

DrayTek

Vigor2955

Dual-WAN SSL VPN Appliance

DrayTek



Your reliable networking solutions partner

User's Guide

V1.0

Vigor 2955

Dual-WAN SSL VPN Appliance

User's Guide

Version: 1.0

Date: 30/10/2009

Copyright Information

Copyright Declarations

Copyright 2009 All rights reserved. This publication contains information that is protected by copyright. No part may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language without written permission from the copyright holders.

Trademarks

The following trademarks are used in this document:

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

Safety Instructions and Approval

Safety Instructions

- Read the installation guide thoroughly before you set up the 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

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

<http://www.draytek.com>

European Community Declarations

Manufacturer: DrayTek Corp.
Address: No. 26, Fu Shing Road, HuKou Township, HsinChu Industrial Park, Hsin-Chu, Taiwan 303
Product: Vigor2955 Series Router

DrayTek Corp. declares that Vigor2955 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 device might cause interference of radio frequency under the environment of dwelling. In such condition, the users might be asked to adopt some proper strategies.

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



This product is designed for the POTS network throughout the EC region and Switzerland with restrictions in France.

Table of Contents

1

Preface	1
1.1 Web Configuration Buttons Explanation	1
1.2 LED Indicators and Connectors	2
1.3 Hardware Installation	3
1.4 Printer Installation	4

2

Configuring Basic Settings	9
2.1 Changing Password	9
2.2 Quick Start Wizard	11
2.2.1 PPPoE	12
2.2.2 PPTP	14
2.2.3 L2TP	15
2.2.4 Static IP	16
2.2.5 DHCP	17
2.3 Online Status	18
2.4 Saving Configuration	20

3

Advanced Web Configuration	21
3.1 WAN	21
3.1.1 Basics of Internet Protocol (IP) Network	21
3.1.2 General Setup	22
3.1.3 Internet Access	25
3.1.4 Load-Balance Policy	32
3.2 LAN	35
3.2.1 Basics of LAN	35
3.2.2 General Setup	37
3.2.3 Static Route	39
3.2.4 VLAN	42
3.2.5 Bind IP to MAC	42
3.3 NAT	44
3.3.1 Port Redirection	45
3.3.2 DMZ Host	47
3.3.3 Open Ports	51
3.3.4 Address Mapping	52
3.4 Firewall	54
3.4.1 Basics for Firewall	54
3.4.2 General Setup	56
3.4.3 Filter Setup	57
3.4.4 DoS Defense	62

3.5 Objects Settings	65
3.5.1 IP Object	65
3.5.2 IP Group	67
3.5.3 Service Type Object	68
3.5.4 Service Type Group	69
3.5.5 IM Object	70
3.5.6 P2P Object	72
3.5.7 Protocol Object	73
3.5.8 Misc Object	74
3.6 CSM	75
3.6.1 APP Enforcement Profile	76
3.6.2 URL Content Filter Profile	78
3.6.3 Web Content Filter Profile	80
3.7 Bandwidth Management	81
3.7.1 Sessions Limit	81
3.7.2 Bandwidth Limit	82
3.7.3 Quality of Service	83
3.8 Applications	90
3.8.1 Dynamic DNS	90
3.8.2 Schedule	92
3.8.3 RADIUS/LDAP	94
3.8.4 UPnP	95
3.8.5 Wake on LAN	96
3.9 VPN and Remote Access	98
3.9.1 VPN Client Wizard	98
3.9.2 VPN Server Wizard	104
3.9.3 Remote Access Control	108
3.9.4 PPP General Setup	109
3.9.5 IPSec General Setup	110
3.9.6 IPSec Peer Identity	111
3.9.7 Remote Dial-in User	114
3.9.8 LAN to LAN	118
3.9.9 VPN TRUNK Management	128
3.9.10 Connection Management	139
3.10 Certificate Management	140
3.10.1 Local Certificate	140
3.10.2 Trusted CA Certificate	143
3.10.3 Certificate Backup	145
3.11 SSL VPN	145
3.11.1 General Setup	145
3.11.2 SSL Web Proxy	146
3.11.3 SSL Application	147
3.11.4 User Account	149
3.11.5 Online User Status	151
3.12 System Maintenance	152
3.12.1 System Status	152
3.12.2 TR-069 Setting	153
3.12.3 Administrator Password	155
3.12.4 Configuration Backup	155
3.12.5 Syslog/Mail Alert	157
3.12.6 Time and Date	159
3.12.7 Management	160

3.12.8 Reboot System	161
3.12.9 Firmware Upgrade	162
3.13 Diagnostics.....	163
3.13.1 Dial-out Trigger	163
3.13.2 Routing Table	164
3.13.3 ARP Cache Table	164
3.13.4 DHCP Table.....	165
3.13.5 NAT Sessions Table	165
3.13.6 Data Flow Monitor.....	166
3.13.7 Traffic Graph.....	168
3.13.8 Ping Diagnosis.....	169
3.13.9 Trace Route	170
3.14 Support Area	171

4

Application and Examples	173
4.1 Create a LAN-to-LAN Connection Between Remote Office and Headquarter	173
4.2 Create a Remote Dial-in User Connection Between the Teleworker and Headquarter.....	181
4.3 QoS Setting Example.....	185
4.4 LAN – Created by Using NAT	187
4.5 Upgrade Firmware for Your Router	189
4.6 Request a certificate from a CA server on Windows CA Server	191
4.7 Request a CA Certificate and Set as Trusted on Windows CA Server	195
4.8 ERD Mechanism for VPN TRUNK	197
4.9 VPN Load Balance Application	199

5

Trouble Shooting	203
5.1 Checking If the Hardware Status Is OK or Not.....	203
5.2 Checking If the Network Connection Settings on Your Computer Is OK or Not	204
5.3 Pinging the Router from Your Computer	206
5.4 Checking If the ISP Settings are OK or Not.....	208
5.5 Backing to Factory Default Setting If Necessary	210
5.6 Contacting Your Dealer	211

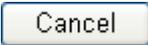
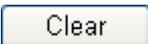
1

Preface

The Vigor2950 series router provides Dual-WAN interface (which is a configuration second WAN) for Internet access to make the Internet connection more reliable. The wireless LAN supports more secure features and the transmission speed is up to 108Mbps (SuperG™). Object-oriented firewall is flexible and allows your network be safe. In addition, through VoIP function, the communication fee for you and remote people can be reduced.

1.1 Web Configuration Buttons Explanation

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

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

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

1.2 LED Indicators and Connectors

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

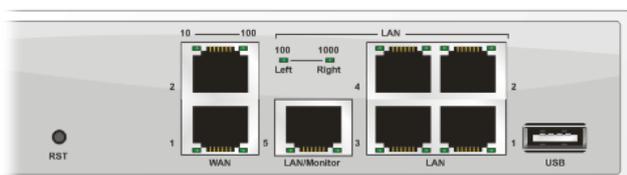
The displays of LED indicators and connectors for the routers are different slightly. The following sections will introduce them respectively.



LED	Status	Explanation
ACT (Activity)	Blinking	The router is powered on and running normally.
	Off	The router is powered off.
DMZ	On	DMZ Host is specified in certain site.
Monitor	On	LAN traffic monitor is active.
VPN	On	The VPN tunnel is launched.
	Off	The VPN tunnel is closed.
QoS	On	The QoS function is active.
USB	On	The USB device is active.

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.
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 USB device (e.g., printer).

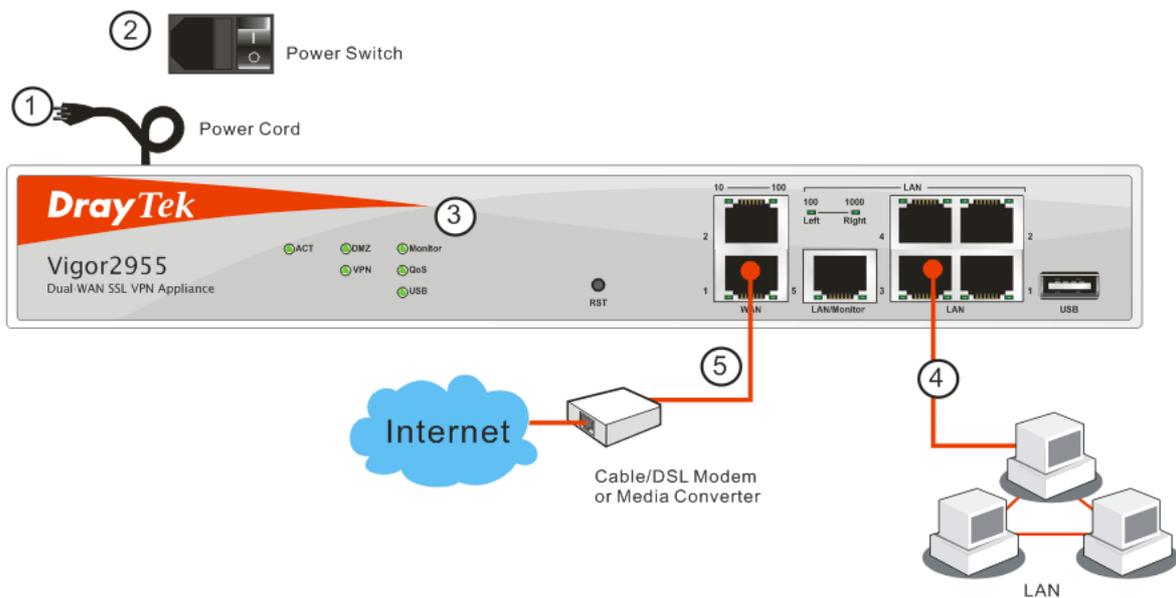
	Connector for a power cord with 100-240VAC (inlet).
	Power Switch.

1.3 Hardware Installation

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

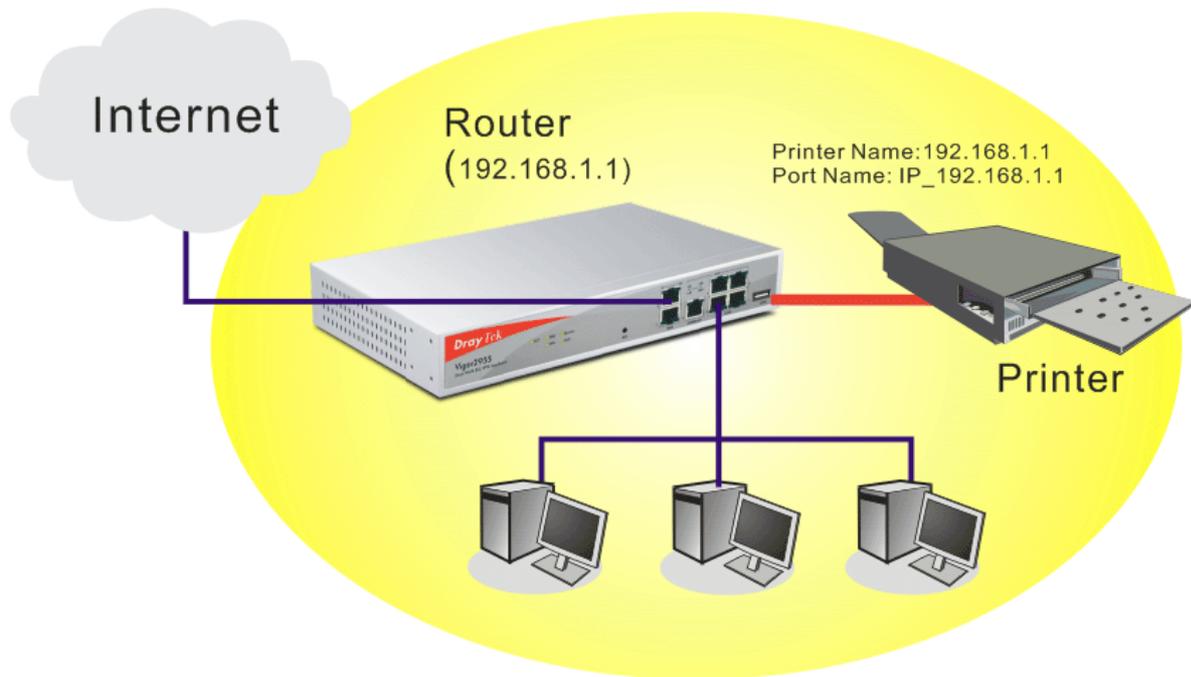
1. Connect the power cord to the router's power port on the rear panel, and the other side into a wall outlet.
2. Power on the device by pressing down the power switch on the rear panel.
3. The system starts to initiate. After completing the system test, the **ACT** LED will light up and start blinking.
4. 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 (that device also can connect to other computers to form a small area network). The **LAN** LED (Left or Right) will light up according to the network card feature (1000 or 100) of the device that it connected.
5. 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 network card feature (100 or 10) of the device that it connected.

(For the detailed information of LED status, please refer to section 1.1.)



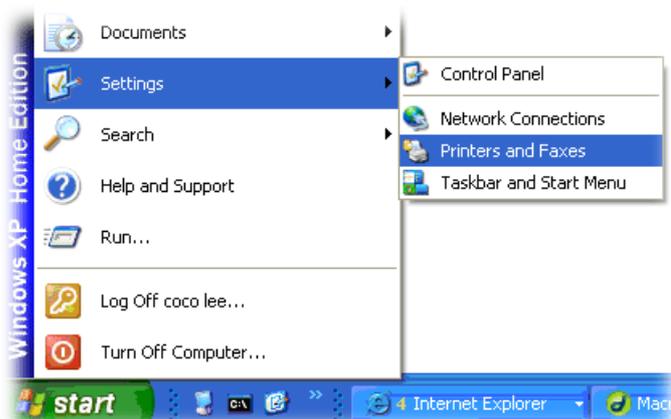
1.4 Printer Installation

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/Vista. For Windows 98/SE, please visit www.draytek.com.

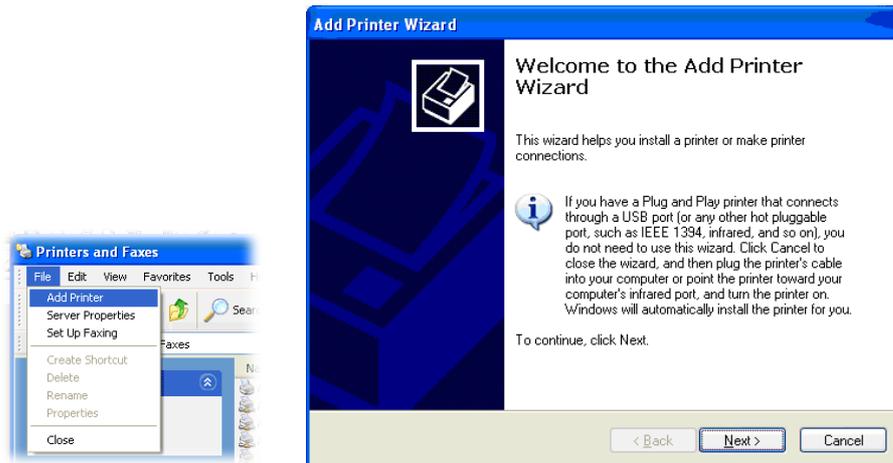


Before using it, please follow the steps below to configure settings for connected computers.

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



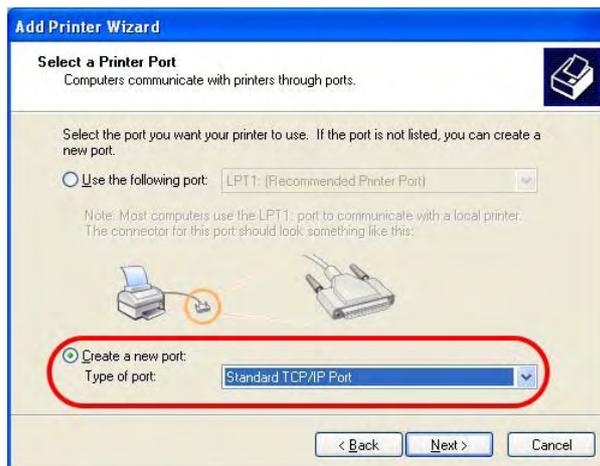
3. Open **File->Add a New Computer**. A welcome dialog will appear. Please click **Next**.



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**.



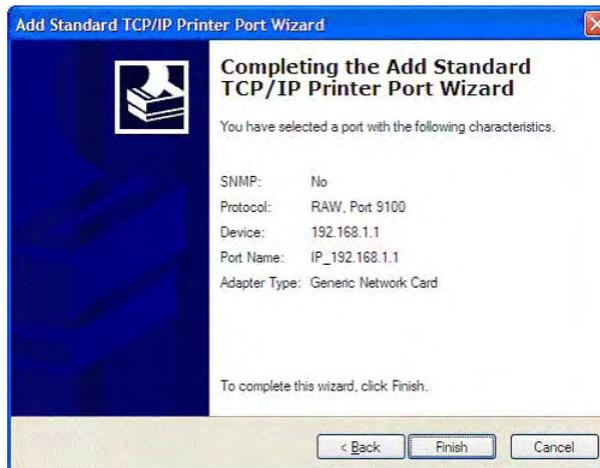
- In the following dialog, type **192.168.1.1** (router's LAN IP) in the field of **Printer Name or IP Address** and type **IP_192.168.1.1** as the port name. Then, click **Next**.



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



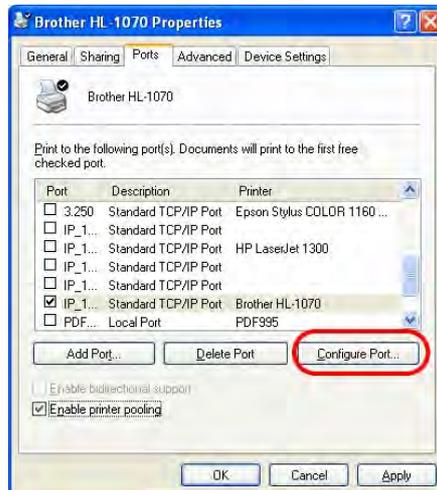
- Then, in the following dialog, click **Finish**.



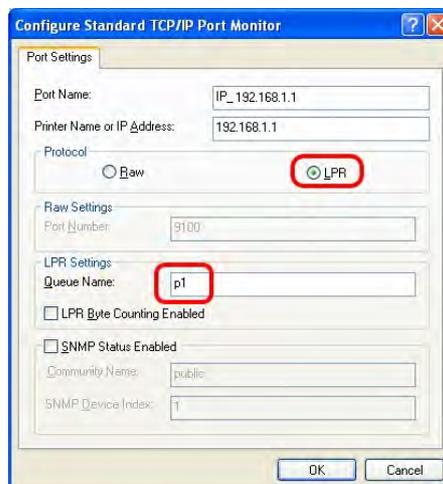
9. Now, your system will ask you to choose right name of the printer that you installed onto the router. Such step can make correct driver loaded onto your PC. When you finish the selection, click **Next**.



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.



12. 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.

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” as the username and leave blank for the 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.

Vigor2955
Dual-WAN SSL VPN Appliance

DrayTek

Auto Logout ▾
Quick Start Wizard
Online Status

WAN
LAN
NAT
Firewall
Objects Setting
CSM
Bandwidth Management
Applications
VPN and Remote Access
Certificate Management
SSL VPN
System Maintenance
Diagnostics

Support Area
Application Note
FAQ
Product Registration

Logout
All Rights Reserved.

System Status You logged in at 2009-10-5 01:43:59 last time, from 192.168.1.10.

Model Name : Vigor2955 Series
Firmware Version : v3.2.5_RC3
Build Date/Time : Wed Sep 16 11:32:14.5 2009

System	
CPU Usage	: 2 %
Total Memory	: 64M
Memory usage	: 47 %

LAN	
MAC Address	: 00-50-7F-C7-86-88
1st IP Address	: 192.168.1.1
1st Subnet Mask	: 255.255.255.0
DHCP Server	: Yes
Primary DNS	:
Secondary DNS	:

WAN 1	
Link Status	: Disconnected
MAC Address	: 00-50-7F-C7-86-89
Connection	: DHCP Client
IP Address	: ---
Default Gateway	: ---
Primary DNS	:
Secondary DNS	:

WAN 2	
Link Status	: Connected
MAC Address	: 00-50-7F-C7-86-8A
Connection	: DHCP Client
IP Address	: 192.168.5.24
Default Gateway	: 192.168.5.1
Primary DNS	: 168.95.1.1
Secondary DNS	:

- 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 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.

Username

Password

Login

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

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

< Back Next > Finish Cancel

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:

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

< Back Next > Finish Cancel

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
- L2TP
- Static IP
- DHCP

In the **Quick Start Wizard**, you can configure the router to access the Internet with different protocol/modes such as **PPPoE**, **PPTP**, **L2TP**, **Static IP** or **DHCP**.

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

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 to confirm it.

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.

< 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 !!!

2.2.2 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

Password

Confirm Password

WAN IP Configuration

Obtain an IP address automatically

Specify an IP address

IP Address

Subnet Mask

Gateway

Primary DNS

Second DNS

PPTP Server

< Back Next > Finish Cancel

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.

< 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 !!!

2.2.3 L2TP

Click **L2TP** as the protocol. Type in all the information that your ISP provides for this protocol.

Quick Start Wizard

L2TP Client Mode

WAN 1
Enter the user name, password, WAN IP configuration and L2TP server IP provided by your ISP.

User Name

Password

Confirm Password

WAN IP Configuration

Obtain an IP address automatically

Specify an IP address

IP Address

Subnet Mask

Gateway

Primary DNS

Second DNS

L2TP Server

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: L2TP

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

2.2.4 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="255.255.255.0"/>
Gateway	<input type="text" value="172.16.3.1"/>
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 !!!

2.2.5 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 require 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 Online Status

The online status shows the system status, WAN status, 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** or **Drop PPPoE** in the Online Status web page.

Online status for PPPoE

Online Status

System Status					System Uptime: 0:0:41	
LAN Status		Primary DNS: 61.31.233.1		Secondary DNS: 139.175.55.244		
IP Address		TX Packets		RX Packets		
192.168.50.111		240		210		
WAN 1 Status					>> Drop PPPoE	
Enable	Line	Name	Mode	Up Time		
Yes	Ethernet		PPPoE	0:00:00		
IP	GW IP	TX Packets	TX Rate	RX Packets	RX Rate	
219.81.160.205	211.78.218.40	6	29	6	12	
WAN 2 Status						
Enable	Line	Name	Mode	Up Time		
Yes	Ethernet		Static IP	0:00:32		
IP	GW IP	TX Packets	TX Rate	RX Packets	RX Rate	
192.168.4.103	192.168.4.1	1	3	1	9	

Online status for PPTP (for WAN2)

Online Status

System Status					System Uptime: 0:12:8	
LAN Status		Primary DNS: 194.109.6.66		Secondary DNS: 194.98.0.1		
IP Address		TX Packets		RX Packets		
192.168.50.111		4910		3663		
WAN 1 Status						
Enable	Line	Name	Mode	Up Time		
Yes	Ethernet	WAN1	Static IP	0:10:08		
IP	GW IP	TX Packets	TX Rate	RX Packets	RX Rate	
192.168.22.111	192.168.22.105	91	21	99	3	
WAN 2 Status					>> Drop PPTP	
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)

Online Status

System Status					System Uptime: 0:12:8	
LAN Status		Primary DNS: 194.109.6.66		Secondary DNS: 194.98.0.1		
IP Address		TX Packets		RX Packets		
192.168.50.111		4910		3663		
WAN 1 Status						
Enable	Line	Name	Mode	Up Time		
Yes	Ethernet	WAN1	Static IP	0:10:08		
IP	GW IP	TX Packets	TX Rate	RX Packets	RX Rate	
192.168.22.111	192.168.22.105	91	21	99	3	
WAN 2 Status					>> Drop PPTP	
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 DHCP

Online Status

System Status				System Uptime: 0:1:57	
LAN Status		Primary DNS: 168.95.1.1		Secondary DNS: 168.95.1.1	
IP Address	TX Packets	RX Packets			
192.168.50.111	856	783			
WAN 1 Status					>> Release
Enable	Line	Name	Mode	Up Time	
Yes	Ethernet		DHCP Client	0:01:49	
IP	GW IP	TX Packets	TX Rate	RX Packets	RX Rate
192.168.22.10	192.168.22.105	3	3	7	9
WAN 2 Status					>> Drop PPPoE
Enable	Line	Name	Mode	Up Time	
Yes	Ethernet		PPPoE	0:01:39	
IP	GW IP	TX Packets	TX Rate	RX Packets	RX Rate
202.211.100.176	202.211.100.170	35	8	46	4

Detailed explanation is shown below:

Primary DNS Display the IP address of the primary DNS.

Secondary DNS Display the IP address of the secondary DNS.

LAN Status

IP Address Display the IP address of the LAN interface.

TX Packets Display the total transmitted packets at the LAN interface.

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

WAN1/2 Status

Line Display the physical connection (Ethernet) of this interface.

Name Display the name set in WAN1/WAN web page.

Mode Display the type of WAN connection (e.g., PPPoE).

Up Time Display the total uptime of the interface.

IP Display the IP address of the WAN interface.

GW IP Display the IP address of the default gateway.

TX Packets Display the total transmitted packets at the WAN interface.

TX Rate Display the speed of transmitted octets at the WAN interface.

RX Packets Display the total number of received packets at the WAN interface.

RX Rate Display 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.

2.4 Saving Configuration

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



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

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

3

Advanced Web Configuration

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

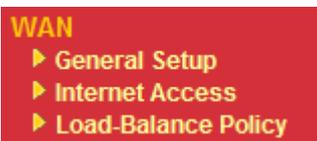
Network Connection by 3G USB Modem

For 3G mobile communication through Access Point is popular more and more, Vigor2955 adds the function of 3G network connection for such purpose. By connecting 3G USB Modem to the USB port of Vigor2955, it can support HSDPA/UMTS/EDGE/GPRS/GSM and the future 3G standard (HSUPA, etc). Vigor2955 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.



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 Internet Access.



3.1.2 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.

WAN >> General Setup

General Setup

WAN1	WAN2
Enable: <input type="checkbox"/> Yes	Enable: <input type="checkbox"/> Yes
Display Name: <input type="text"/>	Display Name: <input type="text"/>
Physical Mode: Ethernet	Physical Mode: 3G USB Modem
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"/> UpLink <input type="text"/>	Line Speed(Kbps): DownLink <input type="text"/> UpLink <input type="text"/>
Active Mode: Always On	Active Mode: Always On
Active on demand: <input type="radio"/> WAN2 Fail <input checked="" type="radio"/> WAN2 Upload speed exceed <input type="text"/> Kbps WAN2 Download speed exceed <input type="text"/> Kbps	Active on demand: <input type="radio"/> WAN1 Fail <input checked="" type="radio"/> WAN1 Upload 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 through Ethernet port; yet the physical connection for WAN2 is done through an Ethernet port (P1) or USB port.

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 enable **PPP** as the access mode and complete further configuration.

WAN >> Internet Access

WAN 2

PPP Client Mode Enable Disable

SIM PIN code

Modem Initial String (Default: AT&FE0V1X1&D2&C1S0=0)

APN Name

Modem Dial String (Default: ATDT*99#)

PPP Username (Optional)

PPP Password (Optional)

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

Physical Type

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

Physical Type:

Auto negotiation
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:

Auto Weigh
Auto Weigh
According to Line Speed

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:

Active on demand
Always On
Active on demand

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.

3.1.3 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 <input type="button" value="Details Page"/>
WAN2		Ethernet	None <input type="button" value="Details Page"/>

or

WAN >> Internet Access

Internet Access			
Index	Display Name	Physical Mode	Access Mode
WAN1		Ethernet	Static or Dynamic IP <input type="button" value="Details Page"/>
WAN2		3G USB Modem	None <input type="button" value="Details Page"/>

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

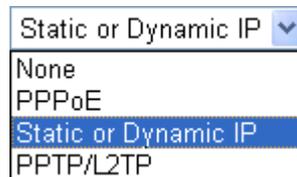
It shows the name of the WAN1/WAN2 that entered in general setup.

Physical Mode

It shows the physical port (Ethernet/3G USB Modem) for WAN1/WAN2.

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.



There are three access modes provided for PPPoE, Static or Dynamic IP and PPTP/L2TP.

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. The following web page will be shown.

WAN >> Internet Access

WAN 1

<p>PPPoE Client Mode <input type="radio"/> Enable <input checked="" type="radio"/> Disable</p> <hr/> <p>ISP Access Setup Username <input style="width: 100%;" type="text"/> Password <input style="width: 100%;" type="password"/> Index(1-15) in Schedule Setup: => <input style="width: 20px;" type="text"/>, <input style="width: 20px;" type="text"/>, <input style="width: 20px;" type="text"/>, <input style="width: 20px;" type="text"/></p> <hr/> <p>WAN Connection Detection Mode <input type="text" value="ARP Detect"/> Ping IP <input style="width: 100%;" type="text"/> TTL: <input style="width: 100%;" type="text"/></p> <hr/> <p>MTU <input style="width: 50px;" type="text" value="1442"/> (Max:1492)</p>	<p>PPP/MP Setup PPP Authentication <input type="text" value="PAP or CHAP"/> Idle Timeout <input style="width: 50px;" type="text" value="-1"/> second(s)</p> <p>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 style="width: 100%;" type="text"/></p> <hr/> <p><input checked="" type="radio"/> Default MAC Address <input type="radio"/> Specify a MAC Address MAC Address: <input style="width: 20px;" type="text" value="00"/> <input style="width: 20px;" type="text" value=".50"/> <input style="width: 20px;" type="text" value=".7F"/> <input style="width: 20px;" type="text" value="C7"/> <input style="width: 20px;" type="text" value=".86"/> <input style="width: 20px;" type="text" value=".89"/></p>
--	---

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.

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) – Display value for your reference. TTL value is set by telnet command.

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.

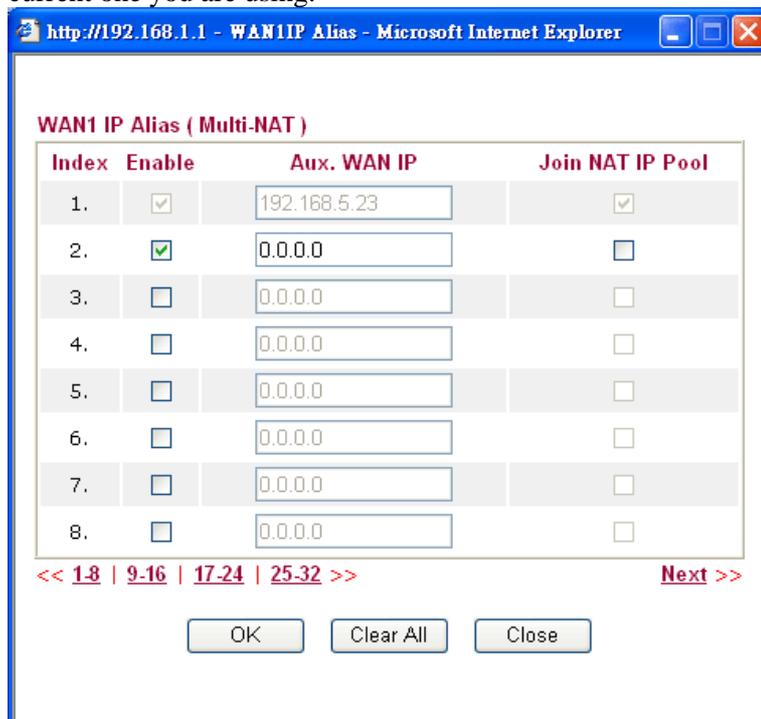
MTU

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

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 32 public IP addresses other than the current one you are using.



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 WAN2. The following web page will be shown.

WAN >> Internet Access

WAN 1

<p>Static or Dynamic IP (DHCP Client)</p> <p><input checked="" type="radio"/> Enable <input type="radio"/> Disable</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"/></p> <p>TTL: <input type="text"/></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</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="172.16.3.229"/></p> <p>Subnet Mask <input type="text" value="255.255.0.0"/></p> <p>Gateway IP Address <input type="text" value="172.16.3.4"/></p> <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:</p> <p><input type="text" value="00"/> <input type="text" value="50"/> <input type="text" value="7F"/> <input type="text" value="C7"/> <input type="text" value="86"/> <input type="text" value="89"/></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.

Keep WAN Connection

Normally, this function is designed for Dynamic IP environments 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) – Display 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 32 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"/>	192.168.5.23	<input checked="" type="checkbox"/>
2.	<input checked="" 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/L2TP

To use **PPTP/L2TP** as the accessing protocol of the internet, please choose **Internet Access** from **WAN** menu. Then, select **PPTP/L2TP** mode for WAN2/WAN2. The following web page will be shown.

WAN 1

<p>PPTP/L2TP Client Mode</p> <p><input checked="" type="radio"/> Enable PPTP <input type="radio"/> Enable L2TP <input type="radio"/> Disable</p> <p>Server Address <input type="text" value="10.0.0.138"/></p> <p>Specify Gateway IP Address <input type="text"/></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>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) <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> <p>WAN IP Network Settings</p> <p><input checked="" type="radio"/> Obtain an IP address automatically</p> <p><input 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>
---	---

PPTP/L2TP Client Mode

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

Click **Enable L2TP** to enable a L2TP client to establish a tunnel to a DSL modem on the WAN interface.

Click **Disable** to disable PPTP/L2TP client mode. All the settings configured in this page will be invalid.

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

Specify Gateway IP Address - Specify the WAN IP address for the router if the server is not in the same subnet.

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.

MTU

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

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.

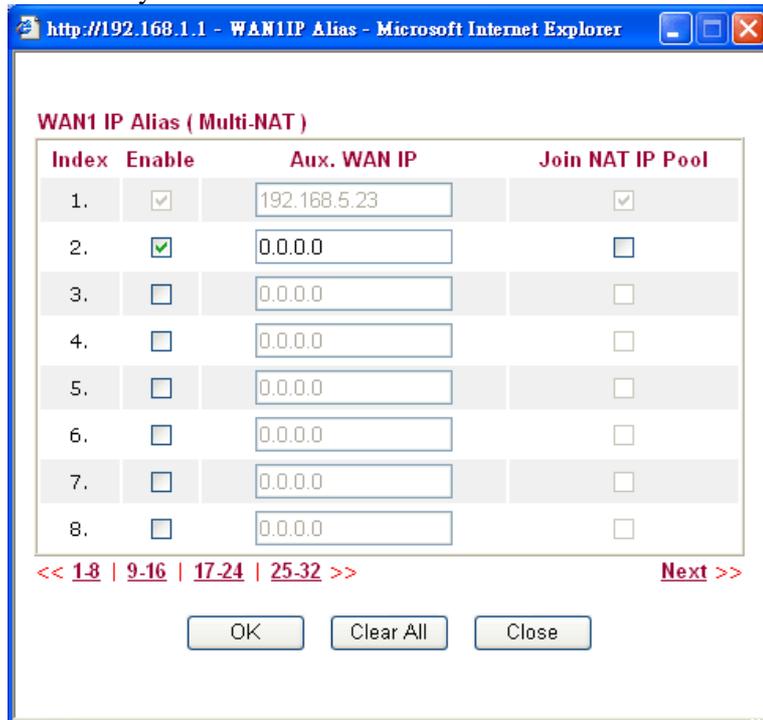
IP Address Assignment Method(IPCP)

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 32 public IP addresses other than the current one you are using. Notice that this setting is available for WAN1 only.



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 in WAN2

Such mode is active only **3G USB Modem** was chosen as the physical mode in General Setup. To use **PPTP** as the accessing protocol of the Internet, select **PPTP** mode. The following web page will appear.

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 filed is blank and the function will always work.

3.1.4 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.

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.
- Src IP Start** Display the IP address for the start of the source IP.
- Src IP End** Display the IP address for the end of the source IP.
- Dest IP Start** Display the IP address for the start of the destination IP.
- Dest IP End** Display the IP address for the end of the destination IP.
- Dest Port Start** Display the IP address for the start of the destination port.
- Dest Port End** Display 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	
Src IP End	
Dest IP Start	
Dest IP End	
Dest Port Start	
Dest Port End	

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.

Protocol	any
----------	-----

- any
- TCP
- UDP
- TCP/UDP
- ICMP
- IGMP

Binding WAN interface

Choose the WAN interface (WAN1 or WAN2) for binding.
Auto failover to other WAN – Check this button to lead the data passing through other WAN automatically when the selected WAN interface is failover.

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.

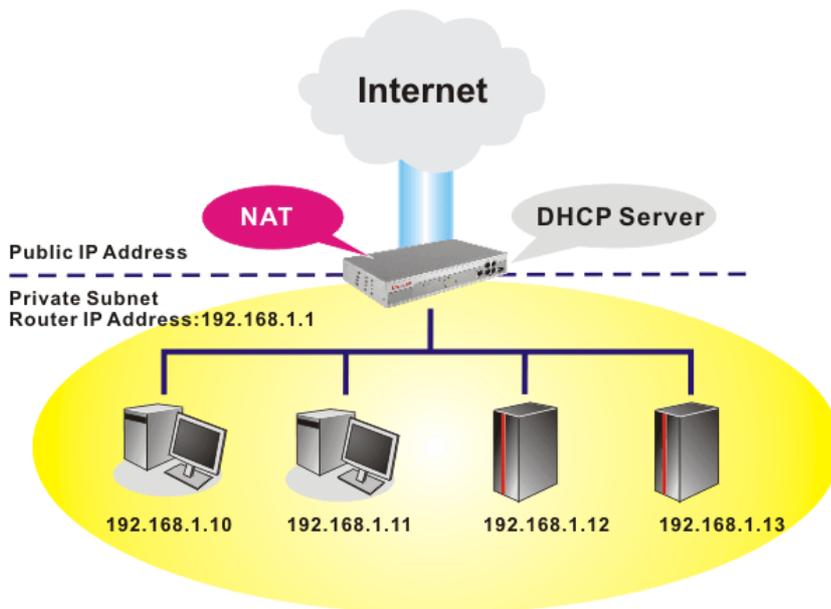
3.2 LAN

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.

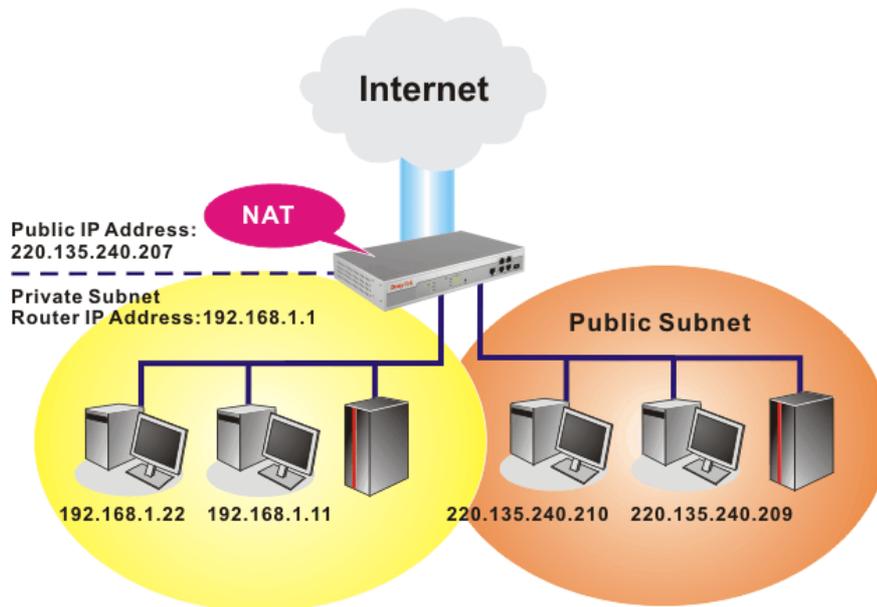


3.2.1 Basics of LAN

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)

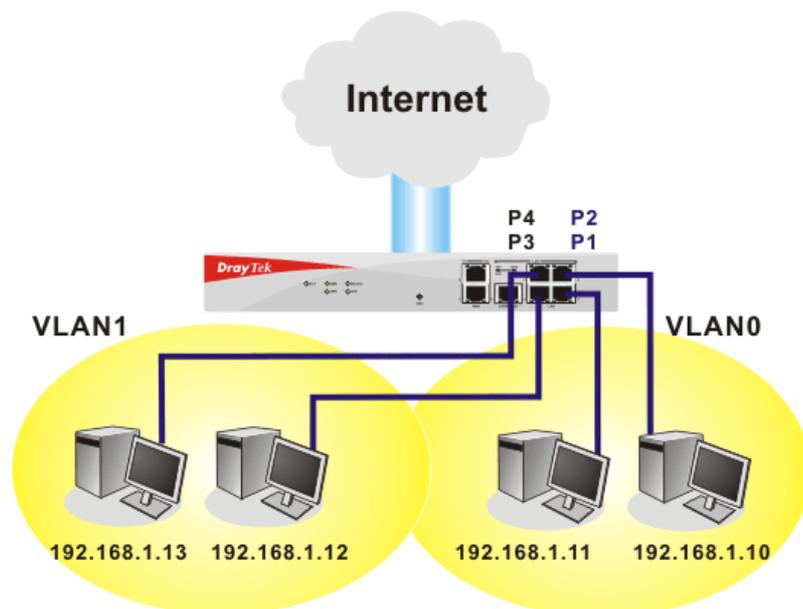
Vigor router will exchange routing information with neighboring routers using the RIP to accomplish IP routing. This allows users to change the information of the router such as IP address and the routers will automatically inform for each other.

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 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"/> <input checked="" type="checkbox"/> 2nd Subnet DHCP Server RIP Protocol Control: <input type="text" value="Disable"/>	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"/> 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.

2nd DHCP Server

Start IP Address:

IP Pool Counts: (max. 10)

Index	Matched MAC Address	given IP Address
-------	---------------------	------------------

MAC Address: : : : :

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.

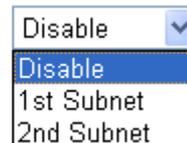
IP Pool Counts: Enter the number of IP addresses in the pool. The maximum is 10. For example, if you type 3 and the 2nd IP address of your router is 220.135.240.1, the range of IP address by the DHCP server will be from 220.135.240.2 to 220.135.240.11.

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.
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 Server Configuration

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

Force DNS manual setting - Force Vigor2910 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: 0-13:37	
LAN Status	Primary DNS: 194.109.6.66		Secondary DNS: 168.95.1.1
IP Address	TX Packets	RX Packets	
192.168.1.1	830	805	
WAN 1 Status			

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.	???	?	6.	???	?
2.	???	?	7.	???	?
3.	???	?	8.	???	?
4.	???	?	9.	???	?
5.	???	?	10.	???	?

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

- Index** The number (1 to 10) under Index allows you to open next page to set up static route.
- Destination Address** Display the destination address of the static route.
- Status** Display the status of the static route.
- Viewing Routing Table** Display the routing table for your reference.

[Diagnostics >> View Routing Table](#)

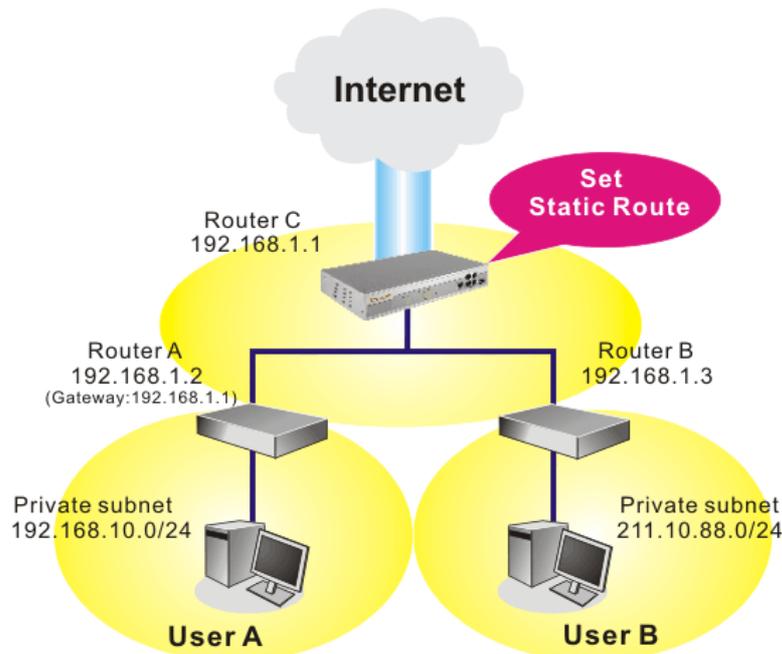
Current Running Routing Table				Refresh
Key: C - connected, S - static, R - RIP, * - default, ~ - private				
*	0.0.0.0/	0.0.0.0 via 172.16.3.1,	WAN1	
C~	192.168.1.0/	255.255.255.0 is directly connected,	LAN	
C	172.16.3.0/	255.255.255.0 is directly connected,	WAN1	

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.



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

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

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

LAN >> Static Route Setup

Index No. 1

Enable

Destination IP Address: 192.168.10.0

Subnet Mask: 255.255.255.0

Gateway IP Address: 192.168.1.2

Network Interface: LAN

OK Cancel

- 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

S~	192.168.10.0/	255.255.255.0	via 192.168.1.2,	LAN
C~	192.168.1.0/	255.255.255.0	is directly connected,	LAN
S~	211.100.88.0/	255.255.255.0	via 192.168.1.3,	LAN

3.2.4 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 **LAN >> 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.

LAN >> VLAN Configuration

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

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.

3.2.5 Bind IP to MAC

This function is used to bind the IP and MAC address in LAN to have a strengthen 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
192.168.1.10	00-0E-A6-2A-D5-A1
192.168.1.230	00-1A-92-E7-36-6A

Index	IP Address	Mac Address
-------	------------	-------------

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.

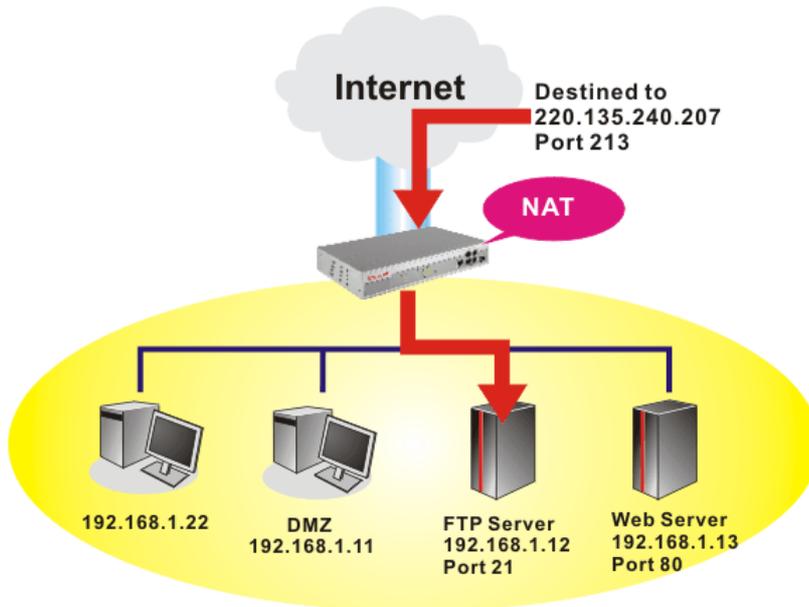
Note: On NAT page, you will see the private IP address defined in RFC-1918. Usually we use the 192.168.1.0/24 subnet for the router. As stated before, the NAT facility can map one or more IP addresses and/or service ports into different specified services. In other words, the NAT function can be achieved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

| [Set to Factory Default](#) |

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

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

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

Index No. 1

<input type="checkbox"/> Enable	
Mode	Single
Service Name	
Protocol	---
WAN Interface	ALL
Public Port	0
Private IP	
Private Port	0

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

OK Clear Cancel

- Enable** Check this box to enable such port redirection setting.
- Mode** Two options (Single and Range) are provided here for you to choose. To set a range for the specific service, select **Range**. In Range mode, if the public port (start port and end port) and the starting IP of private IP had been entered, the system will calculate and display the ending IP of private IP automatically.
- Service Name** Enter the description of the specific network service.
- Protocol** Select the transport layer protocol (TCP or UDP).
- WAN Interface** Select the WAN interface used for the port redirection. The default setting is **All** which means all the incoming data from any port will be redirected to WAN1 and WAN2.
- Public Port** Specify which port can be redirected to the specified **Private IP and Port** of the internal host. If you choose **Range** as the port redirection mode, you will see two boxes on this field. Simply type the required number on the first box. The second one will be assigned automatically later.
- Private IP** Specify the private IP address of the internal host providing the service. If you choose **Range** as the port redirection mode, you will see two boxes on this field. Type a complete IP address in the first box (as the starting point) and the fourth digits in the second box (as the end point).
- Private Port** Specify the private port number of the service offered by the internal host.

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.

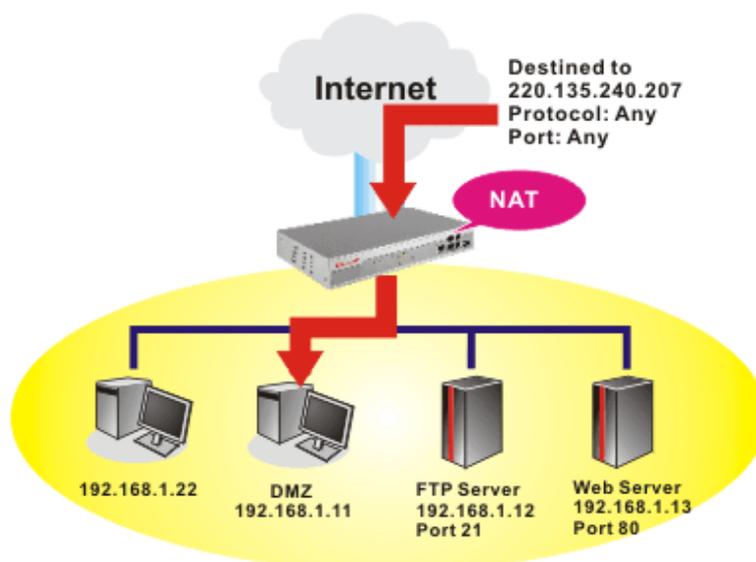
For example, the built-in web configurator in the router is with default port 80, which may conflict with the web server in the local network, http://192.168.1.13:80. Therefore, you need to **change the router's http port to any one other than the default port 80** to avoid conflict, such as 8080. This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

Management Setup													
Management Access Control <input checked="" type="checkbox"/> Allow management from the Internet <input type="checkbox"/> FTP Server <input checked="" type="checkbox"/> HTTP Server <input checked="" type="checkbox"/> HTTPS Server <input checked="" type="checkbox"/> Telnet Server <input type="checkbox"/> SSH Server <input checked="" type="checkbox"/> Disable PING from the Internet	Management Port Setup <input checked="" type="radio"/> User Define Ports <input type="radio"/> Default Ports Telnet Port: <input type="text" value="23"/> (Default: 23) HTTP Port: <input type="text" value="80"/> (Default: 80) HTTPS Port: <input type="text" value="443"/> (Default: 443) FTP Port: <input type="text" value="21"/> (Default: 21) SSH Port: <input type="text" value="22"/> (Default: 22)												
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

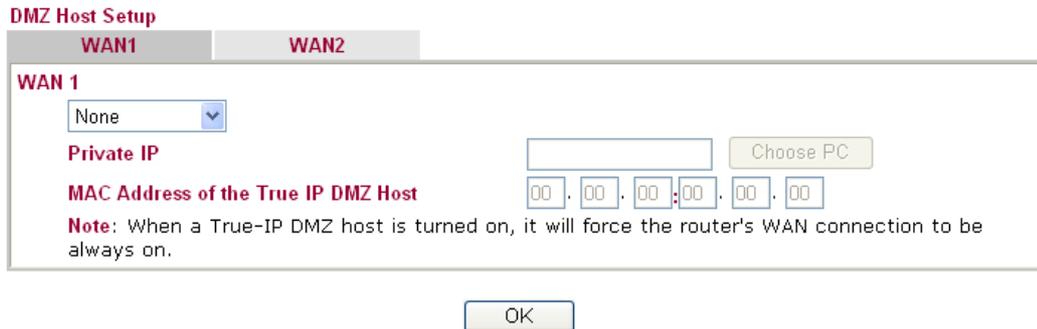
3.3.2 DMZ Host

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.



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:



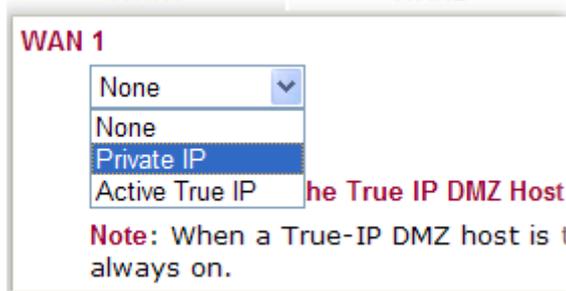
For WAN 1

WAN Selection

In WAN 1, DMZ host can be specified with **Private IP** or **Active True IP**. Choose the one you want.

Private IP

Enter the private IP address of the DMZ host, or click Choose PC to select one. It will be available when you choose **Private IP** as the WAN interface.

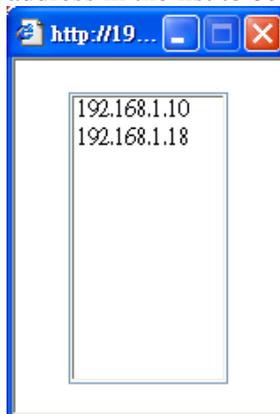


MAC Address of the True IP DMZ Host

Enter the MAC address of the DMZ host. It will be available when you choose **Active True IP** as the WAN interface.

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		Aux. WAN IP	Private IP	
Index	Enable			
1.	<input checked="" type="checkbox"/>	192.168.5.23	192.168.1.10	Choose PC
2.	<input type="checkbox"/>	192.168.1.69	0.0.0.0	Choose PC

OK Clear

For WAN 2

Click WAN2 tab to open the following page:

NAT >> DMZ Host Setup

DMZ Host Setup

WAN1 **WAN2**

Enable	Private IP	
<input checked="" type="checkbox"/>	0.0.0.0	Choose PC

OK

Enable

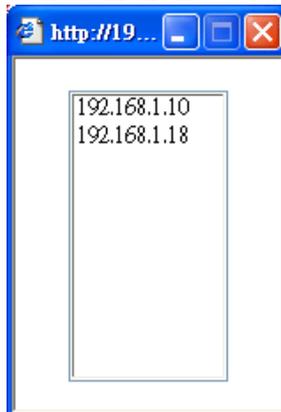
Check to enable the DMZ Host function.

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"/>	192.168.5.23	<input type="text" value="192.168.1.10"/> <input type="button" value="Choose PC"/>
2.	<input type="checkbox"/>	192.168.1.69	<input type="text" value="0.0.0.0"/> <input type="button" value="Choose PC"/>

Note: If you previously have set up WAN Alias in Internet Access>>PPPoE/Static IP/PPTP, 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"/>	192.168.5.23	<input type="text" value="0.0.0.0"/> <input type="button" value="Choose PC"/>
2.	<input type="checkbox"/>	192.168.1.69	<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

Enable Open Ports

Comment

WAN Interface

WAN IP

Local Computer

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

- Enable Open Ports** Check to enable this entry.
- Comment** Make a name for the defined network application/service.
- WAN Interface** Specify the WAN interface that will be used for this entry.
- WAN IP** Such drop down list will be shown only if you have entered other WAN IP address in **WAN IP Alias** window. Choose one of them to apply open port configuration.
- 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.

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

- Protocol** Display the protocol used for this address mapping.
- Public IP** Display the public IP address selected for this entry, e.g., 86.123.123.2.
- Private IP** Display the private IP set for this address mapping, e.g., 192.168.1.10
- Mask** Display the subnet mask selected fro this address mapping.
- Status** Display the status for the entry, enable or disable.

Click the index number link to open the configuration page.

Index No. 1

Enable

Protocol: ALL ▾

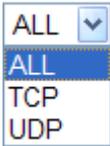
WAN Interface: WAN1 ▾

WAN IP: ▾

Private IP:

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 Interface** Specify the WAN interface that will be used for this entry.
- 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 on 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:

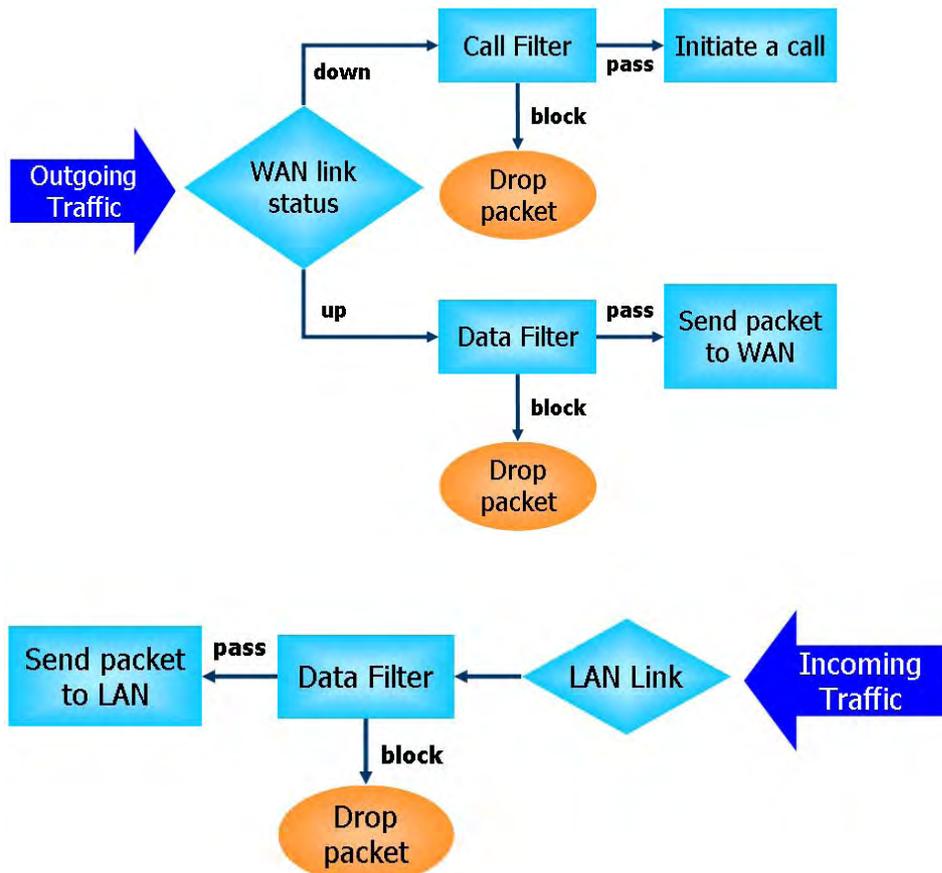
- User-configurable IP filter (Call Filter/ Data Filter).
- Stateful Packet Inspection (SPI): tracks packets and denies unsolicited incoming data
- Selectable Denial of Service (DoS) /Distributed DoS (DDoS) attacks protection
- URL Content Filter

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.

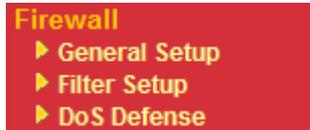
Also the Vigor router monitors the traffic. Any abnormal traffic flow violating the pre-defined parameter, such as the number of thresholds, is identified as an attack and the Vigor router will activate its defense mechanism to mitigate in a real-time manner.

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

1. SYN flood attack
9. SYN fragment

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

Below shows the menu items for Firewall.



3.4.2 General Setup

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

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

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"/>
APP Enforcement	None	<input type="checkbox"/>

Apply IP filter to VPN incoming packets
 Accept large incoming fragmented UDP or ICMP packets (for some games, ex. CS)

OK
Cancel

- 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.
- Start Filter Set** Choose one of the filter sets as the base for call filter/data filter.
- Action/Profile** Select **Pass** or **Block** for the packets that do not match with the filter rules.
- Syslog** For troubleshooting needs you can specify the filter log and/or CSM log here by checking the box. The log will be displayed on Draytek Syslog window.
- APP Enforcement** Select one of the **APP Enforcement Profile** settings (created in **CSM>> APP Enforcement Profile**) for applying with this router.

Please set at least one profile for choosing in **CSM>> APP Enforcement Profile** web page first. For troubleshooting needs, you can specify to record information for **APP Enforcement Profile** by checking the Log box. It will be sent to Syslog server. Please refer to section **Syslog/Mail Alert** for more detailed information.

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

3.4.3 Filter Setup

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

Firewall >> Filter Setup

Filter Setup		Set to Factory Default	
Set	Comments	Set	Comments
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.

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

Filter Set 1 Rule 1

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

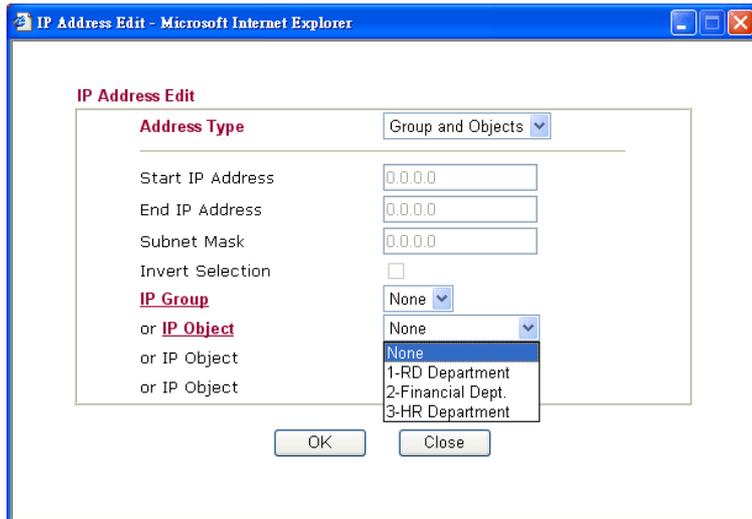
Check to enable the Filter Rule Check this box to enable the filter rule.

Comments Enter filter set comments/description. Maximum length is 14-character long.

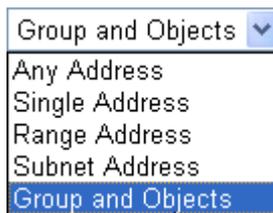
Index(1-15) Set PCs on LAN to work at certain time interval only. You may choose up to 4 schedules out of the 15 schedules pre-defined in **Applications >> Schedule** setup. The default setting of this field is blank and the function will always work.

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.



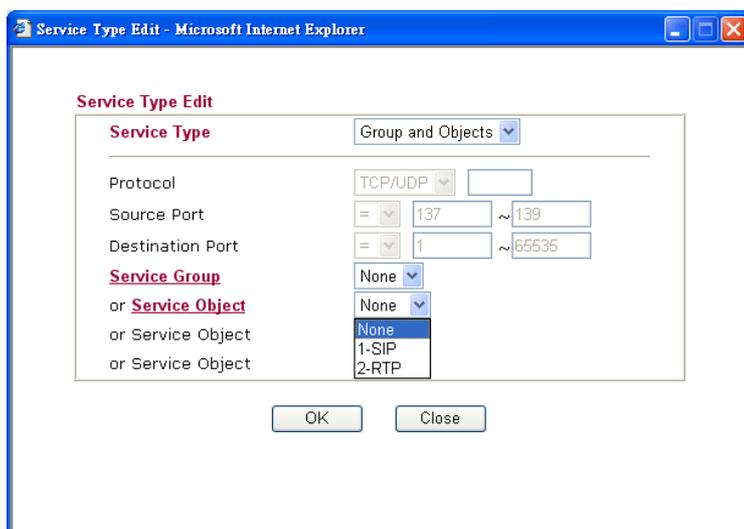
To set the IP address manually, please choose **Any Address/Single Address/Range Address/Subnet Address** as the Address Type and type them in this dialog. In addition, if you want to use the IP range from defined groups or objects, please choose **Group and Objects** as the Address Type.



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.

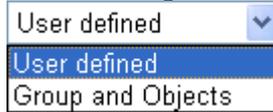
Service Type

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.

APP Enforcement

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

SysLog

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

Example

As stated before, all the traffic will be separated and arbitrated using one of two IP filters: call filter or data filter. You may preset 12 call filters and data filters in **Filter Setup** and even link them in a serial manner. Each filter set is composed by 7 filter rules, which can be further defined. After that, in **General Setup** you may specify one set for call filter and one set for data filter to execute first.

Firewall >> General Setup

General Setup

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

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

Actions for default rule:
 Application: Pass
 Filter: None
 APP Enforcement: None

Apply IP filter to VPN incoming packets
 Accept large incoming fragmented UDP or ICMP packets

OK Clear

Firewall >> Filter Setup

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

Set to Factory Default

Firewall >> Filter Setup >> Edit Filter Set

Filter Set 1

Comments: Default Call Filter

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

OK Clear

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 any Edit
 Fragments: Don't Care

Application: Pass If No Further Match
 Filter: Pass If No Further Match
 Branch to Other Filter Set: None
 APP Enforcement: None

Syslog

OK Clear Cancel

3.4.4 DoS Defense

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

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

[Firewall >> DoS defense Setup](#)

DoS defense Setup

Enable DoS Defense

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

Block IP options Block TCP flag scan
 Block Land Block Tear Drop
 Block Smurf Block Ping of Death
 Block trace route Block ICMP fragment
 Block SYN fragment Block UnknownProtocol
 Block Fraggle Attack

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

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 *no flag scan*, *FIN without ACK scan*, *SYN FINscan*, *Xmas scan* and *full Xmas scan*.
- Block Tear Drop** Check the box to activate the Block Tear Drop function. Many machines may crash when receiving ICMP datagrams (packets) that exceed the maximum length. To avoid this type of attack, the Vigor router is designed to be capable of discarding any fragmented ICMP packets with a length greater than 1024 octets.
- Block Ping of Death** Check the box to activate the Block Ping of Death function. This attack involves the perpetrator sending overlapping packets to the target hosts so that those target hosts will hang once they re-construct the packets. The Vigor routers will block any packets realizing this attacking activity.
- Block ICMP Fragment** Check the box to activate the Block ICMP fragment function. Any ICMP packets with more fragment bit set are dropped.
- Block 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 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.

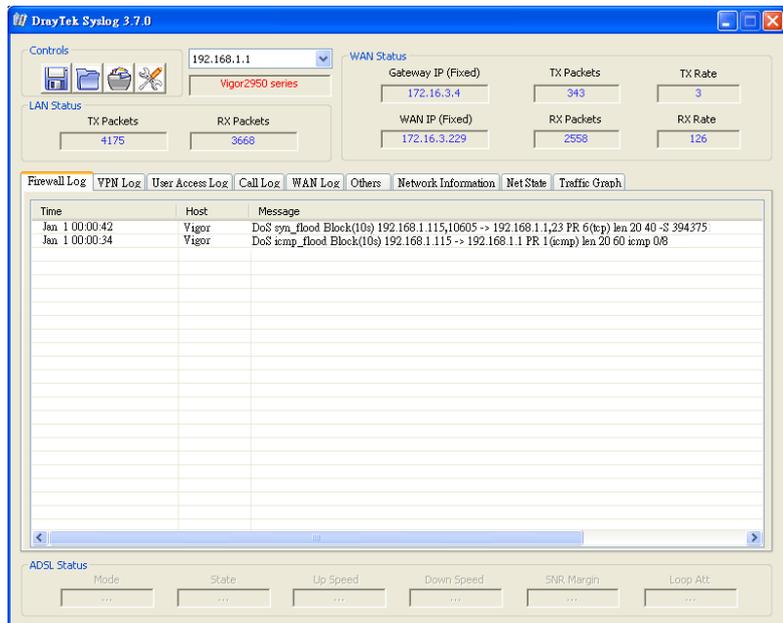
All the warning messages related to **DoS defense** will be sent to user and user can review it through Syslog daemon. Look for the keyword **DoS** in the message, followed by a name to indicate what kind of attacks is detected.

System Maintenance >> SysLog / Mail Alert Setup

SysLog / Mail Alert Setup

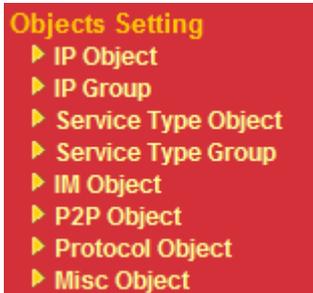
<p>SysLog Access Setup</p> <input checked="" type="checkbox"/> Enable Router Name: <input type="text" value="2950"/> Server IP Address: <input type="text" value="192.168.1.10"/> Destination Port: <input type="text" value="514"/> Enable syslog message: <input checked="" type="checkbox"/> Firewall Log <input checked="" type="checkbox"/> VPN Log <input checked="" type="checkbox"/> User Access Log <input checked="" type="checkbox"/> Call Log <input checked="" type="checkbox"/> WAN Log <input checked="" type="checkbox"/> Router/DSL information	<p>Mail Alert Setup</p> <input type="checkbox"/> Enable SMTP Server: <input type="text"/> Mail To: <input type="text"/> Return-Path: <input type="text"/> <input type="checkbox"/> Authentication User Name: <input type="text"/> Password: <input type="text"/>
---	---

OK Clear Cancel



3.5 Objects Settings

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



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.

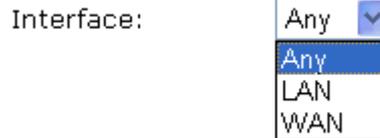
Objects Setting >> IP Object

Profile Index : 1

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

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

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



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

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

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

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

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

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

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
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 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 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="www"/>
Protocol	TCP <input type="text" value="6"/>
Source Port	= <input type="text" value="1"/> ~ <input type="text" value="65535"/>
Destination Port	= <input type="text" value="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
- IGMP
- 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
1.	SIP
2.	RTP
3.	

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
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 settings in detail.

Profile Index : 1

Name:

Available Service Type Objects

1-SIP
2-RTP

Selected Service Type Objects

- Name** Type a name for this profile.
- Available Service Type Objects** You can add IP objects from IP Objects 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 IM Object

This page allows you to set 32 profiles for Instant Messenger. These profiles will be applied in **CSM>>APP Enforcement Profile** for filtering.

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(<= v5.9)	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 checked="" type="checkbox"/>		<input type="checkbox"/>	<input type="checkbox"/>
Conference	<input type="checkbox"/>	<input type="checkbox"/>		<input type="checkbox"/>
Other Activities	<input type="checkbox"/>	<input type="checkbox"/>		<input type="checkbox"/>

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"/> Kubao
<input type="checkbox"/> Qnext	<input type="checkbox"/> Meetro	<input type="checkbox"/> POCO/PP365	<input type="checkbox"/> AresChat	<input type="checkbox"/> Gizmo
<input type="checkbox"/> AliWW	<input type="checkbox"/> KC	<input type="checkbox"/> Lava-Lava	<input type="checkbox"/> ICU2	<input type="checkbox"/> SIP
<input type="checkbox"/> iSpQ	<input type="checkbox"/> UC	<input type="checkbox"/> MobileMSN		

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

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.

3.5.6 P2P Object

This page allows you to set 32 profiles for peer-to-peer application. These profiles will be applied in **CSM>>APP Enforcement 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>>APP Enforcement 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	<input type="checkbox"/> Pando

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.

3.5.7 Protocol Object

This page allows you to set 32 profiles for applications in protocol communication. These profiles will be applied in **CSM>>APP Enforcement Profile** for filtering.

Objects Setting >> Protocol Object Profile

Protocol 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. Internet protocols are listed in the page for you to choose to disallow people using. Any computer controlled or passed through the router will be restricted by this profile if it tries to use the protocol to communicate with others.

Simple check the box(es) and then click **OK**. Later, in the **CSM>>APP Enforcement Profile** page, you can use **Protocol Object** drop down list to choose the proper profile configured here as the standard for the host(s) to follow.

Objects Setting >> Protocol Object Profile

Profile Index: 1

Profile Name:

Check for Disallow:

Protocol				
<input type="checkbox"/> DNS	<input type="checkbox"/> FTP	<input type="checkbox"/> HTTP	<input type="checkbox"/> IMAP	<input type="checkbox"/> IRC
<input type="checkbox"/> NNTP	<input type="checkbox"/> POP3	<input type="checkbox"/> SMB	<input type="checkbox"/> SMTP	<input type="checkbox"/> SNMP
<input type="checkbox"/> SSH	<input type="checkbox"/> SSL/TLS	<input type="checkbox"/> TELNET		

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.

3.5.8 Misc Object

This page allows you to set 32 profiles for miscellaneous applications. These profiles will be applied in **CSM>> APP Enforcement 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: 1

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"/> PPStream
<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 Filter

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

URL Content Filter

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.

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.

Web Content Filter

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 different policy of IM (Instant Messenger)/P2P (Peer to Peer) application. Such profile will be used in **Firewall>>General Setup** and **Firewall>>Filter Setup** pages.

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.

Click the number under Index column for settings in detail.

Profile Index: 1

Profile Name:

IM Object	None ▾
P2P Object	None ▾
Protocol Object	None ▾
Misc Object	None ▾

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

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

CSM >> URL Content Filter

Content Filter Setup

Enable URL Access Control

Enable URL Access Log

Black List (block those matching keyword)

White List (pass those matching keyword)

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

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

Prevent web access from IP address

Enable Restrict Web Feature

Java ActiveX Compressed files Executable files Multimedia files

Cookie Proxy

Enable Excepting Subnets

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

Time Schedule

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

Note: Action and Idle Timeout settings will be ignored.

Enable URL Access Control

Check the box to activate URL Access Control.

Black List (block those matching keyword)

Click this button to restrict accessing into the corresponding webpage with the keywords listed on the box below.

White List (pass those matching keyword)

Click this button to allow accessing into the corresponding webpage with the keywords listed on the box below.

Keyword

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

Prevent web access from IP address

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

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

Enable Restrict Web Feature

Check the box to activate the function.

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

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

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

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

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

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

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

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

.mov .mp3 .rm .ra .au .wmv

.wav .asf .mpg .mpeg .avi .ram

Enable Excepting Subnets

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

Time Schedule Specify what time should perform the URL content filtering facility.

3.6.3 Web Content Filter Profile

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.

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

CSM >> Web Content Filter Setup

Web Content Filter Setup

Select a server: global shortest site ▼

[Test a site to verify whether it is categorized](#)

Enable Web Content Filter

Groups	Categories (Tick categories to block. Untick to unblock)		
Child Protection <input type="button" value="Select All"/> <input type="button" value="Clear All"/>	<input type="checkbox"/> Chat <input type="checkbox"/> Gambling <input type="checkbox"/> Sex	<input type="checkbox"/> Criminal <input type="checkbox"/> Hacking <input type="checkbox"/> Violence	<input type="checkbox"/> Drugs/Alcohol <input type="checkbox"/> Hate speech <input type="checkbox"/> Weapons
Leisure <input type="button" value="Select All"/> <input type="button" value="Clear All"/>	<input type="checkbox"/> Advertisements <input type="checkbox"/> Games <input type="checkbox"/> Hobbies <input type="checkbox"/> Personals <input type="checkbox"/> Sports	<input type="checkbox"/> Entertainment <input type="checkbox"/> Glamour <input type="checkbox"/> Lifestyle <input type="checkbox"/> Photo Searches <input type="checkbox"/> Streaming Media	<input type="checkbox"/> Food <input type="checkbox"/> Health <input type="checkbox"/> Motor Vehicles <input type="checkbox"/> Shopping <input type="checkbox"/> Travel
Business <input type="button" value="Select All"/> <input type="button" value="Clear All"/>	<input type="checkbox"/> Computing/Internet <input type="checkbox"/> Politics <input type="checkbox"/> Remote proxies	<input type="checkbox"/> Finance <input type="checkbox"/> Real Estate <input type="checkbox"/> Search Engine	<input type="checkbox"/> Job Search/Career <input type="checkbox"/> Reference <input type="checkbox"/> Web Mail
Others <input type="button" value="Select All"/> <input type="button" value="Clear All"/>	<input type="checkbox"/> Education <input type="checkbox"/> News <input type="checkbox"/> Usenet news	<input type="checkbox"/> Hosting sites <input type="checkbox"/> Religion <input type="checkbox"/> Block all uncategorized sites	<input type="checkbox"/> Kid Sites <input type="checkbox"/> Sex Education

Time Schedule

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

Note: Action and Idle Timeout settings will be ignored.

For this section, please refer to **Web Content Filter** user's guide.

3.7 Bandwidth Management

Below shows the menu items for Bandwidth Management.

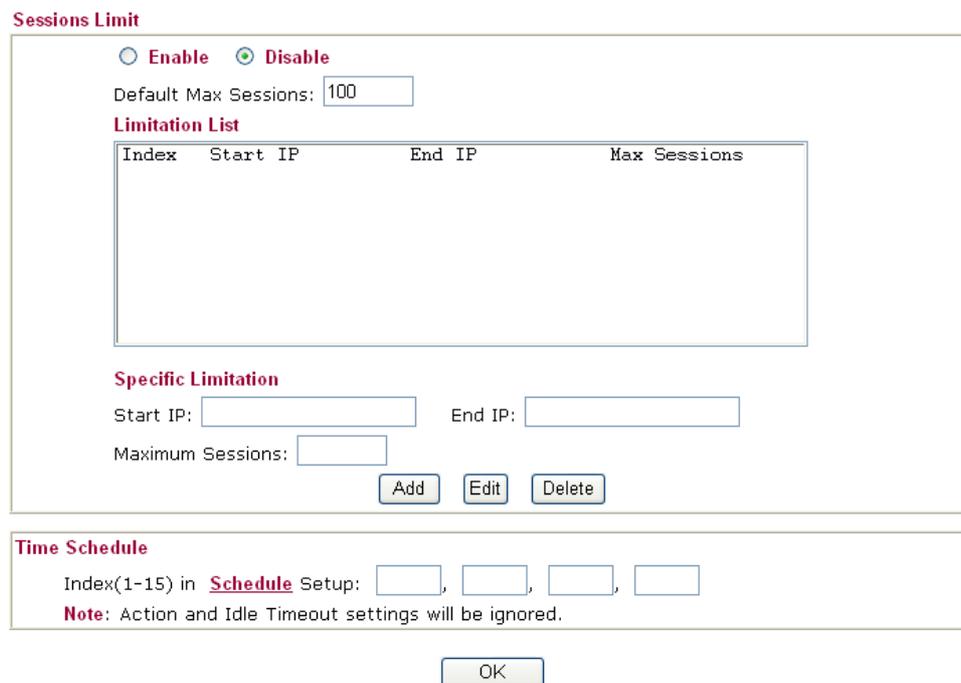


3.7.1 Sessions Limit

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.

[Bandwidth Management >> Sessions Limit](#)



The screenshot shows the "Sessions Limit" configuration page. At the top, there are radio buttons for "Enable" (unselected) and "Disable" (selected). Below this is a text input field for "Default Max Sessions" with the value "100". A section titled "Limitation List" contains an empty table with columns: "Index", "Start IP", "End IP", and "Max Sessions". Below the table is a "Specific Limitation" section with input fields for "Start IP", "End IP", and "Maximum Sessions". There are "Add", "Edit", and "Delete" buttons below these fields. At the bottom, there is a "Time Schedule" section with a text input for "Index(1-15) in Schedule Setup" and a "Note" stating "Action and Idle Timeout settings will be ignored." An "OK" button is located at the very bottom of the page.

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 Display 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 Sessions	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	Remove 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.

3.7.2 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.

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

[Bandwidth Management >> Bandwidth Limit](#)

Bandwidth Limit

Enable
 Apply to 2nd Subnet
 Disable

Default TX Limit: Kbps
 Default RX Limit: Kbps

Allow auto adjustment to make the best utilization of [available bandwidth](#).

Limitation List

Index	Start IP	End IP	TX limit	RX limit	Shared

Specific Limitation

Start IP:
 End IP:

Each
 Shared
 TX Limit: Kbps
 RX Limit: Kbps

Time Schedule

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

Note: Action and Idle Timeout settings will be ignored.

To activate the function of limit bandwidth, simply click **Enable** and set the default upstream and downstream limit.

Enable Click this button to activate the function of limit bandwidth.
Apply to 2nd Subnet – Check this box to apply the bandwidth limit to the second subnet specified in **LAN>>General Setup**.

Disable Click this button to close the function of limit bandwidth.

Default TX limit	Define the default speed of the upstream for each computer in LAN.
Default RX limit	Define the default speed of the downstream for each computer in LAN.
Allow auto adjustment to make the best utilization of available bandwidth	Router will detect if there is enough bandwidth remained for using according to the bandwidth limit set by the user. If yes, the router will adjust the available bandwidth for users to enhance the total utilization.
Limitation List	Display a list of specific limitations that you set on this web page.
Start IP	Bandwidth limit can be applied on certain IP range. That's, only the PCs within the range will be influenced by the bandwidth limitation set here. Please define the start IP address for the specific limitation.
End IP	Define the end IP address for the specific limitation.
Each /Shared	Click the radio button to determine the specific limitation will be applied to. Each - The bandwidth limit for transmission and receiving (TX limit and RX limit) will be applied to each PC on certain IP range. Shared - The bandwidth limit for transmission and receiving (TX limit and RX limit) will be shared by all of the PCs on certain IP range.
TX limit	Define the limitation for the speed of the upstream to be applied as specific limitation. 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 to be applied as specific limitation. 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	Allows you to edit the settings for the selected limitation.
Delete	Remove 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.

3.7.3 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?

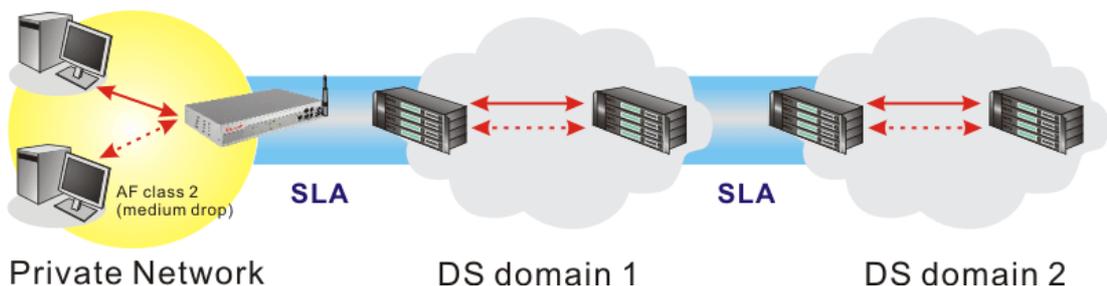
There are two components within Primary configuration of QoS deployment:

- **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.

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	

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		<input type="text" value="10000"/> Kbps
WAN Outbound Bandwidth		<input type="text" value="10000"/> Kbps
Note: Before enable QoS, you should test the real bandwidth first. QoS may not work properly if the bandwidth is not accurate.		
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"/> %
<input type="checkbox"/> Enable UDP Bandwidth Control		Limited_bandwidth Ratio <input type="text" value="25"/> %

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.

Note: Before enable QoS control, you should test the real bandwidth first. QoS may not work properly if the bandwidth is not accurate. You can visit www.speedtest.net or contact with your ISP to get speed test page. Type proper inbound/outbond bandwidth value according to the value obtained from the speed test results.

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 10000kbps 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

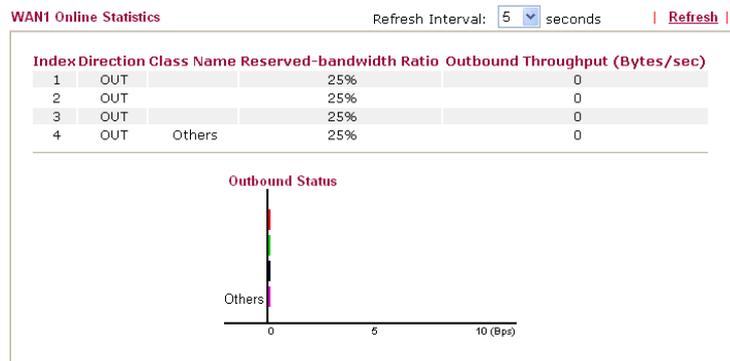
Reserved Bandwidth Ratio It is reserved for the group index in the form of ratio of **reserved bandwidth to upstream speed** and **reserved bandwidth to downstream speed**.

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.

Limited_bandwidth Ratio The ratio typed here is reserved for limited bandwidth of UDP application.

On Line Statistics Display an online statistics for quality of service for your reference.

[Bandwidth Management >> Quality of Service](#)



Such function is available only after QoS Control is enabled and access **Setup** link from **Quality of Service** page again.

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	
Class 2		Edit	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	-	-	-	-

[Add](#) [Edit](#) [Delete](#)

[OK](#) [Cancel](#)

For adding a new rule, click **Add** to open the following page.

Bandwidth Management >> Quality of Service

Rule Edit

ACT

Local Address [Edit](#)

Remote Address [Edit](#)

DiffServ CodePoint

Service Type

Note: Please choose/setup the **Service Type** first.

[OK](#) [Cancel](#)

ACT

Check this box to invoke these settings.

Local Address

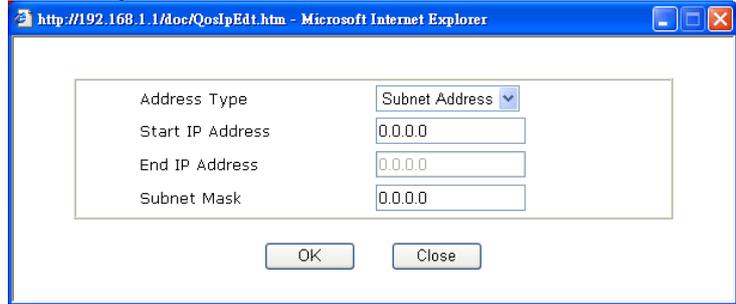
Click the **Edit** button to set the local IP address (on LAN) for the rule.

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.

Bandwidth Management >> Quality of Service

Class Index #1

Name

NO	Status	Local Address	Remote Address	DiffServ CodePoint	Service Type
<input type="radio"/> 1	Active	Any	Any	IP precedence 2	SYSLOG(UDP:514)
<input type="radio"/> 2	Active	192.168.1.15	192.168.1.65	AF Class1 (Low Drop)	FTP(TCP:20)

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.

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	

After you click the **Edit** link, you will see the following page.

Bandwidth Management >> Quality of Service

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"/>
Service Type	TCP <input type="button" value="v"/> <input type="text" value="6"/>
Port Configuration	
Type	<input checked="" type="radio"/> Single <input type="radio"/> Range
Port Number	<input type="text" value="0"/> - <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.

3.8 Applications

Below shows the menu items for Applications.



3.8.1 Dynamic DNS

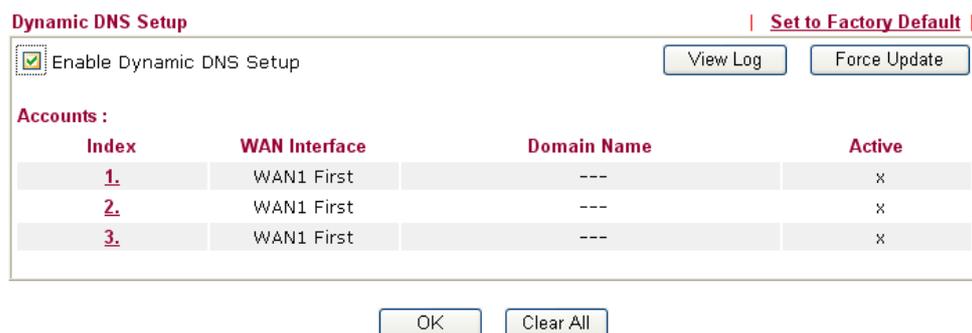
The ISP often provides you with a dynamic IP address when you connect to the Internet via your ISP. It means that the public IP address assigned to your router changes each time you access the Internet. The Dynamic DNS feature lets you assign a domain name to a dynamic WAN IP address. It allows the router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

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

Enable the Function and Add a Dynamic DNS Account

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

[Applications >> Dynamic DNS Setup](#)



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

Enable Dynamic DNS Setup

Accounts :

Index	WAN Interface	Domain Name	Active
1.	WAN1 First	---	x
2.	WAN1 First	---	x
3.	WAN1 First	---	x

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

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

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

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 a 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.

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.

3.8.2 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.

[Applications >> Schedule](#)

Index No. 1

Enable Schedule Setup

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

Start Time (hh:mm) 0 : 0

Duration Time (hh:mm) 0 : 0

Action Force On

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

How Often

Once

Weekdays

Sun Mon Tue Wed Thu Fri Sat

Enable Schedule Setup

Check to enable the schedule.

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

Example

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

Office

Hour:

(Force On)



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

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

3.8.3 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 and/or LDAP client feature. |
| Server IP Address | Enter the IP address of RADIUS and/or LDAP server. |
| Destination Port | The UDP port number that the RADIUS and/or LDAP server is using. The default value is 1812 for RADIUS based on RFC 2138 and 389 for LDAP. |
| 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.

3.8.4 UPnP

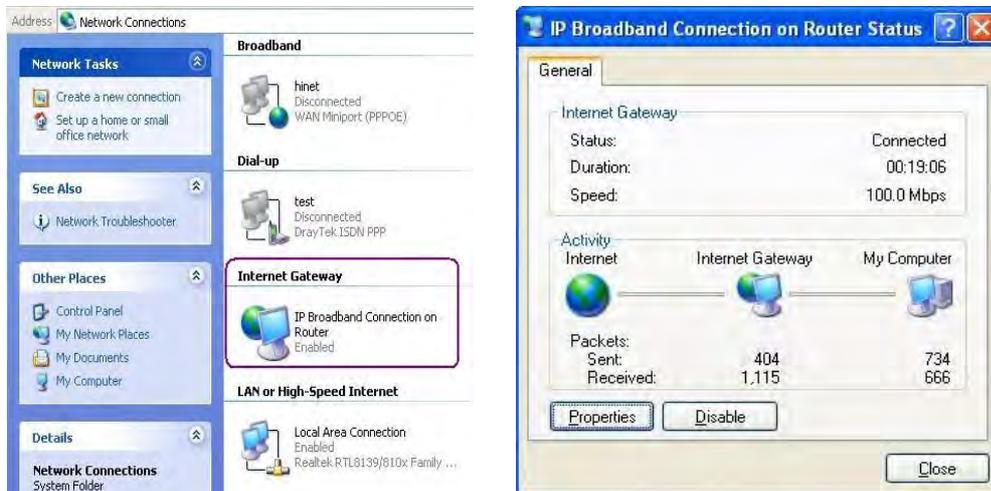
The **UPnP** (Universal Plug and Play) protocol is supported to bring to network connected devices the ease of installation and configuration which is already available for directly connected PC peripherals with the existing Windows 'Plug and Play' system. For NAT routers, the major feature of UPnP on 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

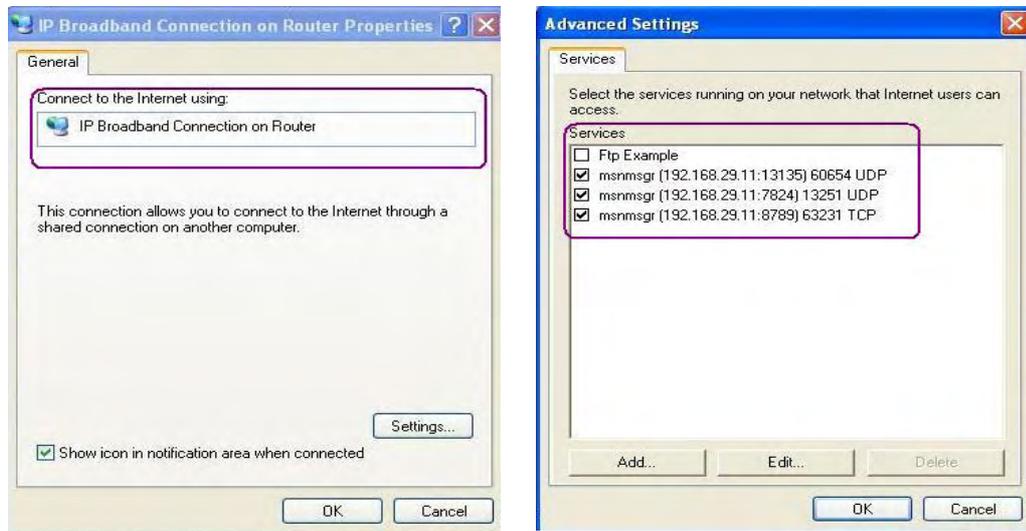


Enable UPNP Service Accordingly, you can enable either the **Connection Control Service** or **Connection Status Service**.

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.

3.8.5 Wake on LAN

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

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

Application >> Wake on LAN

Wake on LAN

Note: Wake on LAN cooperate 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 **Firewall>>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 cooperate 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.

3.9 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.



3.9.1 VPN Client Wizard

Such wizard is used to configure VPN settings for VPN client. Such wizard will guide to set the LAN-to-LAN profile for VPN dial out connection (from server to client) step by step.

VPN and Remote Access >> VPN Client Wizard

Choose VPN Establishment Environment

LAN-to-LAN VPN Client Mode Selection:

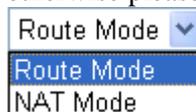
Please choose a LAN-to-LAN Profile:

Note: If the remote network only allows you to dial in with single IP, please choose NAT mode, otherwise choose Route Mode.

LAN-to-LAN Client Mode Selection

Choose the client mode.

Route Mode/NAT Mode – If the remote network only allows you to dial in with single IP, please choose this mode, otherwise please choose Route Mode.



Please choose a

There are 32 VPN profiles for users to set.

LAN-to-LAN Profile

[Index]	[Status]	[Name]
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	???
18	x	???
19	x	???
20	x	???
21	x	???
22	x	???
23	x	???
24	x	???
25	x	???
26	x	???
27	x	???
28	x	???
29	x	???

When you finish the mode and profile selection, please click **Next** to open the following page.

VPN and Remote Access >> VPN Client Wizard

VPN Connection Setting

Security ranking (1 is the highest; 5 is the lowest)

1. L2TP over IPSec
2. IPSec
3. PPTP (Encryption)
4. L2TP
5. PPTP (None Encryption)

Throughput ranking (1 is the highest; 5 is the lowest)

1. PPTP (None Encryption)
2. L2TP
3. IPSec
4. L2TP over IPSec
5. PPTP (Encryption)

Select VPN Type:

- PPTP (None Encryption)
- PPTP (Encryption)
- IPSec
- L2TP
- L2TP over IPSec (Nice to Have)
- L2TP over IPSec (Must)

< Back Next > Finish Cancel

In this page, you have to select suitable VPN type for the VPN client profile. There are six types provided here. Different type will lead to different configuration page. After making the choices for the client profile, please click **Next**. You will see different configurations based on the selection(s) you made.

- When you choose **PPTP (None Encryption)** or **PPTP (Encryption)**, you will see the following graphic:

VPN and Remote Access >> VPN Client Wizard

VPN Client PPTP None Encryption Settings

Profile Name	???
VPN Dial-Out Through	WAN1 First
<input type="checkbox"/> Always on	
Server IP/Host Name for VPN (e.g. 5551234, draytek.com or 123.45.67.89)	draytek.com
Username	marketing
Password	●●●●●●●●
Remote Network IP	192.168.1.6
Remote Network Mask	255.255.255.0

< Back Next > Finish Cancel

- When you choose **IPSec**, you will see the following graphic:

VPN and Remote Access >> VPN Client Wizard

VPN Client IPSec Settings

Profile Name	VPN-1
VPN Dial-Out Through	WAN1 First
<input type="checkbox"/> Always on	
Server IP/Host Name for VPN (e.g. 5551234, draytek.com or 123.45.67.89)	draytek.com
IKE Authentication Method	
<input type="radio"/> Pre-Shared Key	
Confirm Pre-Shared Key	
<input checked="" type="radio"/> Digital Signature (X.509)	
Peer ID	None
Local ID	
<input checked="" type="radio"/> Alternative Subject Name First	
<input type="radio"/> Subject Name First	
Local Certificate	None
IPSec Security Method	
<input checked="" type="radio"/> Medium (AH)	
<input type="radio"/> High (ESP)	DES without Authentication
Remote Network IP	192.168.1.6
Remote Network Mask	255.255.255.0

< Back Next > Finish Cancel

- When you choose **L2TP**, you will see the following graphic:

VPN Client L2TP Settings

Profile Name	VPN-1
VPN Dial-Out Through	WAN1 First
<input type="checkbox"/> Always on	
Server IP/Host Name for VPN (e.g. 5551234, draytek.com or 123.45.67.89)	draytek.com
Username	marketing
Password	••••••••
Remote Network IP	192.168.1.6
Remote Network Mask	255.255.255.0

< Back Next > Finish Cancel

- When you choose **L2TP over IPSec (Nice to Have)**, you will see the following graphic:

VPN Client L2TP over IPSec (Nice to Have) Settings

Profile Name	VPN-1
VPN Dial-Out Through	WAN1 First
<input type="checkbox"/> Always on	
Server IP/Host Name for VPN (e.g. 5551234, draytek.com or 123.45.67.89)	draytek.com
IKE Authentication Method	
<input type="radio"/> Pre-Shared Key	
Confirm Pre-Shared Key	
<input checked="" type="radio"/> Digital Signature (X.509)	
Peer ID	None
Local ID	
<input checked="" type="radio"/> Alternative Subject Name First	
<input type="radio"/> Subject Name First	
Local Certificate	None
IPSec Security Method	
<input checked="" type="radio"/> Medium (AH)	
<input type="radio"/> High (ESP)	DES without Authentication
Username	marketing
Password	••••••••
Remote Network IP	192.168.1.6
Remote Network Mask	255.255.255.0

< Back Next > Finish Cancel

- When you choose **L2TP over IPSec (Must)**, you will see the following graphic:

VPN Client L2TP over IPSec (Must) Settings

Profile Name	VPN-1
VPN Dial-Out Through	WAN1 First
<input type="checkbox"/> Always on	
Server IP/Host Name for VPN (e.g. 5551234, draytek.com or 123.45.67.89)	draytek.com
IKE Authentication Method	
<input type="radio"/> Pre-Shared Key	
Confirm Pre-Shared Key	
<input checked="" type="radio"/> Digital Signature (X.509)	
Peer ID	None
Local ID	
<input checked="" type="radio"/> Alternative Subject Name First	
<input type="radio"/> Subject Name First	
Local Certificate	None
IPSec Security Method	
<input checked="" type="radio"/> Medium (AH)	
<input type="radio"/> High (ESP)	DES without Authentication
Username	marketing
Password	●●●●●●●●
Remote Network IP	192.168.1.6
Remote Network Mask	255.255.255.0

Profile Name

Type a name for such profile. The length of the file is limited to 10 characters.

VPN Dial-Out Through

Use the drop down menu to choose a proper WAN interface for this profile. This setting is useful for dial-out 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.

Always On

Check to enable router always keep VPN connection.

Pre-Shared Key

IKE Authentication Method 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.

Pre-Shared Key- Specify a key for IKE authentication
Confirm Pre-Shared Key- Confirm the pre-shared key.

Digital Signature (X.509) Check the box of Digital Signature to invoke this function.

Peer ID – Select one predefined in the X.509 Peer ID Profiles (set from **VPN and Remote Access>>IPsec Peer Identity**). If you choose **None**, it means that you will accept any peer regardless of its identity.

Local ID – Click **Alternative Subject Name First** to make a specific field of digital signature to accept the peer with matching value. The field can be IP Address, Domain, or E-mail Address. Or click **Subject Name First** to make a specific field 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). You have to configure one certificate at least previously in **Certificate Management >> Local Certificate**. Otherwise, the setting you choose here will not be effective.

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 **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.

User Name This field is used to authenticate for connection when you select PPTP or L2TP with or without IPsec policy above.

Password This field is used to authenticate for connection when you select PPTP or L2TP with or without IPsec policy above.

Remote Network IP Please type one LAN IP address (according to the real location of the remote host) for building VPN connection.

Remote Network Mask Please type the network mask (according to the real location of the remote host) for building VPN connection.

After finishing the configuration, please click **Next**. The confirmation page will be shown as follows. If there is no problem, you can click one of the radio buttons listed on the page and click **Finish** to execute the next action.

Please confirm your settings

LAN-to-LAN Index:	3
Profile Name:	VPN-1
VPN Connection Type:	L2TP over IPSec (Must)
VPN Connection Through:	WAN1 First
Always on:	No
Server IP/Host Name:	draytek.com
IKE Authentication Method:	Digital Signature (X.509)
IPSec Security Method:	AH-SHA1
Remote Network IP:	192.168.1.6
Remote Network Mask:	255.255.255.0

Click **Back** to modify changes if necessary. Otherwise, click **Finish** to save the current settings and proceed to the following action:

- Go to the VPN Connection Management.
- Do another VPN Client Wizard setup.
- View more detailed configurations.

< Back Next > Finish Cancel

Go to the VPN Connection Management Click this radio button to access **VPN and Remote Access>>Connection Management** for viewing VPN Connection status.

Do another VPN Server Wizard Setup Click this radio button to set another profile of VPN Server through VPN Server Wizard.

View more detailed configuration Click this radio button to access **VPN and Remote Access>>LAN to LAN** for viewing detailed configuration.

3.9.2 VPN Server Wizard

Such wizard is used to configure VPN settings for VPN server. Such wizard will guide to set the LAN-to-LAN profile for VPN dial in connection (from client to server) step by step.

Choose VPN Establishment Environment

VPN Server Mode Selection:	Site to Site VPN (LAN-to-LAN) ▾
Please choose a LAN-to-LAN Profile:	[Index] [Status] [Name] ▾
Please choose a Dial-in User Accounts:	[Index] [Status] [Name] ▾
Allowed Dial-in Type:	<input type="checkbox"/> PPTP <input type="checkbox"/> IPSec <input type="checkbox"/> L2TP with IPSec Policy None ▾

< Back Next > Finish Cancel

VPN Server Mode Choose the direction for the VPN server.

Selection

Site to Site VPN/Remote Dial-in User – To set a LAN-to-LAN profile automatically, please choose Site to Site VPN.

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 VPN connection.



Please choose a LAN-to-LAN Profile

This item is available when you choose **Site to Site VPN (LAN-to-LAN)** as VPN server mode. There are 32 VPN profiles for users to set.

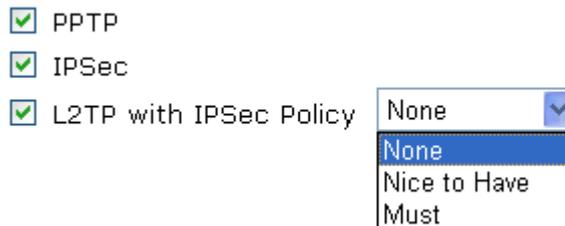
[Index]	[Status]	[Name]
1	x	???
2	x	???
3	x	???
4	x	???
5	x	???
6	x	???
7	x	???
8	x	???
9	x	???
10	x	???
11	x	???
12	x	???
13	x	???
14	x	???
15	x	???
16	x	???
17	x	???
18	x	???
19	x	???
20	x	???
21	x	???
22	x	???
23	x	???
24	x	???
25	x	???
26	x	???
27	x	???
28	x	???
29	x	???

Please choose a Dial-in User Accounts

This item is available when you choose Remote Dial-in User (Teleworker) as VPN server mode. There are 32 VPN tunnels for users to set.

Allowed Dial-in Type

This item is available after you choose any one of dial-in user account profiles. Next, you have to select suitable dial-in type for the VPN server profile. There are six types provided here (similar to VPN Client Wizard).



Different Dial-in Type will lead to different configuration

page.

After making the choices for the server profile, please click **Next**. You will see different configurations based on the selection you made.

- When you check **PPTP/IPSec/L2TP** (three types) or **PPTP/IPSec** (two types) or **L2TP with Policy (Nice to Have/Must)**, you will see the following graphic:

VPN and Remote Access >> VPN Server Wizard

VPN Authentication Setting

Profile Name	VPN-Ser1
PPTP / L2TP / L2TP over IPSec Authentication	
Username	server1
Password	●●●●●●
IPSec / L2TP over IPSec Authentication	
<input checked="" type="checkbox"/> Pre-Shared Key	
Confirm Pre-Shared Key	
<input checked="" type="checkbox"/> Digital Signature (X.509)	
Peer ID	None
Local ID	
<input checked="" type="radio"/> Alternative Subject Name First	
<input type="radio"/> Subject Name First	
Peer IP/VPN Client IP	192.168.1.99
Peer ID	
Site to Site Information	
Remote Network IP	0.0.0.0
Remote Network Mask	255.255.255.0

< Back Next > Finish Cancel

- When you check **PPTP/L2TP** (two types) or **PPTP** or **L2TP with Policy (None)**, you will see the following graphic:

VPN and Remote Access >> VPN Server Wizard

VPN Authentication Setting

Profile Name	VPN-Ser1
PPTP / L2TP / L2TP over IPSec Authentication	
Username	server1
Password	●●●●●●
Peer IP/VPN Client IP	
Site to Site Information	
Remote Network IP	0.0.0.0
Remote Network Mask	255.255.255.0

< Back Next > Finish Cancel

- When you check **IPSec**, you will see the following graphic:

VPN Authentication Setting

Profile Name	<input type="text" value="VPN-Ser1"/>
IPSec / L2TP over IPSec Authentication	
<input checked="" type="checkbox"/> Pre-Shared Key	<input type="text"/>
Confirm Pre-Shared Key	<input type="text"/>
<input type="checkbox"/> Digital Signature (X.509)	
Peer ID	<input type="text" value="None"/>
Local ID	
<input type="radio"/> Alternative Subject Name First	
<input type="radio"/> Subject Name First	
Peer IP/VPN Client IP	<input type="text"/>
Peer ID	<input type="text"/>
Site to Site Information	
Remote Network IP	<input type="text" value="0.0.0.0"/>
Remote Network Mask	<input type="text" value="255.255.255.0"/>

- Profile Name** Type a name for such profile. The length of the file is limited to 10 characters.
- User Name** This field is used to authenticate for connection when you select PPTP or L2TP with or without IPSec policy above.
- Password** This field is used to authenticate for connection when you select PPTP or L2TP with or without IPSec policy above.
- Pre-Shared Key** For IPSec/L2TP IPSec authentication, you have to type a pre-shared key.
- Confirm Pre-Shared Key** Type the pre-shared key again for confirmation.
- Digital Signature (X.509)** Check the box of Digital Signature to invoke this function.
Peer ID – Select one predefined in the X.509 Peer ID Profiles (set from **VPN and Remote Access>>IPSec Peer Identity**). If you choose **None**, it means that you will accept any peer regardless of its identity.
- Local ID** – Click **Alternative Subject Name First** to make a specific field of digital signature to accept the peer with matching value. The field can be IP Address, Domain, or E-mail Address. Or click **Subject Name First** to make a specific field 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). You have to configure one certificate at least previously in **Certificate Management >> Local Certificate**. Otherwise, the setting you choose here will not be effective.
- Peer IP/VPN Client IP** Type the WAN IP address or VPN client IP address for the remote client.
- Peer ID** Type the ID name for the remote client.

- Remote Network IP** Please type one LAN IP address (according to the real location of the remote host) for building VPN connection.
- Remote Network Mask** Please type the network mask (according to the real location of the remote host) for building VPN connection.

After finishing the configuration, please click **Next**. The confirmation page will be shown as follows. If there is no problem, you can click one of the radio buttons listed on the page and click **Finish** to execute the next action.

VPN and Remote Access >> VPN Server Wizard

Please Confirm Your Settings

VPN Environment:	Site to Site VPN (LAN-to-LAN)
Index:	3
Profile Name:	VPN-Ser1
Username:	server1
Allowed Service:	PPTP+IPSec
Peer IP/VPN Client IP:	
Peer ID:	
Remote Network IP:	0.0.0.0
Remote Network Mask:	255.255.255.0

Click **Back** to modify changes if necessary. Otherwise, click **Finish** to save the current settings and proceed to the following action:

- Go to the VPN Connection Management.
- Do another VPN Server Wizard setup.
- View more detailed configurations.

- Go to the VPN Connection Management** Click this radio button to access **VPN and Remote Access>>Connection Management** for viewing VPN Connection status.
- Do another VPN Server Wizard Setup** Click this radio button to set another profile of VPN Server through VPN Server Wizard.
- View more detailed configuration** Click this radio button to access **VPN and Remote Access>>LAN to LAN** for viewing detailed configuration.

3.9.3 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.

The Vigor router will not accept the ISDN dial-in connection if the box of **Enable ISDN Dial-in** is not checked.

3.9.4 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	
Dial-In PPP Authentication	<input type="text" value="PAP or CHAP"/>
Dial-In PPP Encryption (MPPE)	<input type="text" value="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	<input type="text" value="192.168.1.200"/>

Dial-In PPP Authentication PAP Only PAP or CHAP

Select this option to force the router to authenticate dial-in users with the PAP protocol.

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.

<input type="text" value="Optional MPPE"/>
<input type="text" value="Optional MPPE"/>
<input type="text" value="Require MPPE(40/128 bit)"/>
<input type="text" value="Maximum MPPE(128 bit)"/>

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.

Start IP Address

Enter a start 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.

3.9.5 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 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.

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 -When the client executes remote dial-in with IPSec mode, the router will transfer the certificate to the client based on the setting selected here. Please use the drop down list to choose one of the certificates configured in **Certificate Management>>Local Certificate**.

Pre-Shared Key- Currently only support Pre-Shared Key authentication. 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.

3.9.6 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.

X509 Peer ID Accounts: [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 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.

Profile Index : 1

Profile Name	<input type="text" value="one"/>
<input checked="" type="checkbox"/> Enable this account	
<input type="radio"/> Accept Any Peer ID	
<input checked="" type="radio"/> Accept Subject Alternative Name	
Type	IP Address <input type="button" value="v"/>
IP	<input type="text"/>
<input type="radio"/> Accept 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"/>

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)**.

3.9.7 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 (ISDN Dial-In connection, VPN connection - including PPTP, IPSec Tunnel, L2TP by itself or over IPSec, and SSL) corresponding security methods and available server(s) for SSL Web Proxy, etc.

The router provides **200** access accounts for dial-in users (10 SSL simultaneous tunnels can be established). 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.	???	×	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 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

<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 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 <input style="width: 50px;" type="text" value="None"/></p> <p><input checked="" type="checkbox"/> SSL Tunnel / Microsoft® SSTP</p> <p><input type="checkbox"/> Specify Remote Node</p> <p>Remote Client IP or Peer ISDN Number <input style="width: 100px;" type="text"/></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>Multicast via VPN <input type="radio"/> Pass <input checked="" type="radio"/> Block (for some IGMP,IP-Camera,DHCP Relay..etc.)</p> <p>SSL VPN</p> <p>Set SSL Web Proxy</p> <p>Set SSL Application</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 style="width: 50px;" type="text" value="None"/></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>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>

Enable this account

Check the box to enable this function.

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.

ISDN

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. 2

User account and Authentication

Enable this account

Idle Timeout: 300 second(s)

Allowed Dial-In Type

ISDN

PPTP

IPSec Tunnel

L2TP with IPSec Policy | None

SSL Tunnel → **SSL Tunnel**

Specify Remote Node
Remote Client IP or Peer ISDN Number

IKE Authentication Method

Pre-Shared Key

IKE Pre-Shared Key: [text box]

Digital Signature (X.509)

None

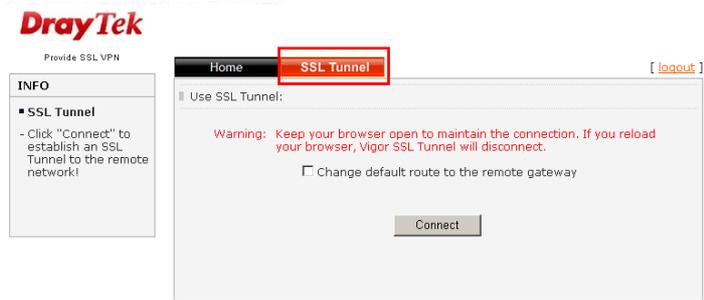
IPSec Security Method

Medium (AH)

High (ESP)

DES 3DES AES

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.

Multicast via VPN

Some programs might send multicast packets via VPN connection.

Pass – Click this button to let multicast packets pass through the router.

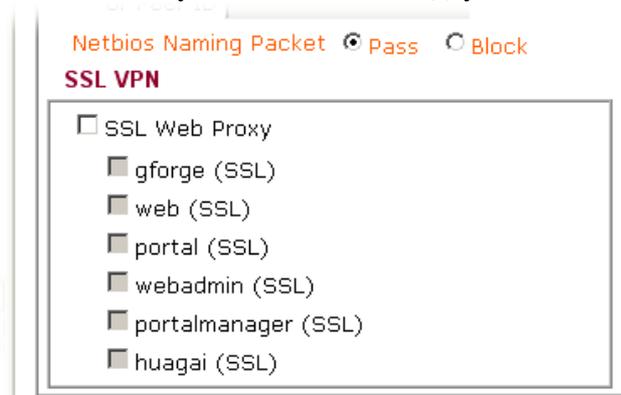
Block – This is default setting. Click this button to let multicast packets be blocked by the router.

SSL VPN

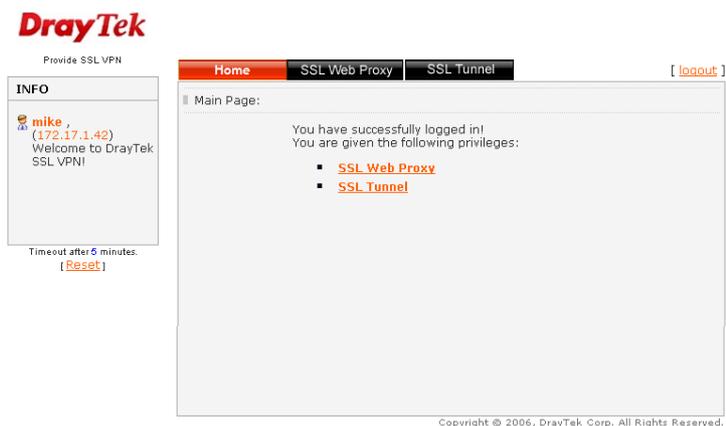
Set SSL Web Proxy - It allows the remote dial-in user to access internal web over SSL VPN, suitable for the application through web only (e.g., HTTP). Click **SSL**

VPN>> **SSL Web Proxy** to set profiles.

If you 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.



Set SSL Web Proxy – If you haven't set any SSL VPN web proxy profiles, you will 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.

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.

3.9.8 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 (ISDN connection, 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.

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 Connection Through: <input type="text" value="WAN1 First"/> Netbios Naming Packet <input checked="" type="radio"/> Pass <input type="radio"/> Block Multicast via VPN <input type="radio"/> Pass <input checked="" type="radio"/> Block (for some IGMP,IP-Camera,DHCP Relay..etc.)	

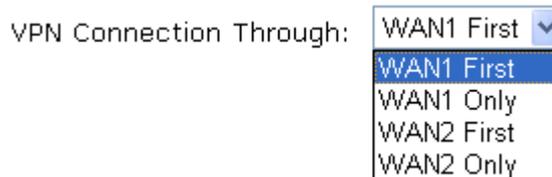
2. Dial-Out Settings

<p>Type of Server I am calling</p> <input checked="" type="radio"/> ISDN <input 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="???"/> 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 IKE Pre-Shared Key <input type="text"/> <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.



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.

Multicast via VPN

Some programs might send multicast packets via VPN connection.

Pass – Click this button to let multicast packets pass through the router.

Block – This is default setting. Click this button to let multicast packets be blocked by the router.

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 ...

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.

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 set to **Yes** to improve bandwidth utilization.

IKE Authentication Method

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.

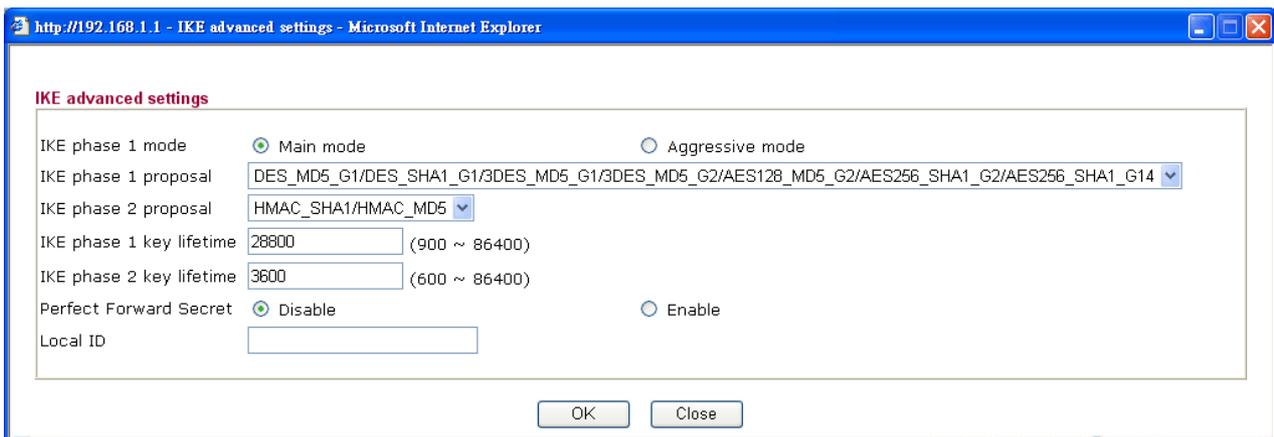
3DES with Authentication-Use triple DES encryption algorithm and apply MD5 or SHA-1 authentication algorithm.

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.

```

DES_MD5_G1
DES_SHA1_G1
3DES_MD5_G1
3DES_SHA1_G1
AES128_MD5_G1
AES128_SHA1_G1
AES192_MD5_G1
AES192_SHA1_G1
AES256_MD5_G1
AES256_SHA1_G1
DES_MD5_G2
DES_SHA1_G2
3DES_MD5_G2
3DES_SHA1_G2
AES128_MD5_G2
AES128_SHA1_G2
AES192_MD5_G2
AES192_SHA1_G2
AES256_MD5_G2
AES256_SHA1_G2
DES_MD5_G14
DES_SHA1_G14
3DES_MD5_G14
3DES_SHA1_G14
AES128_MD5_G14
AES128_SHA1_G14
AES192_MD5_G14
AES192_SHA1_G14
AES256_MD5_G14
AES256_SHA1_G14
AES256_SHA1_G14

```

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.

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.

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

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 None		Username <input type="text" value="???"/> Password <input type="text"/> VJ Compression <input checked="" type="radio"/> On <input type="radio"/> Off
<input type="checkbox"/> Specify ISDN CLID or Remote VPN Gateway Peer ISDN Number or Peer VPN Server IP <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) Peer ID None Local ID <input checked="" type="radio"/> Alternative Subject Name First <input type="radio"/> Subject Name First
		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)

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 type="text"/> Peer GRE IP <input type="text"/>

5. TCP/IP Network Settings

My WAN IP <input type="text" value="0.0.0.0"/>	RIP Direction Disable
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="0.0.0.0"/>	<input type="button" value="Route"/>
Remote Network Mask <input type="text" value="255.255.255.0"/>	<input type="checkbox"/> Change default route to this VPN tunnel (Only single WAN supports this)
<input type="button" value="More"/>	

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 - 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.

Specify CLID or Remote VPN Gateway - 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* model only.). Also, you should further specify the corresponding security methods on the right side.

If you uncheck the checkbox, the connection type you select above will apply the authentication methods and security methods in the general settings.

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> <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.</p>
Callback Function (CPCB)	<p>The callback function provides a callback service only for the ISDN LAN-to-LAN connection (this feature is useful for <i>i</i> model only). The remote user will be charged the connection fee by the telecom.</p> <p>Enable Callback function-Enables the callback function.</p>

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. Please 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.

TCP/IP Network Settings

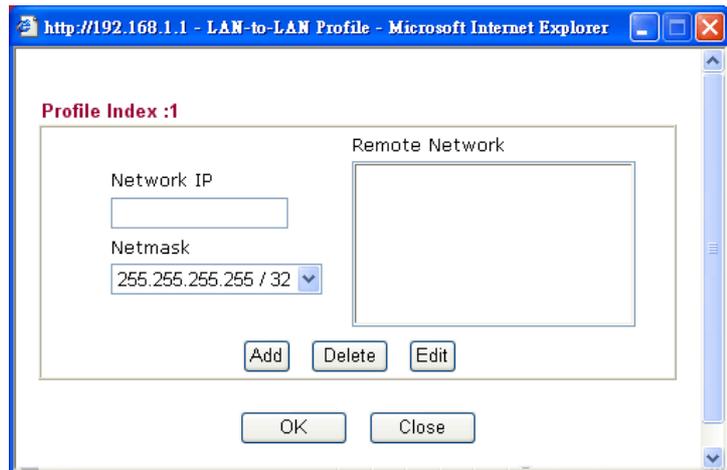
My WAN IP - This field is only applicable when you select ISDN, PPTP or L2TP with or without IPsec policy above. The default value is 0.0.0.0, which means the Vigor router will get a PPP IP address from the remote router during the IPCP negotiation phase. If the PPP IP address is fixed by remote side, 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 - 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.

3.9.9 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 Sit 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.

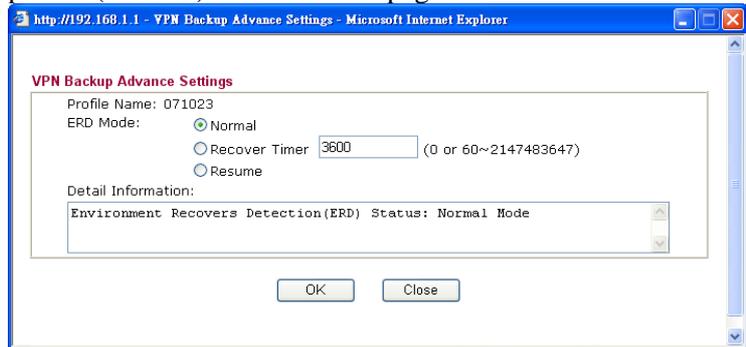
Member1 (on Backup Profile field) - Display the dial-out profile selected from the Member1 drop down list below.

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.

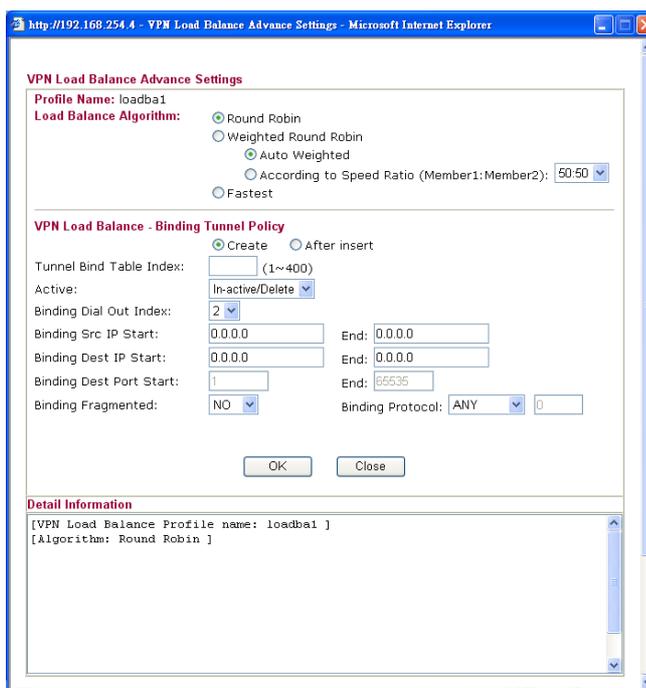
Member1 - Display the dial-out profile selected from the Member1 drop down list below.

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: 071023

Member1: Please choose the combination that you want.

Member2: Please choose the combination that you want.

Attribute Mode

No.	<Name>	<Connection-Type>	<VPN ServerIP(Private Network)>
1	To-A PlaceIPSec		192.168.2.25(20.20.20.0)
2	To-B Site IPsec		192.168.2.26(20.20.21.0)

Add Edit Delete

4. 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	▼
5	???	▼

How can you set a GRE over IPSec profile?

1. Please go to LAN to LAN to set a profile with IPSec.
2. 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.

Callback Budget minute(s)

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)

More

OK Clear Cancel

3. 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.

Callback Budget minute(s)

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)

More

OK Clear Cancel

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

VPN Load Balance Advance Settings

Profile Name: loadba1

Load Balance Algorithm:

- Round Robin
- Weighted Round Robin
- Auto Weighted
- According to Speed Ratio (Member1:Member2): 50:50
- Fastest

VPN Load Balance - Binding Tunnel Policy

Create After insert

Tunnel Bind Table Index: (1~400)

Active:

Binding Dial Out Index:

Binding Src IP Start: End:

Binding Dest IP Start: End:

Binding Dest Port Start: End:

Binding Fragmented: Binding Protocol:

OK Close

Detail Information

[VPN Load Balance Profile name: loadba1]
[Algorithm: Round Robin]

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 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.

VPN Load Balance – Binding Tunnel Policy

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:

VPN Load Balance - Binding Tunnel Policy

Create After insert

Tunnel Bind Table Index: (1~400)

Active:

Binding Dial Out Index:

Binding Src IP Start: End:

Binding Dest IP Start: End:

Binding Dest Port Start: End:

Binding Fragmented: Binding Protocol:

Finish setting up!

OK Close

Detail Information

[VPN Load Balance Profile name: VpnLB1]
[Algorithm: Fastest]

No.1 ---> Tunnel Bind Table Idnex :2

Binding Dial Out Index = 1
Binding protocol = TCP Protocol 6
Binding Src IP = 192.168.10.24 ~ 192.168.10.24
Binding Dest IP = 192.168.1.20 ~ 192.168.1.20
Binding Dest Port = 20 ~ 21
Binding Fragmented = NO

Note : To configure a successful binding tunnel, you have to:

- Type Binding Src IP range (Start and End) and Binding Dest 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 Dest 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

http://192.168.1.1 - VPN Backup Advance Settings - Microsoft Internet Explorer

VPN Backup Advance Settings

Profile Name: 071023

ERD Mode: Normal
 Recover Timer (0 or 60~2147483647)
 Resume

Detail Information:
Environment Recovers Detection(ERD) Status: Normal Mode

OK Close

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.

3.9.10 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. After adding a new VPN TRUNK profile, it will be listed in Backup/Load Balance Mode drop-down list for you to choose for dialing.

[VPN and Remote Access >> Connection Management](#)

Dial-out Tool Refresh Seconds : 10 Refresh

General Mode: (Alfa) 192.168.0.26 Dial

Backup Mode: (VpnBackup) 192.168.2.103 Dial

Load Balance Mode: (LoadBalance) 192.168.2.104 Dial

VPN Connection Status

Current Page: 1

Page No. Go >>

VPN	Type	Remote IP	Virtual Network	Tx Pkts	Tx Rate	Rx Pkts	Rx Rate	UpTime
-----	------	-----------	-----------------	---------	---------	---------	---------	--------

General Mode

This filed displays the profile configured in LAN-to-LAN (with Index number and VPN Server IP address). The VPN connection built by General Mode does not support VPN backup function.

Refresh Seconds :

General Mode: (Alfa) 192.168.0.26 Dial

Backup Mode: (Alfa) 192.168.0.26 Dial

Load Balance Mode: Bentley) 192.168.0.27 Dial

Audi) 192.168.0.28

BMW) 192.168.0.29

Buick) 192.168.0.30

Cadillac) 192.168.0.31

Chrysler) 192.168.0.32

Citroen) 192.168.0.33

Daihatsu) 192.168.0.34

Ferrari) 192.168.0.35

Fiat) 192.168.0.36

Page No. | Rx Pkts Rx Rate | : Data is er | : Data isn't

Backup Mode

This filed displays the profile name saved in VPN TRUNK Management (with Index number and VPN Server IP address). The VPN connection built by Backup Mode supports VPN backup function.

General Mode: (Alfa) 192.168.0.26 Dial

Backup Mode: (VpnBackup) 192.168.2.103 Dial

Load Balance Mode: (VpnBackup) 192.168.2.103 Dial

(VpnBackup) 192.168.2.203

Load Balance Mode

This filed displays the profile name saved in VPN TRUNK Management (with Index number and VPN Server IP address). The VPN connection built by Load Balance Mode supports

VPN Load Balance function.

General Mode:	(Alfa) 192.168.0.26	Dial
Backup Mode:	(VpnBackup) 192.168.2.103	Dial
Load Balance Mode:	(VpnLB1) 192.168.2.104	Dial
	(VpnLB1) 192.168.2.104	
	(VpnLB1) 192.168.2.204	

- Dial** Click this button to execute dial out function under 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.

3.10 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.



3.10.1 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	
---	---	---	View	Delete
---	---	---	View	Delete
---	---	---	View	Delete

GENERATE IMPORT REFRESH

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.

Certificate Management >> Local Certificate

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” can be configured with router’s WAN IP or domain name.

After clicking **GENERATE**, the generated information will be displayed on the window below:

Certificate Management >> Local Certificate

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.

[Certificate Management >> Local Certificate](#)

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”.

Import X509 Local Certificate

Congratulation!
Local Certificate has been imported successfully.
Please click to view the certificate.

X509 Local Certificate Configuration

Name	Subject	Status	Modify	
draytekdemo	/O=Draytek/OU=Draytek Sales/...	OK	<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"/>

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

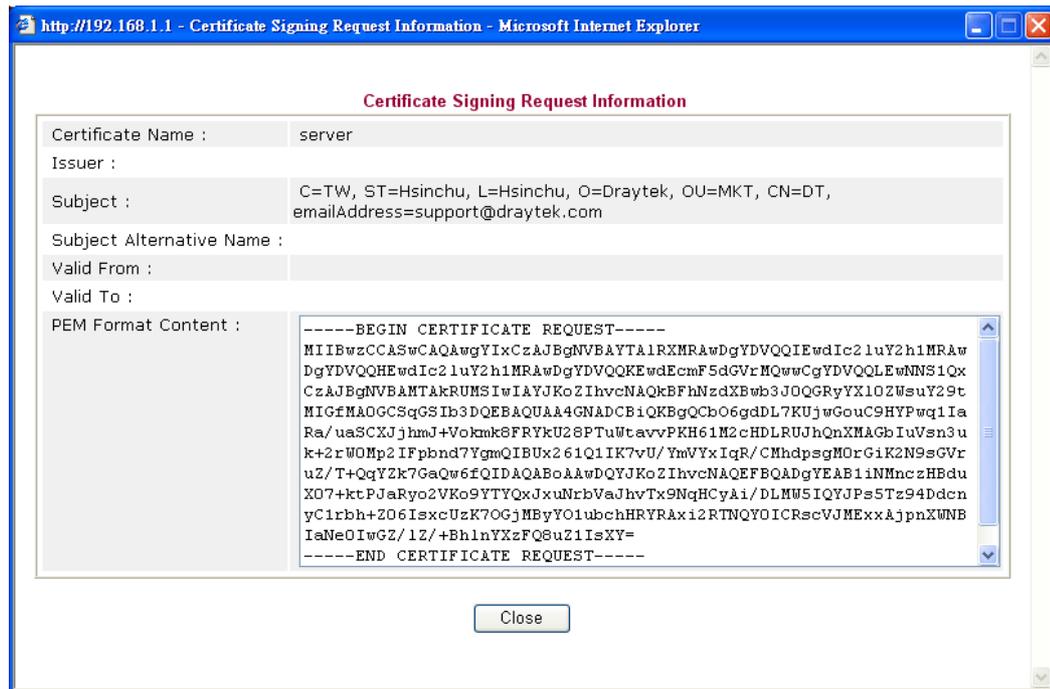
It is useful when users have separated certificates and private keys. And the password is needed if the private key is encrypted.

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.

3.10.2 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	---	---	View	Delete
Trusted CA-2	---	---	View	Delete
Trusted CA-3	---	---	View	Delete

[IMPORT](#)

[REFRESH](#)

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.



3.10.3 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: <input type="text"/>
Retype password: <input type="text"/>
Click <input type="button" value="Backup"/> to download certificates to your local PC as a file.
Restoration
Select a backup file to restore.
<input type="text"/> <input type="button" value="Browse.."/>
Decrypt password: <input type="text"/>
Click <input type="button" value="Restore"/> to upload the file.

3.11 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.



3.11.1 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.

3.11.2 SSL Web Proxy

SSL Web Proxy will allow the remote users to access the internal web sites over SSL.

SSL VPN >> 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

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 filed to set detailed configuration.

Profile Index : 1

Name	<input type="text"/>
URL	<input type="text"/>
Host IP Address	<input type="text"/>
Access Method	<div style="border: 1px solid black; padding: 2px;"> Disable ▾ <ul style="list-style-type: none"> Disable Secured Port Redirection SSL </div>

Note: URL format must be **http://ip:port/directory**.

- 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.

3.11.3 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 Applications Profiles: | [Set to Factory Default](#) |

Index	Name	Host Address	Service	Active
<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

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 filed to make detailed configuration.

SSL VPN >> SSL Application

Profile Index : 1

<input checked="" type="checkbox"/> Enable Application Service
Application Name <input type="text"/>
Application <input type="text" value="---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.

<input type="text" value="---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.

SSL VPN >> SSL Application

Profile Index : 1

<input type="checkbox"/> Enable Application Service
Application Name <input type="text"/>
Application <input type="text" value="Virtual Network Computing (VNC)"/>
IP Address <input type="text"/>
Port <input type="text" value="5900"/>
Scaling <input type="text" value="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 ▼

1024*768
800*600
640*480

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.

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.

3.11.4 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**.

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](#) >>

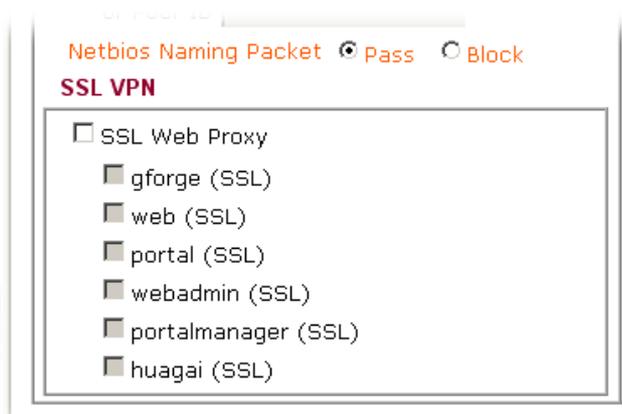
You can find out the link of Set SSL Web Proxy on the profile setting page. If you haven't set any SSL Web Proxy Profile in **SSL VPN>> SSL Web Proxy** web page, there is no check box but a link appeared below.

However, if you have set several SSL Web Proxy Profiles in **SSL VPN>> SSL Web Proxy** web page:

SSL Web Proxy Servers Profiles: | [Set to Factory Default](#) |

Index	Name	URL	Active
1.	gforge	http://swm.draytek.com	v
2.	web	http://www.draytek.com.cn	v
3.	portal	http://www.vigorpro.com	v
4.	webadmin	http://www.draytek.com.cn/admin	v
5.	portalmanager	http://www.vigorpro.com/manager	v
6.	huagai	http://www.huagai.com.cn	v
7.			x
8.			x
9.			x
10.			x

The SSL Web Proxy profile names will be displayed (together with check box) as shown below.



3.11.5 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.



Copyright © 2006, DrayTek Corp. All Rights Reserved.

Next, users can open **SSL VPN>> Online Status** to view logging status of SSL VPN.

SSL VPN >> Online Status

Refresh Seconds :

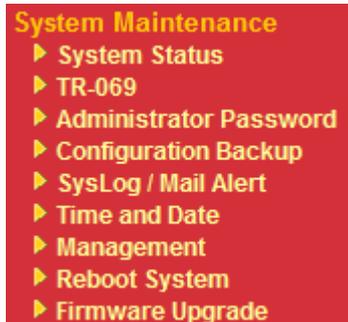
Active User	Host IP	Time out(seconds)	Action
caesar	172.17.1.42	292	<input type="button" value="Drop"/>

- Active User** Display current user who visit SSL VPN server.
- Host IP** Display 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.

3.12 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.



3.12.1 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 2009-10-1 05:35:26 last time, from 192.168.1.10.	
Model Name	: Vigor2950 Series		
Firmware Version	: v3.2.5_RC3		
Build Date/Time	: Wed Sep 16 11:32:14.5 2009		
System		WAN 1	
CPU Usage	: 3 %	Link Status	: Disconnected
Total Memory	: 64M	MAC Address	: 00-50-7F-C0-2F-F5
Memory usage	: 72 %	Connection	: DHCP Client
LAN		IP Address	: ---
MAC Address	: 00-50-7F-C0-2F-F4	Default Gateway	: ---
1st IP Address	: 192.168.1.1	Primary DNS	:
1st Subnet Mask	: 255.255.255.0	Secondary DNS	:
DHCP Server	: Yes	WAN 2	
Primary DNS	:	Link Status	: Connected
Secondary DNS	:	MAC Address	: 00-50-7F-C0-2F-F6
		Connection	: DHCP Client
		IP Address	: 192.168.5.31
		Default Gateway	: 192.168.5.1
		Primary DNS	: 168.95.1.1
		Secondary DNS	:

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.

3.12.2 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.

[System Maintenance >> TR-069 Setting](#)

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://192.168.5.31:8069/cwm/CRN.html"/>
Port	<input type="text" value="8069"/>
Username	<input type="text" value="vigor"/>
Password	<input type="password" value="password"/>

Periodic Inform Settings

<input type="radio"/> Disable	<input checked="" 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.

3.12.3 Administrator Password

This page allows you to set new password.

[System Maintenance >> Administrator Password Setup](#)

Administrator Password

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

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

New Password Type in new password in this field.

Confirm New Password Type in the new password again.

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

3.12.4 Configuration Backup

Backup the Configuration

Follow the steps below to backup your configuration.

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

[System Maintenance >> Configuration Backup](#)

Configuration Backup / Restoration

Restoration

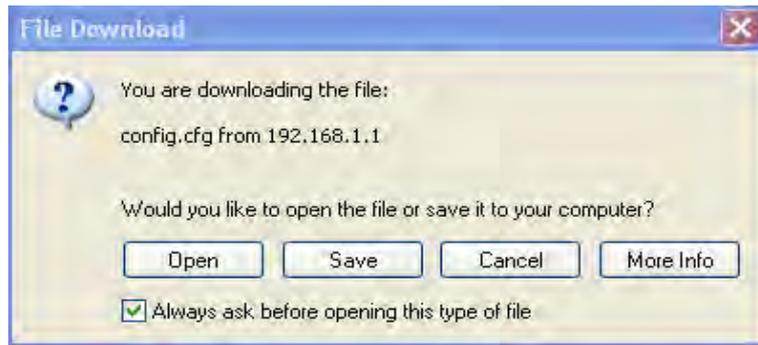
Select a configuration file.

Click Restore to upload the file.

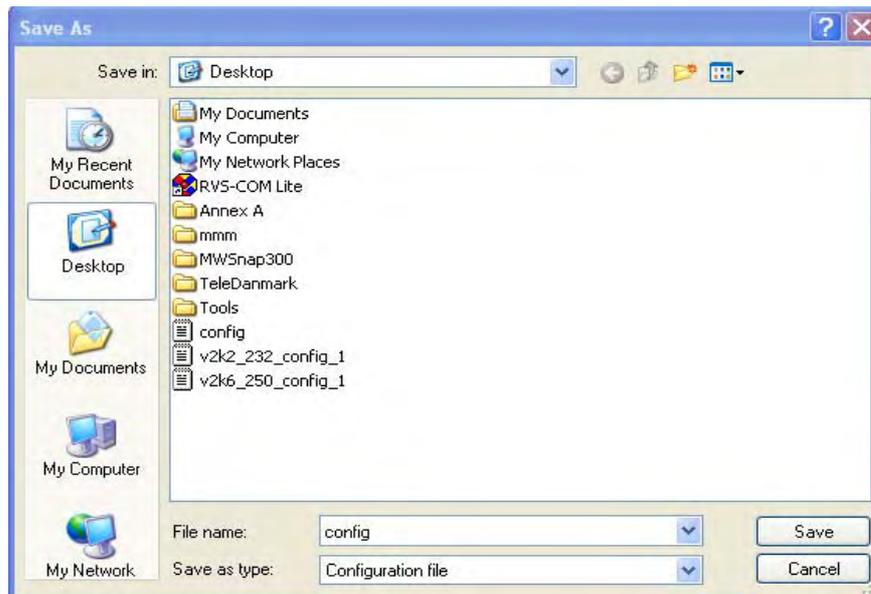
Backup

Click Backup to download current running configurations as a file.

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



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



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

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

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

Restore Configuration

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

System Maintenance >> Configuration Backup

Configuration Backup / Restoration

Restoration

Select a configuration file.

Click Restore to upload the file.

Backup

Click Backup to download current running configurations as a file.

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

3.12.5 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.

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" value="2950"/></p> <p>Server IP Address <input type="text" value="192.168.1.10"/></p> <p>Destination Port <input type="text" value="514"/></p> <p>Enable syslog message:</p> <p><input checked="" type="checkbox"/> Firewall Log</p> <p><input checked="" type="checkbox"/> VPN Log</p> <p><input checked="" type="checkbox"/> User Access Log</p> <p><input checked="" type="checkbox"/> Call Log</p> <p><input checked="" type="checkbox"/> WAN Log</p> <p><input checked="" type="checkbox"/> Router/DSL information</p>	<p>Mail Alert Setup</p> <p><input type="checkbox"/> Enable</p> <p>SMTP Server <input type="text"/></p> <p>Mail To <input type="text"/></p> <p>Return-Path <input type="text"/></p> <p><input type="checkbox"/> Authentication</p> <p>User Name <input type="text"/></p> <p>Password <input type="text"/></p>
---	---

Enable

Click “**Enable**” to activate this function.

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.

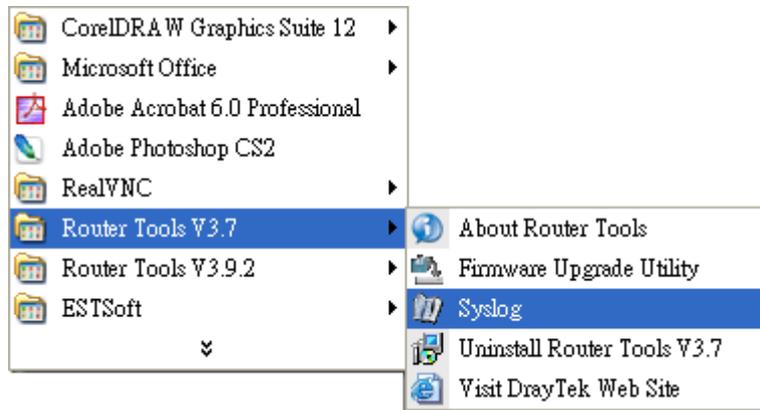
SMTP Server

The IP address of the SMTP server.

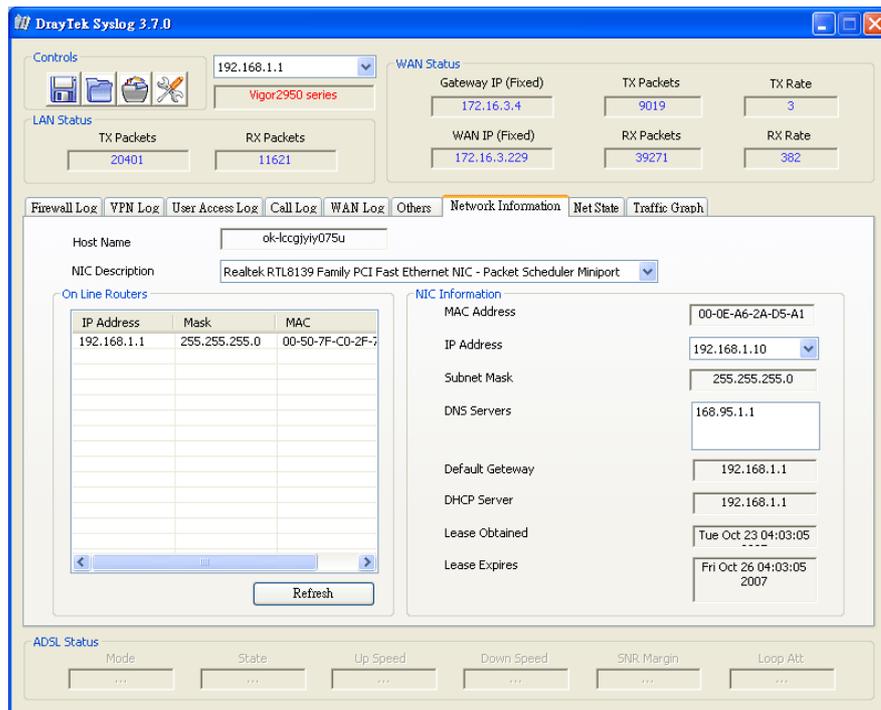
- Mail To** Assign a mail address for sending mails out.
- Return-Path** Assign a path for receiving the mail from outside.
- Authentication** Check this box to activate this function while using e-mail application.
- User Name** Type the user name for authentication.
- Password** Type the password for authentication.
- Click **OK** to save these settings.

For viewing the Syslog, please do the following:

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



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



3.12.6 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 Jun 12 Mon 8 : 45 : 0	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.

Enable Daylight Saving

Such feature is available only for certain area.

Automatically Update Interval

Select a time interval for updating from the NTP server.

Click **OK** to save these settings.

3.12.7 Management

This page allows you to manage the settings for access control, access list, port setup, and SMP setup. For example, as to management access control, the port number is used to send/receive SIP message for building a session. 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> <ul style="list-style-type: none"> <input type="checkbox"/> FTP Server <input checked="" type="checkbox"/> HTTP Server <input checked="" type="checkbox"/> HTTPS Server <input checked="" type="checkbox"/> Telnet Server <input type="checkbox"/> SSH Server <p><input checked="" type="checkbox"/> Disable PING from the Internet</p> <hr/> <p>Access List</p> <table style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="text-align: left;">List</th> <th style="text-align: left;">IP</th> <th style="text-align: left;">Subnet Mask</th> </tr> </thead> <tbody> <tr> <td>1</td> <td><input type="text"/></td> <td><input style="border-bottom: none; border-top: none; border-right: none; border-left: none; width: 100%;" type="text"/> ▼</td> </tr> <tr> <td>2</td> <td><input type="text"/></td> <td><input style="border-bottom: none; border-top: none; border-right: none; border-left: none; width: 100%;" type="text"/> ▼</td> </tr> <tr> <td>3</td> <td><input type="text"/></td> <td><input style="border-bottom: none; border-top: none; border-right: none; border-left: none; width: 100%;" type="text"/> ▼</td> </tr> </tbody> </table>	List	IP	Subnet Mask	1	<input type="text"/>	<input style="border-bottom: none; border-top: none; border-right: none; border-left: none; width: 100%;" type="text"/> ▼	2	<input type="text"/>	<input style="border-bottom: none; border-top: none; border-right: none; border-left: none; width: 100%;" type="text"/> ▼	3	<input type="text"/>	<input style="border-bottom: none; border-top: none; border-right: none; border-left: none; width: 100%;" type="text"/> ▼	<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> <p>SSH Port <input type="text" value="22"/> (Default: 22)</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> <hr/> <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: none; border-top: none; border-right: none; border-left: none; width: 100%;" type="text"/> ▼											
2	<input type="text"/>	<input style="border-bottom: none; border-top: none; border-right: none; border-left: none; width: 100%;" type="text"/> ▼											
3	<input type="text"/>	<input style="border-bottom: none; border-top: none; border-right: none; border-left: none; width: 100%;" type="text"/> ▼											

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.

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 Defined 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.

3.12.8 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

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

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

3.12.9 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](ftp://ftp.draytek.com).

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

System Maintenance >> Firmware Upgrade

Web Firmware Upgrade

Select a firmware file.

Click Upgrade to upload the file.

TFTP Firmware Upgrade from LAN

Current Firmware Version: v3.2.5_RC3

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

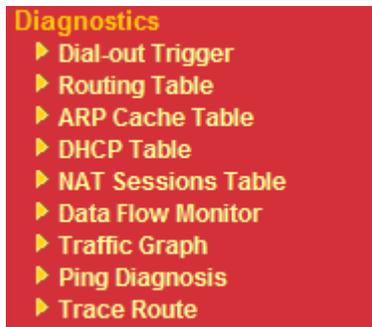
 TFTP server is running. Please execute a Firmware Upgrade Utility software to upgrade router's firmware. This server will be closed by itself when the firmware upgrading finished.

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

3.13 Diagnostics

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

Below shows the menu items for Diagnostics.



3.13.1 Dial-out Trigger

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

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

Dial-out Triggered Packet Header

| [Refresh](#) |

HEX Format:

```
00 50 7F 22 33 44-00 0E A6 2A D5 A1-08 00
```

```
45 00 00 4B BE 54 00 00-7F 11 12 3B C0 A8 01 0A  
A8 5F 01 01 05 CB 00 35-00 37 E3 91 01 74 01 00  
00 01 00 00 00 00 00-07 67 61 74 65 77 61 79  
09 6D 65 73 73 65 6E 67-65 72 07 68 6F 74 6D 61  
69 6C 03 63 6F 6D 00 00-01 00 01 E6 84 1A 00 00
```

Decoded Format:

```
192.168.1.10,1483 -> 168.95.1.1,domain  
Pr udp HLen 20 TLen 75
```

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.

3.13.2 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.

3.13.3 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
172.16.3.112	00-40-CA-6B-56-BA
172.16.3.132	00-05-5D-E4-ED-86
172.16.3.20	00-0D-60-6F-83-BC
172.16.3.121	00-0C-6E-E7-79-99
172.16.3.141	00-11-2F-C7-39-0B
172.16.3.133	00-50-7F-23-4D-B1
172.16.3.179	00-11-2F-4B-15-F2
172.16.3.21	00-05-5D-A1-2E-FF
172.16.3.2	00-11-D8-68-0D-AE
172.16.3.18	00-50-FC-2F-3D-17
172.16.3.151	00-50-7F-2F-33-FF
172.16.3.19	00-0D-60-6F-89-CA

Refresh

Click it to reload the page.

Clear

Click it to clear the whole table.

3.13.4 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](#)

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.

3.13.5 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
192.168.1.11 2491	52078	24.9.93.189 443	WAN1
192.168.1.11 2493	52080	207.46.25.2 80	WAN1
192.168.1.10 3079	52665	207.46.5.10 80	WAN1

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

Refresh Seconds

Use the drop down list to choose the time interval of refreshing data flow that will be done by the system automatically.

Refresh Seconds:

10
15
30

Refresh

Click this link to refresh this page manually.

Index

Display the number of the data flow.

IP Address

Display the IP address of the monitored device.

TX rate (kbps)

Display the transmission speed of the monitored device.

RX rate (kbps)

Display the receiving speed of the monitored device.

Sessions

Display the session number that you specified in Limit Session web page.

Action

Block - can prevent specified PC accessing into Internet within 5 minutes.

Page: | [Refresh](#) |

	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: | [Refresh](#) |

	Sessions	Action
	blocked / 299	Unblock

Current /Peak/Speed

Current means current transmission rate and receiving rate for WAN1/WAN.

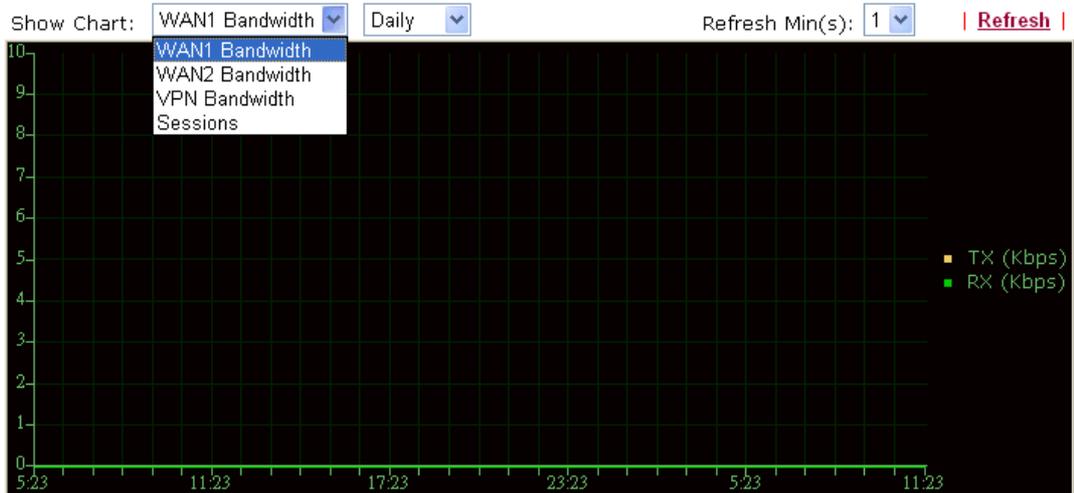
Peak means the highest peak value detected by the router in data transmission.

Speed means line speed specified in **WAN>>General**. If you do not specify any rate at that page, here will display **Auto** for instead.

3.13.7 Traffic Graph

Click **Diagnostics** and click **Traffic Graph** to pen the web page. Choose WAN1 Bandwidth/WAN2 Bandwidth, VPN 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



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.

3.13.8 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 ping through, please select "Unspecified".

Ping through:

Ping to: IP Address:

Result [Clear](#)

Host / IP
GateWay1
GateWay2
DNS

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

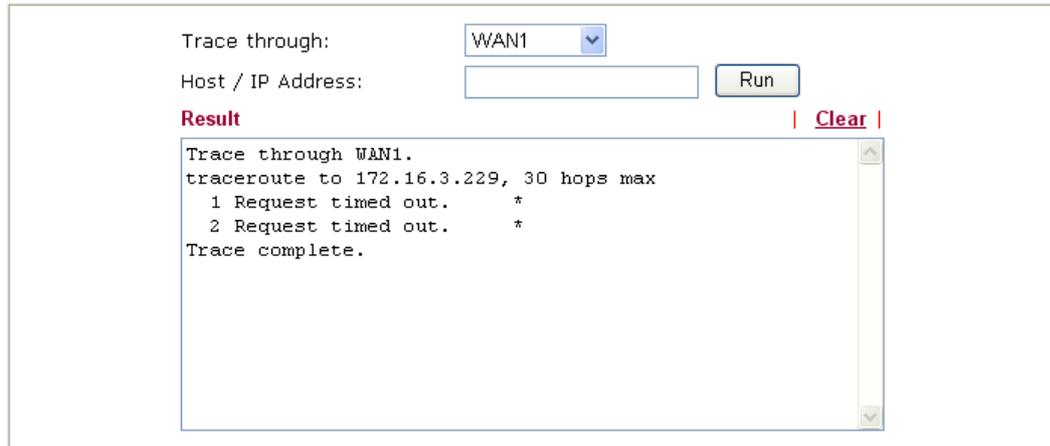
Click this link to remove the result on the window.

3.13.9 Trace Route

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

[Diagnostics >> Trace Route](#)

Trace Route

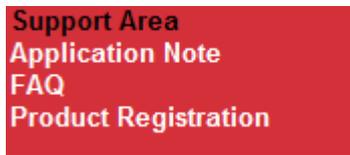


Trace through:
Host / IP Address:
Result | [Clear](#) |
Trace through WAN1.
traceroute to 172.16.3.229, 30 hops max
 1 Request timed out. *
 2 Request timed out. *
Trace complete.

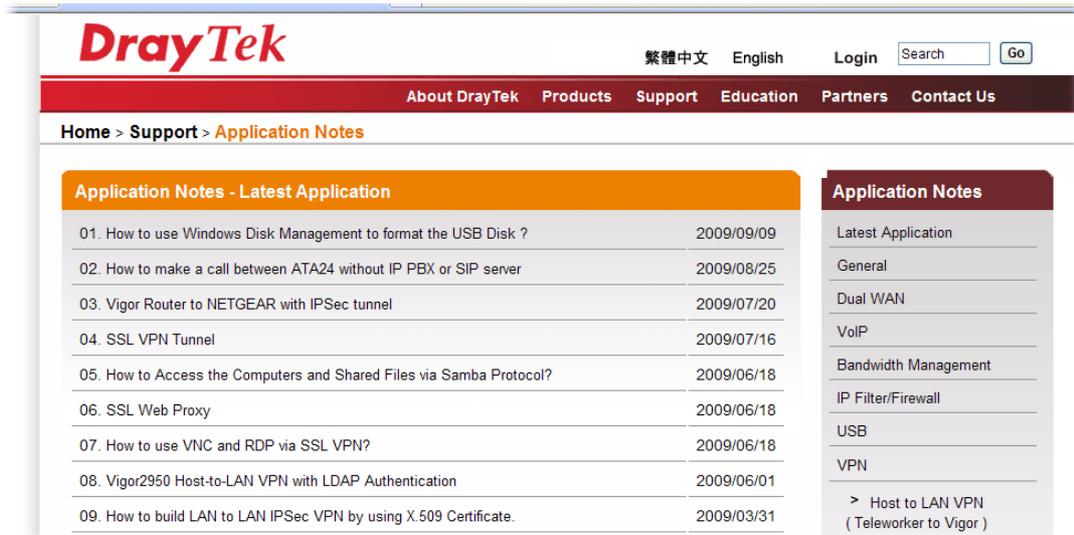
- Trace through** Use the drop down list to choose the WAN interface that you want to ping through or choose **Unspecified** to be determined by the router automatically.
- Host/IP Address** It indicates the IP address of the host.
- Run** Click this button to start route tracing work.
- Clear** Click this link to remove the result on the window.

3.14 Support Area

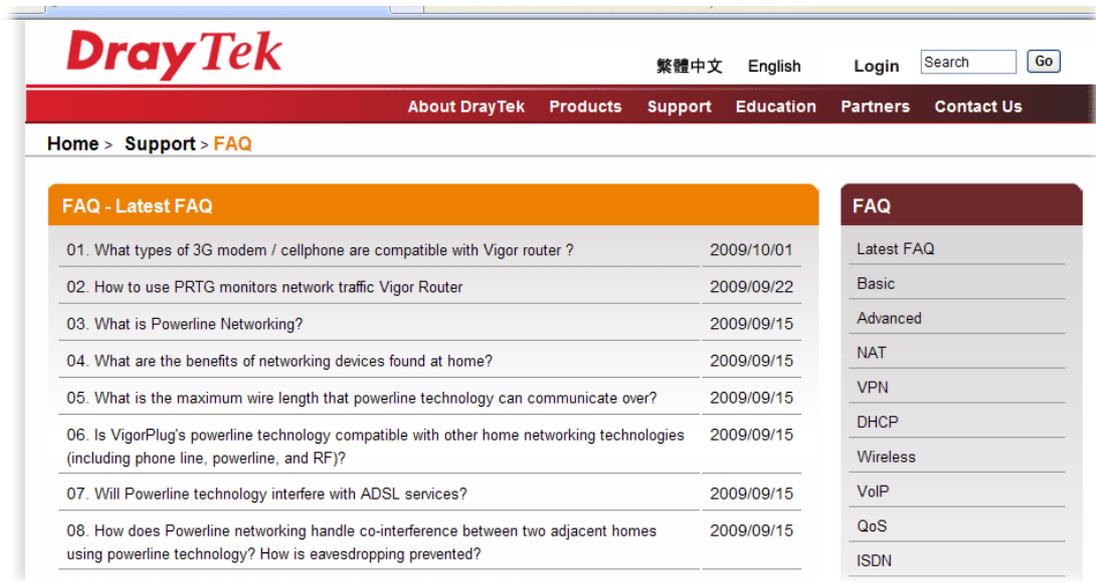
When you click the menu item under **Support Area**, you will be guided to visit www.draytek.com and open the corresponding pages directly.



Click **Support Area>>Application Note**, the following web page will be displayed.



Click **Support Area>>FAQ**, the following web page will be displayed.



Click **Support Area**>>**Product Registration**, the following web page will be displayed.

DrayTek English Login

[About DrayTek](#) [Products](#) [Support](#) [Education](#) [Partners](#) [Contact Us](#)

[Home](#) > [DrayTek Member](#)

DrayTek Member

Dear DrayTek new & existing users,

For enhancing the users' satisfaction level while utilizing our site and receiving even better service from DrayTek, we have designed this membership page. Please complete the membership registration and then register your product(s).

Already a DrayTek Member – Just sign-in below.
Want to become a DrayTek Member – Click "Create Account" and then fill out the membership form.
Forgot username or password – Click "Forgot Username / Password."

Benefits for DrayTek Members

- Receiving e-news letters about latest firmware version for your purchased products.
- Software and firmware available online for download.
- Chances to win prizes.

Many more benefits only for DrayTek members are coming soon.

[Sign up](#)

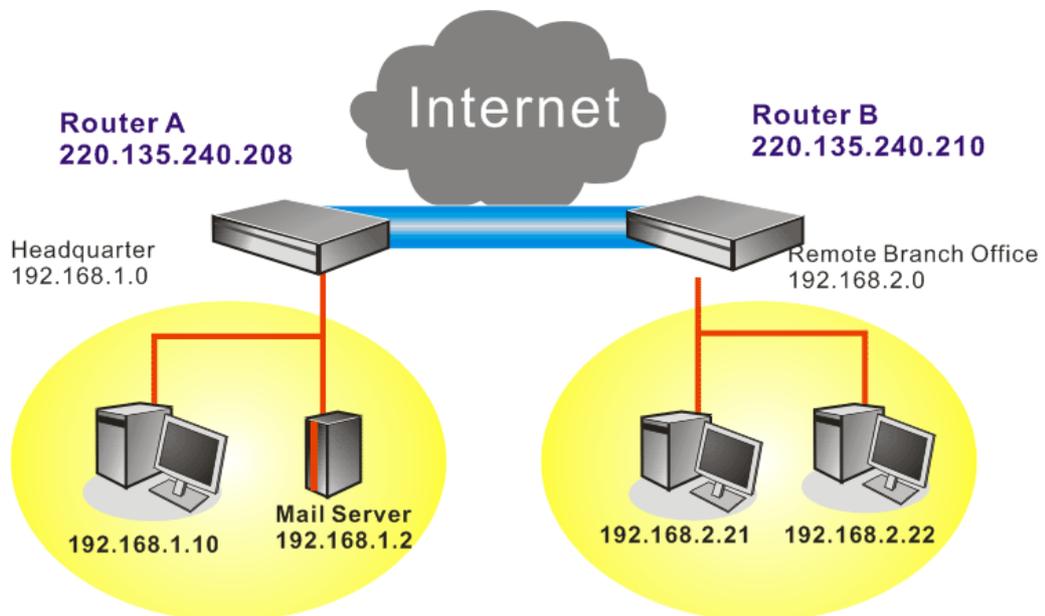
[Forgot Password](#)

4

Application and Examples

4.1 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	
Dial-In PPP Authentication	PAP or CHAP	Start IP Address	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	
Certificate for Dial-in	None
Pre-Shared Key	
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 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	
Multicast via VPN	<input type="radio"/> Pass <input checked="" type="radio"/> Block	PING to the IP	<input type="text"/>
(for some IGMP,IP-Camera,DHCP Relay..etc.)			

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.

Multicast via VPN Pass Block
(for some IGMP,IP-Camera,DHCP Relay..etc.)

2. Dial-Out Settings

Type of Server I am calling

ISDN
 PPTP
 IPsec Tunnel
 L2TP with IPsec Policy None

Dial Number for ISDN or
Server IP/Host Name for VPN.
(such as 5551234, draytek.com or 123.45.67.89)

Link Type 64k bps
Username
Password
PPP Authentication PAP/CHAP
VJ Compression On Off

IKE Authentication Method

Pre-Shared Key
IKE Pre-Shared Key
 Digital Signature(X.509)
Peer ID None
Local ID
 Alternative Subject Name First
 Subject Name First
Local Certificate None

IPsec Security Method

Medium(AH)
 High(ESP) DES without Authentication

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.

Multicast via VPN Pass Block
(for some IGMP,IP-Camera,DHCP Relay..etc.)

2. Dial-Out Settings

Type of Server I am calling

ISDN
 PPTP
 IPsec Tunnel
 L2TP with IPsec Policy None

Dial Number for ISDN or
Server IP/Host Name for VPN.
(such as 5551234, draytek.com or 123.45.67.89)

Link Type 64k bps
Username
Password
PPP Authentication PAP/CHAP
VJ Compression On Off

IKE Authentication Method

Pre-Shared Key
IKE Pre-Shared Key
 Digital Signature(X.509)
Peer ID None
Local ID
 Alternative Subject Name First
 Subject Name First
Local Certificate None

IPsec Security Method

Medium(AH)
 High(ESP) DES without Authentication

- 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> <p><input type="checkbox"/> ISDN <input type="checkbox"/> PPTP <input checked="" type="checkbox"/> IPSec Tunnel <input type="checkbox"/> L2TP with IPSec Policy None</p> <p><input checked="" type="checkbox"/> Specify ISDN CLID or Remote VPN Gateway Peer ISDN Number or Peer VPN Server IP <input type="text" value="220.135.240.210"/> or Peer ID <input type="text"/></p>	<p>Username <input type="text" value="???"/> Password <input type="password"/> VJ Compression <input checked="" type="radio"/> On <input type="radio"/> Off</p> <p>IKE Authentication Method</p> <p><input checked="" type="checkbox"/> Pre-Shared Key <input type="text" value="IKE Pre-Shared Key"/> <input type="text"/> <input type="checkbox"/> Digital Signature(X.509) Peer ID None Local ID <input checked="" type="radio"/> Alternative Subject Name First <input type="radio"/> Subject Name First</p> <p>IPSec Security Method</p> <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> <p>Callback Function (CBCP)</p> <p><input type="checkbox"/> Enable Callback Function <input type="checkbox"/> Use the Following Number to Callback</p>
---	---

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> <p><input type="checkbox"/> ISDN <input checked="" type="checkbox"/> PPTP <input type="checkbox"/> IPSec Tunnel <input type="checkbox"/> L2TP with IPSec Policy None</p> <p><input checked="" type="checkbox"/> Specify ISDN CLID or Remote VPN Gateway Peer ISDN Number or Peer VPN Server IP <input type="text" value="220.135.240.210"/> or Peer ID <input type="text"/></p>	<p>Username <input type="text" value="draytek"/> Password <input type="password" value="....."/> VJ Compression <input checked="" type="radio"/> On <input type="radio"/> Off</p> <p>IKE Authentication Method</p> <p><input checked="" type="checkbox"/> Pre-Shared Key <input type="text" value="IKE Pre-Shared Key"/> <input type="text"/> <input type="checkbox"/> Digital Signature(X.509) Peer ID None Local ID <input checked="" type="radio"/> Alternative Subject Name First <input type="radio"/> Subject Name First</p> <p>IPSec Security Method</p> <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> <p>Callback Function (CBCP)</p> <p><input type="checkbox"/> Enable Callback Function <input type="checkbox"/> Use the Following Number to Callback</p>
---	---

7. 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.

5. TCP/IP Network Settings

My WAN IP	<input type="text" value="0.0.0.0"/>	RIP Direction	<input type="text" value="Disable"/>
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="192.168.2.0"/>	<input type="text" value="Route"/>	
Remote Network Mask	<input type="text" value="255.255.255.0"/>	<input type="checkbox"/> Change default route to this VPN tunnel	
<input type="button" value="More"/>			

Settings in Router B in the remote 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	IP Address Assignment for Dial-In Users
Dial-In PPP Authentication	<input type="text" value="192.168.2.200"/>
Dial-In PPP Encryption (MPPE)	
Mutual Authentication (PAP)	
Username	
Password	

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	<input type="text" value="None"/>
Pre-Shared Key	
Pre-Shared Key	<input type="text" value="•••••"/>
Confirm Pre-Shared Key	<input type="text" 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.	

- 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

Profile Name <input type="text" value="Branch1"/> <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 Connection Through: <input type="text" value="WAN1 First"/> Netbios Naming Packet <input checked="" type="radio"/> Pass <input type="radio"/> Block Multicast via VPN <input type="radio"/> Pass <input checked="" type="radio"/> Block (for some IGMP,IP-Camera,DHCP Relay..etc.)	

- 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.

Multicast via VPN <input type="radio"/> Pass <input checked="" type="radio"/> Block (for some IGMP,IP-Camera,DHCP Relay..etc.)	
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 <input type="text" value="IKE Pre-Shared Key"/> <input type="text" value="•••••"/> <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"/>
	IPSec Security Method <input checked="" type="radio"/> Medium(AH) <input type="radio"/> High(ESP) <input type="text" value="DES without Authentication"/>

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.

Multicast via VPN Pass Block
(for some IGMP,IP-Camera,DHCP Relay..etc.)

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="password" 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="password" value="....."/> <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"/>
	IPSec Security Method <input checked="" type="radio"/> Medium(AH) <input type="radio"/> High(ESP) <input type="text" value="DES without Authentication"/>

- 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"/> Password <input type="password"/> VJ Compression <input checked="" type="radio"/> On <input type="radio"/> Off IKE Authentication Method <input checked="" type="checkbox"/> Pre-Shared Key IKE Pre-Shared Key <input type="password"/> <input type="checkbox"/> 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 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
--	--

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

ISDN
 PPTP
 IPsec Tunnel
 L2TP with IPsec Policy None

Specify ISDN CLID or Remote VPN Gateway
Peer ISDN Number or Peer VPN Server IP

or Peer ID

Username
Password
VJ Compression On Off

IKE Authentication Method

Pre-Shared Key
IKE Pre-Shared Key
 Digital Signature(X.509)
Peer ID None
Local ID
 Alternative Subject Name First
 Subject Name First

IPsec Security Method

Medium (AH)
High (ESP)
 DES 3DES AES

Callback Function (CBCP)

Enable Callback Function
 Use the Following Number to Callback

7. 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.

5. TCP/IP Network Settings

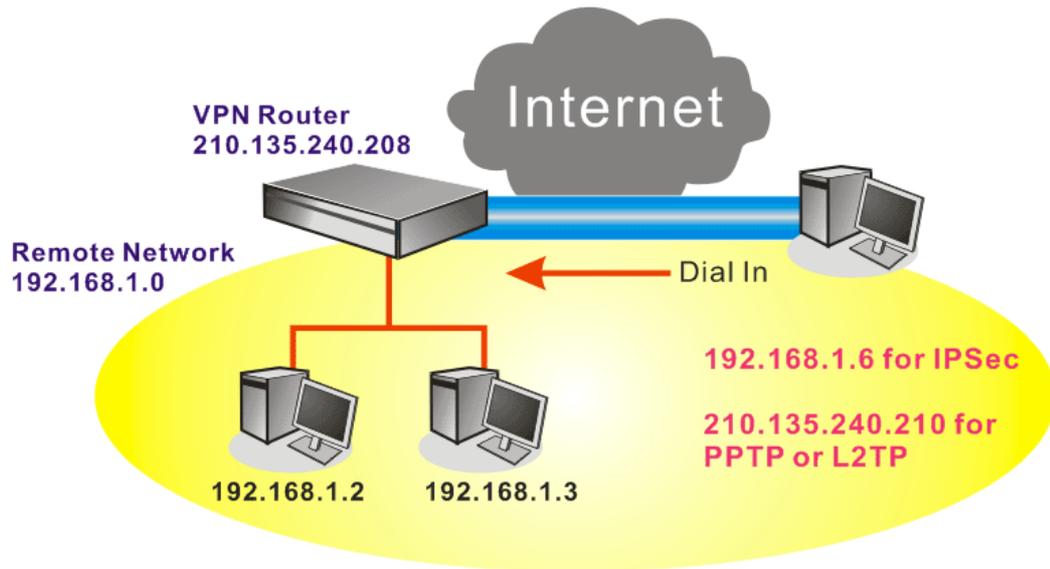
My WAN IP
Remote Gateway IP
Remote Network IP
Remote Network Mask

RIP Direction Disable
From first subnet to remote network, you have to do

Change default route to this VPN tunnel

4.2 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**.

PPP General Setup

PPP/MP Protocol		IP Address Assignment for Dial-In Users	
Dial-In PPP Authentication	<input type="text" value="PAP or CHAP"/>	Start IP Address	<input type="text" value="192.168.1.200"/>
Dial-In PPP Encryption (MPPE)	<input type="text" value="Optional MPPE"/>		
Mutual Authentication (PAP)	<input type="radio"/> Yes <input checked="" type="radio"/> No		
Username	<input type="text"/>		
Password	<input type="text"/>		

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

Certificate for Dial-in: None

Pre-Shared Key

Pre-Shared Key: [Masked]

Confirm Pre-Shared Key: [Masked]

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

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-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.

VPN and Remote Access >> Remote Dial-in User

Index No. 1

User account and Authentication

Enable this account

Idle Timeout: 300 second(s)

Allowed Dial-In Type

ISDN

PPTP

IPSec Tunnel

L2TP with IPsec Policy: None

SSL Tunnel / Microsoft® SSTP

Specify Remote Node

Remote Client IP or Peer ISDN Number: 210.135.240.210

or Peer ID: [Field]

Netbios Naming Packet: Pass Block

Multicast via VPN: Pass Block
(for some IGMP, IP-Camera, DHCP Relay..etc.)

Username: ???

Password: [Field]

IKE Authentication Method

Pre-Shared Key

IKE Pre-Shared Key: [Field]

Digital Signature (X.509)

None

IPSec Security Method

Medium (AH)

High (ESP)

DES 3DES AES

Local ID: [Field] (optional)

Callback Function

Check to enable Callback function

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.

Index No. 1

User account and Authentication

Enable this account
 Idle Timeout second(s)

Allowed Dial-In Type

ISDN
 PPTP
 IPsec Tunnel
 L2TP with IPsec Policy
 SSL Tunnel / Microsoft® SSTP

Specify Remote Node
 Remote Client IP or Peer ISDN Number

 or Peer ID

Netbios Naming Packet Pass Block
 Multicast via VPN Pass Block
 (for some IGMP, IP-Camera, DHCP Relay..etc.)

Username
 Password

IKE Authentication Method

Pre-Shared Key
 IKE Pre-Shared Key
 Digital Signature (X.509)

IPsec Security Method

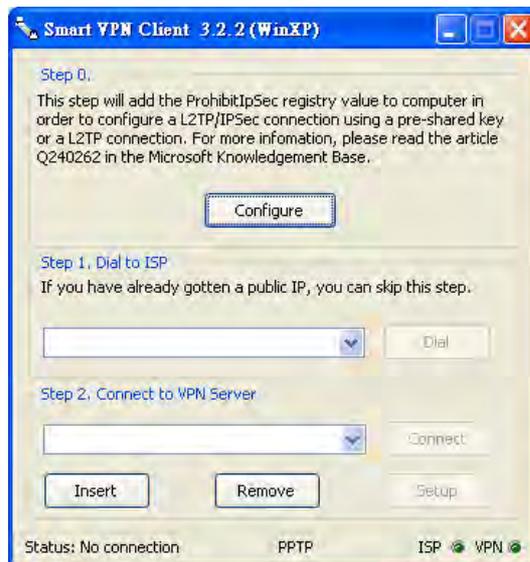
Medium (AH)
 High (ESP)
 DES 3DES AES
 Local ID (optional)

Callback Function

Check to enable Callback function

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.

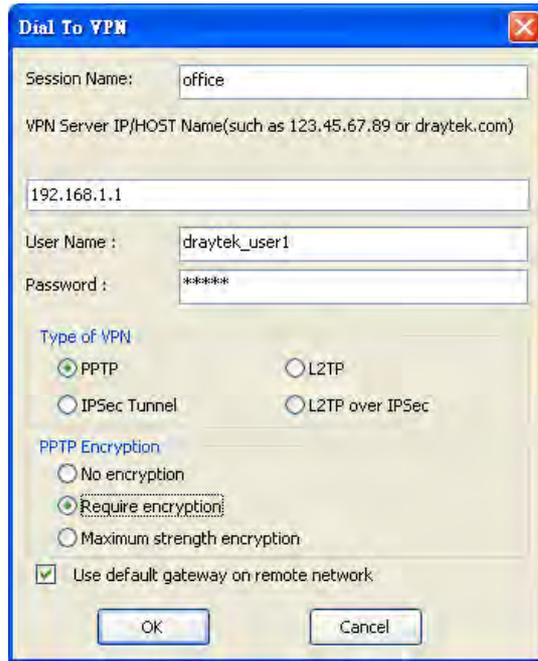
If an IPsec-based service is selected as shown below,



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.



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.



4. Click **Connect** button to build connection. When the connection is successful, you will find a green light on the right down corner.

4.3 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 VoIP or Skype in the restroom.

1. Make sure the QoS Control on the left corner is checked. And select **BOTH** in **Direction**.



2. Enter the Name of Index Class 1 by clicking **Edit** link. In this index, the user will set reserve bandwidth for Email using protocol POP3 and SMTP.

[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	
Class 2		Edit	Edit
Class 3		Edit	

- Enter the Name of Index Class 2 by clicking **Edit** link. In this index, the user will set reserve bandwidth for HTTPS. And click Basic button on the right.

[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	

- Click **Setup** link for WAN1. Check **Enable UDP Bandwidth Control** on the bottom to prevent enormous UDP traffic of VoIP influent other application.

[Bandwidth Management >> Quality of Service](#)

WAN1 General Setup

Enable the QoS Control BOTH

WAN Inbound Bandwidth Kbps

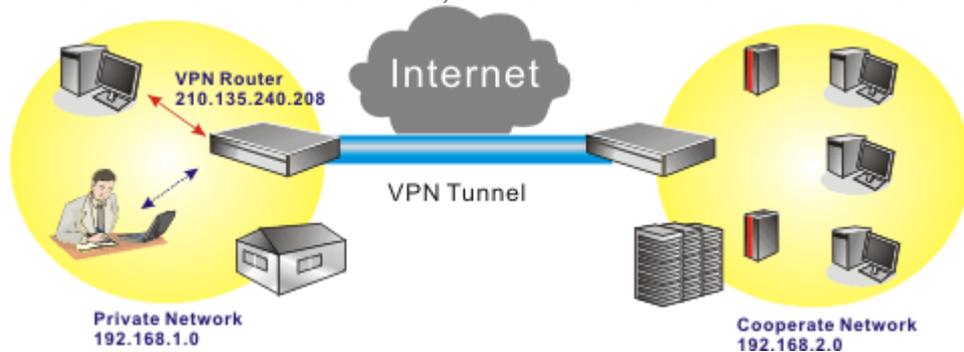
WAN Outbound Bandwidth Kbps

Index	Class Name	Reserved_bandwidth Ratio
Class 1	E-mail	<input type="text" value="25"/> %
Class 2	HTTP	<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 %

[Online Statistics](#)

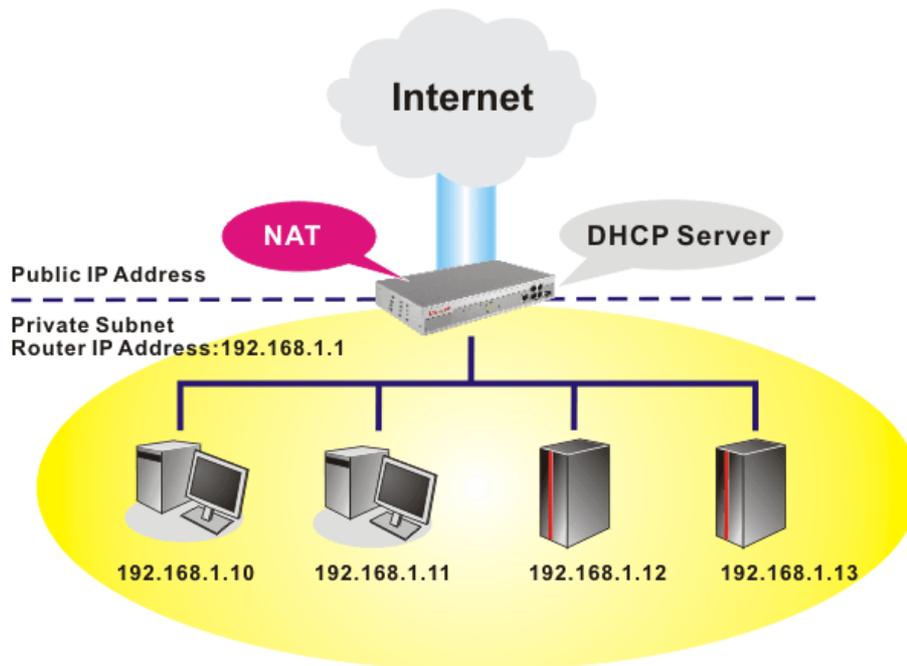
- If the worker has connected to the headquarter using host to host VPN tunnel. (Please refer to Chapter 3 VPN for detailed instruction), he may set up an index for it. Enter the Class Name of Index 3. In this index, he will set reserve bandwidth for 1 VPN tunnel.



- Click edit to open a new window. First, check the ACT box. Then click **SrcEdit** to set a worker's subnet address. Click **DestEdit** to set headquarter's subnet address. Leave other fields and click OK.

4.4 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.

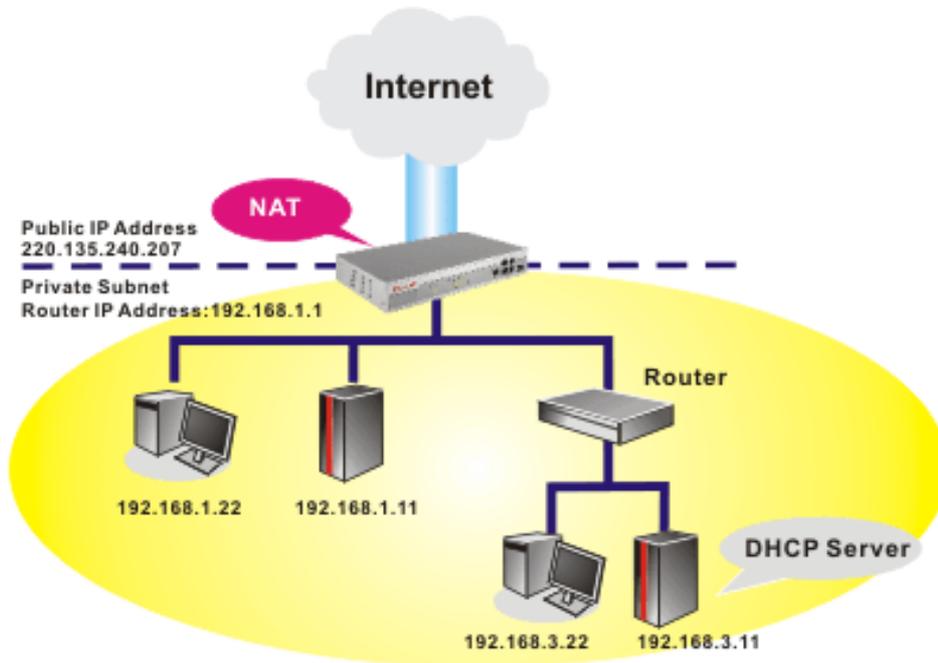


You can just set the settings wrapped inside the red rectangles to fit the request of NAT usage.

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"/>
<input type="button" value="2nd Subnet DHCP Server"/>	
RIP Protocol Control	<input type="text" value="Disable"/>
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"/>
Secondary IP Address	<input type="text"/>

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

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

OK

4.5 Upgrade Firmware for Your Router

Before upgrading your router firmware, you need to install the Router Tools. The file **RTSxxx.exe** will be asked to copy onto your computer. Remember the place of storing the execution file.

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.

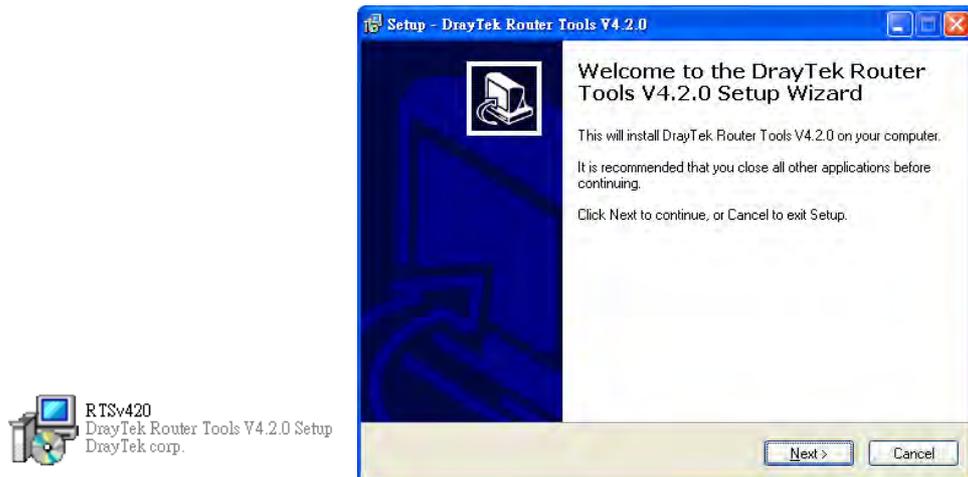
Model Name	Firmware Version	Release Date
Vigor120 series	3.2.2.1	26/06/2009
Vigor2100 series	2.6.2	26/02/2008
Vigor2104 series	2.5.7.3	13/02/2008
Vigor2110 series	3.3.0	25/06/2009
Vigor2200/X/W/E	2.3.11	22/09/2004
Vigor2200Eplus	2.5.7	18/02/2009
Vigor2200USB	2.3.10	16/03/2005

3. Access into **Support >> Downloads**. Please find out **Utility** menu and click it.

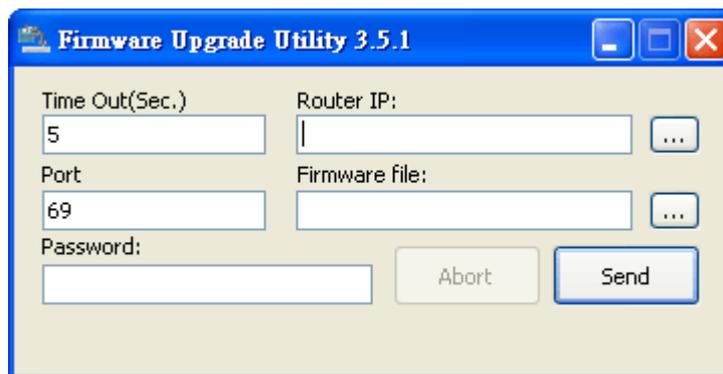
Tools Name	Release Date	Version	OS	Support Model
Router Tools	2009/06/18	4.2.0	MS-Windows	All Modules
Syslog Tools	2009/06/18	4.2.0	MS-Windows XP MS-Vista	All Modules
VigorPro Alert Notice Tools	2009/06/03	1.1.0 (Multi-language)	MS-Windows XP MS-Vista	VigorPro 100 series VigorPro 5500 series VigorPro 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 5510 series

4. Click on the link of **Router Tools** to download the file. After downloading the files, please decompressed the file onto your host.

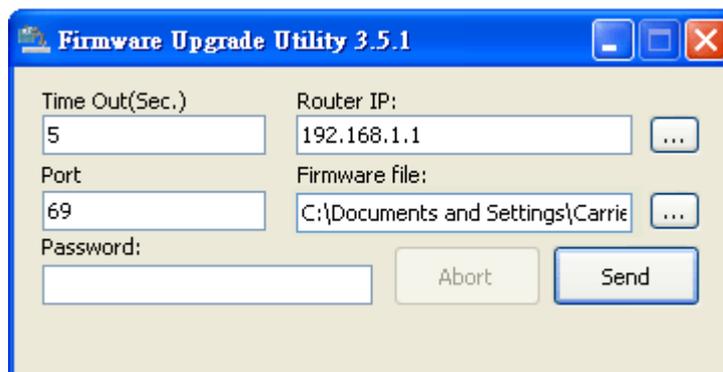
5. Double click on the router tool icon. The setup wizard will appear.



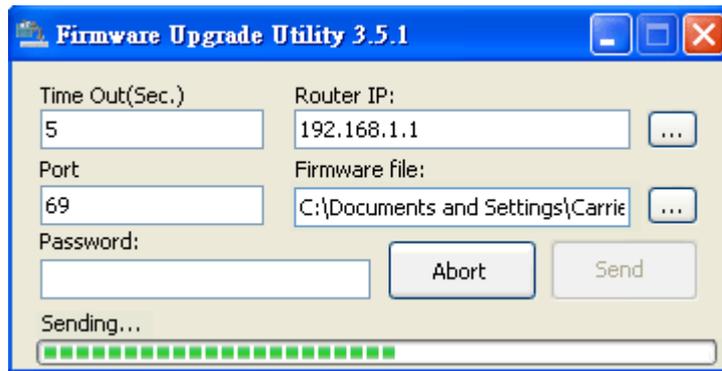
6. Follow the onscreen instructions to install the tool. Finally, click **Finish** to end the installation.
7. From the **Start** menu, open **Programs** and choose **Router Tools XXX >> Firmware Upgrade Utility**.



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.

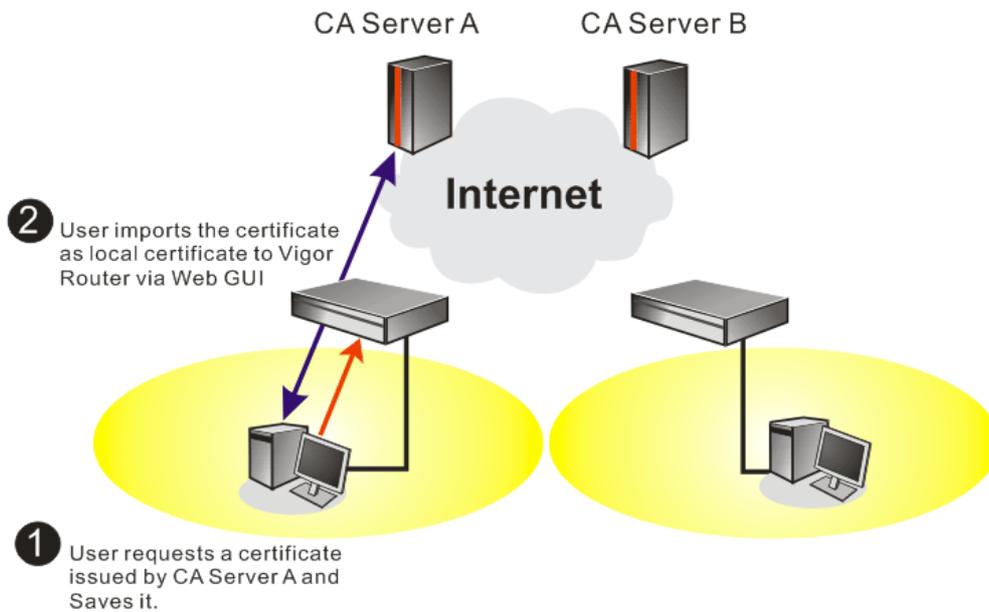


10. Click **Send**.



11. Now the firmware update is finished.

4.6 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
Local	---	---	View Delete

[GENERATE](#)
[IMPORT](#)
[REFRESH](#)

X509 Local Certificate

2. You can click **GENERATE** button to start to edit a certificate request. Enter the information in the certificate request.

[Certificate Management >> Local Certificate](#)

Generate Certificate Request

Subject Alternative Name

Type: ▼

Domain Name:

Subject Name

Country (C):

State (ST):

Location (L):

Organization (O):

Organization Unit (OU):

Common Name (CN):

Email (E):

Key Type: ▼

Key Size: ▼

[Generate](#)

3. Copy and save the X509 Local Certificate Request as a text file and save it for later use.

[Certificate Management >> Local Certificate](#)

X509 Local Certificate Configuration

Name	Subject	Status	Modify
Local	/C=TW/O=Draytek/emailAddress...	Requesting	View Delete

[GENERATE](#)
[IMPORT](#)
[REFRESH](#)

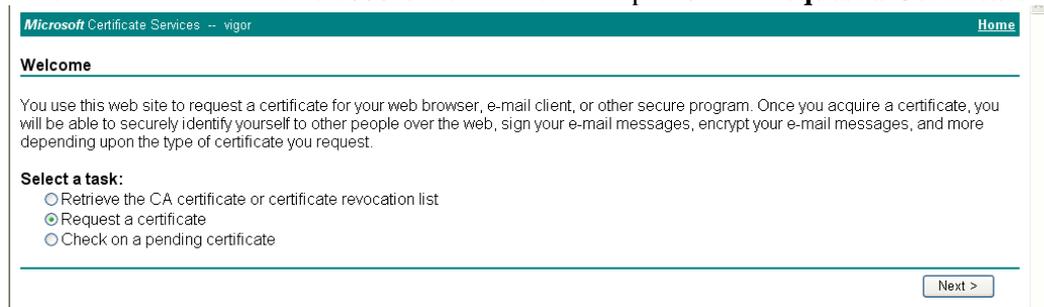
X509 Local Certificate Request

```

-----BEGIN CERTIFICATE REQUEST-----
MIIBqjCCARMCAQAwQTElMAkGA1UEBhMCVFcxEDAOBgNVB AoTB0RyYX10ZWsxIDAe
BgkqhkiG9wOBCQFEWEXByZXNzQGRyYX10ZWsxY29tMIGfMA0GCsgqSB3DQEB AQUA
A4GNADCB1QKBgQDP1oaahu/gFQaYB1ce5OERSDfWknIdHb1o1kt9cTdLUDaFk6s8d
3wDeQytoV1LBjz2IDFOxjX6ip7ev187twwTsg4lg26Qk/rGhuVTKd9j6P1crnkP7
du84t23tWBdMD4W5c8VmsyDjShLhjdXVYPWpNKVlrOT2RZjkRMAHEUpVpWIDAQAB
oCkwJwYJKoZlIhvcNAQkOMRowGDAWBGNVHREEDzANggtkcmF5dGVrLnMvbnTANBgkq
hkiG9w0BAQUFAA0BgQAuSBRUGt4W1hH9N6/HwToem1tHQbcwjXvg/t7kf1zTJ1Hh
uRLq4CiE16nV4hMRytcx2pE26Mar3gRREr86Ro08JxOI45560xCZ/N1Gh9VQ9I1
I9FgkjJNihp4TCjecSNNZjmQo5WU+Bce8TG+SCBCyejqu/fo/AJQFajB7Gviw==
-----END CERTIFICATE REQUEST-----

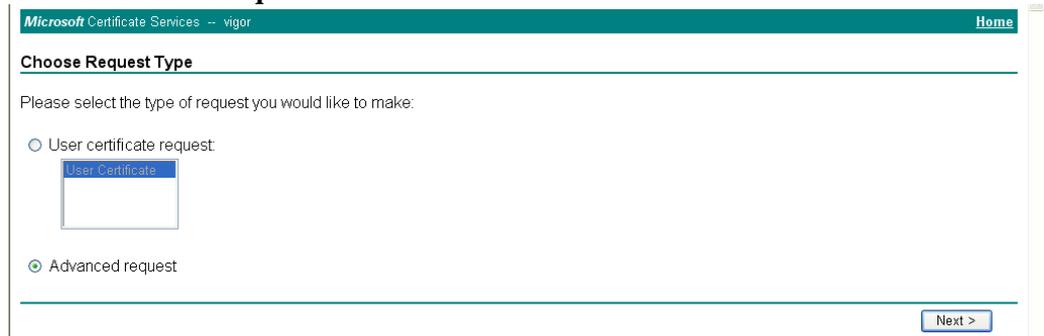
```

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**.



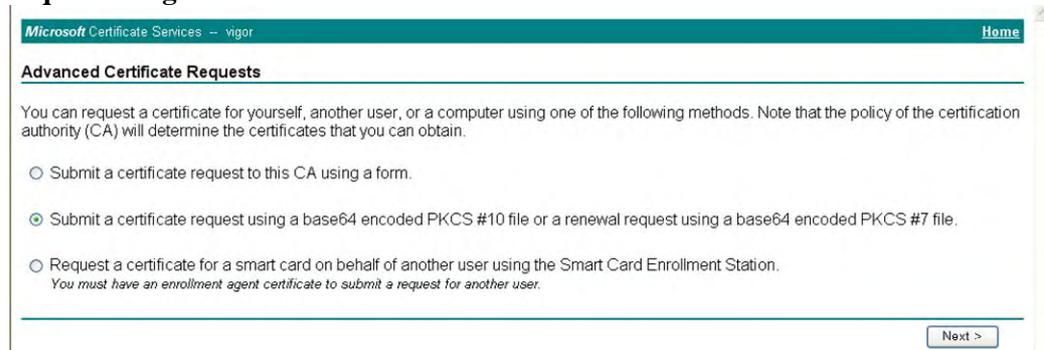
The screenshot shows the 'Microsoft Certificate Services' website. The page title is 'Microsoft Certificate Services -- vigor' and there is a 'Home' link in the top right. The main heading is 'Welcome'. Below the heading, there is a paragraph explaining the purpose of the site: 'You use this web site to request a certificate for your web browser, e-mail client, or other secure program. Once you acquire a certificate, you will be able to securely identify yourself to other people over the web, sign your e-mail messages, encrypt your e-mail messages, and more depending upon the type of certificate you request.' Underneath, there is a section titled 'Select a task:' 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**.



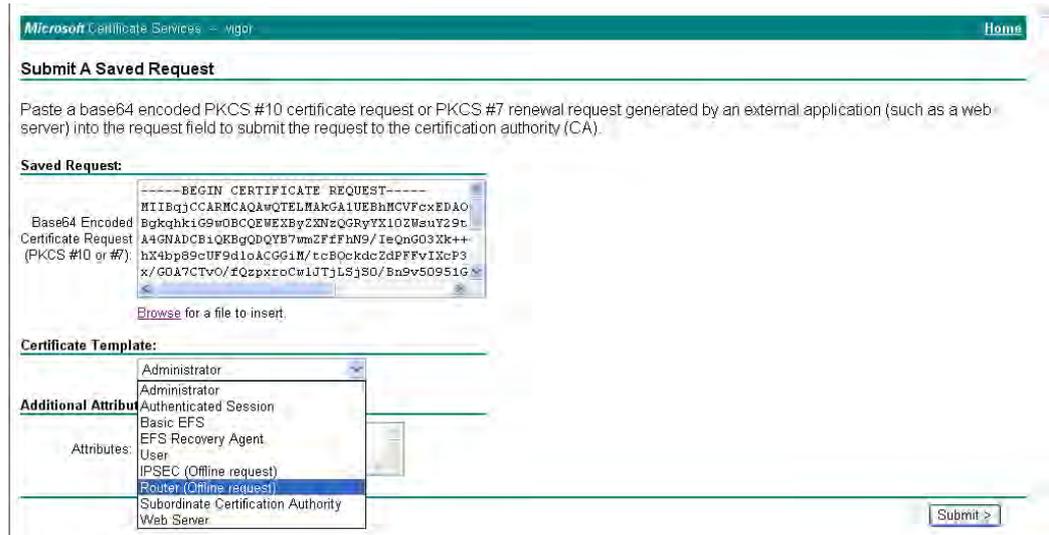
The screenshot shows the 'Microsoft Certificate Services' website. The page title is 'Microsoft Certificate Services -- vigor' and there is a 'Home' link in the top right. The main heading is 'Choose Request Type'. Below the heading, there is a paragraph: 'Please select the type of request you would like to make:'. There are two radio button options: 'User certificate request' and 'Advanced request' (which is selected). Under the 'User certificate request' option, there is a small rectangular box with the text 'User Certificate' inside. 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**



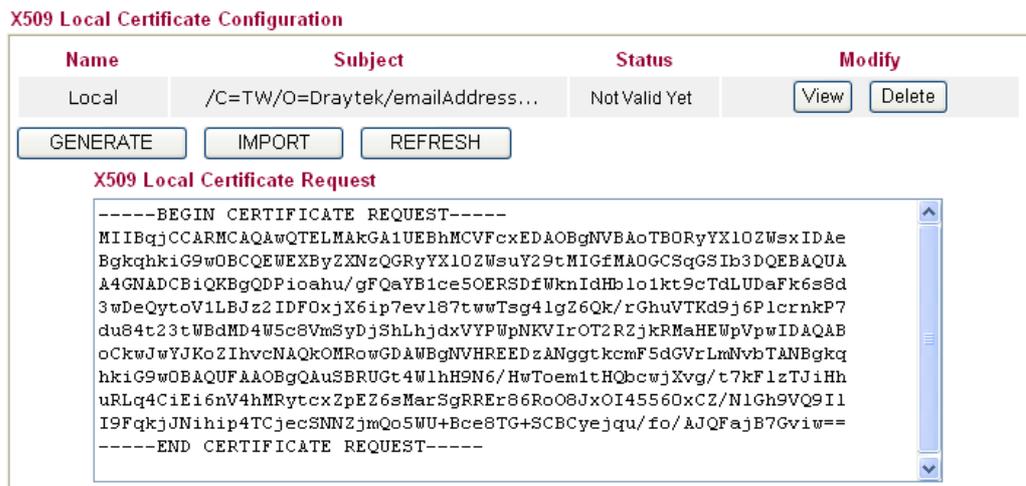
The screenshot shows the 'Microsoft Certificate Services' website. The page title is 'Microsoft Certificate Services -- vigor' and there is a 'Home' link in the top right. The main heading is 'Advanced Certificate Requests'. Below the heading, there is a paragraph: 'You can request a certificate for yourself, another user, or a computer using one of the following methods. Note that the policy of the certification authority (CA) will determine the certificates that you can obtain.' There are 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.' Below the third option, there is a note: '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.



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.

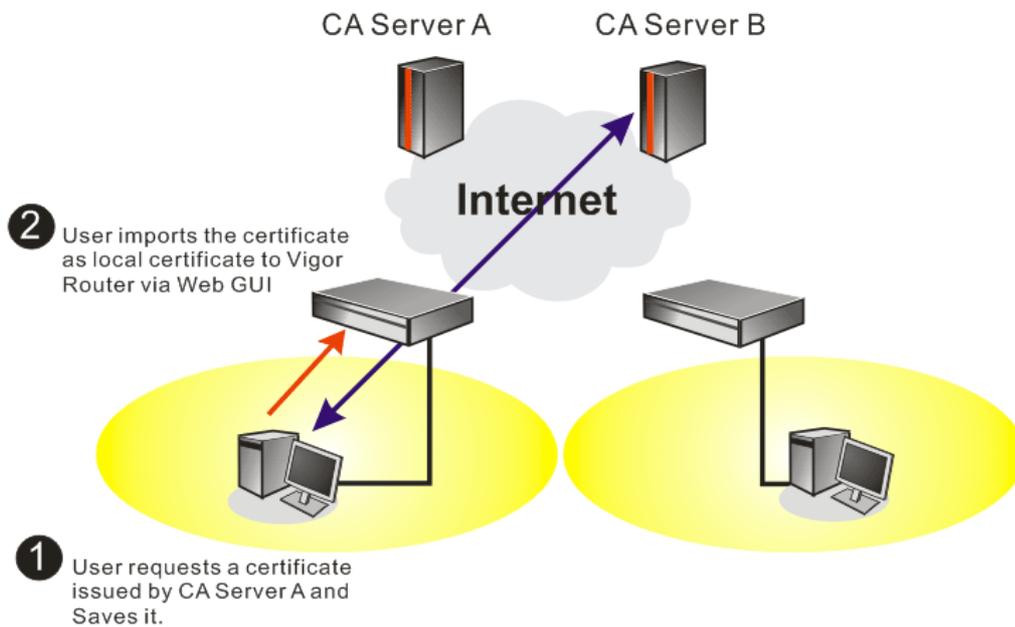
- Back to Vigor router, go to **Local Certificate**. Click **IMPORT** button and browse the file to import the certificate (.cer file) into Vigor router. When finished, click refresh and you will find the below window showing “-----BEGIN CERTIFICATE-----.....”
[Certificate Management >> Local Certificate](#)



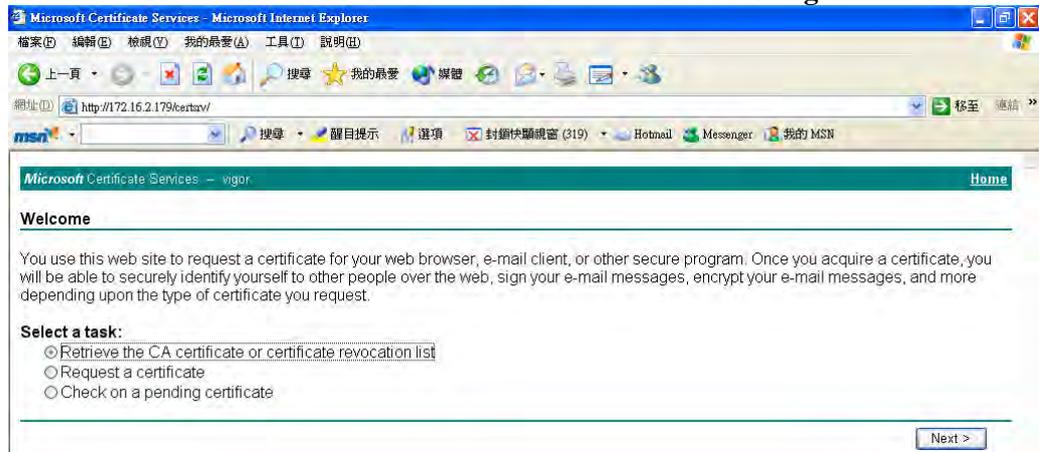
- You may review the detail information of the certificate by clicking **View** button.

Name :	Local
Issuer :	/C=US/CN=vigor
Subject :	/emailAddress=press@draytek.com/C=TW/O=Draytek
Subject Alternative Name :	DNS: draytek.com
Valid From :	Aug 30 23:08:43 2005 GMT
Valid To :	Aug 30 23:17:47 2007 GMT

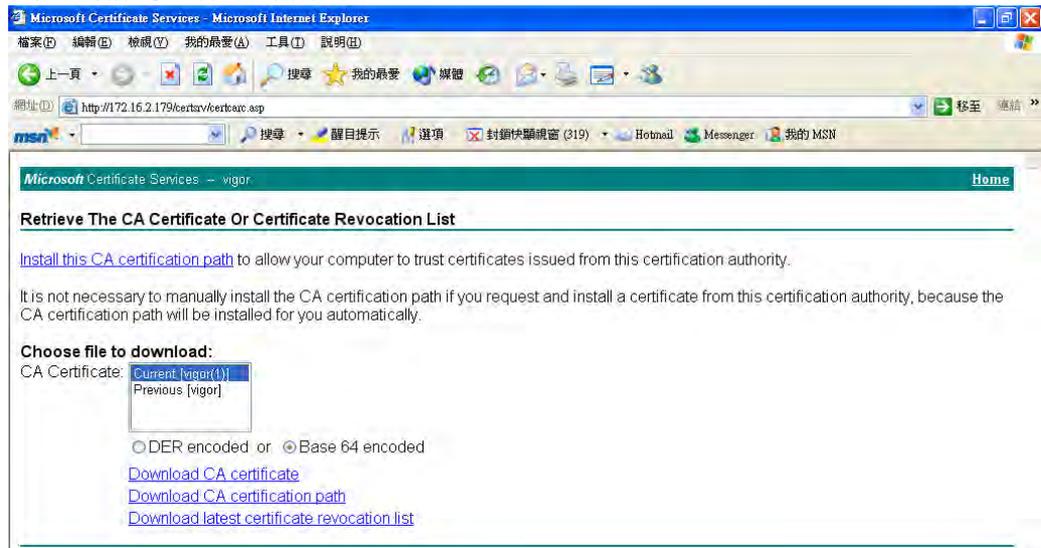
4.7 Request a CA Certificate and Set as Trusted on Windows CA Server



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=US/CN=vigor	Not Yet Valid	<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"/>

- You may review the detail information of the certificate by clicking **View** button.

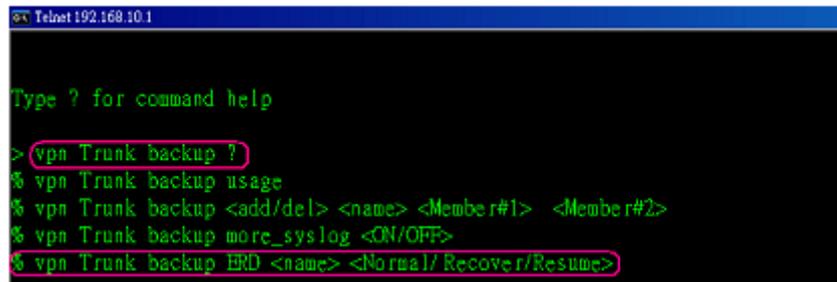
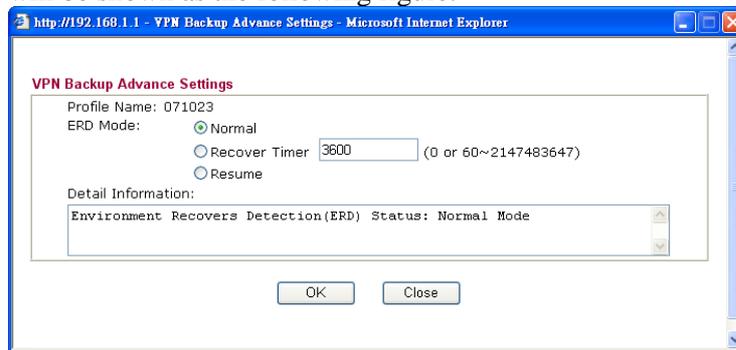
Name :	Trusted CA-1
Issuer :	/C=US/CN=vigor
Subject :	/C=US/CN=vigor
Subject Alternative Name :	DNS: draytek.com
Valid From :	Aug 30 23:08:43 2005 GMT
Valid To :	Aug 30 23:17:47 2007 GMT

Note: Before setting certificate configuration, please go to **System Maintenance >> Time and Date** to reset current time of the router first.

4.8 ERD Mechanism for VPN TRUNK

To use ERD (Environment Recovery Detection) mechanism for VPN TRUNK, please follow the steps listed below:

1. Click **Start >> Run** and type **Telnet 192.168.1.1** in the Open box as below. Note that the IP address in the example is the default address of the router. If you have changed the default, enter the current IP address of the router.
2. Click OK. The Telnet terminal will be open. If an administrator password has not already been assigned, follow the on-screen instructions to assign one.
3. After assigning a password, type **?**. You will see a list of valid/common commands depending on the router that your use.
4. For using ERD mechanism, please type “vpn Trunk backup?”. The available commands will be shown as the following figure.



(1) To inquire current ERD setting

```
> vpn Trunk backup ERD VpnBackup -----> (name of Trunk profile)
```

(2) Normal Mode (Default Setting)

Such mode makes all of the dial-out VPN TRUNK backup profiles being activated alternately.

Request Background: Some of users think if VPN tunnel connected again, it is Environment Recovery Detection. For such users, use Normal mode.

To set ERD Normal mode

```
> vpn Trunk backup ERD VpnBackup Normal
```

(3) Resume Mode

When VPN connection breaks down, Member1 is a top priority for the system to do VPN connection again.

Request Background: Some of users hope the connection can be continuous and not breaking down (maybe they will have thousands of orders coming within one minute). If the network connection breaks down, the users must connect from the first VPN server and spend lots of time. Such mode can solve their problems.

To set ERD Resume mode

```
> vpn Trunk backup ERD VpnBackup Resume
```

(4) Recover Mode

Detect VPN connection periodically (by setting value for “second”). If VPN server for Member 1 has completed the network connection, current VPN Tunnel backup connection will be off-line.

Request Background: Some of users think it is not really environment recovery detection to borrow VPN tunnels from branches for connecting with the headquarters. The system should connect to headquarters automatically and that is called ERD.

To set ERD Recover mode

- To check current status of Recover

```
> vpn Trunk backup ERD VpnBackup Recover
```

- To set Recover

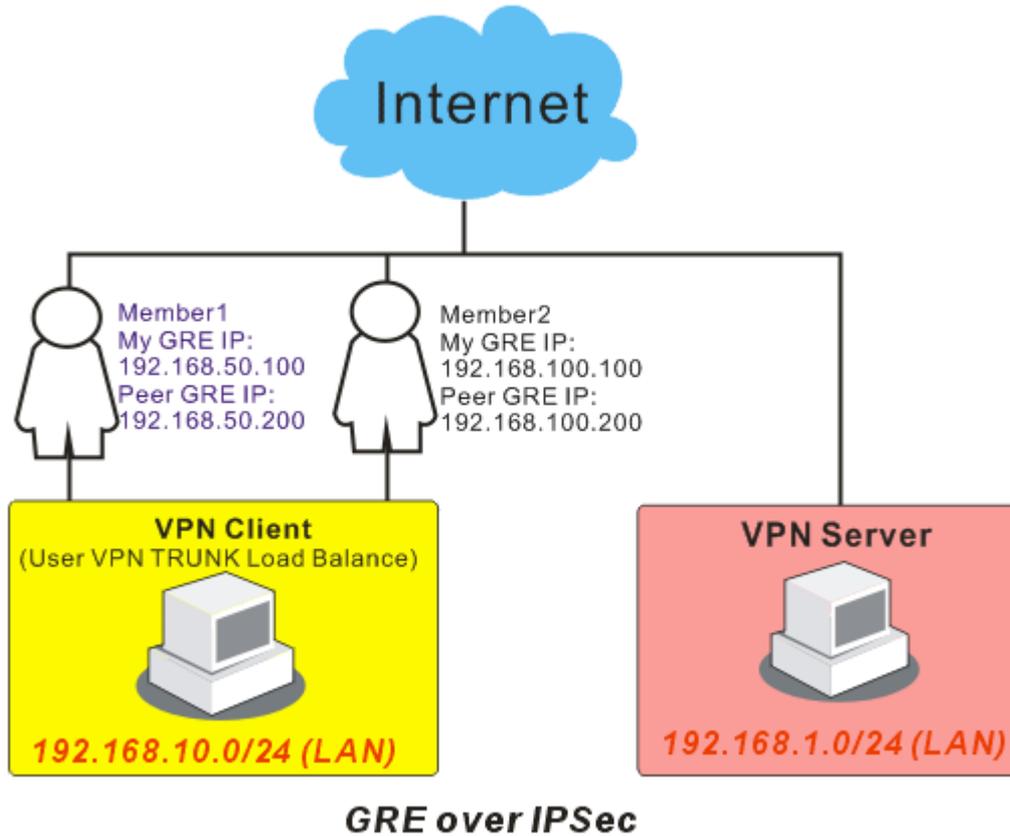
```
> vpn Trunk backup ERD VpnBackup Recover 3600
```

- Why use <second> - Recover might cause unstable condition for data transmitting. To solve the problem, you can set value for second to specify valid time for sending data out.
- When set value for <second> with “0”: VPN tunnel that does not join Member1 will try to connect with VPN server of Member1 for every six seconds. Once the connection is successful, current transmitting data (mail, video conference, or other) will be dropped immediately.
- When set value for <second> with “1 ~ 2147483647”: The administrator can try to connect with VPN server within certain time. Once the connection is successful, current transmitting data (mail, video conference, or other) will be dropped immediately. For example, if you type “3600” as the value for <second>, Recover will be done with 30 seconds (3531 ~ 3600) for the backup VPN tunnel. If you set “30” as the value for <second>, it will be regarded as “0”.

4.9 VPN Load Balance Application

Here provides two situations that you can take advantages of VPN TRUNK Load Balance profile mechanism.

Example 1: A VPN TRUNK profile with member 1 (GRE over IPsec type-LAN to LAN Router Mode) and Member 2(GRE over IPsec type-LAN to LAN Router Mode) has been created for Router A (VPN Client) for connecting with Router B (VPN Server).



(1) VPN Client site

For LAN-to-LAN Dial out for member1 and member2, please finish:

- LAN-to-LAN IPsec Dial Out (Router Mode) configuration.
- Member1 LAN-to-LAN Dial out Profile GRE over IPsec configuration.

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)

- Finish Member2 LAN-to-LAN Dial out Profile with GRE over IPsec configuration. Check Enable IPsec Dial-Out function GRE over IPsec. Type 192.168.100.100 as My GRE IP and 192.168.100.200 as Peer GRE IP.

After adding VpnLB1 under VPN TRUNK Management, press Advanced for Load Balance Profile List and choose suitable algorithm for VPN Load Balance Algorithm.

VPN Load Balance Advance Settings

Profile Name: VpnLB1

Load Balance Algorithm:

- Round Robin
- Weighted Round Robin
 - Auto Weighted
 - According to Speed Ratio (Member1:Member2):
- Fastest

(2) VPN Server site

For LAN-to-LAN Dial out for member1 and member2, please finish:

- LAN-to-LAN IPsec Dial In configuration
- Finish GRE over IPsec setting in LAN-to-LAN Dial In Profile for matching with VPN Client Member1 configuration

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)

- Finish GRE over IPsec setting in LAN-to-LAN Dial In Profile for matching with VPN Client Member2 configuration

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)

(3) Dialing from VPN Client site

VPN and Remote Access >> Connection Management

Dial-out Tool Refresh Seconds : Refresh

General Mode:	<input type="text" value="(Alfa) 192.168.0.26"/>	<input type="button" value="Dial"/>
Backup Mode:	<input type="text" value="(VpnBackup) 192.168.2.103"/>	<input type="button" value="Dial"/>
Load Balance Mode:	<input type="text" value="(VpnLB1) 192.168.2.104"/>	<input type="button" value="Dial"/>

VPN Connection Status

Current Page: 1 Page No. Go >>

VPN	Type	Remote IP	Virtual Network	Tx Pkts	Tx Rate	Rx Pkts	Rx Rate	UpTime
-----	------	-----------	-----------------	---------	---------	---------	---------	--------

This page is left blank.

5

Trouble Shooting

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

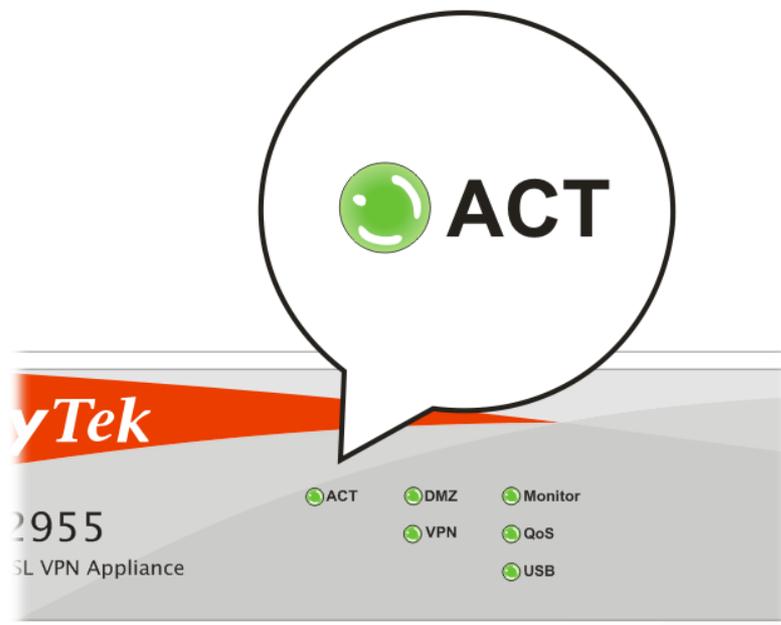
- Checking if the hardware status is OK or not.
- Checking if the network connection settings on your computer are OK or not.
- Pinging the router from your computer.
- Checking if the ISP settings are OK or not.
- Backing to factory default setting if necessary.

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

5.1 Checking If the Hardware Status Is OK or Not

Follow the steps below to verify the hardware status.

1. Check the power line and 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.

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

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

For Windows

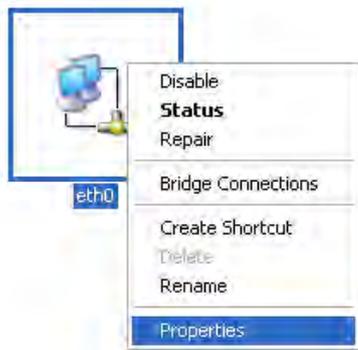


The example is based on Windows XP. As to the examples for other operation systems, please refer to the similar steps or find support notes in www.draytek.com.

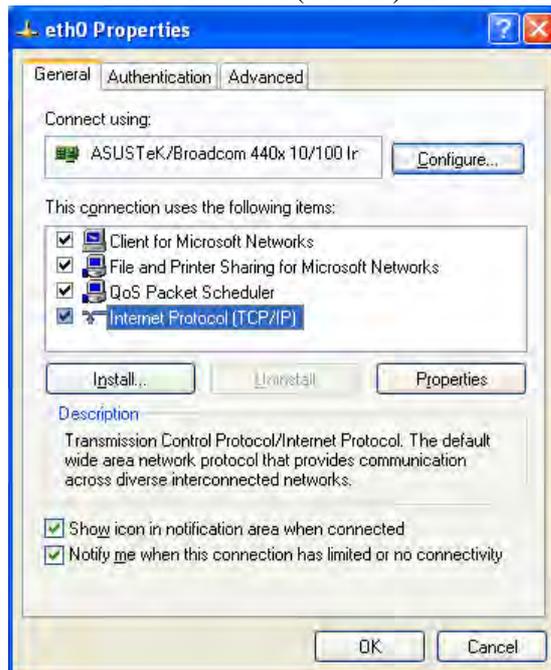
1. Go to Control Panel and then double-click on Network Connections.



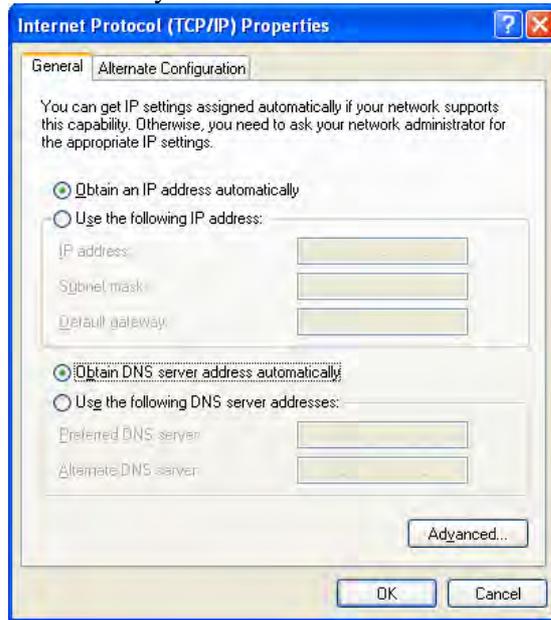
2. Right-click on Local Area Connection and click on Properties.



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

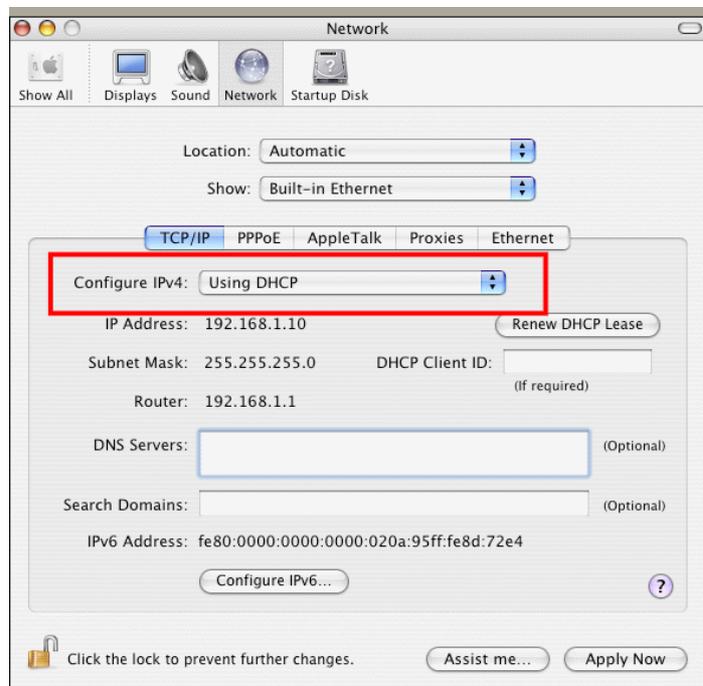


4. Select Obtain an IP address automatically and Obtain DNS server address automatically.



For MacOs

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



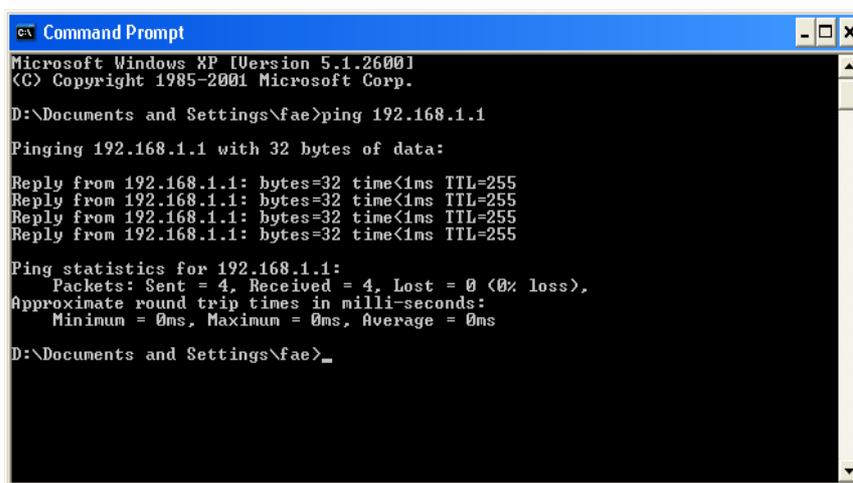
5.3 Pinging the Router from Your Computer

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

Please follow the steps below to ping the router correctly.

For Windows

1. Open the **Command Prompt** window (from **Start menu**> **Run**).
2. Type **command** (for Windows 95/98/ME) or **cmd** (for Windows NT/ 2000/XP/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 ttys1
Welcome to Darwin!
Vigor10:~ draytek$ ping 192.168.1.1
PING 192.168.1.1 (192.168.1.1): 56 data bytes
64 bytes from 192.168.1.1: icmp_seq=0 ttl=255 time=0.755 ms
64 bytes from 192.168.1.1: icmp_seq=1 ttl=255 time=0.697 ms
64 bytes from 192.168.1.1: icmp_seq=2 ttl=255 time=0.716 ms
64 bytes from 192.168.1.1: icmp_seq=3 ttl=255 time=0.731 ms
64 bytes from 192.168.1.1: icmp_seq=4 ttl=255 time=0.72 ms
^C
--- 192.168.1.1 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 0.697/0.723/0.755 ms
Vigor10:~ draytek$
```

5.4 Checking If the ISP Settings are OK or Not

Click **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/L2TP

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>	<p>PPP/MP Setup</p> <p>PPP Authentication ▾ PAP or CHAP</p> <p>Idle Timeout <input type="text" value="-1"/> second(s)</p>
<p>ISP Access Setup</p> <p>Username <input type="text" value="84005676@hinet.net"/></p> <p>Password <input type="password" value="••••••••"/></p> <p>Index(1-15) in Schedule Setup:</p> <p>=> <input type="text"/> , <input type="text"/> , <input type="text"/> , <input type="text"/></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>
<p>WAN Connection Detection</p> <p>Mode ▾ ARP Detect</p> <p>Ping IP <input type="text"/></p> <p>TTL: <input type="text"/></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=".C7"/> <input type="text" value=".86"/> <input type="text" value=".89"/></p>
<p>MTU <input type="text" value="1442"/> (Max:1492)</p>	

For Static or 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 (DHCP Client)</p> <p><input checked="" type="radio"/> Enable <input type="radio"/> Disable</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"/></p> <p>TTL: <input type="text"/></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 checked="" type="radio"/> Obtain an IP address automatically</p> <p>Router Name <input type="text"/> *</p> <p>Domain Name <input type="text"/> *</p> <p>* : Required for some ISPs</p> <p><input type="radio"/> Specify an IP address</p> <p>IP Address <input type="text"/></p> <p>Subnet Mask <input type="text"/></p> <p>Gateway IP Address <input type="text"/></p> <p>DNS Server IP Address</p> <p>Primary IP Address <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="C7"/> <input type="text" value="86"/> <input type="text" value="89"/></p>
--	--

For PPTP/L2TP Users

1. Check if the **Enable** option for **PPTP Link** is selected.

WAN >> Internet Access

WAN 1

<p>PPTP/L2TP Client Mode</p> <p><input checked="" type="radio"/> Enable PPTP <input type="radio"/> Enable L2TP <input type="radio"/> Disable</p> <p>Server Address <input type="text" value="10.0.0.138"/></p> <p>Specify Gateway IP Address <input type="text"/></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:</p> <p>=> <input type="text"/> , <input type="text"/> , <input type="text"/> , <input type="text"/></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) <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> <p>WAN IP Network Settings</p> <p><input checked="" type="radio"/> Obtain an IP address automatically</p> <p><input 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 **Server Address, Username, Password** and **WAN IP address** are set correctly (must identify with the values from your ISP).

5.5 Backing to Factory Default Setting If Necessary

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



Warning: After pressing **factory default setting**, you will 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

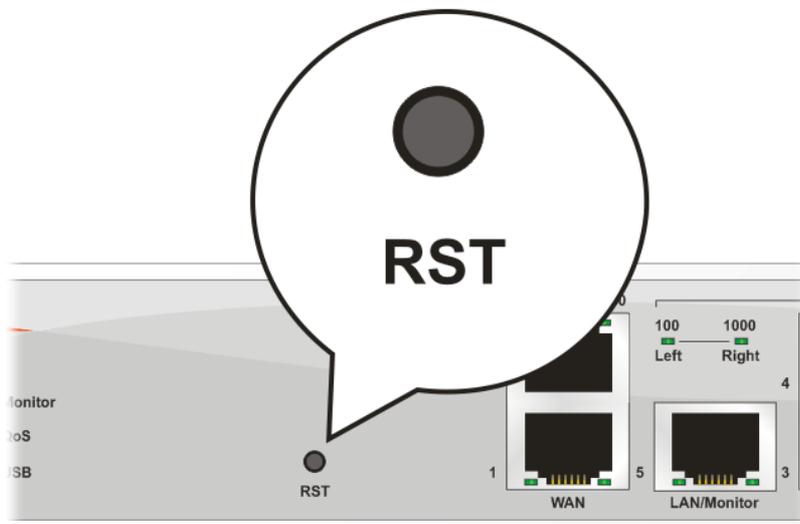
Do You want to reboot your router ?

- Using current configuration
- Using factory default configuration

OK

Hardware Reset

While the router is running (ACT LED blinking), press the **Factory Reset** 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.

5.6 Contacting Your Dealer

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