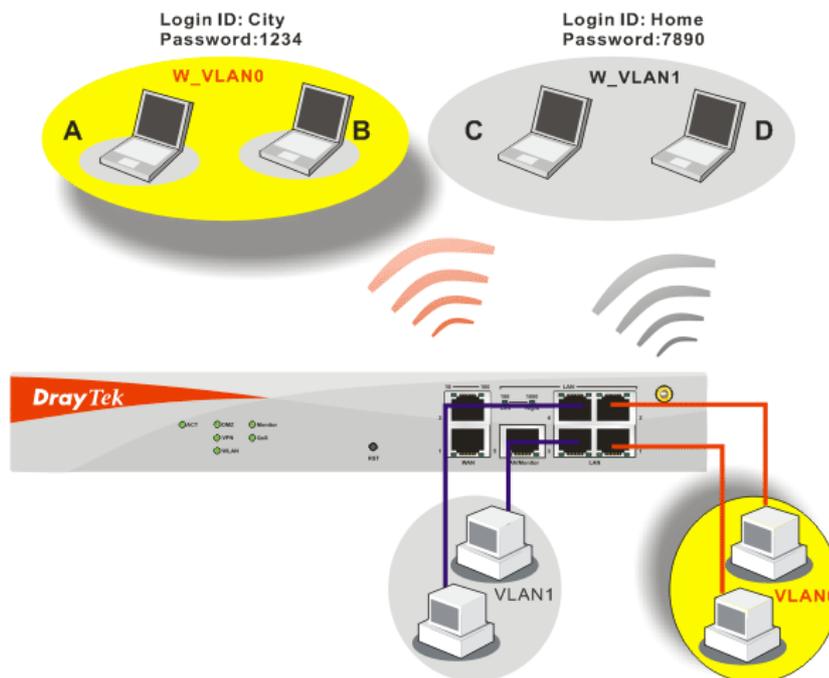
- You can go to **Diagnostics>>Wireless VLAN Online Station** for viewing the connection status whenever you want.

Diagnostics >> Wireless VLAN Online Station

Wireless VLAN Online Station Table			Refresh
IP Address	MAC Address	Login ID	
192.168.1.15	00-14-85-26-00-8C	City	
192.168.1.16	00-0E-35-A8-A4-E7	Home	

3.14.3 VLAN Cross Setup

This function allows the router to integrate VLAN and W_VLAN for managing different computers (notebooks). See the following picture for an example. With **VLAN Cross Setup**, notebook A/B and PCs on VLAN0 can share resources without difficulty.



The **VLAN >> VLAN Cross Setup** allows you to set a communication bridge between computers in Wireless VLAN and wired VLAN. To achieve the intention of the above illustration, simply check the box under VLAN0 on the line of W_VLAN0.

VLAN Cross Configuration

Enable

	VLAN0	VLAN1	VLAN2	VLAN3
W_VLAN0	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
W_VLAN1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
W_VLAN2	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
W_VLAN3	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
W_VLAN4	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
W_VLAN5	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
W_VLAN6	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
W_VLAN7	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
W_VLAN8	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
W_VLAN9	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
W_VLAN10	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
W_VLAN11	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
W_VLAN12	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
W_VLAN13	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
W_VLAN14	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
W_VLAN15	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
WDS	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Notes:
 1. W_VLANi: wireless VLAN i, see **Wireless VLAN Setup** for details.
 2. All WDS links belong to the same VLAN group.
 3. VLANi: wired VLAN i, see **Wired VLAN Setup** for details.
 4. Both wired and wireless VLANs must be enabled for VLAN cross settings to be effective.

Enable

Check this box to invoke VLAN Cross Setup function.

VLAN0-3

It represents the groups of virtual LAN connected by Ethernet interface.

W_VLAN0-15

It represents the groups of wireless VLAN communicated by wireless interface.

3.14.4 Wireless Rate Control

Rate Control manages the transmission rate of data in and out through the router. You can also manage the in/out rate of each wireless VLAN. Go to **VLAN** menu and select **Wireless Rate Control**. The following page will appear. Click **Enable** to invoke VLAN function.

For the rate control of wireless connection, please open VLAN menu and choose **Wireless Rate Control**. The following page will be shown for you to adjust.

VLAN >> Wireless VLAN Rate Control

Wireless VLAN Rate Control

Enable Range : 100~100,000 Kbps, Increment : 100 Kbps

W_VLAN	Upload Rate (Kbps)	Download Rate (Kbps)	W_VLAN	Upload Rate (Kbps)	Download Rate (Kbps)
0	1000 00	1000 00	8	1000 00	1000 00
1	1000 00	1000 00	9	1000 00	1000 00
2	1000 00	1000 00	10	1000 00	1000 00
3	1000 00	1000 00	11	1000 00	1000 00
4	1000 00	1000 00	12	1000 00	1000 00
5	1000 00	1000 00	13	1000 00	1000 00
6	1000 00	1000 00	14	1000 00	1000 00
7	1000 00	1000 00	15	1000 00	1000 00

Note: Specified rate is an aggregate rate for the VLAN group.

Enable Check this box to enable this function (for Rate Control). The rate control will limit the transmission rate for upload and download.

Upload Rate It decides the rate of data transmission for output. The default setting is 300. The range must be between 100 kbps to 20,000kbps. Adjust the values according to your necessity.

Download Rate It decides the rate of data transmission for input. The default setting is 300. The range must be between 100 kbps to 20,000kbps. Adjust the values according to your necessity.

3.15 SSL VPN

An SSL VPN (Secure Sockets Layer virtual private network) is a form of VPN that can be used with a standard Web browser.

There are two benefits that SSL VPN provides:

- It is not necessary for users to preinstall VPN client software for executing SSL VPN connection.
- There are less restrictions for the data encrypted through SSL VPN in comparing with traditional VPN.



3.15.1 General Setup

This page determines the general configuration for SSL VPN Server and SSL Tunnel.

SSL VPN >> General Setup

SSL VPN General Setup

Port	<input type="text" value="443"/> (Default: 443)
Server Certificate	<input type="text" value="self-signed"/> ▼
Encryption Key Algorithm	<input type="radio"/> High - AES(128 bits) and 3DES <input checked="" type="radio"/> Default - RC4(128 bits) <input type="radio"/> Low - DES

Note: The settings will act on all SSL applications.

Port Such port is set for SSL VPN server. It will not affect the HTTPS Port configuration set in **System Maintenance>>Management**. In general, the default setting is 443.

Server Certificate When the client does not set any certificate, default certificate will be used for HTTPS and SSL VPN server. Choose any one of the user-defined certificates from the drop down list if users set several certificates previously. Otherwise, choose **Self-signed** to use the router's built-in default certificate. The default certificate can be used in SSL VPN server and HTTPS Web Proxy.

Encryption Key Algorithm Choose the encryption level for the data connection in SSL VPN server.

3.15.2 SSL Web Proxy

SSL Web Proxy will allow the remote users to access the internal web sites over SSL. It is used to access web servers on LAN side from browser. With such function, user(s) or administrator (s) can register and access the specified web server on LAN behind the router through any web browser.

Such page allows you to set interior web server profiles.

Web Access Control >> SSL Web Proxy

SSL Web Proxy Servers Profiles: | [Set to Factory Default](#) |

Index	Name	URL	Active
1.			x
2.			x
3.			x
4.			x
5.			x
6.			x
7.			x
8.			x
9.			x
10.			x
11.			x
12.			x
13.			x
14.			x
15.			x
16.			x
17.			x

- Name** Display the name of the profile that you create.
- URL** Display the URL.
- Active** Display current status (active or inactive) of such profile.

Click number link under Index field to set detailed configuration.

SSL VPN >> SSL Web Proxy

Profile Index : 1

Name

URL

Host IP Address

Access Method Disable ▾

Note: URL format must be entered as http://Domain_name/directory where Domain_name is a FQDN.

- Name** Type name of the profile.
- URL** Type the address (function variation or IP address) or path of the proxy server.
- Host IP Address** If you type function variation as URL, you have to type

corresponding IP address in this field. Such field must match with URL setting.

Access Method

There are three modes for you to choose.

Disable – the profile will be inactive. If you choose **Disable**, all the web proxy profile appeared under VPN remote dial-in web page will disappear.

Secured Port Redirection – such technique applies private port mapping to random WAN port. There are two restrictions for proxy web server for such selection: 1) it is only used for WAN to LAN access, the web server must be configured behind vigor router; 2) web server gateway must be indicated to vigor router. In addition, users must execute “Connect” manually in SSL Client Portal page.

SSL – if you choose such selection, web proxy over SSL will be applied for VPN.

3.15.3 SSL Application

It provides a secure and flexible solution for network resources, including VNC (Virtual Network Computer) /RDP (Remote Desktop Protocol) /SAMBA, to any remote user with access to Internet and a web browser.

SSL VPN >> SSL Application

SSL Applications Profiles:

| [Set to Factory Default](#) |

Index	Name	Host Address	Service	Active
1.				x
2.				x
3.				x
4.				x
5.				x
6.				x
7.				x
8.				x
9.				x
10.				x

- Name** Display the application name of the profile that you create.
- Host Address** Display the IP address for VNC/RDP or SAMBA path.
- Service** Display the type of the service selected, e.g., VNC/RDP/SAMBA.
- Active** Display current status (active or inactive) of the selected profile.

Click number link under Index field to make detailed configuration.

Profile Index : 1

<input type="checkbox"/> Enable Application Service	
Application Name	<input type="text"/>
Application	---Please Select--- 

OK Clear Cancel

Enable Application Service

Check this box to enable this application.

Application Name

Type the profile name for the application.

Application

Use the drop down list to choose an application applied to this profile.

---Please Select--- 
---Please Select---
Virtual Network Computing (VNC)
Remote Desktop Protocol (RDP)
Samba Application

Different application type will lead different web pages. Refer to the following:

- **Virtual Network Computing** – Choose this item for accessing and controlling a remote PC through VNC protocol.

Profile Index : 1

<input type="checkbox"/> Enable Application Service	
Application Name	<input type="text"/>
Application	Virtual Network Computing (VNC) 
IP Address	<input type="text"/>
Port	5900
Scaling	100% 

OK Clear Cancel

IP Address

Type the IP address for this protocol.

Port

Specify the port used for this protocol. The default setting is 5900.

Scaling

Chose the percentage (100%, 80%, 60%) for such application.

- **Remote Desktop Protocol** - Choose this item for accessing and controlling a remote PC through RDP protocol.

SSL VPN >> SSL Application

Profile Index : 1

<input type="checkbox"/> Enable Application Service	
Application Name	<input type="text"/>
Application	Remote Desktop Protocol (RDP) ▾
IP Address	<input type="text"/>
Port	3389
Screen Size	1024*768 ▾

OK Clear Cancel

IP Address Type the IP address for this protocol.

Port Specify the port used for this protocol. The default setting is 3389.

Screen Size Chose the screen size for such application.

- **Samba Application** - Any remote user can upload/download/delete certain files on a local Samba server through web browser with this application.

SSL VPN >> SSL Application

Profile Index : 1

<input type="checkbox"/> Enable Application Service	
Application Name	<input type="text"/>
Application	Samba Application ▾
Samba Path	<input type="text"/>

Note: Samba Path format must be entered as \\ip\directory or \\Computer Name\directory.

OK Clear Cancel

Samba Path Specify the path for this application.

3.15.4 User Account

For SSL VPN, identity authentication and power management are implemented through deploying user accounts. Therefore, the user account for SSL VPN must be set together with remote dial-in user web page. Such menu item will guide to access into **VPN and Remote Access>>Remote Dial-in user**. For the detailed configuration of user account, please refer to section of **Remote Dial-in user**.

Remote Access User Accounts: | [Set to Factory Default](#) |

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

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

You can find out the link of Set SSL Web Proxy on the profile setting page. If you haven't set any SSL Web Proxy Profile in **SSL VPN>> SSL Web Proxy** web page, there is no check box but a link appeared below.

or Peer ID

Netbios Naming Packet Pass Block

SSL VPN

[Set SSL Web Proxy](#)

Local ID (optional)

Callback Function

Check to enable Callback function

Specify the callback number

Callback Number

Check to enable Callback Budget Control

Callback Budget minute(s)

OK Clear Cancel

However, if you have set several SSL Web Proxy Profiles in **SSL VPN>> SSL Web Proxy** web page:

SSL VPN >> SSL Web Proxy

SSL Web Proxy Servers Profiles:

Index	Name	URL
1.	gforge	http://swm.draytek.com
2.	web	http://www.draytek.com.cn
3.		
4.		

The SSL Web Proxy profile names will be displayed (together with check box) as shown below.

Netbios Naming Packet Pass Block

SSL VPN

SSL Web Proxy

gforge (Secured Port Redirection)

web (SSL)

Callback Function

Check to enable Ca

Specify the call

Callback Number

Check to enable

Callback Budget

OK Clear Cancel

3.15.5 Online User Status

If you have finished the configuration of SSL Web Proxy (server), users can find out corresponding settings when they access into Draytek SSL VPN portal interface.

DrayTek

Provide SSL VPN

Home SSL Web Proxy SSL Tunnel [logout]

INFO

mike ,
(172.17.1.42)
Welcome to DrayTek
SSL VPN!

Timeout after 5 minutes.
[Reset]

Main Page:

You have successfully logged in!
You are given the following privileges:

- [SSL Web Proxy](#)
- [SSL Tunnel](#)

Copyright © 2006, DrayTek Corp. All Rights Reserved.

Next, users can open **SSL VPN>> Online Status** to view login status of SSL VPN.

Web Access Control >> Online User Status

Refresh Seconds : 10

Active User	Host IP	Time out(seconds)	Action
caesar	172.17.1.42	292	<input type="button" value="Drop"/>

Active User

Display current user who visit SSL VPN server.

Host IP

Displays the IP address for the host.

Time out

Display the time remaining for logging out.

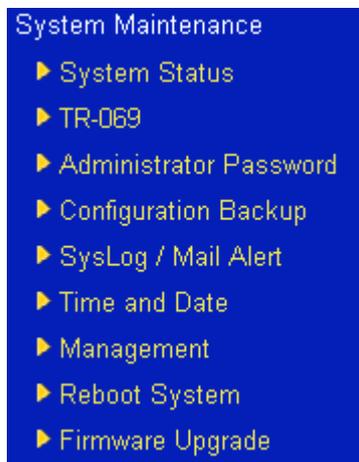
Action

You can click **Drop** to drop certain login user from the router's SSL Portal UI.

3.16 System Maintenance

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

Below shows the menu items for System Maintenance.



3.16.1 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		You logged in at 2010-6-8 01:55:52 last time, from 192.168.1.11.
Model Name	: VigorPro5510 series	
Firmware Version	: 3.3.4	
Build Date/Time	: Nov 25 2009 09:53:01	
Signature Version	: basic	
Signature Build Date	: Tue Aug 29 09:16:25.00 2006	

System	
CPU Usage	: 3 %
Total Memory	: 256M
Memory usage	: 15 %

LAN	
MAC Address	: 00-50-7F-C4-CC-44
1st IP Address	: 192.168.1.1
1st Subnet Mask	: 255.255.255.0
DHCP Server	: Yes
DNS	: 168.95.1.1

WAN 1	
Link Status	: Disconnected
MAC Address	: 00-50-7F-C4-CC-45
Connection	: Static IP
IP Address	: 172.16.3.229
Default Gateway	: 172.16.1.1
Mode	: NAT

WAN 2	
Link Status	: Connected
MAC Address	: 00-50-7F-C4-CC-46
Connection	: Static IP
IP Address	: 172.16.3.102
Default Gateway	: 172.16.1.1
Mode	: NAT

Model Name	Display the model name of the router.
Firmware Version	Display the firmware version of the router.
Build Date/Time	Display the date and time of the current firmware build.
System ---	
CPU Usage	Display current usage of CPU.
Total Memory	Display the total memory of your hard disk.
Memory Usage	Display current usage of memory.

LAN ---

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

WANI/WAN2 ---

Link Status	Display the connection status.
MAC Address	Display the MAC address of the WAN Interface.
Connection	Display the connection mode used currently.
IP Address	Display the IP address of the WAN interface.
Default Gateway	Display the assigned IP address of the default gateway.

Wireless LAN ---

MAC Address	Display the MAC address of the wireless LAN.
Frequency Domain	It can be Europe (13 usable channels), USA (11 usable channels) etc. The available channels supported by the wireless products in different countries are various.
Firmware Version	Display information about equipped WLAN miniPCi card. This also helps to provide availability of some features that are bound with some WLAN miniPCi card.
SSID	Display the identification name for the WLAN.

3.16.2 TR-069 Setting

Vigor router with TR-069 is available for matching with VigorACS server. Such page provides VigorACS and CPE settings under TR-069 protocol. All the settings configured here is for CPE to be controlled and managed with VigorACS server. Users need to type URL, username and password for the VigorACS server that such device will be connected. However URL, username and password under CPE client are fixed that users cannot change it. The default CPE username and password are "vigor" and "password". You will need it when you configure VigorACS server.

ACS and CPE Settings

ACS Server	
URL	<input type="text"/>
Username	<input type="text"/>
Password	<input type="password"/>
CPE Client	
<input type="radio"/> Enable <input checked="" type="radio"/> Disable	
URL	<input type="text" value="http://172.16.3.102:8069/cwm/CRN.html"/>
Port	<input type="text" value="8069"/>
Username	<input type="text" value="vigor"/>
Password	<input type="password" value="•••••••"/>

Periodic Inform Settings

<input checked="" type="radio"/> Disable <input type="radio"/> Enable	
Interval Time	<input type="text" value="900"/> second(s)

STUN Settings

<input checked="" type="radio"/> Disable <input type="radio"/> Enable	
Server IP	<input type="text"/>
Server Port	<input type="text" value="3478"/>
Minimum Keep Alive Period	<input type="text" value="60"/> second(s)
Maximum Keep Alive Period	<input type="text" value="-1"/> second(s)

OK

ACS Server

Such data must be typed according to the ACS (Auto Configuration Server) you want to link. Please refer to VigorACS user's manual for detailed information.

URL - Type the URL for VigorACS server.

If the connected CPE needs to be authenticated, please set URL as the following and type username and password for VigorACS server:

http://{IP address of VigorACS}:8080/ACSServer/services/ACSServlet

If the connected CPE does not need to be authenticated please set URL as the following:

http://{IP address of VigorACS}:8080/ACSServer/services/UnAuthACSServlet

Username/Password - Type username and password for ACS Server for authentication. For example, if you want to use such CPE with VigorACS, you can type as the following:

Username: *acs*

Password: *password*

CPE Client

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

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

Periodic Inform Settings

Disable – The system will not send inform message to ACS server.

Enable – The system will send inform message to ACS server periodically (with the time set in the box of interval time).

The default setting is **Enable**. Please set interval time or schedule time for the router to send notification to CPE. Or click **Disable** to close the mechanism of notification.

STUN Settings

Disable – The system will not send connection request binding message to STUN server. The default setting is **Disable**.

Enable –The system will send connection request binding message to STUN server.

Server IP – Type the domain name or IP address of the STUN server.

Server Port –Type the server port. The default setting is 3478.

Minimum Keep Alive Period – The default setting is 60 seconds. It determines the minimum period that the STUN binding request must be sent by the CPE to maintain the binding.

Maximum Keep Alive Period - It determines the maximum period that the STUN binding request must be sent by the CPE to maintain the binding.

3.16.3 Administrator Password

This page allows you to set new password.

System Maintenance >> Administrator Password Setup

Administrator Password

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

OK

Old Password

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

New Password

Type in new password in this field.

Confirm Password

Type in the new password again.

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

3.16.4 Configuration Backup

Backup the Configuration

Follow the steps below to backup your configuration.

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

System Maintenance >> Configuration Backup

Configuration Backup / Restoration

Restoration

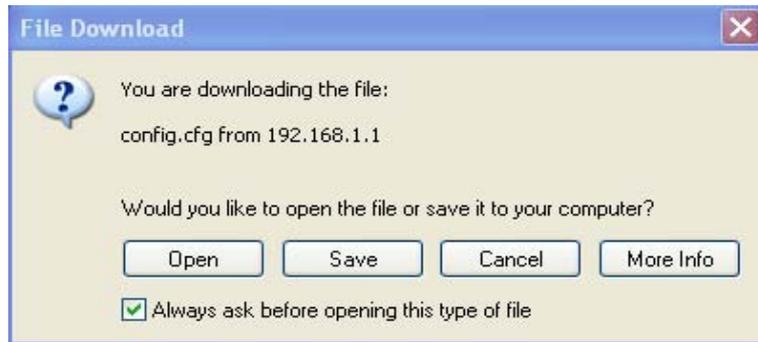
Select a configuration file.

Click Restore to upload the file.

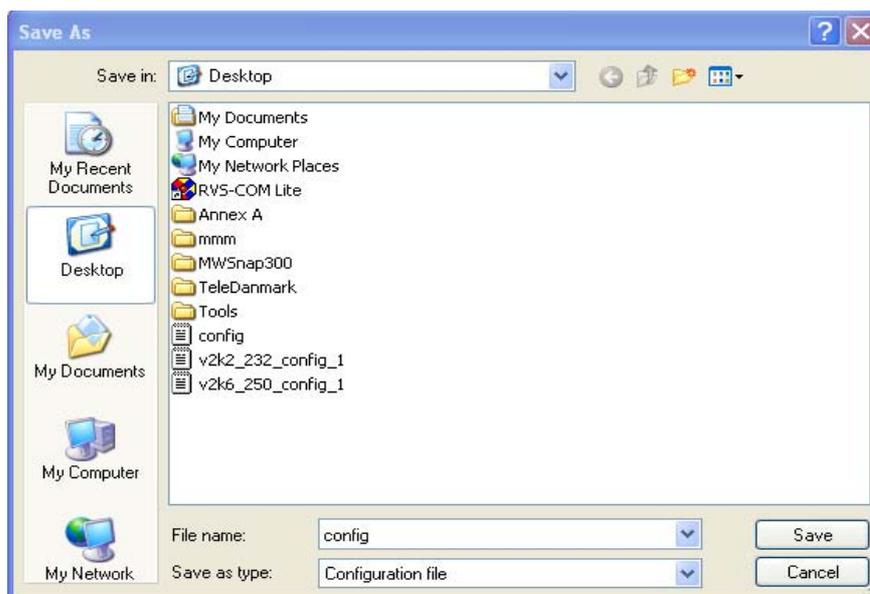
Backup

Click Backup to download current running configurations as a file.

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



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



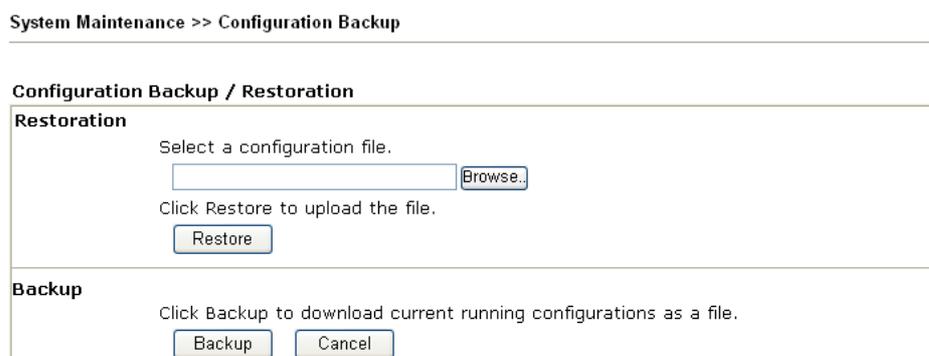
4. Click **Save** button, the configuration will download automatically to your computer as a file named **config.cfg**.

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

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

Restore Configuration

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



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.

3.16.5 Syslog/Mail Alert

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

SysLog / Mail Alert Setup

<p>SysLog Access Setup</p> <p><input checked="" type="checkbox"/> Enable</p> <p>Router Name <input type="text"/></p> <p>Server IP Address <input type="text"/></p> <p>Destination Port <input type="text" value="514"/></p> <p>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>AI/AV AlertLog Setup</p> <p><input checked="" type="checkbox"/> Enable</p> <p>AlertLog Port <input type="text" value="514"/></p> <p><input checked="" type="checkbox"/> AI/AV Attack Log</p> <p><input checked="" type="checkbox"/> Access Block Log</p>	<p>Mail Alert Setup</p> <p><input checked="" type="checkbox"/> Enable <input type="button" value="Send a test e-mail"/></p> <p>SMTP Server <input type="text"/></p> <p>Mail To <input type="text"/></p> <p>Return-Path <input type="text"/></p> <p><input checked="" type="checkbox"/> Authentication</p> <p>User Name <input type="text"/></p> <p>Password <input type="text"/></p> <p>Enable E-Mail Alert:</p> <p><input checked="" type="checkbox"/> DoS Attack</p> <p><input checked="" type="checkbox"/> IM-P2P</p> <p><input checked="" type="checkbox"/> Anti-Intrusion</p> <p><input checked="" type="checkbox"/> Anti-Virus</p>
--	---

SysLog Access Setup

Enable (Syslog Access...)

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

Router Name

Assign a name for the router.

Server IP Address

The IP address of the Syslog server.

Destination Port

Assign a port for the Syslog protocol.

Enable syslog message

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

AI/AV AlertLog Setup

Enable (Alert Setup...)

Check “**Enable**” to activate function of AI/AV attack log.

AlertLog Port

Type the port number for the alertlog and Check the box to send the corresponding message of AI/AV Attack Log, Access Block Log to Syslog.

Mail Alert Setup

Enable (Alert Setup...)

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

Send a test e-mail

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

SMTP Server

The IP address of the SMTP server.

Mail To

Assign a mail address for sending mails out.

Specify an e-mail address of another mailbox to accept all returned messages if some fatal problems occur at the recipient mailbox. The e-mail address typed in this field

also acts as Sender address while Vigor router sends out the alert e-mails.

Authentication

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

User Name

Type the user name for authentication.

Password

Type the password for authentication.

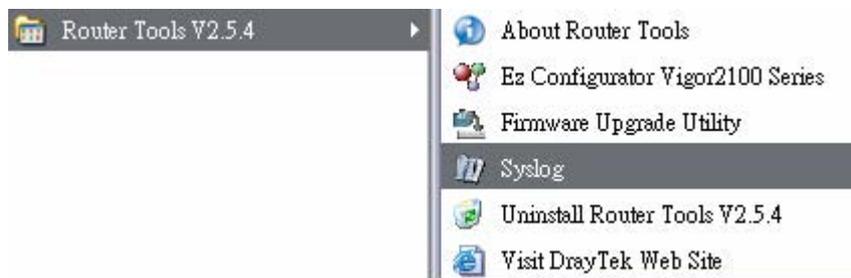
Enable E-Mail Alert

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

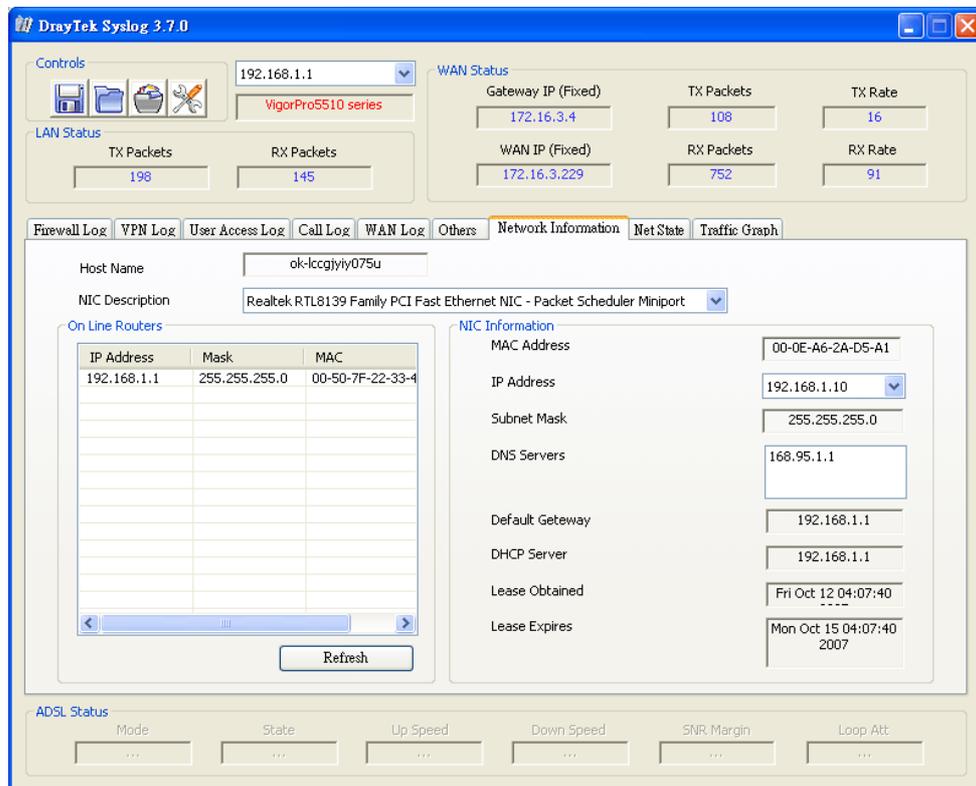
Click **OK** to save these settings.

For viewing the Syslog, please do the following:

1. Just set your monitor PC's IP address in the field of Server IP Address
2. Install the 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.



3.16.6 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	2006 Sep 5 Tue 6 : 44 : 17	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	pool.ntp.org
Time Zone	(GMT) Greenwich Mean Time : Dublin ▼
Enable Daylight Saving	<input type="checkbox"/>
Automatically Update Interval	30 min ▼

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

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.

Automatically Update Interval

Select a time interval for updating from the NTP server.

Click **OK** to save these settings.

3.16.7 Management

This page allows you to manage the settings for access control, access list, port setup, and SNMP setup. For example, as to management access control, the port number is used to send/receive SIP message for building a session. The default value is 5060 and this must match with the peer Registrar when making VoIP calls.

System Maintenance >> Management

Management Setup

<p>Management Access Control</p> <p><input type="checkbox"/> Allow management from the Internet</p> <p style="margin-left: 20px;"><input type="checkbox"/> FTP Server</p> <p style="margin-left: 20px;"><input checked="" type="checkbox"/> HTTP Server</p> <p style="margin-left: 20px;"><input checked="" type="checkbox"/> HTTPS Server</p> <p style="margin-left: 20px;"><input checked="" type="checkbox"/> Telnet Server</p> <p><input checked="" type="checkbox"/> Disable PING from the Internet</p> <p><input checked="" type="checkbox"/> External Device Auto Discovery</p> <hr/> <p>Access List</p> <table border="0" style="width: 100%;"> <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 type="text"/></td> <td><input style="border-bottom: 1px solid #ccc; border-right: 1px solid #ccc; border-top: 1px solid #ccc; border-left: 1px solid #ccc; width: 100px;" type="text"/> <input type="button" value="v"/></td> </tr> <tr> <td>2</td> <td><input type="text"/></td> <td><input style="border-bottom: 1px solid #ccc; border-right: 1px solid #ccc; border-top: 1px solid #ccc; border-left: 1px solid #ccc; width: 100px;" type="text"/> <input type="button" value="v"/></td> </tr> <tr> <td>3</td> <td><input type="text"/></td> <td><input style="border-bottom: 1px solid #ccc; border-right: 1px solid #ccc; border-top: 1px solid #ccc; border-left: 1px solid #ccc; width: 100px;" type="text"/> <input type="button" value="v"/></td> </tr> </tbody> </table>	List	IP	Subnet Mask	1	<input type="text"/>	<input style="border-bottom: 1px solid #ccc; border-right: 1px solid #ccc; border-top: 1px solid #ccc; border-left: 1px solid #ccc; width: 100px;" type="text"/> <input type="button" value="v"/>	2	<input type="text"/>	<input style="border-bottom: 1px solid #ccc; border-right: 1px solid #ccc; border-top: 1px solid #ccc; border-left: 1px solid #ccc; width: 100px;" type="text"/> <input type="button" value="v"/>	3	<input type="text"/>	<input style="border-bottom: 1px solid #ccc; border-right: 1px solid #ccc; border-top: 1px solid #ccc; border-left: 1px solid #ccc; width: 100px;" 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 type="text" value="23"/> (Default: 23)</p> <p>HTTP Port <input type="text" value="80"/> (Default: 80)</p> <p>HTTPS Port <input type="text" value="443"/> (Default: 443)</p> <p>FTP Port <input type="text" value="21"/> (Default: 21)</p> <hr/> <p>SNMP Setup</p> <p><input type="checkbox"/> Enable SNMP Agent</p> <p>Get Community <input type="text" value="public"/></p> <p>Set Community <input type="text" value="private"/></p> <p>Manager Host IP <input type="text"/></p> <p>Trap Community <input type="text" value="public"/></p> <p>Notification Host IP <input type="text"/></p> <p>Trap Timeout <input type="text" value="10"/> seconds</p>
List	IP	Subnet Mask											
1	<input type="text"/>	<input style="border-bottom: 1px solid #ccc; border-right: 1px solid #ccc; border-top: 1px solid #ccc; border-left: 1px solid #ccc; width: 100px;" type="text"/> <input type="button" value="v"/>											
2	<input type="text"/>	<input style="border-bottom: 1px solid #ccc; border-right: 1px solid #ccc; border-top: 1px solid #ccc; border-left: 1px solid #ccc; width: 100px;" type="text"/> <input type="button" value="v"/>											
3	<input type="text"/>	<input style="border-bottom: 1px solid #ccc; border-right: 1px solid #ccc; border-top: 1px solid #ccc; border-left: 1px solid #ccc; width: 100px;" type="text"/> <input type="button" value="v"/>											

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

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

External Device Auto Discovery Check the checkbox to detect external devices connected to current router automatically.

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.

User Define Ports Check to specify user-defined port numbers for the Telnet and HTTP servers.

Default Ports Check to use standard port numbers for the Telnet 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.

3.16.8 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

Auto Reboot Time Schedule

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

Note: Action and Idle Timeout settings will be ignored.

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 **Reboot Now**. The router will take 5 seconds to reboot the system.

In addition, you can enter the index of schedule profiles to reboot your system according to the preconfigured schedules. When you finish the reboot time schedule, please click **OK** to save it. For detailed configuration of time schedule, please refer to section **Schedule**.

3.16.9 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>.

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

System Maintenance >> Firmware Upgrade

Web Firmware Upgrade

Select a firmware file.

Click Upgrade to upload the file.

TFTP Firmware Upgrade from LAN

Current Firmware Version: 3.3.4

Firmware Upgrade Procedures:

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

Do you want to upgrade firmware ?

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

System Maintenance >> Firmware Upgrade

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

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

3.17 Diagnostics

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



3.17.1 Dial-out Trigger

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

Diagnostics >> Dial-out Trigger

[Refresh](#)

Dial-out Triggered Packet Header

HEX Format:

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

Decoded Format:

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

Decoded Format

It shows the source IP address (local), destination IP (remote) address, the protocol and length of the package.

Refresh

Click it to reload the page.

3.17.2 Routing Table

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

Diagnostics >> View Routing Table

Current Running Routing Table | Refresh |

Key: C - connected, S - static, R - RIP, * - default, ~ - private			
*	0.0.0.0/	0.0.0.0 via 172.16.3.1,	WAN1
C~	192.168.1.0/	255.255.255.0 is directly connected,	LAN
C	172.16.3.0/	255.255.255.0 is directly connected,	WAN1

Refresh

Click it to reload the page.

3.17.3 ARP Cache Table

Click **Diagnostics** and click **ARP Cache Table** to view the content of the ARP (Address Resolution Protocol) cache held in the 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
172.16.3.19	00-0D-60-6F-89-CA
172.16.3.163	00-50-7F-1A-58-89
172.16.3.156	00-50-7F-1A-56-0E
172.16.3.153	00-50-7F-1A-57-07
172.16.3.131	00-07-40-82-14-EF
172.16.3.112	00-40-CA-6B-56-BA
172.16.3.114	00-0E-A6-4F-10-C4
172.16.3.8	00-11-25-22-66-22
172.16.3.181	00-50-7F-1A-58-CF
172.16.3.198	00-50-7F-1A-57-AE
172.16.3.174	00-0C-6E-5E-C8-60
172.16.3.160	00-0E-A6-5C-5C-D9
172.16.3.188	00-E0-18-72-AE-11
172.16.3.20	00-0D-60-6F-83-BC

Refresh

Click it to reload the page.

Clear

Click it to clear the whole table.

3.17.4 DHCP Table

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

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

Diagnostics >> View DHCP Assigned IP Addresses

DHCP IP Assignment Table					Refresh
DHCP server: Running					
Index	IP Address	MAC Address	Leased Time	HOST ID	
1	192.168.1.10	00-0E-A6-2A-D5-A1	0:00:02.630	ok-lccgjyiy075u	

- 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.

3.17.5 NAT Sessions Table

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

Diagnostics >> NAT Sessions Table

NAT Active Sessions Table							Refresh
Private IP	:Port	#Pseudo Port	Peer IP	:Port	Interface		
192.168.1.10	3381	52967	207.46.106.104	80	WAN1		
192.168.1.10	45590	62408	124.102.28.72	31123	WAN1		
192.168.1.10	45590	62408	124.39.5.85	7064	WAN1		
192.168.1.10	45590	62408	84.123.128.129	25165	WAN1		
192.168.1.10	45590	62408	84.152.196.48	25817	WAN1		
192.168.1.10	45590	62408	67.174.114.63	47118	WAN1		
192.168.1.10	45590	62408	72.198.84.127	44963	WAN1		
192.168.1.10	45590	62408	98.233.151.47	35944	WAN1		
192.168.1.10	45590	62408	78.137.8.174	57138	WAN1		
192.168.1.10	45590	62408	201.234.159.9	42322	WAN1		
192.168.1.10	45590	62408	24.197.127.19	5362	WAN1		
192.168.1.10	45590	62408	78.131.23.114	14882	WAN1		
192.168.1.10	45590	62408	82.30.30.61	10667	WAN1		

- 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.

3.17.6 Wireless VLAN Online Station Table

Click **Diagnostics** and click **Wireless VLAN Online Station Table** to open the web page. It will display the IP address, MAC address and Login ID information for all the Wireless VLAN stations.

Diagnostics >> Wireless VLAN Online Station

Wireless VLAN Online Station Table			Refresh
IP Address	MAC Address	Login ID	

IP Address	Display the IP address of the wireless station.
MAC Address	Display the MAC address of the wireless station.
Login ID	Display the login ID that the wireless station belongs to.

Note: Such feature is available for Vigor5510Gi only.

3.17.7 LAN Security Monitor

This page displays the running procedure for the IP address monitored and refreshes the data in an interval of several seconds. The IP address listed here is configured in Bandwidth Management. You have to enable IP bandwidth limit and IP session limit before invoke Data Flow Monitor. If not, a notification dialog box will appear to remind you enabling it.

Bandwidth Management >> Sessions Limit

Sessions Limit

Enable
 Disable

Default Max Sessions:

Limitation List

Index	Start IP	End

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

Page: 1 | Refresh

bps)	Sessions	Action
	1 / 100	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

Current /Peak/Speed

Current means current transmission rate and receiving rate for WAN1/WAN2.

Peak means the highest peak value detected by the router in data transmission.

Speed means line speed specified in **WAN>>General**. If you do not specify any rate at that page, here will display **Auto** for instead.

3.17.8 Traffic Graph

Click **Diagnostics** and click **Traffic Graph** to pen the web page. Choose WAN1 Bandwidth/WAN2 Bandwidth, Sessions, daily or weekly for viewing different traffic graph. Click **Refresh** to renew the graph at any time. The following two figures display different charts by daily and weekly.

Diagnostics >> Traffic Graph





The horizontal axis represents time. Yet the vertical axis has different meanings. For WAN1/WAN2 Bandwidth chart, the numbers displayed on vertical axis represent the numbers of the transmitted and received packets in the past.

For Sessions chart, the numbers displayed on vertical axis represent the numbers of the NAT sessions during the past.

3.17.9 Ping Diagnosis

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

Diagnostics >> Ping Diagnosis

Ping Diagnosis

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

Ping through:

Ping to: IP Address:

Result

Ping through

Use the drop down list to choose the WAN interface that you want to ping through or choose **Unspecified** to be determined by the router automatically.

Ping through:

- Unspecified
- WAN1
- WAN2

Ping to

Use the drop down list to choose the destination that you want to ping.



IP Address

Type in the IP address of the Host/IP that you want to ping.

Run

Click this button to start the ping work. The result will be displayed on the screen.

Clear

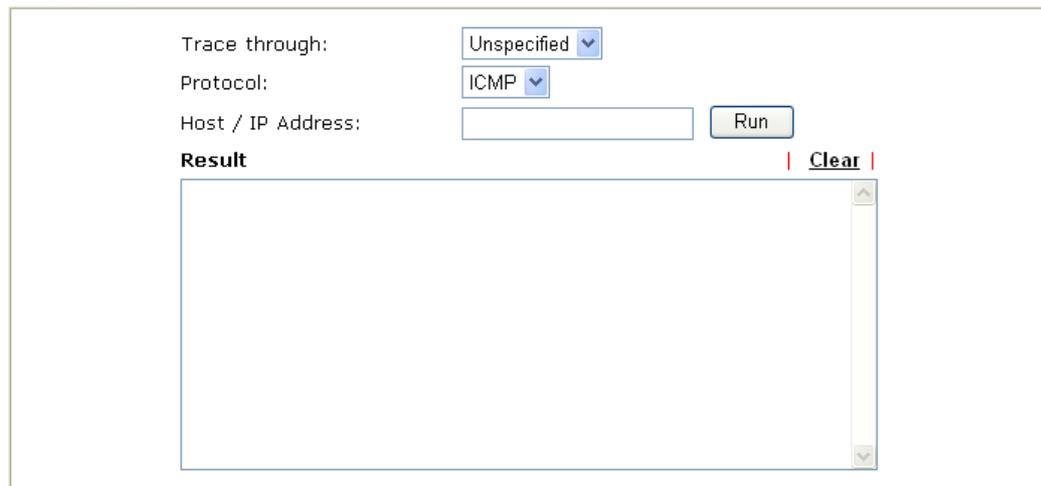
Click this link to remove the result on the window.

3.17.10 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



Trace through

Use the drop down list to choose the WAN interface that you want to ping through or choose **Unspecified** to be determined by the router automatically.



Protocol

Use the drop down list to choose suitable protocol.



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.

3.17.11 AV/AI Top 10

This page provides information for the Top 10 of Anti-Virus and Anti-Intrusion signatures used frequently.

Diagnostics >> Top 10 Information

AV Top 10 List

| [Refresh](#) |

No	SID	count	Name
1	21593	0	Bagle.AC
2	22361	0	Bagle.AF
3	22417	0	Bagle.AG
4	34196	0	Bagle.BL
5	35493	0	Bagle.BY-2
6	35496	0	Bagle.BZ-1
7	35497	0	Bagle.BZ-2
8	35682	0	Bagle.CB
9	35686	0	Bagle.CD-1
10	35687	0	Bagle.CD-2

AI Top 10 List

No	SID	count	Name
1	1336	0	Format String %n%n%n%n
2	1467	0	SHELLCODE MIPS Ultrix NOOP
3	432	0	Trin00 attacker to master
4	433	0	Trin00 attacker to master2
5	434	0	Trin00 attacker to master3
6	431	0	shaft client login handler
7	285	0	CVS BSD heap overflow
8	286	0	CVS Solaris heap overflow
9	439	0	DNS named overflow ADMROCKS
10	440	0	DNS named overflow

3.17.12 Web Firewall Syslog

This page displays the time and message for firewall settings. You can check Enable Web Firewall Syslog and choose the display mode you want. Later, the event of firewall will be shown for your reference.

Diagnostics >> Web Firewall Syslog

Enable Web Firewall Syslog

Display Mode Stop record when fulls

[Refresh](#) | [Clear](#)

Time	Message
2008-12-03 10:59:51	[FILTER][Pass][lan->wan, 0:59:07.410][@S:R=2:2, 172.16.2.25:48430->139.175.55.244:53][UDP][HLen=20, TLen=78]
2008-12-03 10:59:51	[FILTER][Pass][lan->wan, 0:59:07.370][@S:R=2:2, 172.16.2.25:48428->139.175.55.244:53][UDP][HLen=20, TLen=81]
2008-12-03 10:59:51	[FILTER][Pass][lan->wan, 0:59:07.370][@S:R=2:2, 172.16.2.25:60843->208.83.137.114:2703][TCP][HLen=20, TLen=60, Flag=S, Seq=2780745383, Ack=0, Win=5840]
2008-12-03 10:59:51	[FILTER][Pass][lan->wan, 0:59:07.340][@S:R=2:2, 172.16.2.25:48427->139.175.55.244:53][UDP][HLen=20, TLen=78]
2008-12-03 10:59:51	[FILTER][Pass][lan->wan, 0:59:07.330][@S:R=2:2, 172.16.2.25:48426->139.175.55.244:53][UDP][HLen=20, TLen=77]
2008-12-03 10:59:51	[FILTER][Pass][lan->wan, 0:59:07.290][@S:R=2:2, 172.16.2.25:48425->139.175.55.244:53][UDP][HLen=20, TLen=80]
2008-12-03 10:59:51	[FILTER][Pass][lan->wan, 0:59:07.250][@S:R=2:2, 172.16.2.25:48424->139.175.55.244:53][UDP][HLen=20, TLen=76]

Display Mode

Stop record when fulls
Stop record when fulls
Always record the new event

4

Registration for the Router

To use the anti-intrusion, anti-virus, anti-spam and WCF features of VigorPro series router, you have to create a new account, finish the registration for that account by using the router and complete the registration for the Vigor router. After finishing the registration of the router, you can download the newly update types and rules of anti-intrusion, anti-virus, anti-spam and WCF during the valid time of the license key you purchased.

There are two ways to create and activate new account. One is created by accessing <http://myvigor.draytek.com> (refer to section 4.1), the other is from router's web configurator (refer to section 4.2).

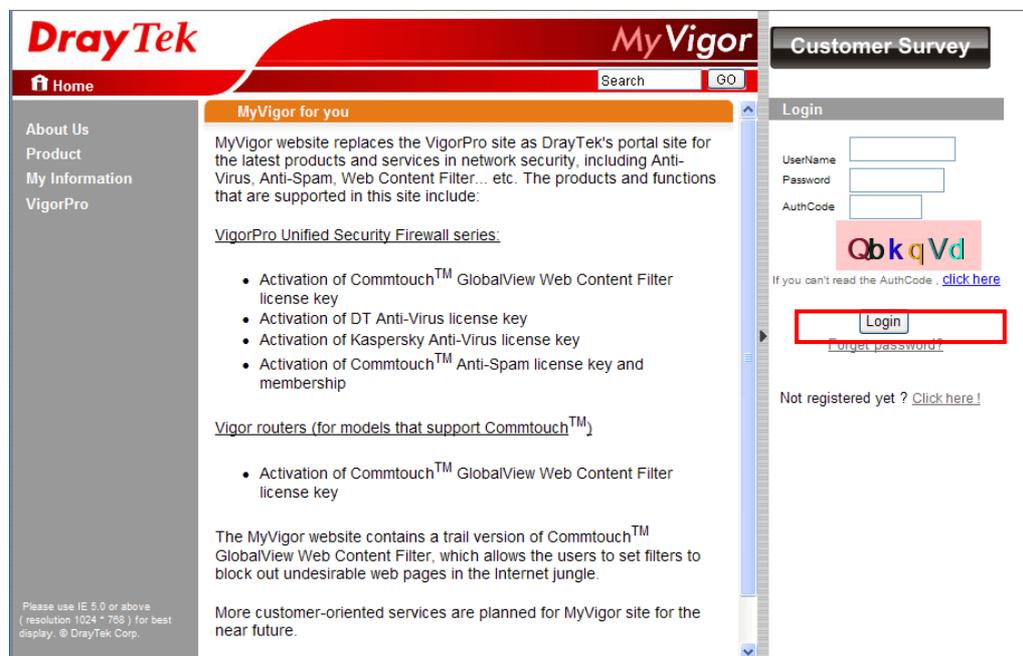
After activating the new account, you have to register your router from router's web configurator (refer to section 4.3). Follow the steps listed below to finish the registration and activation.

Note: The website of MyVigor (a server located on <http://myvigor.draytek.com>) provides several useful services (such as Anti-Spam, Web Content Filter, Anti-Intrusion, and etc.) to filtering the web pages for the sake of protecting your system.

4.1 Creating and Activating an Account from MyVigor Website

Follow the steps below to create an account for MyVigor.

1. Access into <http://myvigor.draytek.com>. Find the line of **Not registered yet?**. Then, click the link **Click here!** to access into next page.



2. Check to confirm that you accept the Agreement and click **Accept**.

Register

Create an account - Please enter personal profile.

1 Agreement

2 Personal Information

3 Preferences

4 Completion

MyVigor Agreement

1. Agreement

Draytek provides MyVigor(myvigor.draytek.com) service according to this agreement. When you use MyVigor service, it means that you have read, understand and agree to accept the items listed in this agreement. Draytek can modify or change the content of the items without any reasons. It is suggested for you to notice the modifications or changes at any time. If you still use MyVigor service after knowing the modifications and changes of this service, it means you have read, understand and agree to accept the modifications and changes. If you do not agree the content of this agreement, please stop using MyVigor service.

2. Registration

To use this service, you have to agree the following conditions:

(a) Provide your complete and correct information according to the registration steps of this service.

(b) If you provide any incorrect or fake information here, DrayTek has the right to pause or terminate your service.

I have read and understand the above Agreement. (Use the scroll bar to view the entire agreement)

<< Back Accept >>

3. Type your personal information in this page and then click **Continue**.

Register

Create an account - Please enter personal profile. (Fields marked by (*) are required)

1 Agreement

2 Personal Information

3 Preferences

4 Completion

Account Information

UserName: * Mary Check Account

(3 ~ 20 characters)

Password: * ●●●●

(4 ~ 20 characters : Do not set the same as the username.)

Confirm Password: * ●●●●

Personal Information

First Name: * Mary

Last Name: * Ted

Company Name: Tech Ltd.

Email Address: * mary_ted@tech.com

Please note that a valid E-mail address is required to receive the Subscription Code. You will need this code to activate your account.

Tel: 0 -

Country: * SWITZERLAND

Career: * Supervisor

<< Back Continue >>

4. Choose proper selection for your computer and click **Continue**.

Register

Create an account - Please enter personal profile.

1 Agreement

2 Personal Information

3 Preferences

4 Completion

How did you find out about this website? Internet

What kind of anti-virus do you use? AntiVir

I would like to subscribe to the MyVigor e-letter.

I would like to receive DrayTek product news.

Please select the mail server for receiving the verification mail. Global Server

<< Back Continue >>

5. Now you have created an account successfully. Click **START**.

Register

Create an account - Please enter personal profile.

1 Agreement

2 Personal Information

3 Preferences

4 Completion

Completion

A confirmation email has been sent to mary_ted@tech.com
Please click on the activation link in the email
to activate your account

START

6. Check to see the confirmation *email* with the title of **New Account Confirmation Letter from myvigor.draytek.com.**

***** This is an automated message from myvigor.draytek.com.*****

Thank you (**Mary**) for creating an account.

Please click on the activation link below to activate your account

Link : [Activate my Account](#)

7. Click the **Activate my Account** link to enable the account that you created. The following screen will be shown to verify the register process is finished. Please click **Login**.

Register Search for this site

Register Confirm

The Confirm message of New Owner(Mary) maybe timeout
Please try again or contact to draytek.com

Close Login

8. When you see the following page, please type in the account and password (that you just created) in the fields of **UserName** and **Password**. Then type the code in the box of Auth Code according to the value displayed on the right side of it.

This service is available for MyVigor member only. Please login to access MyVigor.
If you are not one of the members of MyVigor, please create an account first.

LOGIN

UserName :

Password :

Auth Code : **T4he1C**

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

[Forget password?](#)

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

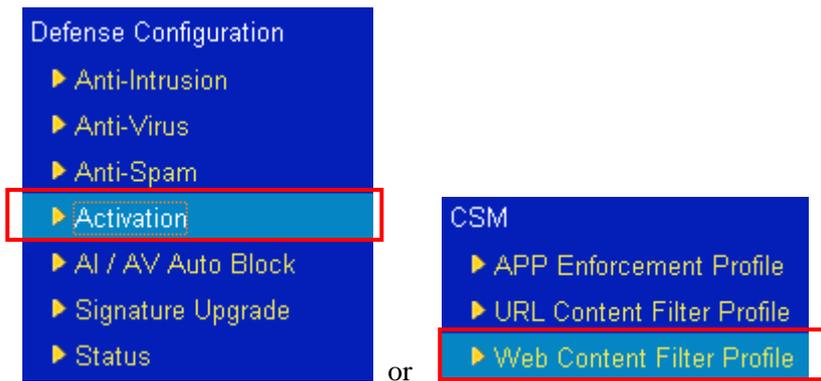
If you are having difficulty logging in, contact our customer service.
Customer Service : (888) 3 597 2727 or
email to : webmaster@draytek.com

9. Now, click **Login**. Your account has been activated. You can access into MyVigor server to activate the service (e.g., WCF) that you want.

4.2 Creating and Activating an Account from Router Web Configurator

You can also create and register a new account from the web configurator of the VigorPro router.

1. Open a web browser on your PC and type **http://192.168.1.1**. A pop-up window will open to ask for username and password. Do not type any word on the window and click **OK**.
2. From the router's web page, please open **Defense Configuration >>Activation**. Or, Click **CSM>> Web Content Filter Profile**.



3. You will get the following page. Click the **Activate** link from the **Activation** web page.



Or



4. Click the **Activate** link. A login page for MyVigor web site will pop up automatically.

**This service is available for MyVigor member only. Please login to access MyVigor.
If you are not one of the members of MyVigor, please create an account first.**

LOGIN

UserName :

Password :

Auth Code : **AYi GXZ**

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

[Forget password?](#)

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

If you are having difficulty logging in, contact our customer service.
Customer Service : (888) 3 597 2727 or
email to :webmaster@draytek.com

5. Click the link of **Create an account now**.
6. Check to confirm that you accept the Agreement and click **Accept**.

Register

Create an account - Please enter personal profile.

1 Agreement

2 Personal Information

3 Preferences

4 Completion

MyVigor Agreement

1. Agreement
Draytek provides MyVigor(myvigor.draytek.com) service according to this agreement. When you use MyVigor service, it means that you have read, understand and agree to accept the items listed in this agreement. Draytek can modify or change the content of the items without any reasons. It is suggested for you to notice the modifications or changes at any time. If you still use MyVigor service after knowing the modifications and changes of this service, it means you have read, understand and agree to accept the modifications and changes. If you do not agree the content of this agreement, please stop using MyVigor service.

2. Registration
To use this service, you have to agree the following conditions:
(a) Provide your complete and correct information according to the registration steps of this service.
(b) If you provide any incorrect or fake information here, DrayTek has the right to pause or terminate your service.

I have read and understand the above Agreement. (Use the scroll bar to view the entire agreement)

7. Type your personal information in this page and then click **Continue**.

Register

Create an account - Please enter personal profile.(Fields marked by (*) are required)

1 Agreement

2 Personal Information

3 Preferences

4 Completion

Account Information

UserName:*
(3 - 20 characters)

Password:*
(4 - 20 characters : Do not set the same as the username.)

Confirm Password:*

Personal Information

First Name:*

Last Name:*

Company Name:

Email Address:*
Please note that a valid E-mail address is required to receive the Subscription Code. You will need this code to activate your account.

Tel: -

Country:*

Career:*

8. Choose proper selection for your computer and click **Continue**.

Register

Create an account - Please enter personal profile.

1 Agreement

2 Personal Information

3 Preferences

4 Completion

How did you find out about this website?

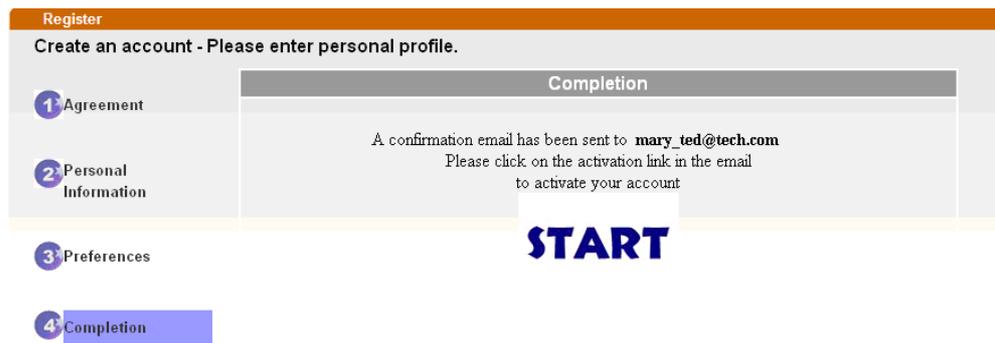
What kind of anti-virus do you use?

I would like to subscribe to the MyVigor e-letter.

I would like to receive DrayTek product news.

Please select the mail server for receiving the verification mail.

9. Now you have created an account successfully. Click START.



10. Check to see the confirmation *email* with the title of **New Account Confirmation Letter from myvigor.draytek.com**.

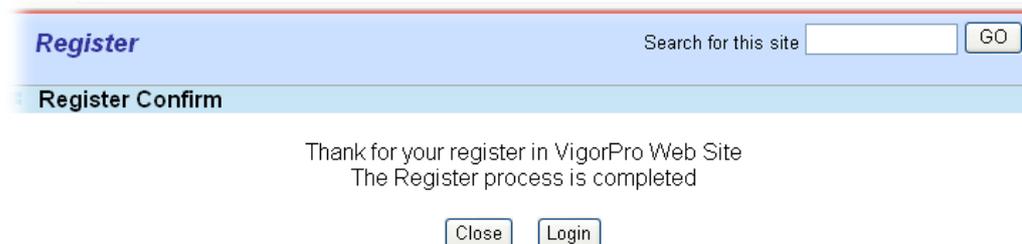
***** This is an automated message from myvigor.draytek.com.*****

Thank you (**Mary**) for creating an account.

Please click on the activation link below to activate your account

Link : [Activate my Account](#)

11. Click the **Activate my Account** link to enable the account that you created. The following screen will be shown to verify the register process is finished. Please click **Login**.



12. When you see the following page, please type in the account and password (that you just created) in the fields of **UserName** and **Password**.

This service is available for MyVigor member only. Please login to access MyVigor. If you are not one of the members of MyVigor, please create an account first.

LOGIN

UserName :

Password :

Auth Code : **T4he1C**

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

[Forget password?](#)

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

If you are having difficulty logging in, contact our customer service.
Customer Service : (888) 3 597 2727 or
email to : webmaster@draytek.com

13. Now, click **Login**. Your account has been activated. You can access into MyVigor server to activate the service (e.g., WCF) that you want.

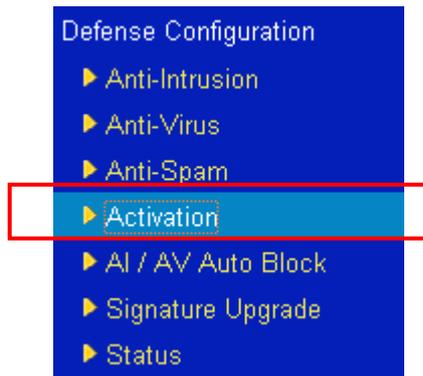


DrayTek will maintain a database of MAC address/serial number of shipped goods. Only products with shipping records can be registered. If your VigorPro 5510 cannot hook up to your account, please contact your reseller or DrayTek's technical support.

4.3 Registering Your Vigor Router

You have activated the new account for the router. Now, it is the time for you to register your vigor router. Open **Defense Configuration >>Activation**. Registering Vigor router should be done just for once. **If the router has been registered previously, the system will not allow you to register the router again.** After finishing the router registration, you can activate Anti-Virus, Anti-Intrusion, Anti-Spam and Web Content Filter respectively.

1. Open a web browser on your PC and type **http://192.168.1.1**. A pop-up window will open to ask for username and password. Do not type any word on the window and click **OK**.
2. From the router's web page, please open **Defense Configuration >>Activation**.



3. You will see the following web page. Click one of the **Activate** links from the **Activation** web page.



4. A **Login** page will be shown on the screen. Please type the account and password that you created previously. And click **Login**.

This service is available for MyVigor member only. Please login to access MyVigor.
If you are not one of the members of MyVigor, please create an account first.

LOGIN

UserName :

Password :

Auth Code : **T4he1C**

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

[Forget password?](#)

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

If you are having difficulty logging in, contact our customer service.
Customer Service : (888) 3 597 2727 or
email to : webmaster@draytek.com

5. The following page will be displayed after you logging in VigorPro server. From this page, please click **Add**.

My Information

Welcome, **Mary**

Last Login Time : --

Last Login From : --

Current Login Time : 2010-03-29 12:09:34

Current Login From : 172.16.3.102

RowNo : PageNo :

Your Device List

Serial Number / Host ID	Device Name	Model	Note
-------------------------	-------------	-------	------

- When the following page appears, please type in Nick Name (for the router) and choose the right purchase date from the popup calendar (it appears when you click on the box of Purchase Date).

My Product Search for this site

Registration Device

Serial number : 20100503140901

Nickname :*

Registration Date :*

May 2010
✕

Wk	Mon	Tue	Wed	Thu	Fri	Sat	Sun
17						1	2
18	3	4	5	6	7	8	9
19	10	11	12	13	14	15	16
20	17	18	19	20	21	22	23
21	24	25	26	27	28	29	30
22	31						

Today is Mon, 3 May 2010

- After adding the basic information for the router, please click **Submit**.

My Product Search for this site

Registration Device

Serial number : 200709210001

Nickname :*

Registration Date :*

- Now, your router information has been added to the database. Click **OK** to leave this web page and return to **My Product** web page.

Your device has been successfully added to the database.



- Now, you have finished the procedure for registering your router.

My Information

Welcome, sandyni
Last Login Time : 2010-05-03 14:23:09
Last Login From : 172.16.1.15
Current Login Time : 2010-05-03 14:28:31
Current Login From : 172.16.1.15

RowNo : PageNo :

Your Device List

Serial Number / Host ID	Device Name	Model	Note
20100503140901	5510ni	VigorPro5510	-

4.4 Activating Anti-Virus/Anti-Intrusion/Anti-Spam/WCF Service

After registering your vigor router, you have to follow the steps listed below to activate anti-virus/anti-intrusion/anti-spam/web content filter (WCF) service to obtain full security for your computer.

4.4.1 For Anti-Virus and Anti-Intrusion Service

- 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.
- From the router's web page, please open **Defense Configuration >>Activation**. You will see the following web page.

The image shows a blue sidebar menu titled "Defense Configuration". The menu items are: Anti-Intrusion, Anti-Virus, Anti-Spam, **Activation** (highlighted with a red box), AI / AV Auto Block, Signature Upgrade, and Status.

- Click the **Activate** link from Anti-Intrusion/Anti-Virus License to activate Anti-Intrusion/Anti-Virus service.

Defense Configuration >> Activation Activate via interface :

Anti-Intrusion/Anti-Virus License [Status:Not Activated]	<div style="border: 2px solid red; padding: 2px;">Activate</div>
Anti-Spam License [Status:Not Activated]	Activate
Web-Filter License [Status:Not Activated]	Activate

Authentication Message

WebFilter, Authenticate successful, 2000-01-01 00:01:25

4. A **Login** page will be shown on the screen. Please type the account and password that you created previously. And click **Login**.

This service is available for MyVigor member only. Please login to access MyVigor.
If you are not one of the members of MyVigor, please create an account first.

LOGIN

UserName :

Password :

Auth Code : T4he1C

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

[Forget password?](#)

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

If you are having difficulty logging in, contact our customer service.
 Customer Service : (886) 3 597 2727 or
 email to : webmaster@draytek.com

5. On the web page of **My Product**, you can find a list of the devices that you add with the above steps. Currently, you just have added VigorPro 5510. Please click the serial number link.

My Information

Welcome, sandyni

Last Login Time : 2010-05-03 14:23:09
 Last Login From : 172.16.1.15
 Current Login Time : 2010-05-03 14:28:31
 Current Login From : 172.16.1.15

RowNo : PageNo :

Your Device List

Serial Number / Host ID	Device Name	Model	Note
20100503140901	5510ni	VigorPro5510	-

6. From the **Device's Service** section, click the **Trial** button for AI-AV (Anti-Intrusion & Anti-Virus) service with provider **DT-DT**.

My Product

Device Information

Nickname : 5510ni
 Serial : 20100503140901
 Model : VigorPro5510

Rename Delete Transfer Back

Device's Service Expired License

Service	Provider	Action	Status	Start Date	Expired Date
 AI-AV	DT-DT	Trial	● On	-	-
 AI-AV	DT-KL	Trial	● On	-	-
 WCF	CT-CF	Trial	● On	-	-
 AS	CTCH	Trial	● On	-	-

● Means such service is in use.
● Means such service is not in use.
● Means such service has not been activated yet.
● Means such service is in use and will be invalid soon (less than one month).

Trial Allows you to have the free trial for service.
Renew Allows you to renew service license.
Activate Allows you to activate service.

Rename

It allows you to change the account name.

Delete

It allows you to delete account name used currently.

Transfer

It allows you to transfer the VigorPro device together with applied license to someone who has already registered another account in www.vigorpro.com. Be sure to press this button to transfer the product to whom you want to give. Otherwise he/she might not be able to maintain the license hooked up to the VigorPro device.

Back

It allows you to return to the previous account.

- In the following page, check the box of “**I have read and accept the above Agreement**”. The system will find out the date for you to activate this version of service. Then, click **Next**.

Confirm Message

User Name : sandyni
Serial : 20100503140901
Model : VigorPro5510

License Number	Service Provider	Status
DrayTek VigorPro Series End-User License Agreement		
<p>IMPORTANT:</p> <p>DrayTek IS WILLING TO LICENSE THE ENCLOSED SOFTWARE TO YOU ONLY UPON THE CONDITION THAT YOU ACCEPT ALL OF THE TERMS CONTAINED IN THIS LICENSE AGREEMENT. PLEASE READ THE TERMS CAREFULLY BEFORE COMPLETING THE INSTALLATION PROCESS AS INSTALLING THE SOFTWARE WILL INDICATE YOUR ASSENT TO THEM. IF YOU DO NOT AGREE TO THESE TERMS, THEN DrayTek IS UNWILLING TO LICENSE THE</p>		
<input checked="" type="checkbox"/> I have read and accept the above Agreement. (Please check this box).		

Note: DT-DT means you can acquire the anti-intrusion and anti-virus services from DrayTek Corporation.

- When this page appears, click **Register**.

Apply For A License Number

Service Name: **AI-AV**

STEP 2

Enable It!! Enable the **VigorPro Statistical Reporting**

Activation Date (MM-DD-YYYY):

- Next, the DrayTek Service Activation screen will be shown as the following:

DrayTek Service Activation

Service Name	Start Date	Expire Date	Status
Anti-Virus	2010-05-03	2011-05-04	DT-DT
Web Content filter	---	---	Not Activated
Anti-Spam	---	---	Not Activated

Please check if the license fits with the service provider of your signature. To ensure normal operation for your router, update your signature again is recommended.

Copyright © DrayTek Corp. All Rights Reserved.

(Above figure supposes you have not activated Anti-Spam and Web Content Filter yet.)

10. Click **Close**.
11. Open **Defense Configuration>>Activation** page of the router's web configurator. The start date and expire date for the license are shown in this page.

Defense Configuration >> Activation Activate via interface : WAN 1

Anti-Intrusion/Anti-Virus License [Activate](#)
 [Status:DT-DT] [Start Date:2010-05-03 Expire Date:2011-05-04]

Anti-Spam License [Activate](#)
 [Status:Not Activated]

Web-Filter License [Activate](#)
 [Status:Not Activated]

Authentication Message

```

AV/AI, Get new license successful, 2010-05-03 06:31:09
Activated Wiz, Activated Wizard query license status Successful, 2010-05-03
06:07:27
WebFilter, service not activate 2010-04-28 05:43:24
Anti-Spam, service not activate 2010-04-28 05:43:24
AV/AI, service not activate 2010-04-28 05:43:24
          
```

Note: If you want to use email alert or syslog, please configure the [SysLog/Mail Alert Setup](#) page.
 If you change the service provider, the configuration of the function will be reset.

12. Click **Activate** to access into VigorPro website again. Open the following page. You will see the AI-AV (with provider DT-DT) service as been activated and in use.

My Product

Device Information

Nickname : 5510ni
 Serial : 20100503140901
 Model : VigorPro5510

Device's Service
Expired License

Service	Provider	Action	Status	Start Date	Expired Date
AV	DT-DT	<input type="button" value="Renew"/>	● <input type="button" value="On"/>	2010-05-03	2011-05-04
AV	DT-KL	<input type="button" value="Trial"/>	● <input type="button" value="On"/>	-	-
WCF	CT-CF	<input type="button" value="Trial"/>	● <input type="button" value="On"/>	-	-
AS	CTCH	<input type="button" value="Trial"/>	● <input type="button" value="On"/>	-	-

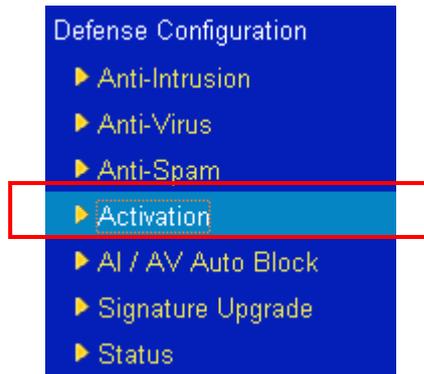
Now, you have finished Anti-Intrusion/Anti-Virus configuration.

4.4.2 For Anti-Spam Service

Please follow the steps below to activate Anti-Spam Service for your system.

Getting 30 Days of Free Charge

1. Open a web browser on your PC and type **http://192.168.1.1**. A pop-up window will open to ask for username and password.
2. From the router's web page, please open **Defense Configuration >>Activation**. You will see the following web page.



3. Click the **Activate** link from Anti-Spam License to activate Anti-Spam service.

Defense Configuration >> Activation Activate via interface : WAN 1

Anti-Intrusion/Anti-Virus License [Activate](#)
[Status:DT-DT] [Start Date:2010-05-03 Expire Date:2011-05-04]

Anti-Spam License [Activate](#)
[Status:Not Activated]

Web-Filter License [Activate](#)
[Status:Not Activated]

Authentication Message

```
AV/AI, Get new license successful, 2010-05-03 06:31:09
Activated Wiz, Activated Wizard query license status Successful, 2010-05-03
06:07:27
WebFilter, service not activate 2010-04-28 05:43:24
Anti-Spam, service not activate 2010-04-28 05:43:24
AV/AI, service not activate 2010-04-28 05:43:24
```

Note: If you want to use email alert or syslog, please configure the [SysLog/Mail Alert Setup](#) page.
If you change the service provider, the configuration of the function will be reset.

- A **Login** page will be shown on the screen. Please type the account and password that you created previously. And click **Login**.

This service is available for MyVigor member only. Please login to access MyVigor. If you are not one of the members of MyVigor, please create an account first.

LOGIN

UserName :

Password :

Auth Code : T4he1C

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

Forget password?

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

If you are having difficulty logging in, contact our customer service.
 Customer Service : (886) 3 597 2727 or
 email to : webmaster@draytek.com

- On the web page of **My Product**, click the **Trial** button for **AS** (Anti-Spam) service.

My Product

Device Information

Nickname : **5510ni**
 Serial : **20100503140901**
 Model : **VigorPro5510**

Device's Service
Expired License

Service	Provider	Action	Status	Start Date	Expired Date
AV	AI- DT-DT	<input type="button" value="Renew"/>	● <input type="button" value="On"/>	2010-05-03	2011-05-04
AV	AI- DT-KL	<input type="button" value="Trial"/>	● <input type="button" value="On"/>	-	-
WCF	CT-CF	<input type="button" value="Trial"/>	● <input type="button" value="On"/>	-	-
AS	CTCH	<input type="button" value="Trial"/>	● <input type="button" value="On"/>	-	-

- In this page, check the box of “**I have read and accept the above Agreement**”. The system will find out the date for you to activate this version of service. Then, click **Next**.

Confirm Message

User Name : sandyni
Serial : 20100503140901
Model : VigorPro5510

License Number	Service Provider	Status
End User License Agreement		
for Anti-Spam service on VigorPro router		
Ver 1.0		
PLEASE READ THIS SOFTWARE LICENSE AGREEMENT (LICENSE) CAREFULLY BEFORE DOWNLOADING OR OTHERWISE USING THE SOFTWARE. BY DOWNLOADING, INSTALLING OR USING THE SOFTWARE, YOU ARE AGREEING TO BE BOUND BY THE TERMS OF THIS LICENSE. IF YOU DO NOT AGREE		
<input checked="" type="checkbox"/> I have read and accept the above Agreement. (Please check this box).		

Note: CTCH means you can acquire anti-spam service from Commtouch.

- When this page appears, click **Register**.

Apply For A License Number

Service Name: **AS**

STEP 2

Activation Date (MM-DD-YYYY):

- Next, the DrayTek Service Activation screen will be shown as the following.

DrayTek Service Activation

Service Name	Start Date	Expire Date	Status
Anti-Virus	2010-05-03	2011-05-04	DT-DT
Web Content filter	---	---	Not Activated
Anti-Spam	2010-05-03	2010-06-02	CTCH

Please check if the license fits with the service provider of your signature. To ensure normal operation for your router, update your signature again is recommended.

Copyright © DrayTek Corp. All Rights Reserved.

- Click **Close**.
- Open **Defense Configuration>>Activation** page of the router's web configurator. The start date and expire date for the license are shown in this page.

Defense Configuration >> Activation Activate via interface : WAN 1

Anti-Intrusion/Anti-Virus License [Status:DT-DT] [Start Date:2010-05-03 Expire Date:2011-05-04]	Activate
Anti-Spam License [Status:CTCH] [Start Date:2010-05-03 Expire Date:2010-06-02]	Activate
Web-Filter License [Status:Not Activated]	Activate

Authentication Message

```
Activated Wiz, Activated Wizard query license status Successful, 2010-05-03
06:07:27
Anti-Spam, Get new license successful, 2010-05-03 06:41:43
AV/AI, Get new license successful, 2010-05-03 06:31:09
```

Note: If you want to use email alert or syslog, please configure the [SysLog/Mail Alert Setup](#) page.
If you change the service provider, the configuration of the function will be reset.

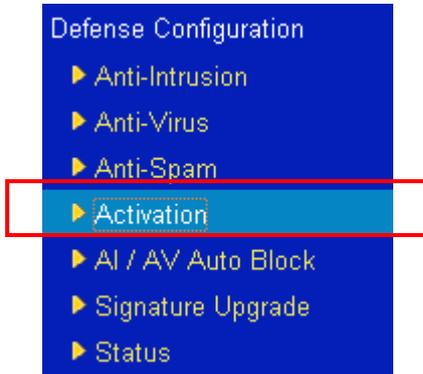
Now, you have finished all the procedure for activating Anti-Spam service for your router.

Note: You are allowed to use this version (with anti-spam feature) for 30 days after registration for your router. In addition, you will be informed with an e-mail before expire date of this version.

4.4.3 For WCF (Web Content Filter) Service

Please follow the steps below to activate WCF Service for your system.

1. Open a web browser on your PC and type **http://192.168.1.1**. A pop-up window will open to ask for username and password.
2. From the router's web page, please open **Defense Configuration >>Activation**. You will see the following web page.



3. Click the **Activate** link from Web-Filter License to activate WCF service.

Defense Configuration >> Activation Activate via interface : WAN 1

Anti-Intrusion/Anti-Virus License [Status:DT-DT] [Start Date:2010-05-03 Expire Date:2011-05-04]	Activate
Anti-Spam License [Status:CTCH] [Start Date:2010-05-03 Expire Date:2010-06-02]	Activate
Web-Filter License [Status:Not Activated]	Activate

Authentication Message

```
Activated Wiz, Activated Wizard query license status Successful, 2010-05-03
06:07:27
Anti-Spam, Get new license successful, 2010-05-03 06:41:43
AV/AI, Get new license successful, 2010-05-03 06:31:09
```

Note: If you want to use email alert or syslog, please configure the [SysLog/Mail Alert Setup](#) page.
If you change the service provider, the configuration of the function will be reset.

- A **Login** page will be shown on the screen. Please type the account and password that you created previously. And click **Login**.

This service is available for MyVigor member only. Please login to access MyVigor. If you are not one of the members of MyVigor, please create an account first.

LOGIN

UserName :

Password :

Auth Code : T4he1C

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

Forget password?

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

If you are having difficulty logging in, contact our customer service.
 Customer Service : (886) 3 597 2727 or
 email to : webmaster@draytek.com

- On the web page of **My Product**, click the **Trial** button for **WCF** (Web Content Filter) service.

My Product

Device Information

Nickname : 5510ni
 Serial : 20100503140901
 Model : VigorPro5510

Device's Service

Expired License

Service	Provider	Action	Status	Start Date	Expired Date
AV	AL-DT-DT	<input type="button" value="Renew"/>	● <input type="button" value="On"/>	2010-05-03	2011-05-04
AV	AL-DT-KL	<input type="button" value="Trial"/>	● <input type="button" value="On"/>	-	-
WCF	CT-CF	<input style="border: 2px solid red;" type="button" value="Trial"/>	● <input type="button" value="On"/>	-	-
AS	CTCH	<input type="button" value="Renew"/>	● <input type="button" value="On"/>	2010-05-03	2010-06-02

● Means such service is in use.

● Means such service is not in use.

● Means such service has not been activated yet.

● Means such service is in use and will be invalid soon (less than one month).

Allows you to have the free trial for service.

Allows you to renew service license.

Allows you to activate service.

- In this page, check the box of “**I have read and accept the above Agreement**”. The system will find out the date for you to activate this version of service. Then, click **Next**.

Confirm Message

User Name : sandyni
Serial : 20100503140901
Model : VigorPro5510

License Number	Service Provider	Status
End User License Agreement		
for Anti-Spam service on VigorPro router		
Ver 1.0		
PLEASE READ THIS SOFTWARE LICENSE AGREEMENT (LICENSE) CAREFULLY BEFORE DOWNLOADING OR OTHERWISE USING THE SOFTWARE. BY DOWNLOADING, INSTALLING OR USING THE SOFTWARE, YOU ARE AGREEING TO BE BOUND BY THE TERMS OF THIS LICENSE. IF YOU DO NOT AGREE		
<input checked="" type="checkbox"/> I have read and accept the above Agreement. (Please check this box).		

- When this page appears, click **Register**.

Apply For A License Number

Service Name: WCF

STEP 2

Activation Date (MM-DD-YYYY):

- Next, the DrayTek Service Activation screen will be shown as the following.

DrayTek Service Activation

Service Name	Start Date	Expire Date	Status
Anti-Virus	2010-05-03	2011-05-04	DT-DT
Web Content filter	2010-05-03	2010-06-02	CT-CF
Anti-Spam	2010-05-03	2010-06-02	CTCH

Please check if the license fits with the service provider of your signature. To ensure normal operation for your router, update your signature again is recommended.

Copyright © DrayTek Corp. All Rights Reserved.

- Click **Close**.
- Open **Defense Configuration>>Activation** page of the router's web configurator. The start date and expire date for the license are shown in this page.

Defense Configuration >> Activation Activate via interface : WAN 1

Anti-Intrusion/Anti-Virus License [Activate](#)
[Status:DT-DT] [Start Date:2010-05-03 Expire Date:2011-05-04]

Anti-Spam License [Activate](#)
[Status:CTCH] [Start Date:2010-05-03 Expire Date:2010-06-02]

Web-Filter License [Activate](#)
[Status:CT-CF] [Start Date:2010-05-03 Expire Date:2010-06-02]

Authentication Message

```
WebFilter, Get new license successful, 2010-05-03 06:57:32
Anti-Spam, Get new license successful, 2010-05-03 06:41:43
AV/AI, Get new license successful, 2010-05-03 06:31:09
```

Note: If you want to use email alert or syslog, please configure the [SysLog/Mail Alert Setup](#) page.
If you change the service provider, the configuration of the function will be reset.

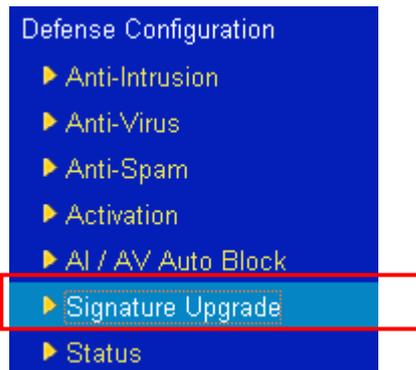
Now, you have finished all the procedure for activating WCF service for your router.

Note: You are allowed to use this version (with WCF feature) for few days after registration for your router. In addition, you will be informed with an e-mail before expire date of this version.

4.5 Backup and Upgrade Signature for Anti-Intrusion/Anti-Virus

You can get the most updated signature from DrayTek's server if the license key of anti-virus/anti-intrusion for the VigorPro 5510 is not expired. Before you upgrade the signature, please check the validation information either from WEB user interface of VigorPro 5510 or account information from www.vigorpro.com.

1. Open a web browser on your PC and type **http://192.168.1.1**. A pop-up window will open to ask for username and password. Do not type any word on the window and click **OK**.
2. From the router's web page, please open **Defense Configuration >>Signature Upgrade**. You will see the following web page.



3. On Signature Upgrade web page, locate **Backup** and **Download Now!!!**.

Defense Configuration >> Signature Upgrade

Signature Upgrade Setting
Signature Version : DT-KL_2_46.0.0
Signature Build Date : Wed Jan 13 10:02:36.00 2010
Upgrade via interface : WAN 1

Setup download server	auto-selected	find more
Setup query server	auto-selected	find more

Signature authentication/download message:

Upgrade Manually

<input type="button" value="Import"/>	<input type="button" value="Backup"/>	<input type="button" value="Download Now !!!"/>
---------------------------------------	---------------------------------------	---

Upgrade Automatically
 Scheduled Update

Time for Backup

Before changing other license, it is suggested for you to backup the original signature first. To backup current signature with the filename `vigorpro.sig`, click **Backup**.

Time for Download

After changing other license, it is suggested for you to download newly update signature for your router. To download newly update anti-intrusion and anti-virus from VigorPro website, please click **Download Now!!!**.

Time for Import

Backup files can be imported whenever you want. To use a saved signature information, please click **Import**.

In addition, users can specify certain time for executing the upgrade automatically by the router. Remember to check the **Schedule Update** box and click **OK** to activate the time settings.

4.6 Enabling Anti-Virus/Anti-Intrusion/Anti-Spam/WCF

After applying an account, registering your account and router, you have to access into the web page of Vigor router to enable Anti-Virus/Anti-Intrusion/Anti-Spam/Web Content Filter (WCF) functions. There are two ways to enable it.

- A. For the default rule of firewall, please open **Firewall>>General Setup** page. Check the box of **Enable** for Anti-Intrusion and choose proper action (profile) from the drop down list of Anti-Virus. Next, click **OK** to finish the procedure of activation.

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

Actions for default rule:

Application	Action/Profile	Syslog
Filter	Pass	<input type="checkbox"/>
IM/P2P Filter	None	<input type="checkbox"/>
URL Content Filter	None	<input type="checkbox"/>
Web Content Filter	None	<input type="checkbox"/>
Anti-Virus	None	<input type="checkbox"/>
Anti-Intrusion	<input type="checkbox"/> Enable	<input type="checkbox"/>
Anti-Spam	None	<input type="checkbox"/>

Advance Setting

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

Strict Security Checking

<input type="checkbox"/> Anti-Virus	<input type="checkbox"/> Anti-Spam	<input type="checkbox"/> In-Sequence
-------------------------------------	------------------------------------	--------------------------------------

- B. For specified filter rule (there are twelve filter sets in Firewall, and each set is allowed to set seven filter rules), please check the box of **Enable** for Anti-Intrusion and choose proper action (profile) from the drop down list of Anti-Virus/Anti-Spam/Web Content Filter. Next, click **OK** to finish the procedure of activation.

Firewall >> Edit Filter Set >> Edit Filter Rule

Filter Set 1 Rule 1

Check to enable the Filter Rule

Comments: Block NetBios

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

Direction: LAN -> WAN

Source IP: Any [Edit]

Destination IP: Any [Edit]

Service Type: TCP/UDP, Port: from 137~139 to undefined [Edit]

Fragments: Don't Care

Application	Action/Profile	Syslog
Filter:	Pass If No Further Match	<input type="checkbox"/>
Branch to Other Filter Set:	None	
IM/P2P Filter:	None	<input type="checkbox"/>
URL Content Filter	None	<input type="checkbox"/>
Web Content Filter	None	<input type="checkbox"/>
Anti-Virus:	None	<input type="checkbox"/>
Anti-Intrusion:	<input type="checkbox"/> Enable	<input type="checkbox"/>
Anti-Spam:	None	<input type="checkbox"/>

Advance Setting [Edit]

OK Clear Cancel

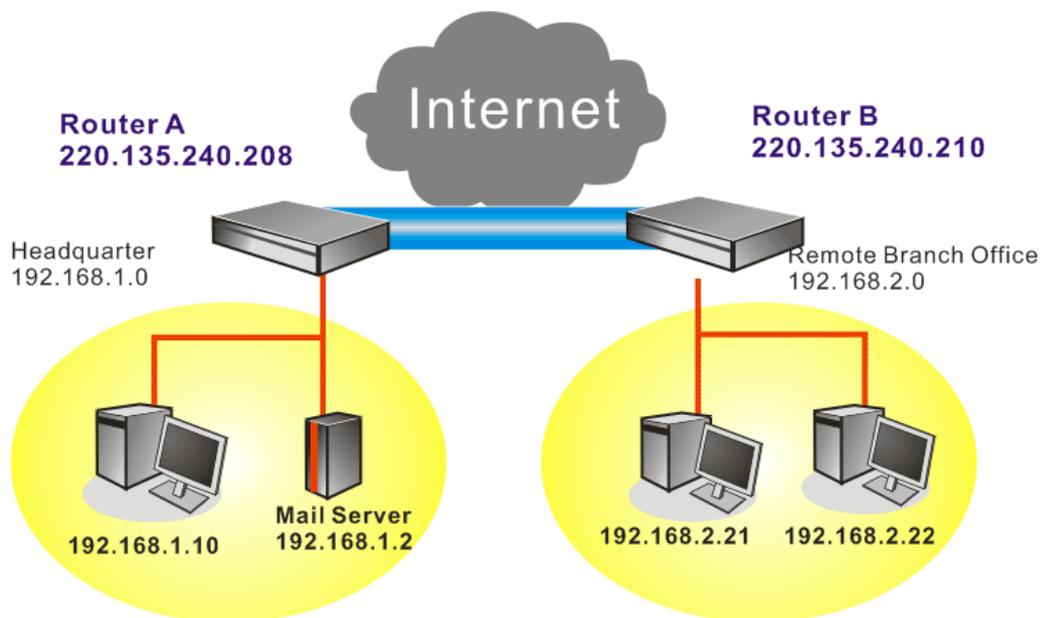
If you **did not** check the Anti-Intrusion box and choose a proper profile for Anti-Virus/Anti-Spam/Web Content Filter, you still **cannot use** the Anti-Intrusion/Anti-Virus/Anti-Spam/Web Content Filter function even if you finished all the relational profiles.

5

Application and Examples

5.1 Create a LAN-to-LAN Connection Between Remote Office and Headquarter

The most common case is that you may want to connect to network securely, such as the remote branch office and headquarter. According to the network structure as shown in the below illustration, you may follow the steps to create a LAN-to-LAN profile. These two networks (LANs) should NOT have the same network address.



Settings in Router A in headquarter:

1. Go to **VPN and Remote Access** and select **Remote Access Control** to enable the necessary VPN service and click **OK**.
2. Then,
For using **PPP** based services, such as PPTP, L2TP, you have to set general settings in **PPP General Setup**.

VPN and Remote Access >> PPP General Setup

PPP General Setup

PPP/MP Protocol		IP Address Assignment for Dial-In Users (When DHCP Disable set)	
Dial-In PPP Authentication	PAP or CHAP	Assigned IP range	192.168.1.200
Dial-In PPP Encryption (MPPE)	Optional MPPE		
Mutual Authentication (PAP)	<input type="radio"/> Yes <input checked="" type="radio"/> No		
Username	<input type="text"/>		
Password	<input type="text"/>		

OK

For using **IPSec**-based service, such as IPSec or L2TP with IPSec Policy, you have to set general settings in **IPSec General Setup**, such as the pre-shared key that both parties have known.

VPN and Remote Access >> IPSec General Setup

VPN IKE/IPSec General Setup
Dial-in Set up for Remote Dial-in users and Dynamic IP Client (LAN to LAN).

IKE Authentication Method	
Pre-Shared Key
Confirm Pre-Shared Key
IPSec Security Method	
<input checked="" type="checkbox"/> Medium (AH) Data will be authentic, but will not be encrypted.	
High (ESP) <input checked="" type="checkbox"/> DES <input checked="" type="checkbox"/> 3DES <input checked="" type="checkbox"/> AES Data will be encrypted and authentic.	

OK Cancel

3. Go to **LAN-to-LAN**. Click on one index number to edit a profile.
4. Set **Common Settings** as shown below. You should enable both of VPN connections because any one of the parties may start the VPN connection.

VPN and Remote Access >> LAN to LAN

Profile Index : 1

1. Common Settings

Profile Name	Branch1	Call Direction	<input checked="" type="radio"/> Both <input type="radio"/> Dial-Out <input type="radio"/> Dial-In
<input checked="" type="checkbox"/> Enable this profile		<input type="checkbox"/> Always on	
VPN Connection Through:	WAN1 First	Idle Timeout	300 second(s)
Netbios Naming Packet	<input checked="" type="radio"/> Pass <input type="radio"/> Block	<input type="checkbox"/> Enable PING to keep alive	
		PING to the IP	<input type="text"/>

5. Set **Dial-Out Settings** as shown below to dial to connect to Router B aggressively with the selected Dial-Out method.

If an **IPSec-based** service is selected, you should further specify the remote peer IP Address, IKE Authentication Method and IPSec Security Method for this Dial-Out connection.

2. Dial-Out Settings

Type of Server I am calling <input type="radio"/> ISDN <input type="radio"/> PPTP <input checked="" type="radio"/> IPsec Tunnel <input type="radio"/> L2TP with IPsec Policy None	Link Type 64k bps Username ??? Password PPP Authentication PAP/CHAP VJ Compression <input checked="" type="radio"/> On <input type="radio"/> Off
Dial Number for ISDN or Server IP/Host Name for VPN. (such as 5551234, draytek.com or 123.45.67.89) 220.135.240.210	IKE Authentication Method <input checked="" type="radio"/> Pre-Shared Key IKE Pre-Shared Key <input type="radio"/> Digital Signature(X.509) None
	IPsec Security Method <input checked="" type="radio"/> Medium(AH) <input type="radio"/> High(ESP) DES without Authentication Advanced
	Index(1-15) in Schedule Setup:
	Callback Function (CBCP) <input type="checkbox"/> Require Remote to Callback <input type="checkbox"/> Provide ISDN Number to Remote

If a **PPP-based service** is selected, you should further specify the remote peer IP Address, Username, Password, PPP Authentication and VJ Compression for this Dial-Out connection.

2. Dial-Out Settings

Type of Server I am calling <input type="radio"/> ISDN <input checked="" type="radio"/> PPTP <input type="radio"/> IPsec Tunnel <input type="radio"/> L2TP with IPsec Policy None	Link Type 64k bps Username draytek Password ***** PPP Authentication PAP/CHAP VJ Compression <input checked="" type="radio"/> On <input type="radio"/> Off
Dial Number for ISDN or Server IP/Host Name for VPN. (such as 5551234, draytek.com or 123.45.67.89) 220.135.240.210	IKE Authentication Method <input checked="" type="radio"/> Pre-Shared Key IKE Pre-Shared Key <input type="radio"/> Digital Signature(X.509) None
	IPsec Security Method <input checked="" type="radio"/> Medium(AH) <input type="radio"/> High(ESP) DES without Authentication Advanced
	Index(1-15) in Schedule Setup:
	Callback Function (CBCP) <input type="checkbox"/> Require Remote to Callback <input type="checkbox"/> Provide ISDN Number to Remote

- Set **Dial-In settings** to as shown below to allow Router B dial-in to build VPN connection.

If an **IPsec-based** service is selected, you may further specify the remote peer IP Address, IKE Authentication Method and IPsec Security Method for this Dial-In connection. Otherwise, it will apply the settings defined in **IPsec General Setup** above.

3. Dial-In Settings

<p>Allowed Dial-In Type</p> <input type="checkbox"/> ISDN <input type="checkbox"/> PPTP <input checked="" type="checkbox"/> IPsec Tunnel <input type="checkbox"/> L2TP with IPsec Policy None	<p>Username <input data-bbox="949 235 1101 257" type="text" value="???"/></p> <p>Password <input data-bbox="949 268 1093 291" type="password"/></p> <p>VJ Compression <input checked="" type="radio"/> On <input type="radio"/> Off</p>
<p><input checked="" type="checkbox"/> Specify ISDN CLID or Remote VPN Gateway Peer ISDN Number or Peer VPN Server IP <input data-bbox="406 414 566 436" type="text" value="220.135.240.210"/></p> <p>or Peer ID <input data-bbox="478 448 638 470" type="text"/></p>	<p>IKE Authentication Method</p> <input checked="" type="checkbox"/> Pre-Shared Key <input data-bbox="949 380 1101 403" type="text" value=""/> <input type="checkbox"/> Digital Signature(X.509) None
	<p>IPsec Security Method</p> <input checked="" type="checkbox"/> Medium (AH) High (ESP) <input checked="" type="checkbox"/> DES <input checked="" type="checkbox"/> 3DES <input checked="" type="checkbox"/> AES
	<p>Callback Function (CBCP)</p> <input type="checkbox"/> Enable Callback Function <input type="checkbox"/> Use the Following Number to Callback Callback Number <input data-bbox="949 660 1101 683" type="text"/> Callback Budget <input data-bbox="949 694 981 716" type="text" value="0"/> minute(s)

If a **PPP-based service** is selected, you should further specify the remote peer IP Address, Username, Password, and VJ Compression for this Dial-In connection.

3. Dial-In Settings

<p>Allowed Dial-In Type</p> <input type="checkbox"/> ISDN <input checked="" type="checkbox"/> PPTP <input type="checkbox"/> IPsec Tunnel <input type="checkbox"/> L2TP with IPsec Policy None	<p>Username <input data-bbox="949 907 1093 929" type="text" value="draytek"/></p> <p>Password <input data-bbox="949 940 1085 963" type="password"/></p> <p>VJ Compression <input checked="" type="radio"/> On <input type="radio"/> Off</p>
<p><input checked="" type="checkbox"/> Specify ISDN CLID or Remote VPN Gateway Peer ISDN Number or Peer VPN Server IP <input data-bbox="406 1075 566 1097" type="text" value="220.135.240.210"/></p> <p>or Peer ID <input data-bbox="478 1108 638 1131" type="text"/></p>	<p>IKE Authentication Method</p> <input checked="" type="checkbox"/> Pre-Shared Key <input data-bbox="949 1041 1101 1064" type="text" value=""/> <input type="checkbox"/> Digital Signature(X.509) None
	<p>IPsec Security Method</p> <input checked="" type="checkbox"/> Medium (AH) High (ESP) <input checked="" type="checkbox"/> DES <input checked="" type="checkbox"/> 3DES <input checked="" type="checkbox"/> AES
	<p>Callback Function (CBCP)</p> <input type="checkbox"/> Enable Callback Function <input type="checkbox"/> Use the Following Number to Callback Callback Number <input data-bbox="949 1321 1101 1344" type="text"/> Callback Budget <input data-bbox="949 1355 981 1377" type="text" value="0"/> minute(s)

- At last, set the remote network IP/subnet in **TCP/IP Network Settings** so that Router A can direct the packets destined to the remote network to Router B via the VPN connection.

<p>My WAN IP <input data-bbox="630 1556 805 1579" type="text" value="0.0.0.0"/></p> <p>Remote Gateway IP <input data-bbox="630 1590 805 1612" type="text" value="0.0.0.0"/></p> <p>Remote Network IP <input data-bbox="630 1624 805 1646" type="text" value="192.168.2.0"/></p> <p>Remote Network Mask <input data-bbox="630 1657 805 1680" type="text" value="255.255.255.0"/></p> <p><input data-bbox="630 1702 710 1724" type="button" value="More"/></p>	<p>RIP Direction Disable</p> <p>From first subnet to remote network, you have to do</p> <p><input data-bbox="1109 1635 1189 1657" type="button" value="Route"/></p> <p><input type="checkbox"/> Change default route to this VPN tunnel (Only single WAN supports this)</p>
--	--

Settings in Router B in the remote office:

- Go to **VPN and Remote Access** and select **Remote Access Control** to enable the necessary VPN service and click **OK**.

- Then, for using **PPP based** services, such as PPTP, L2TP, you have to set general settings in **PPP General Setup**.

VPN and Remote Access >> PPP General Setup

PPP General Setup

<p>PPP/MP Protocol</p> <p>Dial-In PPP Authentication <input type="text" value="PAP or CHAP"/></p> <p>Dial-In PPP Encryption (MPPE) <input type="text" value="Optional MPPE"/></p> <p>Mutual Authentication (PAP) <input type="radio"/> Yes <input checked="" type="radio"/> No</p> <p>Username <input type="text"/></p> <p>Password <input type="text"/></p>	<p>IP Address Assignment for Dial-In Users (When DHCP Disable set)</p> <p>Assigned IP range <input type="text" value="192.168.2.200"/></p>
---	---

For using **IPSec-based** service, such as IPSec or L2TP with IPSec Policy, you have to set general settings in **IPSec General Setup**, such as the pre-shared key that both parties have known.

VPN and Remote Access >> IPSec General Setup

VPN IKE/IPSec General Setup

Dial-in Set up for Remote Dial-in users and Dynamic IP Client (LAN to LAN).

<p>IKE Authentication Method</p> <p>Pre-Shared Key <input type="text" value="....."/></p> <p>Confirm Pre-Shared Key <input type="text" value="....."/></p> <p>IPSec Security Method</p> <p><input checked="" type="checkbox"/> Medium (AH) Data will be authentic, but will not be encrypted.</p> <p>High (ESP) <input checked="" type="checkbox"/> DES <input checked="" type="checkbox"/> 3DES <input checked="" type="checkbox"/> AES Data will be encrypted and authentic.</p>
--

- Go to **LAN-to-LAN**. Click on one index number to edit a profile.
- Set **Common Settings** as shown below. You should enable both of VPN connections because any one of the parties may start the VPN connection.

VPN and Remote Access >> LAN to LAN

Profile Index : 1

1. Common Settings

<p>Profile Name <input type="text" value="Branch1"/></p> <p><input checked="" type="checkbox"/> Enable this profile</p> <p>VPN Connection Through: <input type="text" value="WAN1 First"/></p> <p>Netbios Naming Packet <input checked="" type="radio"/> Pass <input type="radio"/> Block</p>	<p>Call Direction <input checked="" type="radio"/> Both <input type="radio"/> Dial-Out <input type="radio"/> Dial-In</p> <p><input type="checkbox"/> Always on</p> <p>Idle Timeout <input type="text" value="300"/> second(s)</p> <p><input type="checkbox"/> Enable PING to keep alive</p> <p>PING to the IP <input type="text"/></p>
---	--

- Set **Dial-Out Settings** as shown below to dial to connect to Router B aggressively with the selected Dial-Out method.

If an **IPSec-based** service is selected, you should further specify the remote peer IP Address, IKE Authentication Method and IPSec Security Method for this Dial-Out

connection.

2. Dial-Out Settings

Type of Server I am calling <input type="radio"/> ISDN <input type="radio"/> PPTP <input checked="" type="radio"/> IPsec Tunnel <input type="radio"/> L2TP with IPsec Policy <input type="text" value="None"/>	Link Type <input type="text" value="64k bps"/> Username <input type="text" value="???"/> Password <input type="text"/> PPP Authentication <input type="text" value="PAP/CHAP"/> VJ Compression <input checked="" type="radio"/> On <input type="radio"/> Off
Dial Number for ISDN or Server IP/Host Name for VPN. (such as 5551234, draytek.com or 123.45.67.89) <input type="text" value="220.135.240.208"/>	IKE Authentication Method <input checked="" type="radio"/> Pre-Shared Key IKE Pre-Shared Key <input type="text"/> <input type="radio"/> Digital Signature(X.509) <input type="text" value="None"/>
	IPsec Security Method <input checked="" type="radio"/> Medium(AH) <input type="radio"/> High(ESP) <input type="text" value="DES without Authentication"/> <input type="button" value="Advanced"/>
	Index(1-15) in Schedule Setup: <input type="text"/> <input type="text"/> <input type="text"/> <input type="text"/>
	Callback Function (CBCP) <input type="checkbox"/> Require Remote to Callback <input type="checkbox"/> Provide ISDN Number to Remote

If a **PPP-based** service is selected, you should further specify the remote peer IP Address, Username, Password, PPP Authentication and VJ Compression for this Dial-Out connection.

2. Dial-Out Settings

Type of Server I am calling <input type="radio"/> ISDN <input checked="" type="radio"/> PPTP <input type="radio"/> IPsec Tunnel <input type="radio"/> L2TP with IPsec Policy <input type="text" value="None"/>	Link Type <input type="text" value="64k bps"/> Username <input type="text" value="draytek"/> Password <input type="text" value="*****"/> PPP Authentication <input type="text" value="PAP/CHAP"/> VJ Compression <input checked="" type="radio"/> On <input type="radio"/> Off
Dial Number for ISDN or Server IP/Host Name for VPN. (such as 5551234, draytek.com or 123.45.67.89) <input type="text" value="220.135.240.208"/>	IKE Authentication Method <input checked="" type="radio"/> Pre-Shared Key IKE Pre-Shared Key <input type="text"/> <input type="radio"/> Digital Signature(X.509) <input type="text" value="None"/>
	IPsec Security Method <input checked="" type="radio"/> Medium(AH) <input type="radio"/> High(ESP) <input type="text" value="DES without Authentication"/> <input type="button" value="Advanced"/>
	Index(1-15) in Schedule Setup: <input type="text"/> <input type="text"/> <input type="text"/> <input type="text"/>
	Callback Function (CBCP) <input type="checkbox"/> Require Remote to Callback <input type="checkbox"/> Provide ISDN Number to Remote

- Set **Dial-In settings** to as shown below to allow Router A dial-in to build VPN connection.

If an **IPsec-based** service is selected, you may further specify the remote peer IP Address, IKE Authentication Method and IPsec Security Method for this Dial-In connection. Otherwise, it will apply the settings defined in **IPsec General Setup** above.

3. Dial-In Settings

Allowed Dial-In Type <input type="checkbox"/> ISDN <input type="checkbox"/> PPTP <input checked="" type="checkbox"/> IPsec Tunnel <input type="checkbox"/> L2TP with IPsec Policy <input type="text" value="None"/> <input checked="" type="checkbox"/> Specify ISDN CLID or Remote VPN Gateway Peer ISDN Number or Peer VPN Server IP <input type="text" value="220.135.240.208"/> or Peer ID <input type="text"/>	Username <input type="text" value="???"/> Password <input type="text"/> VJ Compression <input checked="" type="radio"/> On <input type="radio"/> Off IKE Authentication Method <input checked="" type="checkbox"/> Pre-Shared Key <input type="text" value="IKE Pre-Shared Key"/> <input type="checkbox"/> Digital Signature(X.509) <input type="text" value="None"/> IPsec Security Method <input checked="" type="checkbox"/> Medium (AH) High (ESP) <input checked="" type="checkbox"/> DES <input checked="" type="checkbox"/> 3DES <input checked="" type="checkbox"/> AES Callback Function (CBCP) <input type="checkbox"/> Enable Callback Function <input type="checkbox"/> Use the Following Number to Callback Callback Number <input type="text"/> Callback Budget <input type="text" value="0"/> minute(s)
--	---

If a **PPP-based** service is selected, you should further specify the remote peer IP Address, Username, Password, and VJ Compression for this Dial-In connection.

3. Dial-In Settings

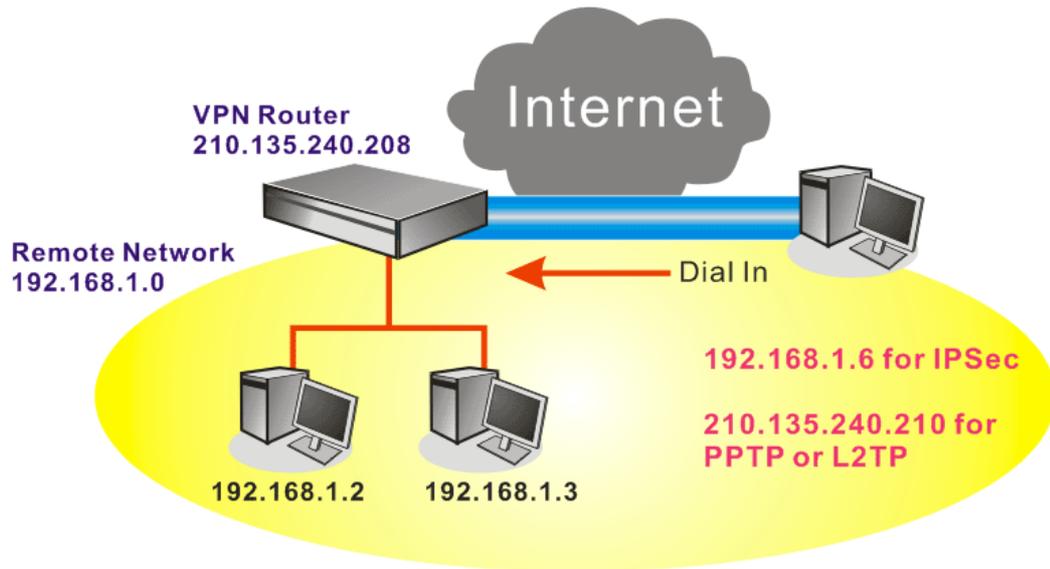
Allowed Dial-In Type <input type="checkbox"/> ISDN <input checked="" type="checkbox"/> PPTP <input type="checkbox"/> IPsec Tunnel <input type="checkbox"/> L2TP with IPsec Policy <input type="text" value="None"/> <input checked="" type="checkbox"/> Specify ISDN CLID or Remote VPN Gateway Peer ISDN Number or Peer VPN Server IP <input type="text" value="220.135.240.208"/> or Peer ID <input type="text"/>	Username <input type="text" value="draytek"/> Password <input type="text" value="*****"/> VJ Compression <input checked="" type="radio"/> On <input type="radio"/> Off IKE Authentication Method <input checked="" type="checkbox"/> Pre-Shared Key <input type="text" value="IKE Pre-Shared Key"/> <input type="checkbox"/> Digital Signature(X.509) <input type="text" value="None"/> IPsec Security Method <input checked="" type="checkbox"/> Medium (AH) High (ESP) <input checked="" type="checkbox"/> DES <input checked="" type="checkbox"/> 3DES <input checked="" type="checkbox"/> AES Callback Function (CBCP) <input type="checkbox"/> Enable Callback Function <input type="checkbox"/> Use the Following Number to Callback Callback Number <input type="text"/> Callback Budget <input type="text" value="0"/> minute(s)
--	---

- At last, set the remote network IP/subnet in **TCP/IP Network Settings** so that Router B can direct the packets destined to the remote network to Router A via the VPN connection.

My WAN IP <input type="text" value="0.0.0.0"/> Remote Gateway IP <input type="text" value="0.0.0.0"/> Remote Network IP <input type="text" value="192.168.1.0"/> Remote Network Mask <input type="text" value="255.255.255.0"/> <input type="button" value="More"/>	RIP Direction <input type="text" value="Disable"/> From first subnet to remote network, you have to do <input type="text" value="Route"/> <input type="checkbox"/> Change default route to this VPN tunnel (Only single WAN supports this)
---	---

5.2 Create a Remote Dial-in User Connection Between the Teleworker and Headquarter

The other common case is that you, as a teleworker, may want to connect to the enterprise network securely. According to the network structure as shown in the below illustration, you may follow the steps to create a Remote User Profile and install Smart VPN Client on the remote host.



Settings in VPN Router in the enterprise office:

1. Go to **VPN and Remote Access** and select **Remote Access Control** to enable the necessary VPN service and click **OK**.
2. Then, for using PPP based services, such as PPTP, L2TP, you have to set general settings in **PPP General Setup**.

VPN and Remote Access >> PPP General Setup

PPP General Setup	
PPP/MP Protocol	
Dial-In PPP Authentication	PAP or CHAP
Dial-In PPP Encryption (MPPE)	Optional MPPE
Mutual Authentication (PAP)	<input type="radio"/> Yes <input checked="" type="radio"/> No
Username	<input type="text"/>
Password	<input type="text"/>
IP Address Assignment for Dial-In Users	
Start IP Address	192.168.1.200

For using IPSec-based service, such as IPSec or L2TP with IPSec Policy, you have to set general settings in **IKE/IPSec General Setup**, such as the pre-shared key that both parties have known.

VPN and Remote Access >> IPSec General Setup

VPN IKE/IPSec General Setup

Dial-in Set up for Remote Dial-in users and Dynamic IP Client (LAN to LAN).

IKE Authentication Method	
Pre-Shared Key	<input type="password" value="....."/>
Confirm Pre-Shared Key	<input type="password" value="....."/>
IPSec Security Method	
<input checked="" type="checkbox"/> Medium (AH)	Data will be authentic, but will not be encrypted.
High (ESP) <input checked="" type="checkbox"/> DES <input checked="" type="checkbox"/> 3DES <input checked="" type="checkbox"/> AES	Data will be encrypted and authentic.

OK Cancel

3. Go to **Remote Dial-In Users**. Click on one index number to edit a profile.
4. Set **Dial-In** settings to as shown below to allow the remote user dial-in to build VPN connection.

If an **IPSec** service is selected, you may further specify the remote peer IP Address, IKE Authentication Method and IPSec Security Method for this Dial-In connection. Otherwise, it will apply the settings defined in **IPSec General Setup** above.

VPN and Remote Access >> Remote Dial-in User

Index No. 1

User account and Authentication <input checked="" type="checkbox"/> Enable this account Idle Timeout <input type="text" value="300"/> second(s)	Username <input type="text" value="???"/> Password <input type="password"/>
Allowed Dial-In Type <input type="checkbox"/> ISDN <input type="checkbox"/> PPTP <input checked="" type="checkbox"/> IPSec Tunnel <input type="checkbox"/> L2TP with IPSec Policy <input type="text" value="None"/> <input type="checkbox"/> SSL Tunnel	IKE Authentication Method <input checked="" type="checkbox"/> Pre-Shared Key IKE Pre-Shared Key <input type="text"/> <input type="checkbox"/> Digital Signature (X.509) <input type="text" value="None"/>
<input checked="" type="checkbox"/> Specify Remote Node Remote Client IP or Peer ISDN Number <input type="text" value="210.135.240.210"/> or Peer ID <input type="text"/> Netbios Naming Packet <input checked="" type="radio"/> Pass <input type="radio"/> Block	IPSec Security Method <input checked="" type="checkbox"/> Medium (AH) High (ESP) <input checked="" type="checkbox"/> DES <input checked="" type="checkbox"/> 3DES <input checked="" type="checkbox"/> AES Local ID <input type="text"/> (optional)
SSL VPN Set SSL Web Proxy	Callback Function <input type="checkbox"/> Check to enable Callback function <input type="checkbox"/> Specify the callback number Callback Number <input type="text"/> <input checked="" type="checkbox"/> Check to enable Callback Budget Control Callback Budget <input type="text" value="30"/> minute(s)

OK Clear Cancel

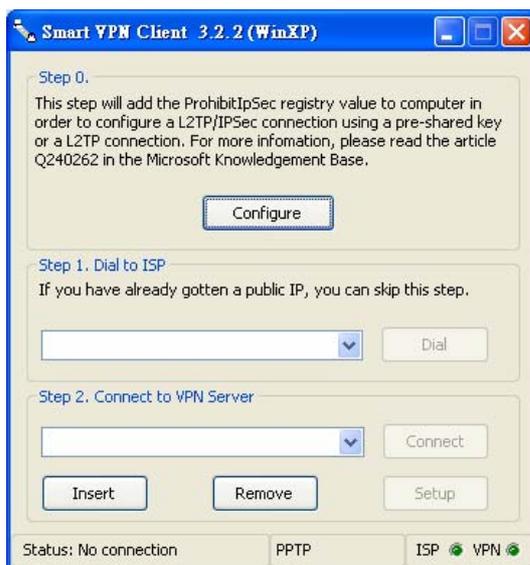
If a **PPTP** service is selected, you should further specify the remote peer IP Address, Username, Password, and VJ Compression for this Dial-In connection.

Index No. 1

<p>User account and Authentication</p> <p><input checked="" type="checkbox"/> Enable this account</p> <p>Idle Timeout <input type="text" value="300"/> second(s)</p>		<p>Username <input style="width: 100px;" type="text" value="???"/></p> <p>Password <input style="width: 100px;" type="password"/></p>
<p>Allowed Dial-In Type</p> <p><input type="checkbox"/> ISDN</p> <p><input checked="" type="checkbox"/> PPTP</p> <p><input type="checkbox"/> IPsec Tunnel</p> <p><input type="checkbox"/> L2TP with IPsec Policy <input type="text" value="None"/></p> <p><input type="checkbox"/> SSL Tunnel</p>		<p>IKE Authentication Method</p> <p><input checked="" type="checkbox"/> Pre-Shared Key</p> <p>IKE Pre-Shared Key <input style="width: 100px;" type="text"/></p> <p><input type="checkbox"/> Digital Signature (X.509)</p> <p><input type="text" value="None"/></p>
<p><input checked="" type="checkbox"/> Specify Remote Node</p> <p>Remote Client IP or Peer ISDN Number <input type="text" value="210.135.240.210"/></p> <p>or Peer ID <input style="width: 100px;" type="text"/></p> <p>Netbios Naming Packet <input checked="" type="radio"/> Pass <input type="radio"/> Block</p>		<p>IPsec Security Method</p> <p><input checked="" type="checkbox"/> Medium (AH)</p> <p>High (ESP)</p> <p><input checked="" type="checkbox"/> DES <input checked="" type="checkbox"/> 3DES <input checked="" type="checkbox"/> AES</p> <p>Local ID <input style="width: 100px;" type="text"/> (optional)</p>
<p>SSL VPN</p> <p>Set SSL Web Proxy</p>		<p>Callback Function</p> <p><input type="checkbox"/> Check to enable Callback function</p> <p><input type="checkbox"/> Specify the callback number</p> <p>Callback Number <input style="width: 100px;" type="text"/></p> <p><input checked="" type="checkbox"/> Check to enable Callback Budget Control</p> <p>Callback Budget <input type="text" value="30"/> minute(s)</p>

Settings in the remote host:

1. For Win98/ME, you may use "Dial-up Networking" to create the PPTP tunnel to Vigor router. For Win2000/XP, please use "Network and Dial-up connections" or "Smart VPN Client", complimentary software to help you create PPTP, L2TP, and L2TP over IPsec tunnel. You can find it in CD-ROM in the package or go to www.draytek.com download center. Install as instructed.
2. After successful installation, for the first time user, you should click on the **Step 0. Configure** button. Reboot the host.



3. In **Step 2. Connect to VPN Server**, click **Insert** button to add a new entry.

If an IPSec-based service is selected as shown below,

Dial To VPN

Session Name: Office

VPN Server IP/HOST Name(such as 123.45.67.89 or draytek.com)

192.168.1.1

User Name : draytek_user1

Password : *****

Type of VPN

PPTP L2TP

IPSec Tunnel L2TP over IPSec

PPTP Encryption

No encryption

Require encryption

Maximum strength encryption

Use default gateway on remote network

OK Cancel

You may further specify the method you use to get IP, the security method, and authentication method. If the Pre-Shared Key is selected, it should be consistent with the one set in VPN router.

IPSec Policy Setting

My IP : 172.16.3.100

Type of IPSec

Standard IPSec Tunnel

Remote Subnet : 0 . 0 . 0 . 0

Remote Subnet Mask : 255 . 255 . 255 . 0

Virture IP DrayTek Virture Interface

Obtain an IP address automatically (DHCP over IPSec)

Specify an IP address

IP Address: 192 . 168 . 1 . 201

Subnet Mask: 255 . 255 . 255 . 0

Security Method

Medium(AH) High(ESP)

MDS DES

Authority Method

Pre-shared Key : *****

Certification Authority: Browse...

OK Cancel

If a PPP-based service is selected, you should further specify the remote VPN server IP address, Username, Password, and encryption method. The User Name and Password should be consistent with the one set up in the VPN router. To use default gateway on remote network means that all the packets of remote host will be directed to VPN server then forwarded to Internet. This will make the remote host seem to be working in the enterprise network.



- Click **Connect** button to build connection. When the connection is successful, you will find a green light on the right down corner.

5.3 QoS Setting Example

Assume a teleworker sometimes works at home and takes care of children. When working time, he would use Vigor router at home to connect to the server in the headquarter office downtown via either HTTPS or VPN to check email and access internal database. Meanwhile, children may chat on Skype in the restroom.

- Go to **Bandwidth Management >> Quality of Service**.

Bandwidth Management >> Quality of Service

General Setup

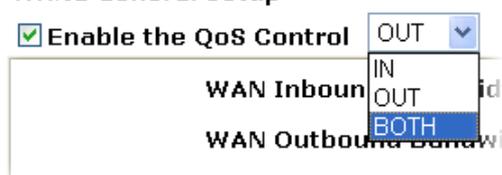
Index	Status	Bandwidth	Direction	Class 1	Class 2	Class 3	Others	UDP Bandwidth Control	
WAN1	Disable	10000Kbps/10000Kbps		25%	25%	25%	25%	Inactive	Setup
WAN2	Disable	10000Kbps/10000Kbps		25%	25%	25%	25%	Inactive	Setup

Class Rule

Index	Name	Rule	Service Type
Class 1		Edit	Edit
Class 2		Edit	
Class 3		Edit	

- Click **Setup** link for WAN1. Make sure the QoS Control on the left corner is checked. And select **BOTH** as the **Direction**.

WAN1 General Setup



- Set Inbound/Outbound bandwidth.

Bandwidth Management >> Quality of Service

WAN1 General Setup

Enable the QoS Control BOTH

WAN Inbound Bandwidth Kbps
 WAN Outbound Bandwidth Kbps

Note: The rate of outbound/inbound must be smaller than the real bandwidth to ensure correct calculation of QoS. It is suggested to set the bandwidth value for inbound/outbound as 80% - 85% of physical network speed provided by ISP to maximize the QoS performance.

- Return to previous page. Enter the Name of Index Class 1 by clicking **Edit** link. Type the name “**E-mail**” for Class 1.

Bandwidth Management >> Quality of Service

Class Index # 1
 Name

NO	Status	Local Address	Remote Address	DiffServ CodePoint	Service Type
1	Active	Any	Any	IP precedence 2	SMTP(TCP:25)

- For this index, the user will set reserved bandwidth (e.g., 25%) for **Email** using protocol POP3 and SMTP.

Bandwidth Management >> Quality of Service

WAN1 General Setup

Enable the QoS Control OUT

WAN Inbound Bandwidth Kbps
 WAN Outbound Bandwidth Kbps

Index	Class Name	Reserved_bandwidth Ratio
Class 1		<input type="text" value="25"/> %
Class 2		<input type="text" value="25"/> %
Class 3		<input type="text" value="25"/> %
	Others	<input type="text" value="25"/> %

Enable UDP Bandwidth Control Limited_bandwidth Ratio %
 Outbound TCP ACK Prioritize

- Return to previous page. Enter the Name of Index Class 2 by clicking **Edit** link. In this index, the user will set reserved bandwidth (e.g., 25%) for **HTTP**.
- Click **Setup** link for WAN1.

Bandwidth Management >> Quality of Service

General Setup

Index	Status	Bandwidth	Directon	Class 1	Class 2	Class 3	Others	UDP Bandwidth Control	
WAN1	Disable	10000Kbps/10000Kbps		25%	25%	25%	25%	Inactive	Setup
WAN2	Disable	10000Kbps/10000Kbps		25%	25%	25%	25%	Inactive	Setup

Class Rule

Index	Name	Rule	Service Type
Class 1		Edit	
Class 2		Edit	Edit
Class 3		Edit	

- Check **Enable UDP Bandwidth Control** on the bottom to prevent enormous UDP traffic of VoIP influent other application, and click OK.

Bandwidth Management >> Quality of Service

WAN1 General Setup

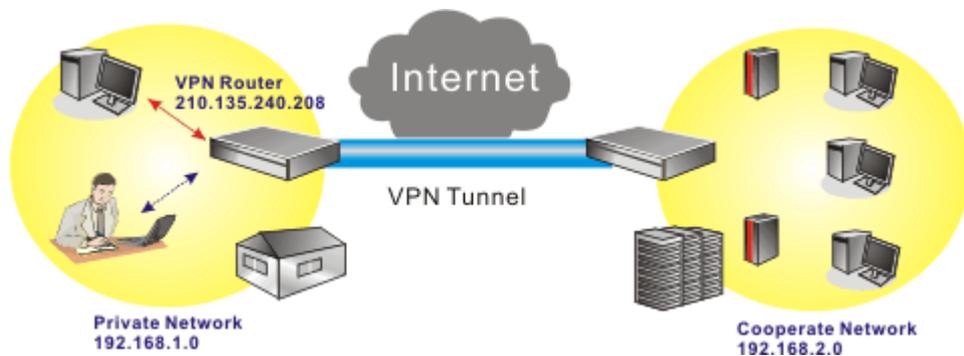
Enable the QoS Control BOTH

WAN Inbound Bandwidth Kbps
 WAN Outbound Bandwidth Kbps

Index	Class Name	Reserved_bandwidth Ratio
Class 1	E-mail	<input type="text" value="25"/> %
Class 2	HTTPS	<input type="text" value="25"/> %
Class 3		<input type="text" value="25"/> %
	Others	<input type="text" value="25"/> %

Enable UDP Bandwidth Control Limited_bandwidth Ratio %
 Outbound TCP ACK Prioritize

- If the worker has connected to the headquarter using host to host VPN tunnel. (Please refer to Chapter 3 VPN for detail instruction), he may set up an index for it. Enter the Class Name of Index 3. In this index, he will set reserve bandwidth for 1 VPN tunnel.



- Click edit to open a new window.

Class Index #1

Name

NO	Status	Local Address	Remote Address	DiffServ CodePoint	Service Type
1	Empty	-	-	-	-

11. First, check the **ACT** box. Then click **Edit** of **Local Address** to set a worker's subnet address. Click **Edit** of **Remote Address** to set headquarter's subnet address. Leave other fields and click **OK**.

Rule Edit

ACT

Local Address

Remote Address

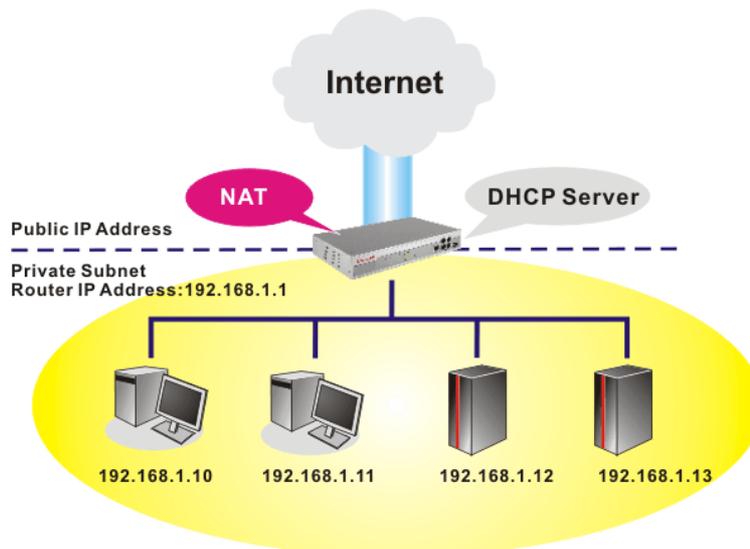
DiffServ CodePoint

Service Type

Note: Please choose/setup the Service Type first.

5.4 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.



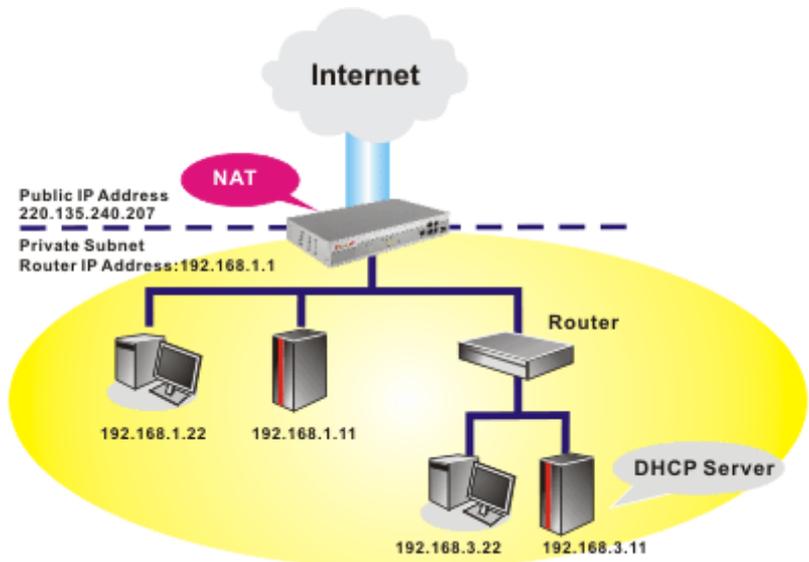
You can just set the settings wrapped inside the red rectangles to fit the request of NAT usage.

LAN >> General Setup

Ethernet TCP / IP and DHCP Setup	
LAN IP Network Configuration For NAT Usage 1st IP Address: <input type="text" value="192.168.1.1"/> 1st Subnet Mask: <input type="text" value="255.255.255.0"/> For IP Routing Usage: <input type="radio"/> Enable <input checked="" type="radio"/> Disable 2nd IP Address: <input type="text" value="192.168.2.1"/> 2nd Subnet Mask: <input type="text" value="255.255.255.0"/> <div style="border: 1px solid black; padding: 2px; display: inline-block;">2nd Subnet DHCP Server</div>	DHCP Server Configuration <input checked="" type="radio"/> Enable Server <input type="radio"/> Disable Server Relay Agent: <input type="radio"/> 1st Subnet <input type="radio"/> 2nd Subnet 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"/> DNS Server IP Address <input type="checkbox"/> Force DNS manual setting Primary IP Address: <input type="text" value="168.95.1.1"/> Secondary IP Address: <input type="text"/>
RIP Protocol Control: <input type="text" value="Disable"/>	

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 For NAT Usage 1st IP Address: <input type="text" value="192.168.1.1"/> 1st Subnet Mask: <input type="text" value="255.255.255.0"/> For IP Routing Usage: <input type="radio"/> Enable <input checked="" type="radio"/> Disable 2nd IP Address: <input type="text" value="192.168.2.1"/> 2nd Subnet Mask: <input type="text" value="255.255.255.0"/> <div style="border: 1px solid black; padding: 2px; display: inline-block;">2nd Subnet DHCP Server</div>	DHCP Server Configuration <input type="radio"/> Enable Server <input checked="" type="radio"/> Disable Server Relay Agent: <input type="radio"/> 1st Subnet <input type="radio"/> 2nd Subnet 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"/> DNS Server IP Address <input type="checkbox"/> Force DNS manual setting Primary IP Address: <input type="text" value="168.95.1.1"/> Secondary IP Address: <input type="text"/>
RIP Protocol Control: <input type="text" value="Disable"/>	

OK

5.5 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. Go to www.draytek.com.
2. Access into **Support >> Downloads**. Please find out **Firmware** menu and click it. Search the model you have and click on it to download the newly update firmware for your router.

Model Name	Firmware Version	Release Date
Vigor120 series	3.2.2.1	26/06/2009
Vigor2100 series	2.6.2	26/02/2008
Vigor2104 series	2.5.7.3	13/02/2008
Vigor2110 series	3.3.0	25/06/2009
Vigor2200/X/W/E	2.3.11	22/09/2004
Vigor2200Eplus	2.5.7	18/02/2009
Vigor2200USB	2.3.10	16/03/2005

3. Access into **Support >> Downloads**. Please find out **Utility** menu and click it.

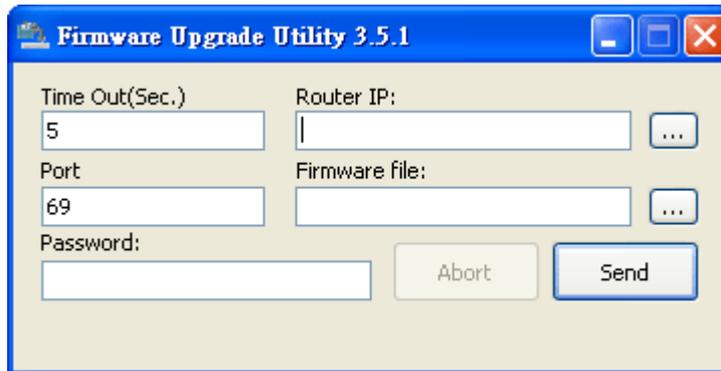
Tools Name	Release Date	Version	OS	Support Model
Router Tools	2009/06/18	4.2.0	MS-Windows	All Modules
Syslog Tools	2009/06/18	4.2.0	MS-Windows XP MS-Vista	All Modules
VigorPro Alert Notice Tools	2009/06/03	1.1.0 (Multi-language)	MS-Windows XP MS-Vista	VigorPro 100 series VigorPro 5500 series VigorPro 5510 series VigorPro 5300 series
Smart VPN Client	2009/05/25	3.6.3 (Multi-language)	MS-Windows XP MS-Vista	All Modules
Smart Monitor	2009/03/25	2.0	MS-Windows XP	Vigor2950 series VigorPro 5500 series

4. Click on the link of **Router Tools** to download the file. After downloading the files, please decompressed the file onto your host.

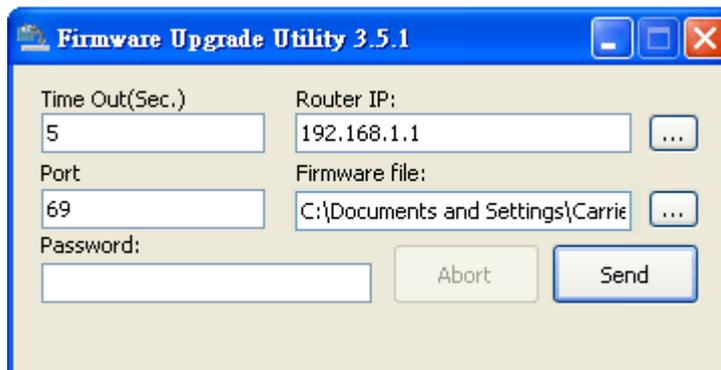
5. Double click on the icon of router tool. The setup wizard will appear.



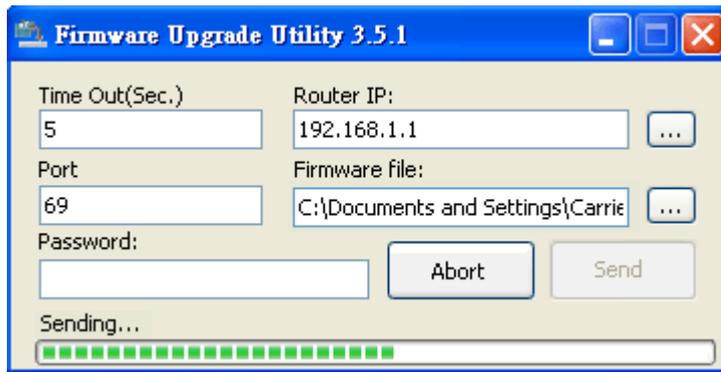
6. Follow the onscreen instructions to install the tool. Finally, click **Finish** to end the installation.
7. From the **Start** menu, open **Programs** and choose **Router Tools XXX >> Firmware Upgrade Utility**.



8. Type in your router IP, usually **192.168.1.1**.
9. 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.

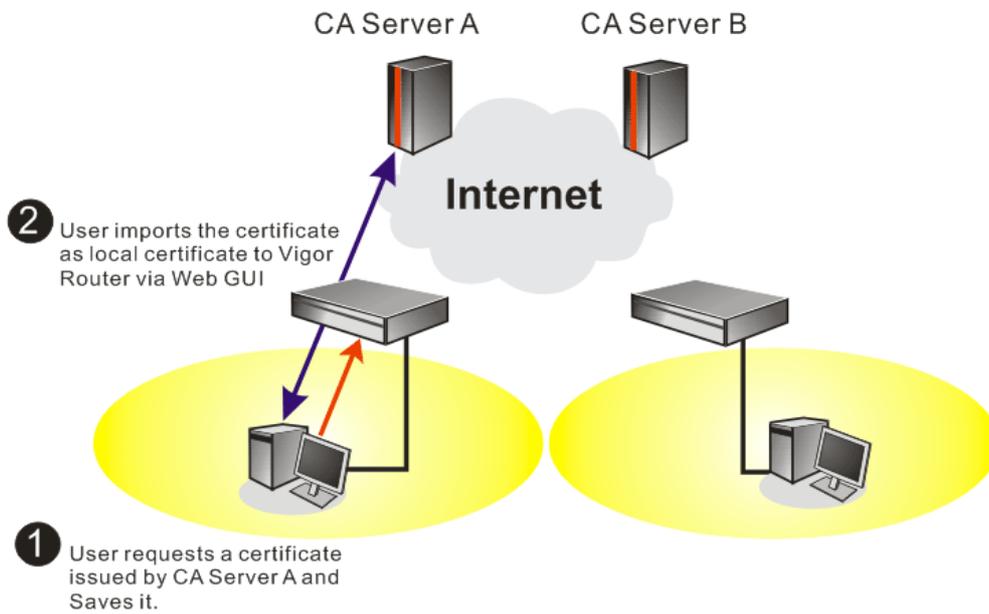


10. Click **Send**.



Now the firmware update is finished.

5.6 Request a certificate from a CA server on Windows CA Server



1. Go to **Certificate Management** and choose **Local Certificate**.

Certificate Management >> Local Certificate

X509 Local Certificate Configuration

Name	Subject	Status	Modify	
---	---	---	<input type="button" value="View"/>	<input type="button" value="Delete"/>
---	---	---	<input type="button" value="View"/>	<input type="button" value="Delete"/>
---	---	---	<input type="button" value="View"/>	<input type="button" value="Delete"/>

4. Connect to CA server via web browser. Follow the instruction to submit the request. Below we take a Windows 2000 CA server for example. Select **Request a Certificate**.

The screenshot shows the 'Welcome' page of Microsoft Certificate Services. The browser title is 'Microsoft Certificate Services -- vigor' and there is a 'Home' link in the top right. The page content includes a 'Welcome' heading, a paragraph explaining the site's purpose, and a 'Select a task:' section with three radio button options: 'Retrieve the CA certificate or certificate revocation list', 'Request a certificate' (which is selected), and 'Check on a pending certificate'. A 'Next >' button is located at the bottom right of the page.

Select **Advanced request**.

The screenshot shows the 'Choose Request Type' page. The browser title is 'Microsoft Certificate Services -- vigor' and there is a 'Home' link in the top right. The page content includes a 'Choose Request Type' heading, a paragraph asking the user to select a request type, and two radio button options: 'User certificate request' and 'Advanced request' (which is selected). Under 'User certificate request', there is a dropdown menu with 'User Certificate' selected. A 'Next >' button is located at the bottom right of the page.

Select **Submit a certificate request a base64 encoded PKCS #10 file or a renewal request using a base64 encoded PKCS #7 file**

The screenshot shows the 'Advanced Certificate Requests' page. The browser title is 'Microsoft Certificate Services -- vigor' and there is a 'Home' link in the top right. The page content includes an 'Advanced Certificate Requests' heading, a paragraph explaining the methods, and three radio button options: 'Submit a certificate request to this CA using a form.', 'Submit a certificate request using a base64 encoded PKCS #10 file or a renewal request using a base64 encoded PKCS #7 file.' (which is selected), and 'Request a certificate for a smart card on behalf of another user using the Smart Card Enrollment Station.' with a note below it: 'You must have an enrollment agent certificate to submit a request for another user.' A 'Next >' button is located at the bottom right of the page.

Import the X509 Local Certificate Request text file. Select **Router (Offline request)** or **IPSec (Offline request)** below.

Microsoft Certificate Services -- vigor Home

Submit A Saved Request

Paste a base64 encoded PKCS #10 certificate request or PKCS #7 renewal request generated by an external application (such as a web server) into the request field to submit the request to the certification authority (CA).

Saved Request:

```
-----BEGIN CERTIFICATE REQUEST-----
MIIBqjCCARMQAwQTElMAkGA1UEBhMVFxY29t
BgkqhkiG9w0BCQEWFxY29tQGRyYXZlLnR1
A4GNADCB1QKBoQYB7mm2FFhN9/ IeQnG03Xk++
hX4bp89cUF9d1oACGG1M/tcBockdcZgPFfVIXcP3
x/G0A7CTv0/fQzpxroCwJtJL5jS0/Bn9v50951G
-----
```

Base64 Encoded Certificate Request (PKCS #10 or #7):

[Browse for a file to insert.](#)

Certificate Template:

Administrator

Additional Attributes:

Attributes:

- Administrator
- Authenticated Session
- Basic EFS
- EFS Recovery Agent
- User
- IPSEC (Offline request)
- Router (Offline request)**
- Subordinate Certification Authority
- Web Server

[Submit >](#)

Then you have done the request and the server now issues you a certificate. Select **Base 64 encoded** certificate and **Download CA certificate**. Now you should get a certificate (.cer file) and save it.

- Back to Vigor router, go to **Local Certificate**. Click **IMPORT** button to open next page.

Certificate Management >> Local Certificate

X509 Local Certificate Configuration

Name	Subject	Status	Modify	
Local 1	/C=TW/O=Draytek/CN=Vigor/ema...	Requesting	View	Delete
---	---	---	View	Delete
---	---	---	View	Delete

[GENERATE](#)
[IMPORT](#)
[REFRESH](#)

- Browse the file to import the certificate (.cer file) into Vigor router.

Certificate Management >> Local Certificate

Import X509 Local Certificate

Upload Local Certificate

Select a local certificate file.

Certificate file: [Browse...](#)

Click [Import](#) to upload the local certificate.

[Import](#) [Cancel](#)

Upload PKCS12 Certificate

Select a PKCS12 file.

PKCS12 file: [Browse...](#)

Password:

Click [Import](#) to upload the PKCS12 file.

[Import](#) [Cancel](#)

Upload Certificate and Private Key

Select a certificate file and a matchable Private Key.

Certificate file: [Browse...](#)

Key file: [Browse...](#)

Password:

Click [Import](#) to upload the local certificate and private key.

[Import](#) [Cancel](#)

- When the file is imported successfully, the following dialog will appear.

Certificate Management >> Local Certificate

Import X509 Local Certificate

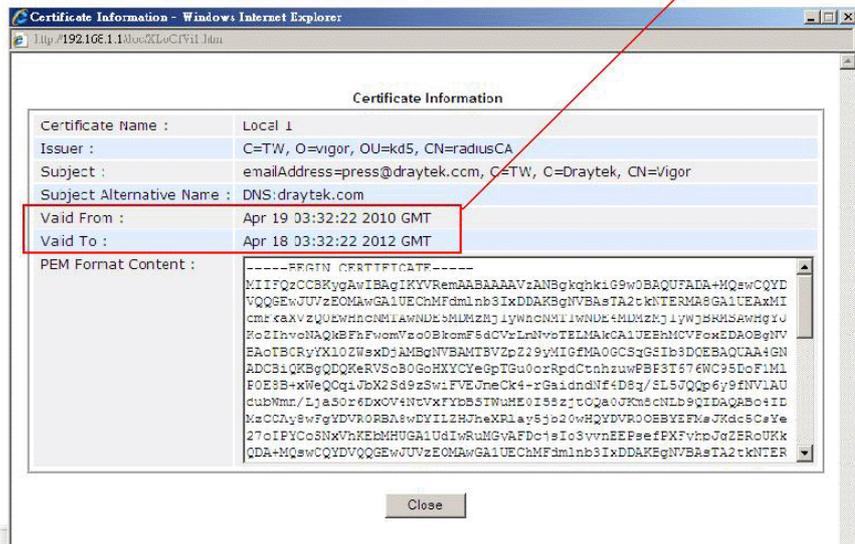


- You may review the detail information of the certificate by clicking **View** button.

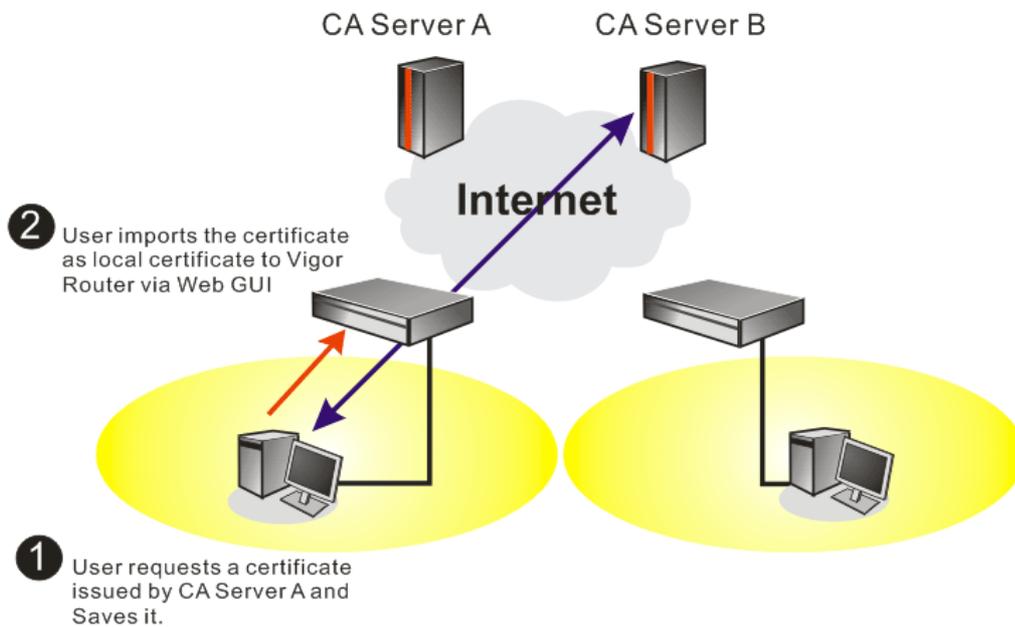
Certificate Management >> Local Certificate

X509 Local Certificate Configuration

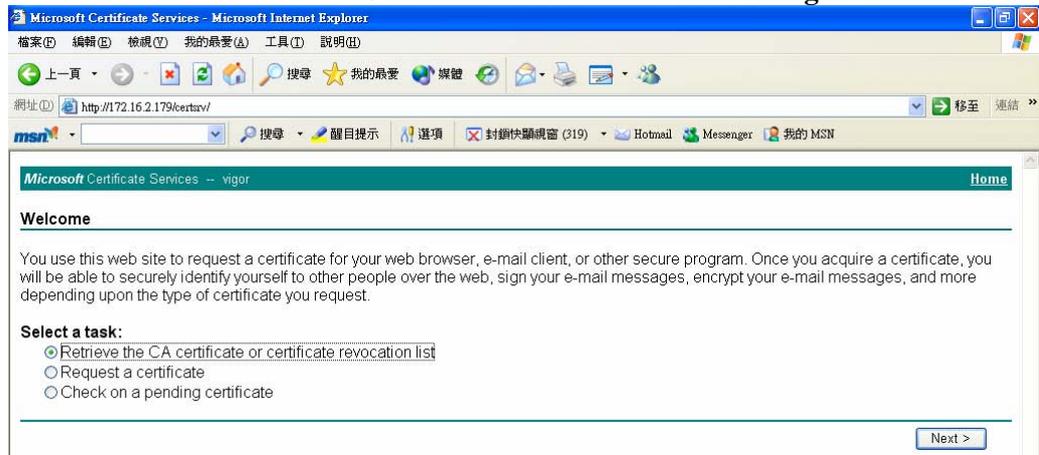
Name	Subject	Status	Modify	
Local 1	/emailAddress=press@draytek....	OK	View	Delete
---	---	---	View	Delete
---	---	---	View	Delete



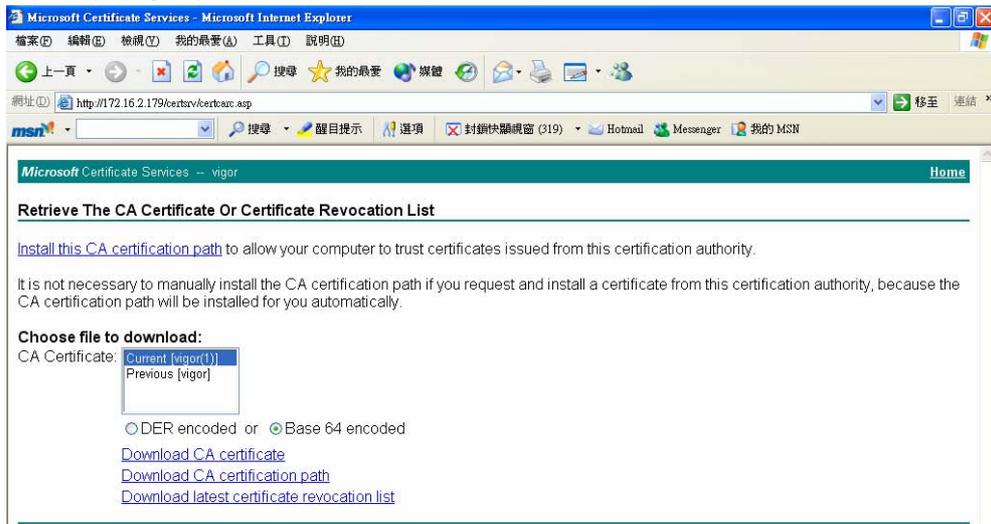
5.7 Request a CA Certificate and Set as Trusted on Windows CA Server



1. Use web browser connecting to the CA server that you would like to retrieve its CA certificate. Click **Retrieve the CA certificate or certificate recoring list**.



- In **Choose file to download**, click **CA Certificate Current** and **Base 64 encoded**, and **Download CA certificate** to save the .cer. file.



- Back to Vigor router, go to **Trusted CA Certificate**. Click **IMPORT** button and browse the file to import the certificate (.cer file) into Vigor router. When finished, click refresh and you will find the below illustration.

Certificate Management >> Trusted CA Certificate

X509 Trusted CA Certificate Configuration

Name	Subject	Status	Modify
Trusted CA-1	/C=TW/O=vigor/OU=kd5/CN=radi...	OK	View Delete
Trusted CA-2	---	---	View Delete
Trusted CA-3	---	---	View Delete

IMPORT

REFRESH

- You may review the detail information of the certificate by clicking **View** button.



Note: Before setting certificate configuration, please go to **System Maintenance >> Time and Date** to reset current time of the router first.

6

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.

6.1 Checking If the Hardware Status Is OK or Not

Follow the steps below to verify the hardware status.

1. Check the power line and WLAN/LAN cable connections. Refer to “**1.3 Hardware Installation**” for details.
2. Turn on the router. Make sure the **ACT LED** blink once per second and the correspondent **LAN LED** is bright.



3. If not, it means that there is something wrong with the hardware status. Simply back to “**1.3 Hardware Installation**” to execute the hardware installation again. And then, try again.

6.2 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

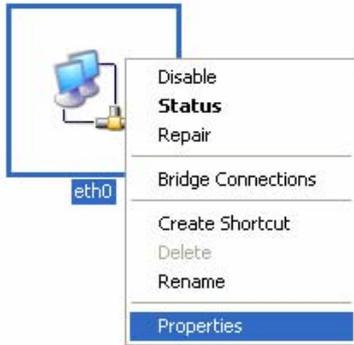


The example is based on Windows XP. As to the examples for other operation systems, please refer to the similar steps or find support notes in www.draytek.com.

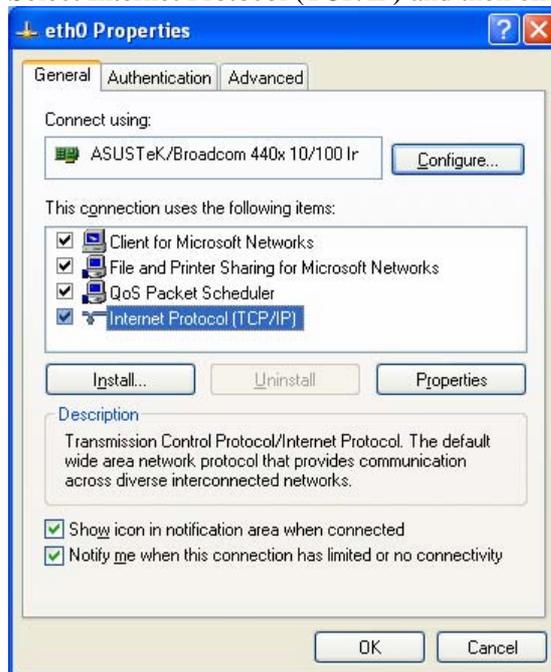
1. Go to Control Panel and then double-click on Network Connections.



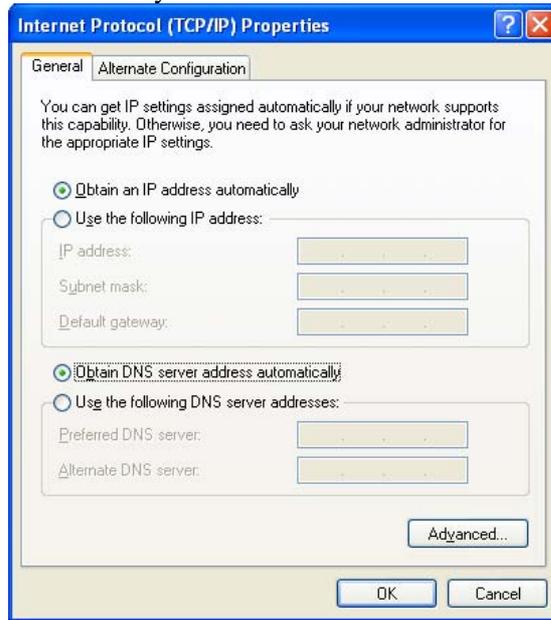
2. Right-click on Local Area Connection and click on Properties.



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

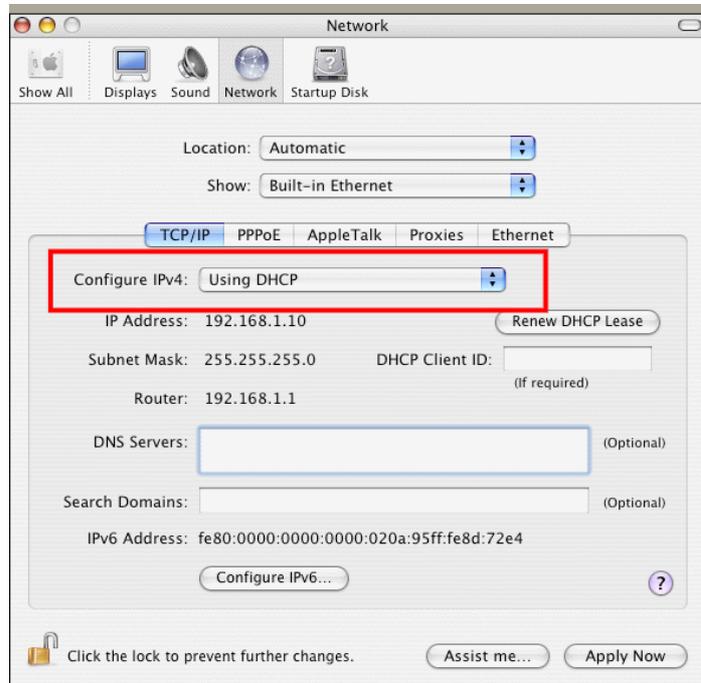


4. Select Obtain an IP address automatically and Obtain DNS server address automatically.



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.



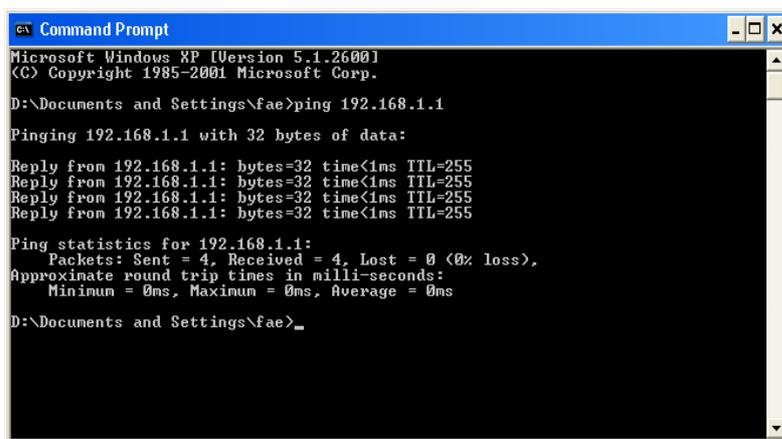
6.3 Pinging the Router from Your Computer

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 6.2)

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/Vista). The DOS command dialog will appear.



```
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

D:\Documents and Settings\fae>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:

Reply from 192.168.1.1: bytes=32 time<1ms TTL=255

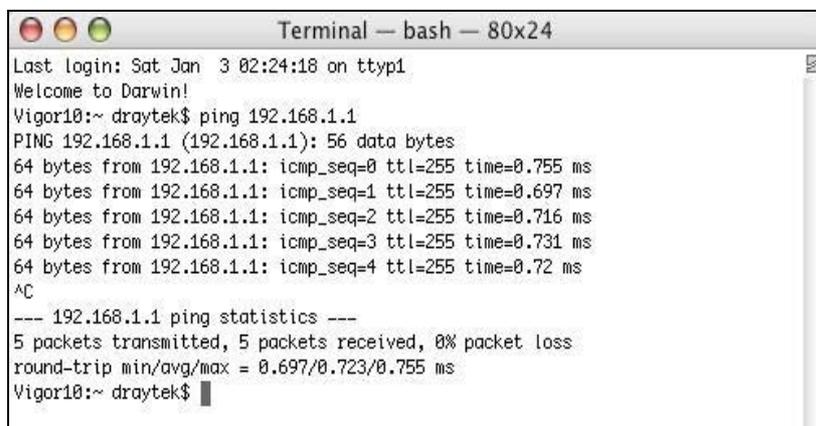
Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

D:\Documents and Settings\fae>_
```

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

For MacOs (Terminal)

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



```
Terminal — bash — 80x24

Last login: Sat Jan 3 02:24:18 on ttty1
Welcome to Darwin!
Vigor10:~ draytek$ ping 192.168.1.1
PING 192.168.1.1 (192.168.1.1): 56 data bytes
64 bytes from 192.168.1.1: icmp_seq=0 ttl=255 time=0.755 ms
64 bytes from 192.168.1.1: icmp_seq=1 ttl=255 time=0.697 ms
64 bytes from 192.168.1.1: icmp_seq=2 ttl=255 time=0.716 ms
64 bytes from 192.168.1.1: icmp_seq=3 ttl=255 time=0.731 ms
64 bytes from 192.168.1.1: icmp_seq=4 ttl=255 time=0.72 ms
^C
--- 192.168.1.1 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 0.697/0.723/0.755 ms
Vigor10:~ draytek$ █
```

6.4 Checking If the ISP Settings are OK or Not

Click **WAN>> Internet Access** and then check whether the ISP settings are set correctly. Click **Details Page** of WAN1/WAN2 to review the settings that you configured previously.

WAN >> Internet Access

Internet Access

Index	Display Name	Physical Mode	Access Mode	
WAN1		Ethernet	Static or Dynamic IP	Details Page
WAN2		Ethernet	None	Details Page

Static or Dynamic IP ▾

None

PPPoE

Static or Dynamic IP

PPTP

For PPPoE 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**.

WAN >> Internet Access

WAN 1

<p>PPPoE Client Mode</p> <p><input checked="" type="radio"/> Enable <input type="radio"/> Disable</p> <hr/> <p>ISP Access Setup</p> <p>Username <input type="text"/></p> <p>Password <input type="text"/></p> <p>Index(1-15) in Schedule Setup: => <input type="text"/>, <input type="text"/>, <input type="text"/>, <input type="text"/></p> <p>ISDN Dial Backup Setup</p> <p>Dial Backup Mode <input type="text" value="None"/></p> <hr/> <p>WAN Connection Detection</p> <p>Mode <input type="text" value="ARP Detect"/></p> <p>Ping IP <input type="text" value="0.0.0.0"/></p> <p>TTL: 255</p> <hr/> <p>MTU <input type="text" value="1442"/> (Max: 1492)</p>	<p>PPP/MP Setup</p> <p>PPP Authentication <input type="text" value="PAP or CHAP"/></p> <p>Idle Timeout <input type="text" value="-1"/> second(s)</p> <p>IP Address Assignment Method (IPCP)</p> <p><input type="text" value="WAN IP Alias"/></p> <p>Fixed IP: <input type="radio"/> Yes <input checked="" type="radio"/> No (Dynamic IP)</p> <p>Fixed IP Address <input type="text"/></p> <hr/> <p><input checked="" type="radio"/> Default MAC Address</p> <p><input type="radio"/> Specify a MAC Address</p> <p>MAC Address: <input type="text" value="00"/> <input type="text" value=".50"/> <input type="text" value=".7F"/> <input type="text" value=":C4"/> <input type="text" value=".CC"/> <input type="text" value=".45"/></p>
---	--

For Static/Dynamic IP Users

1. Check if the **Enable** option is selected.
2. Check if **IP address, Subnet Mask** and **Gateway** are entered with correct values that you **got from your ISP**.

WAN >> Internet Access

WAN 1

<p>Static or Dynamic IP</p> <p><input checked="" type="radio"/> Enable <input type="radio"/> Disable</p> <hr/> <p>ISDN Dial Backup Setup</p> <p>Dial Backup Mode <input type="text" value="None"/></p> <hr/> <p>Keep WAN Connection</p> <p><input type="checkbox"/> Enable PING to keep alive</p> <p>PING to the IP <input type="text"/></p> <p>PING Interval <input type="text" value="0"/> minute(s)</p> <hr/> <p>WAN Connection Detection</p> <p>Mode <input type="text" value="ARP Detect"/></p> <p>Ping IP <input type="text" value="0.0.0.0"/></p> <p>TTL: 255</p> <hr/> <p>MTU <input type="text" value="1442"/> (Max:1500)</p> <hr/> <p>RIP Protocol</p> <p><input type="checkbox"/> Enable RIP</p>	<p>WAN IP Network Settings <input type="button" value="WAN IP Alias"/></p> <p><input type="radio"/> Obtain an IP address automatically (DHCP Client)</p> <p>Router Name <input type="text"/> *</p> <p>Domain Name <input type="text"/> *</p> <p>* : Required for some ISPs</p> <p><input checked="" type="radio"/> Specify an IP address</p> <p>IP Address <input type="text" value="172.16.3.102"/></p> <p>Subnet Mask <input type="text" value="255.255.0.0"/></p> <p>Gateway IP Address <input type="text" value="172.16.1.1"/></p> <hr/> <p>DNS Server IP Address</p> <p>Primary IP Address <input type="text"/></p> <p>Secondary IP Address <input type="text"/></p> <hr/> <p><input checked="" type="radio"/> Default MAC Address</p> <p><input type="radio"/> Specify a MAC Address</p> <p>MAC Address: <input type="text" value="00"/> <input type="text" value=".50"/> <input type="text" value=".7F"/> <input type="text" value=":C4"/> <input type="text" value=":CC"/> <input type="text" value=".45"/></p>
---	---

For PPTP Users

1. Check if the **Enable** option for **PPTP Link** is selected.

WAN >> Internet Access

WAN 1

<p>PPTP Client Mode</p> <p><input checked="" type="radio"/> Enable <input type="radio"/> Disable</p> <p>PPTP Server <input type="text" value="10.0.0.138"/></p> <hr/> <p>ISP Access Setup</p> <p>Username <input type="text"/></p> <p>Password <input type="text"/></p> <p>Index(1-15) in Schedule Setup: => <input type="text"/> , <input type="text"/> , <input type="text"/> , <input type="text"/></p> <hr/> <p>ISDN Dial Backup Setup</p> <p>Dial Backup Mode <input type="text" value="None"/></p> <hr/> <p>MTU <input type="text" value="1442"/> (Max:1460)</p>	<p>PPP Setup</p> <p>PPP Authentication <input type="text" value="PAP or CHAP"/></p> <p>Idle Timeout <input type="text" value="-1"/> second(s)</p> <p>IP Address Assignment Method (IPCP)</p> <p><input type="button" value="WAN IP Alias"/></p> <p>Fixed IP: <input type="radio"/> Yes <input checked="" type="radio"/> No (Dynamic IP)</p> <p>Fixed IP Address <input type="text"/></p> <hr/> <p>WAN IP Network Settings</p> <p><input type="radio"/> Obtain an IP address automatically</p> <p><input checked="" type="radio"/> Specify an IP address</p> <p>IP Address <input type="text" value="10.0.0.150"/></p> <p>Subnet Mask <input type="text" value="255.0.0.0"/></p>
--	--

2. Check if **PPTP Server, Username, Password** and **WAN IP address** are set correctly (must identify with the values from your ISP).

6.5 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 lose all settings you did before. Make sure you have recorded all useful settings before you pressing. The password of factory default is null.

Software Reset

You can reset the 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

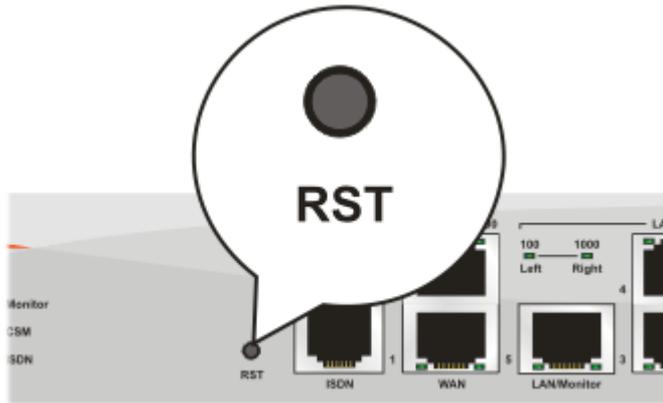
Do You want to reboot your router ?

- Using current configuration
- Using factory default configuration

OK

Hardware Reset

While the router is running (ACT LED blinking), press the **RST** button and hold for more than 5 seconds. When you see the **ACT** 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.

6.6 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.