DrayTek

# Vigor 2700 Series Firewall Router
# User's Guide

**Version: 2.1**

**Date: 2006/4/29**

This page is left blank.

## *Table of Contents*


**Preface ..... 1**

1.1 LED Indicators and Connectors ..... 2

1.1.1 Front and Rear View for Vigor2700 ..... 2
1.1.2 Front and Rear View for Vigor2700G ..... 3
1.1.3 Front and Rear View for Vigor2700Gi ..... 4
1.1.4 Front and Rear View for Vigor2700V (MODULE:2S1L) ..... 5
1.1.5 Front and Rear View for Vigor2700V (MODULE:2S) ..... 6
1.1.6 Front and Rear View for Vigor2700VGi ..... 7
1.1.7 Front and Rear View for Vigor2700VG (MODULE:2S1L) ..... 8
1.1.8 Front and Rear View for Vigor2700VG (MODULE:2S) ..... 9

1.2 Hardware Installation ..... 10

**Configuring Basic Settings ..... 11**

2.1 Changing Password ..... 11

2.2 Quick Start Wizard ..... 13

2.2.1 Adjusting Protocol/Encapsulation ..... 13
2.2.2 PPPoE/PPPoA ..... 14
2.2.3 Bridged IP ..... 16
2.2.4 Routed IP ..... 17

2.3 Online Status for Each Protocol ..... 18

2.4 Status Bar ..... 20

**Advanced Web Configuration ..... 21**

3.1 Internet Access ..... 21

3.1.1 Basics of Internet Protocol (IP) Network ..... 21
3.1.2 PPPoE/PPPoA ..... 22
3.1.3 MPoA ..... 24
3.1.4 Multi-PVCs ..... 27

3.2 LAN ..... 29

3.2.1 Basics of LAN ..... 29
3.2.2 General Setup ..... 30
3.2.3 Static Route ..... 33
3.2.4 VLAN ..... 36

3.3 NAT ..... 37

3.3.1 Port Redirection ..... 37
3.3.2 DMZ Host ..... 39
3.3.3 Open Ports ..... 41
3.3.4 Well-Known Ports List ..... 43

3.4 Firewall ..... 43

3.4.1 Basics for Firewall ..... 43
3.4.2 General Setup ..... 46
3.4.3 Filter Setup ..... 47
3.4.4 IM Blocking ..... 50
3.4.5 P2P Blocking ..... 51
3.4.6 DoS Defense ..... 52
3.4.7 URL Content Filter ..... 54
3.4.8 Web Content Filter ..... 56

3.5 Applications ..... 57

3.5.1 Dynamic DNS ..... 57
3.5.2 Schedule ..... 58
3.5.3 RADIUS ..... 60
3.5.4 UPnP ..... 60
3.5.5 Quality of Service ..... 62
3.5.6 IGMP ..... 67

3.6 VPN and Remote Access ..... 69

3.6.1 Remote Access Control ..... 69
3.6.2 PPP General Setup ..... 69
3.6.3 IPSec General Setup ..... 70
3.6.4 IPSec Peer Identity ..... 72
3.6.5 Remote User Profiles ..... 73
3.6.6 LAN to LAN Profiles ..... 76
3.6.7 Connection Management ..... 83

3.7 Certificate Management ..... 84

3.7.1 Local Certificate ..... 85
3.7.2 Trusted CA Certificate ..... 86

3.8 VoIP ..... 87

3.8.1 DialPlan ..... 88
3.8.2 SIP Accounts ..... 93
3.8.3 Phone Settings ..... 96
3.8.4 PSTN Setup ..... 99
3.8.5 Status ..... 99

3.9 ISDN ..... 101

3.9.1 General Setup ..... 101
3.9.2 Dialing to a Single ISP ..... 101
3.9.3 Dialing to Dual ISPs ..... 103
3.9.4 Virtual TA ..... 103
3.9.5 Call Control ..... 107

3.10 Wireless LAN ..... 108

3.10.1 Basic Concept ..... 109
3.10.2 General Settings ..... 111
3.10.3 Security ..... 112
3.10.4 Access Control ..... 113
3.10.5 WDS ..... 114
3.10.6 AP Discovery ..... 117
3.10.7 Station List ..... 118

3.11 System Maintenance ..... 119

3.11.1 System Status ..... 119
3.11.2 Administrator Password ..... 120
3.11.3 Configuration Backup ..... 120
3.11.4 Syslog/Mail Alert ..... 122
3.11.5 Time and Date ..... 123
3.11.6 Management ..... 124

3.11.7 Reboot System ..... 125
3.11.8 Firmware Upgrade ..... 125
3.12 Diagnostics ..... 126
3.12.1 WAN Connection ..... 126
3.12.2 Dial-out Trigger ..... 128
3.12.3 Routing Table ..... 128
3.12.4 ARP Cache Table ..... 129
3.12.5 DHCP Table ..... 129
3.12.6 NAT Active Sessions Table ..... 130

**Application and Examples ..... 131**

4.1 Create a LAN-to-LAN Connection Between Remote Office and Headquarter ..... 131
4.2 Create a Remote Dial-in User Connection Between the Teleworker and Headquarter ..... 138
4.3 QoS Setting Example ..... 142
4.4 LAN – Created by Using NAT ..... 144
4.5 Calling Scenario for VoIP function ..... 146
4.5.1 Calling via SIP Sever ..... 146
4.5.2 Peer-to-Peer Calling ..... 148
4.6 Upgrade Firmware for Your Router ..... 149
4.7 Request a Certificate from a CA Server on Windows CA Server ..... 152
4.8 Request a CA Certificate and Set as Trusted on Windows CA Server ..... 156

**Trouble Shooting ..... 159**

5.1 Checking If the Hardware Status Is OK or Not ..... 159
5.2 Checking If the Network Connection Settings on Your Computer Is OK or Not ..... 159
5.3 Pinging the Router from Your Computer ..... 162
5.4 Checking If the ISP Settings are OK or Not ..... 164
5.5 Backing to Factory Default Setting If Necessary ..... 165
5.6 Contacting Your Dealer ..... 166

This page is left blank.

# 1 Preface

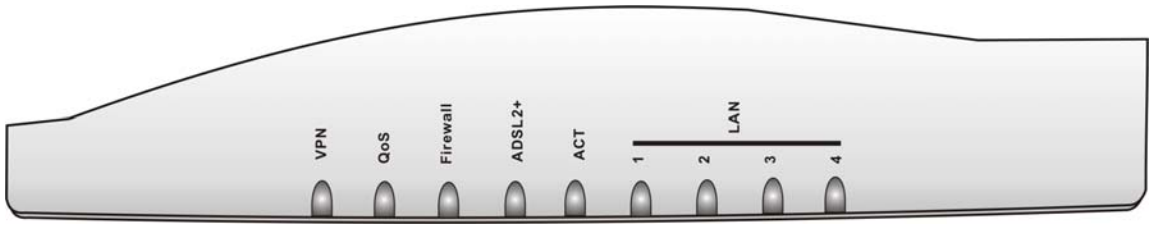
Targeting requirement for residential, SOHO (Small Office and Home Office) and business users, the Vigor270 series is an ADSL2/2+ enabled integrated access device. With downstream speed up to 12Mbps (ADSL2) or 24Mbps (ADSL2+), the Vigor270 series provides exceptional bandwidth for Internet access.

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

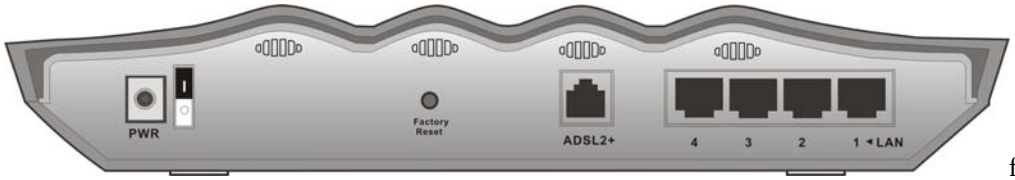
Vigor 2700 G model is embedded with an 802.11g compliant wireless module which provides wireless LAN access with data rate as much as 54Mbps. As for data privacy of wireless network, the Vigor2700 G model can encode all transmissions data with standard WEP and industrial strength WPA2 (IEEE 802.11i) encryption. Additional features include Wireless Client List and MAC Address Control for maintaining control over user's authorization in your network, and Hidden SSID for being invisible to outside intruders scanning.

## 1.1 LED Indicators and Connectors

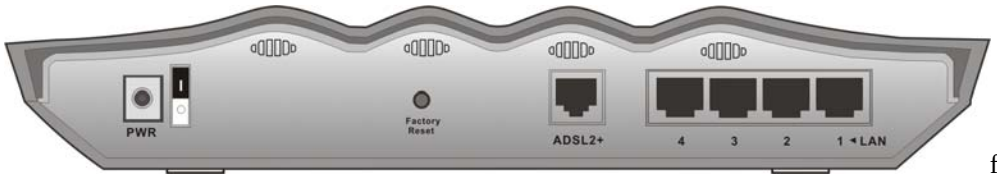
### 1.1.1 Front and Rear View for Vigor2700




| LED | Status | Explanation |
|---|---|---|
| VPN | On | The VPN tunnel is launched. |
| QoS | On | The QoS function is active. |
| | Off | The QoS function is inactive. |
| Firewall | On | The DoS function is enabled. |
| | Blinking | When encountered DoS attacks. |
| ADSL2+ | On (Green) | ADSL is show time. |
| | Blinking (Green) | The device starts handshaking. |
| | Blinking (Orange) | The data is transmitting. |
| ACT (Activity) | On | The router is powered on. |
| | Blinking | The router is powered on and running properly. |
| LAN (1, 2, 3, 4) | Green | A normal connection is through its corresponding port. |
| | Blinking | Ethernet packets are transmitting. |



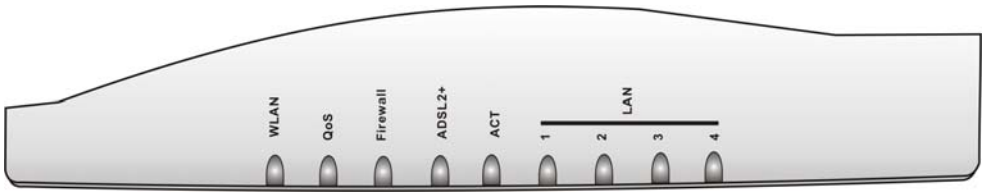

for Annex A



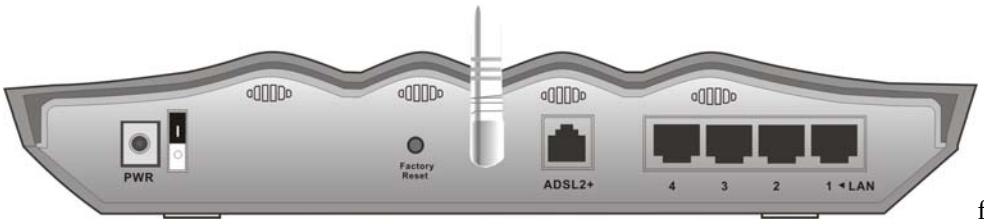

for Annex B

| Interface | Description |
|---|---|
| PWR | Connecter for a power adapter with 12~15VDC. |
| ON/OFF | Power Switch. |
| Factory Reset | Restore the default settings.<br>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. |
| ADSL 2+ | Connecter for accessing the Internet through ADSL2/2+. |
| LAN 4 – 1 | Connecter for local networked devices. |

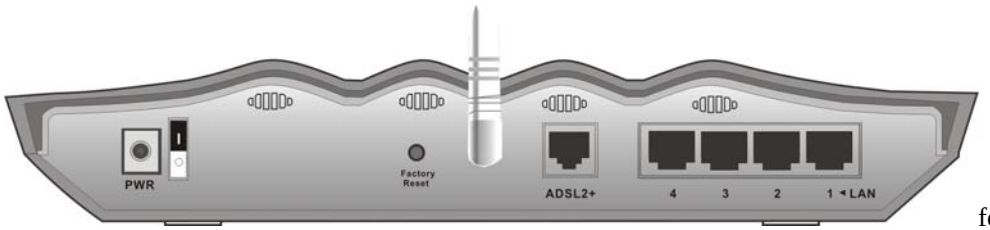
## 1.1.2 Front and Rear View for Vigor2700G




| LED | Status | Explanation |
|---|---|---|
| WLAN | On | Wireless access point is ready. |
| | Blinking | Ethernet packets are transmitting over wireless LAN. |
| | Off | The WLAN function is inactive. |
| QoS | On | The QoS function is active. |
| | Off | The QoS function is inactive. |
| Firewall | On | The DoS function is enabled. |
| | Blinking | When encountered DoS attacks. |
| ADSL2+ | On (Green) | ADSL is show time. |
| | Blinking (Green) | The device starts handshaking. |
| | Blinking (Orange) | The data is transmitting. |
| ACT (Activity) | On | The router is powered on. |
| | Blinking | The router is powered on and running properly. |
| LAN (1, 2, 3, 4) | Green | A normal connection is through its corresponding port. |
| | Blinking | Ethernet packets are transmitting. |



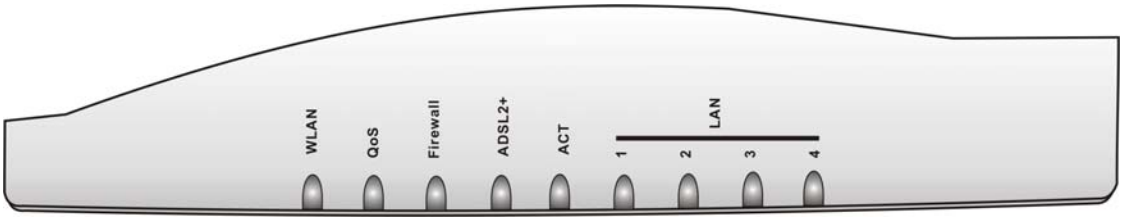

for Annex A



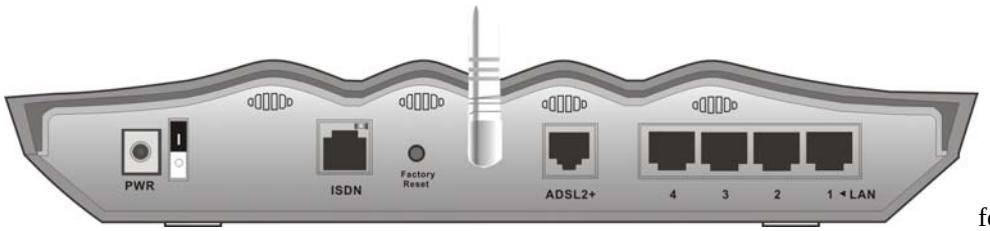

for Annex B

| Interface | Description |
|---|---|
| PWR | Connecter for a power adapter with 12~15VDC. |
| ON/OFF | Power Switch. |
| Factory Reset | Restore the default settings.<br>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. |
| ADSL 2+ | Connecter for accessing the Internet through ADSL2/2+. |
| LAN 4 – 1 | Connecter for local networked devices. |

## 1.1.3 Front and Rear View for Vigor2700Gi



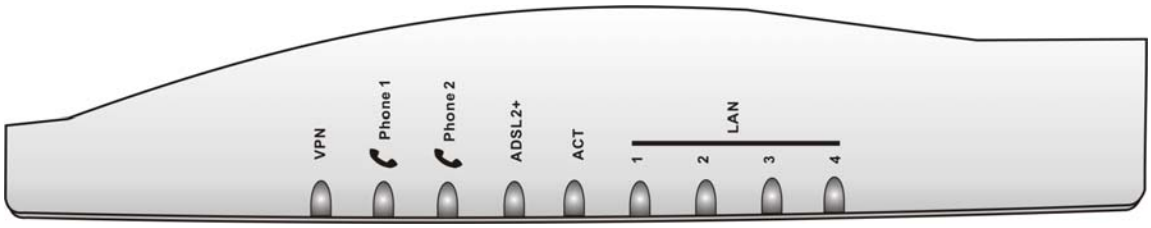

| LED | Status | Explanation |
|---|---|---|
| WLAN | On | Wireless access point is ready. |
| | Blinking | Ethernet packets are transmitting over wireless LAN. |
| | Off | The WLAN function is inactive. |
| QoS | On | The QoS function is active. |
| | Off | The QoS function is inactive. |
| Firewall | On | The DoS function is enabled. |
| | Blinking | When encountered DoS attacks. |
| ADSL2+ | On (Green) | ADSL is show time. |
| | Blinking (Green) | The device starts handshaking. |
| | Blinking (Orange) | The data is transmitting. |
| ACT (Activity) | On | The router is powered on. |
| | Blinking | The router is powered on and running properly. |
| LAN (1, 2, 3, 4) | Green | A normal connection is through its corresponding port. |
| | Blinking | Ethernet packets are transmitting. |



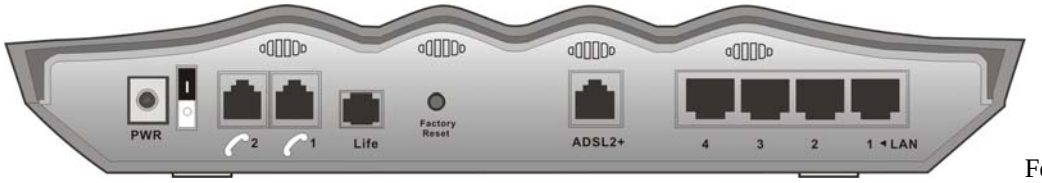

for Annex B

| Interface | Description |
|---|---|
| PWR | Connecter for a power adapter with 12~15VDC. |
| ON/OFF | Power Switch. |
| ISDN | Connecter for NT1 (or NT1+) box provided by ISDN service provider. |
| Factory Reset | Restore the default settings.<br>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. |
| ADSL 2+ | Connecter for accessing the Internet through ADSL2/2+. |
| LAN 4 – 1 | Connecter for local networked devices. |

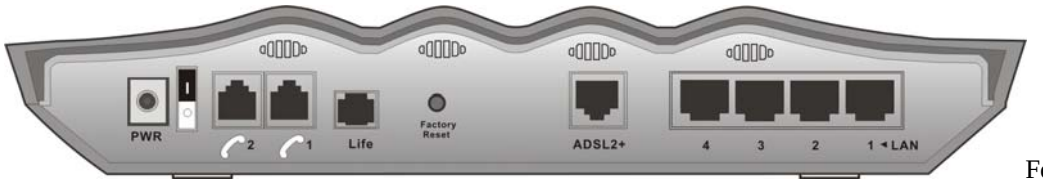
## 1.1.4 Front and Rear View for Vigor2700V (MODULE:2S1L)




| LED | Status | Explanation |
|---|---|---|
| VPN | On | The VPN tunnel is launched. |
| Phone 1 & 2 (FXS1, FXS2) | On | The phone is off hook (the handset of phone is hanging). |
| | Blinking | A phone call is incoming. |
| ADSL2+ | On (Green) | ADSL is show time. |
| | Blinking (Green) | The device starts handshaking. |
| | Blinking (Orange) | The data is transmitting. |
| ACT (Activity) | On | The router is powered on. |
| | Blinking | The router is powered on and running properly. |
| LAN (1, 2, 3, 4) | Green | A normal connection is through its corresponding port. |
| | Blinking | Ethernet packets are transmitting. |



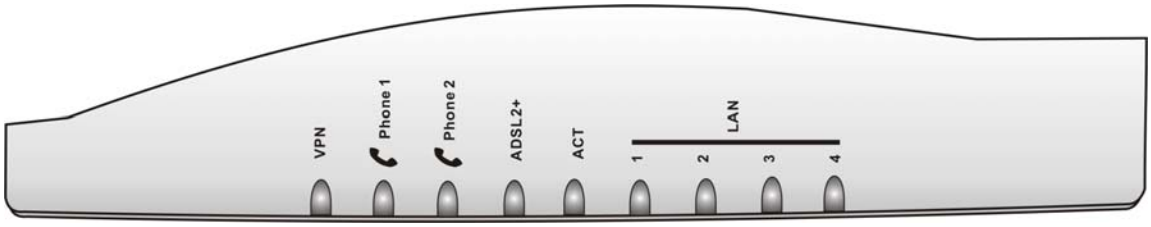

For Annex A



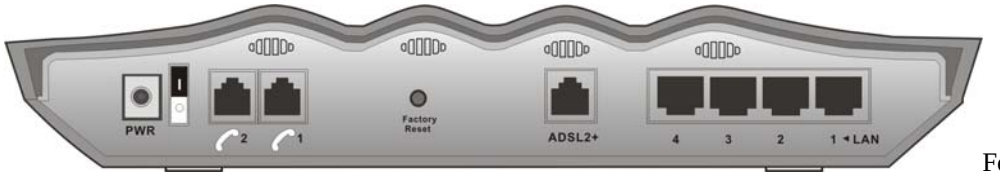

For Annex B

| Interface | Description |
|---|---|
| PWR | Connecter for a power adapter with 12~15VDC. |
| ON/OFF | Power Switch. |
| VoIP 1/2 | Connecter of analog phone for VoIP communication. |
| Life | Connector of analog phone for PSTN life line. |
| Factory Reset | Restore the default settings.<br>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. |
| ADSL 2+ | Connecter for accessing the Internet through ADSL2/2+. |
| LAN 4 – 1 | Connecter for local networked devices. |

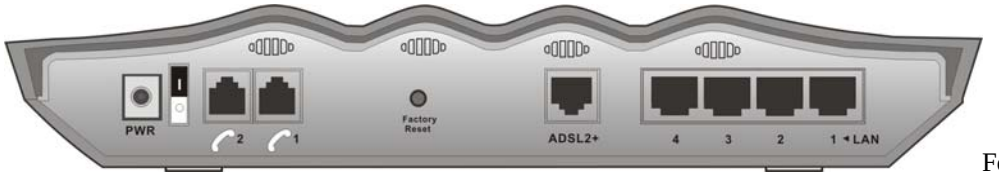
## 1.1.5 Front and Rear View for Vigor2700V (MODULE:2S)




| LED | Status | Explanation |
|---|---|---|
| VPN | On | The VPN tunnel is launched. |
| Phone 1 & 2 (FXS1, FXS2) | On | The phone is off hook (the handset of phone is hanging). |
| | Blinking | A phone call is incoming. |
| ADSL2+ | On (Green) | ADSL is show time. |
| | Blinking (Green) | The device starts handshaking. |
| | Blinking (Orange) | The data is transmitting. |
| ACT (Activity) | On | The router is powered on. |
| | Blinking | The router is powered on and running properly. |
| LAN (1, 2, 3, 4) | Green | A normal connection is through its corresponding port. |
| | Blinking | Ethernet packets are transmitting. |



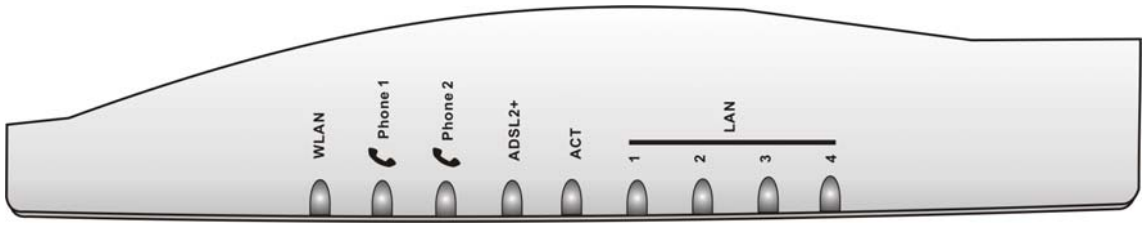

For Annex A



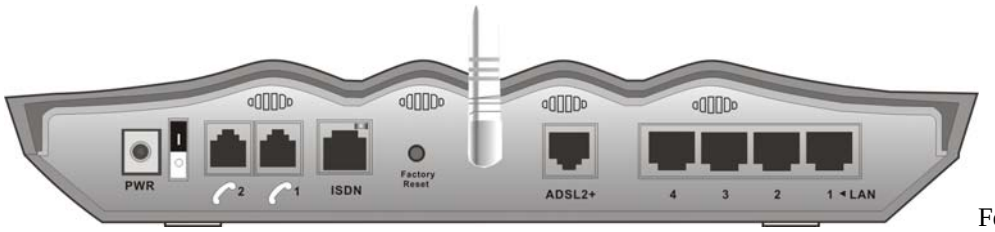

For Annex B

| Interface | Description |
|---|---|
| PWR | Connecter for a power adapter with 12~15VDC. |
| ON/OFF | Power Switch. |
| VoIP 1/2 | Connecter of analog phone for VoIP communication. |
| Factory Reset | Restore the default settings.<br>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. |
| ADSL 2+ | Connecter for accessing the Internet through ADSL2/2+. |
| LAN 4 – 1 | Connecter for local networked devices. |

## 1.1.6 Front and Rear View for Vigor2700VGi



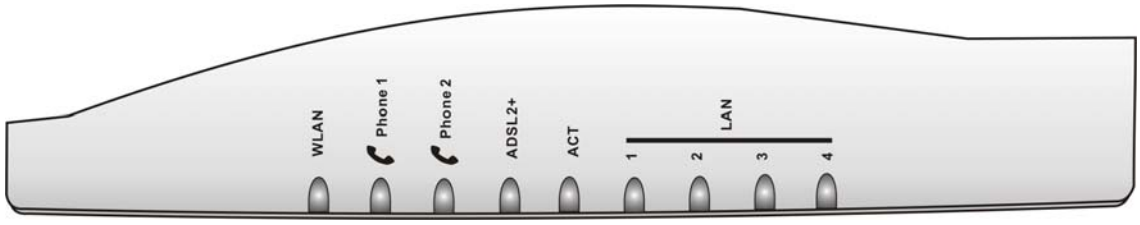

| LED | Status | Explanation |
|---|---|---|
| WLAN | On | Wireless access point is ready. |
| | Blinking | Ethernet packets are transmitting over wireless LAN. |
| | Off | The WLAN function is inactive. |
| Phone 1 & 2 (FXS1, FXS2) | On | The phone is off hook (the handset of phone is hanging). |
| | Blinking | A phone call is incoming. |
| ADSL2+ | On (Green) | ADSL is show time. |
| | Blinking (Green) | The device starts handshaking. |
| | Blinking (Orange) | The data is transmitting. |
| ACT (Activity) | On | The router is powered on. |
| | Blinking | The router is powered on and running properly. |
| LAN (1, 2, 3, 4) | Green | A normal connection is through its corresponding port. |
| | Blinking | Ethernet packets are transmitting. |



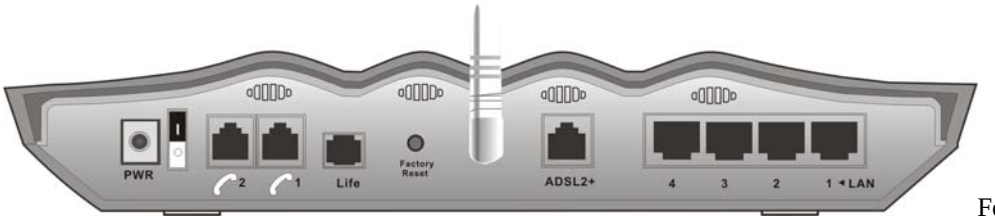

For Annex B

| Interface | Description |
|---|---|
| PWR | Connecter for a power adapter with 12~15VDC. |
| ON/OFF | Power Switch. |
| VoIP 1/2 | Connecter of analog phone for VoIP communication. |
| ISDN | Connecter for NT1 (or NT1+) box provided by ISDN service provider. |
| Factory Reset | Restore the default settings.<br>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. |
| ADSL 2+ | Connecter for accessing the Internet through ADSL2/2+. |
| LAN 4 – 1 | Connecter for local networked devices. |

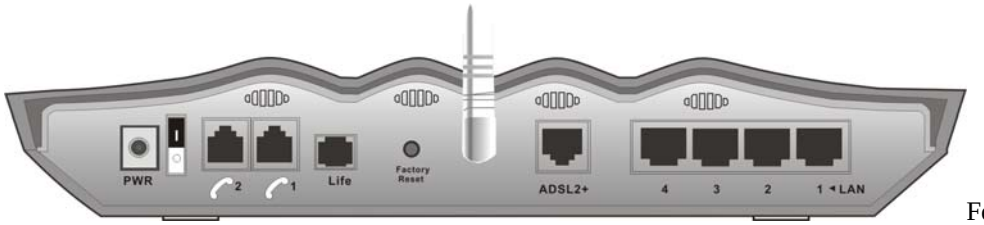
## 1.1.7 Front and Rear View for Vigor2700VG (MODULE:2S1L)




| LED | Status | Explanation |
|---|---|---|
| WLAN | On | Wireless access point is ready. |
| | Blinking | Ethernet packets are transmitting over wireless LAN. |
| | Off | The WLAN function is inactive. |
| Phone 1 & 2 (FXS1, FXS2) | On | The phone is off hook (the handset of phone is hanging). |
| | Blinking | A phone call is incoming. |
| ADSL2+ | On (Green) | ADSL is show time. |
| | Blinking (Green) | The device starts handshaking. |
| | Blinking (Orange) | The data is transmitting. |
| ACT (Activity) | On | The router is powered on. |
| | Blinking | The router is powered on and running properly. |
| LAN (1, 2, 3, 4) | Green | A normal connection is through its corresponding port. |
| | Blinking | Ethernet packets are transmitting. |



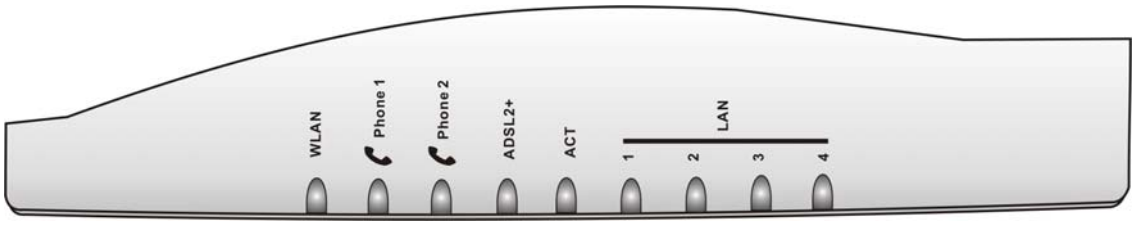

For Annex A



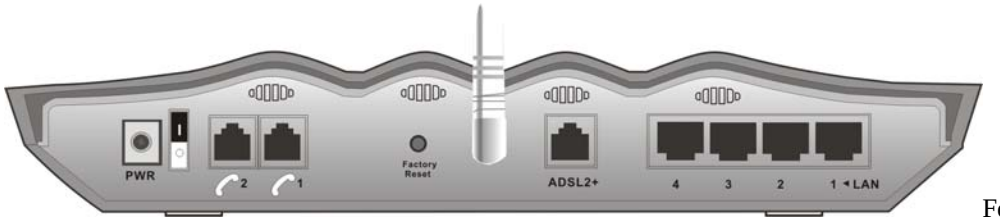

For Annex B

| Interface | Description |
|---|---|
| PWR | Connecter for a power adapter with 12~15VDC. |
| ON/OFF | Power Switch. |
| VoIP 1/2 | Connecter of analog phone for VoIP communication. |
| Life | Connector of analog phone for PSTN life line. |
| Factory Reset | Restore the default settings.<br>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. |
| ADSL 2+ | Connecter for accessing the Internet through ADSL2/2+. |
| LAN 4 – 1 | Connecter for local networked devices. |

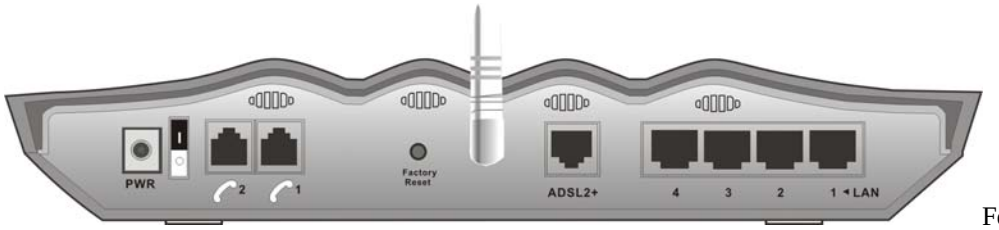
## 1.1.8 Front and Rear View for Vigor2700VG (MODULE:2S)




| LED | Status | Explanation |
|---|---|---|
| WLAN | On | Wireless access point is ready. |
| | Blinking | Ethernet packets are transmitting over wireless LAN. |
| | Off | The WLAN function is inactive. |
| Phone 1 & 2 (FXS1, FXS2) | On | The phone is off hook (the handset of phone is hanging). |
| | Blinking | A phone call is incoming. |
| ADSL2+ | On (Green) | ADSL is show time. |
| | Blinking (Green) | The device starts handshaking. |
| | Blinking (Orange) | The data is transmitting. |
| ACT (Activity) | On | The router is powered on. |
| | Blinking | The router is powered on and running properly. |
| LAN (1, 2, 3, 4) | Green | A normal connection is through its corresponding port. |
| | Blinking | Ethernet packets are transmitting. |




For Annex A




For Annex B

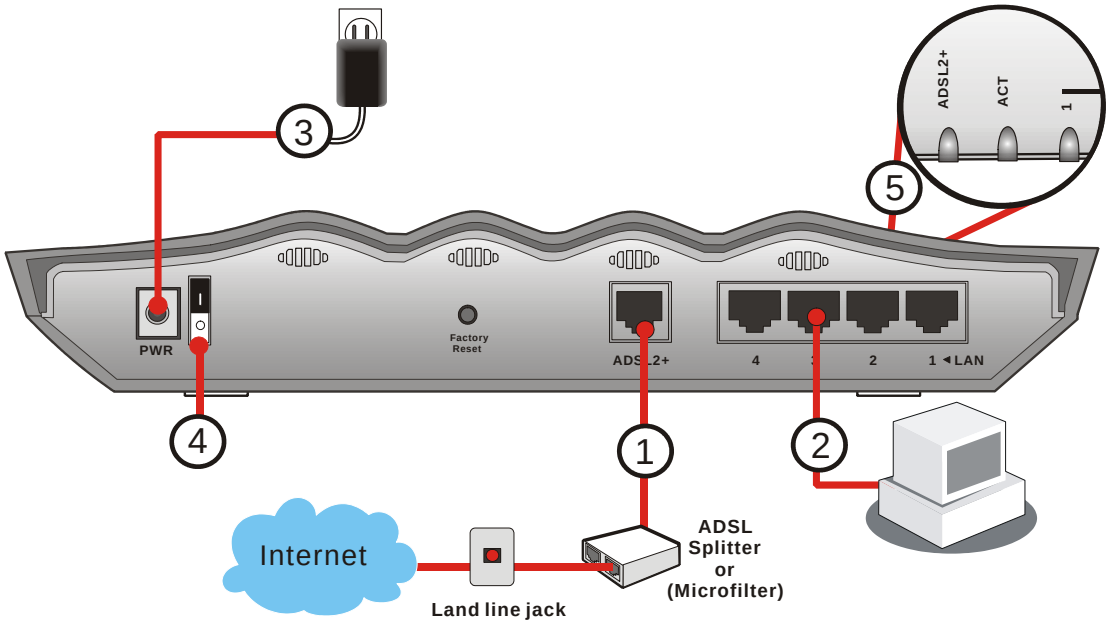
| Interface | Description |
|---|---|
| PWR | Connecter for a power adapter with 12~15VDC. |
| ON/OFF | Power Switch. |
| VoIP 1/2 | Connecter of analog phone for VoIP communication. |
| Factory Reset | Restore the default settings.<br>Usage: Turn on the router (ACT LED is blinking). Press the hole and 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. |
| ADSL 2+ | Connecter for accessing the Internet through ADSL2/2+. |
| LAN 4 – 1 | Connecter for local networked devices. |

## 1.2 Hardware Installation

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

1. Connect the DSL interface to the external ADSL splitter with an ADSL line cable.
2. Connect one port of 4-port switch to your computer with a RJ-45 cable. This device allows you to connect 4 PCs directly.
3. Connect one end of the power cord to the power port of this device. Connect the other end to the wall outlet of electricity.
4. Power on the router.
5. Check the **ACT** and **ADSL2+**, **LAN** LEDs to assure network connections.

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



# 2 Configuring Basic Settings

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

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

## 2.1 Changing Password

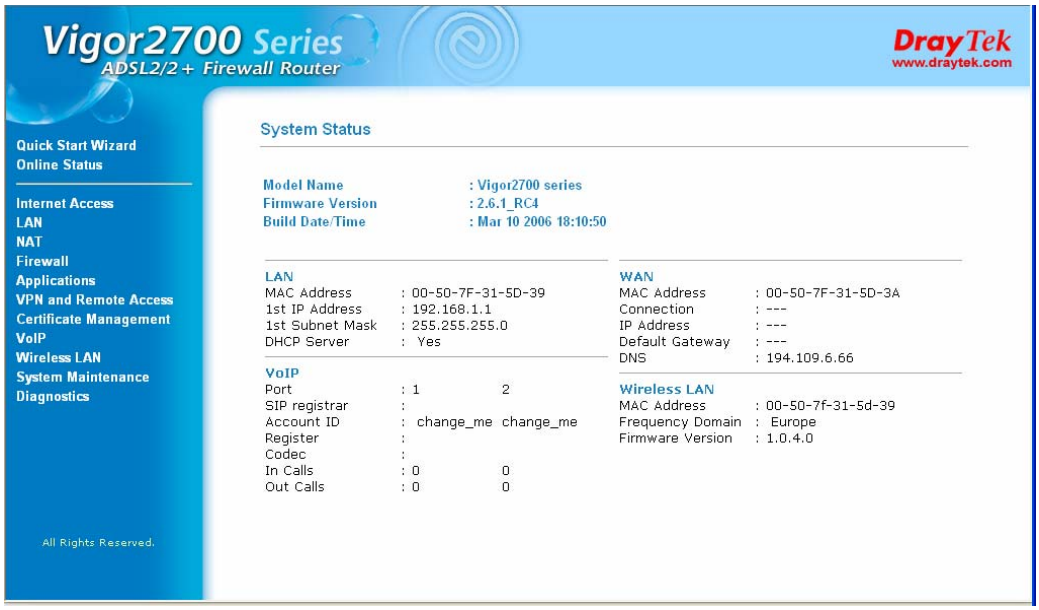
To change the password for this device, you have to access into the web browse with default password first.

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

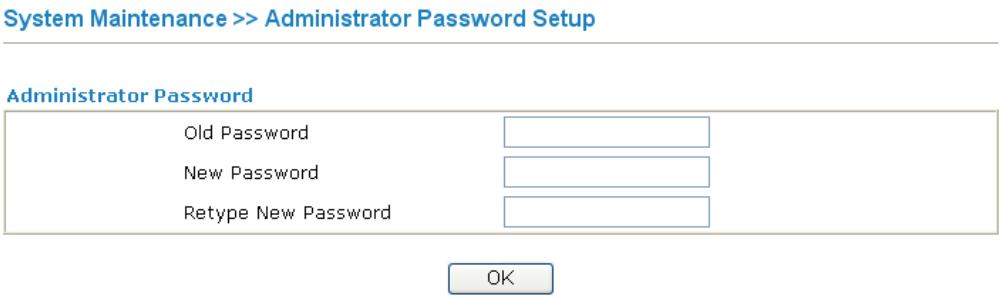
> Notice: You may either simply set up your computer to get IP dynamically from the router or set up the IP address of the computer to be the same subnet as **the default IP address of Vigor router 192.168.1.1**. For the detailed information, please refer to the later section - Trouble Shooting of this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

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


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




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

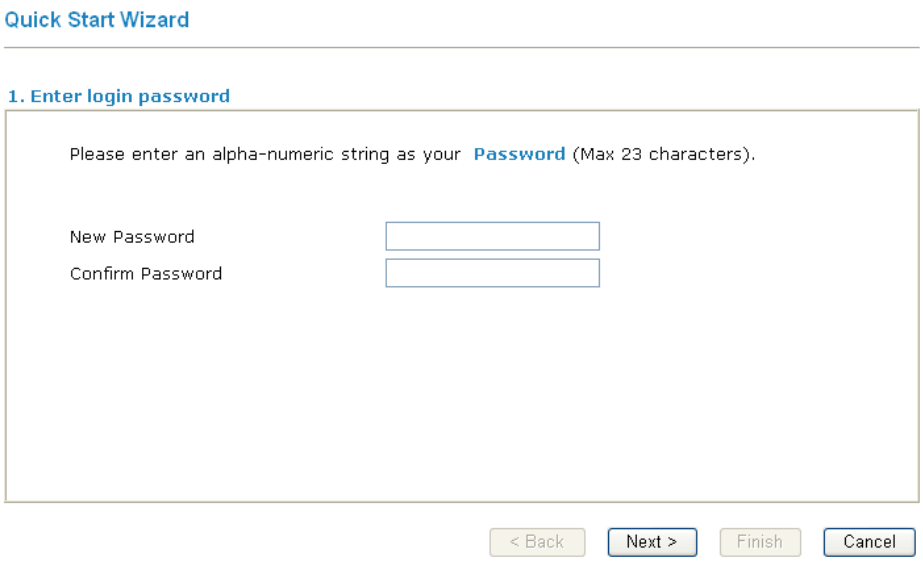



5. Enter the login password (the default is blank) on the field of **Old Password**. Type a new one in the field of **New Password** and retype it on the field of **Retype New Password**. Then click **OK** to continue.

6. Now, the password has been changed. Next time, use the new password to access the Web Configurator for this router.

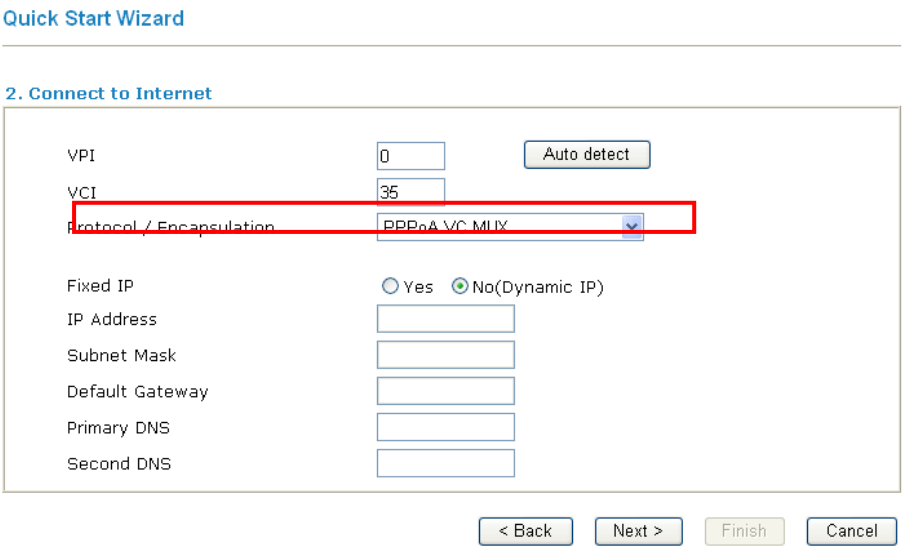
## 2.2 Quick Start Wizard

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




### 2.2.1 Adjusting Protocol/Encapsulation

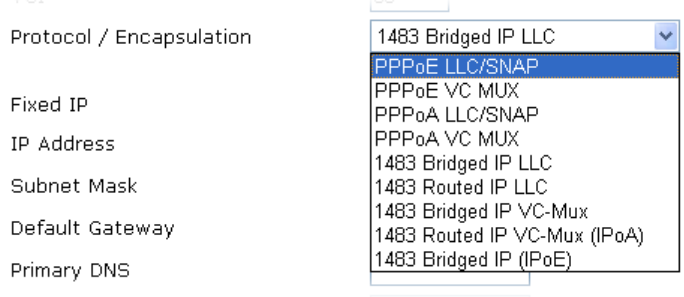
In the **Quick Start Wizard**, you can configure the router to access the Internet with different protocol/modes such as **PPPoE**, **PPPoA, Bridged IP, or Routed IP**. The router supports the Ethernet WAN interface for Internet access.




Now, you have to select an appropriate WAN connection type for connecting to the Internet through this router according to the settings that your ISP provided.

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

| | |
|---|---|
| **VCI** | Stands for **Virtual Channel Identifier.** It is a 16-bit field inside ATM cell's header that indicates the cell's next destination as it travels through the network. A virtual channel is a logical connection between two end devices on the network. |
| **Protocol/Encapsulation** | Select an IP mode for this WAN interface. There are several available modes for Internet access such as **PPPoE**, **PPPoA, Bridged IP** and **Routed IP**. |



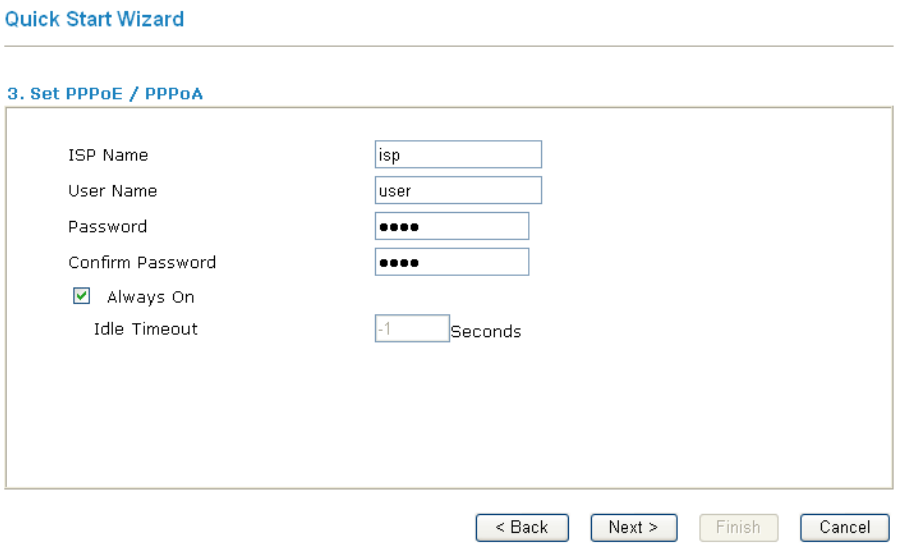

| | |
|---|---|
| **Fixed IP** | Click **Yes** to specify a fixed IP for the router. Otherwise, click **No (Dynamic IP)** to allow the router choosing a dynamic IP. If you choose **No**, the following IP Address, Subnet Mask and Default Gateway will not be changed. |
| **IP Address** | Assign an IP address for the protocol that you select. |
| **Subnet Mask** | Assign a subnet mask value for the protocol of **Routed IP** and **Bridged IP**. |
| **Default Gateway** | Assign an IP address to the gateway for the protocol of **Routed IP** and **Bridged IP**. |
| **Primary DNS** | Assign an IP address to the primary DNS. |
| **Second DNS** | Assign an IP address to the secondary DNS. |

## 2.2.2 PPPoE/PPPoA

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

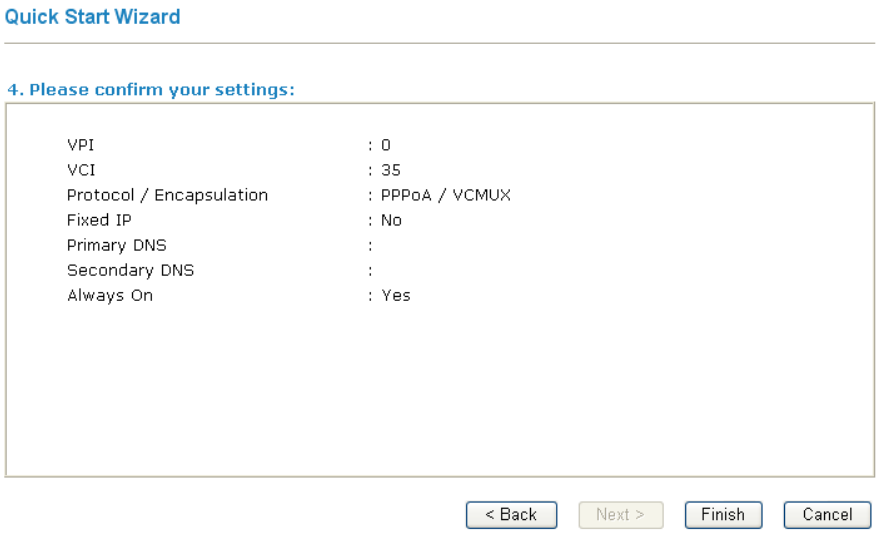
PPPoE or PPPoA is used for most of DSL modem users. All local users can share one PPPoE or PPPoA connection for accessing the Internet. Your service provider will provide you information about user name, password, and authentication mode.

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

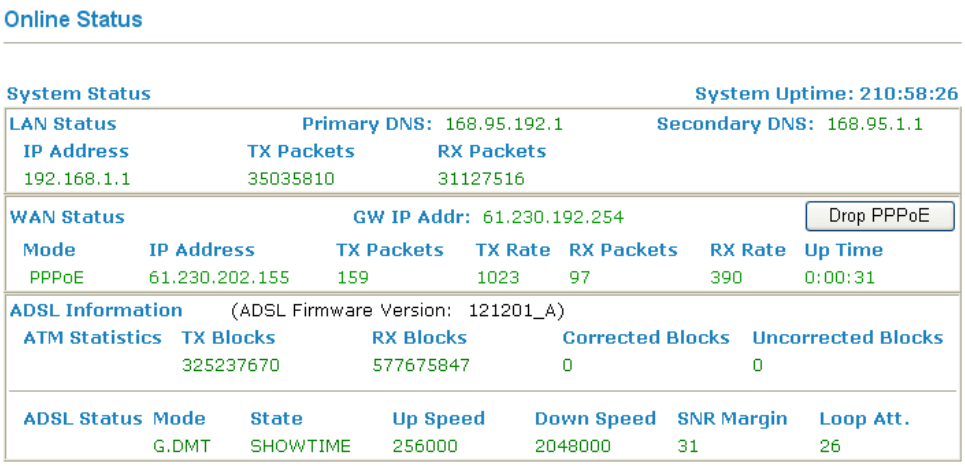



| | |
|---|---|
| **ISP Name** | Assign a specific name for ISP requirement. |
| **User Name** | Assign a specific valid user name provided by the ISP. |
| **Password** | Assign a valid password provided by the ISP. |
| **Confirm Password** | Retype the password. |
| **Always On** | Check this box to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

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

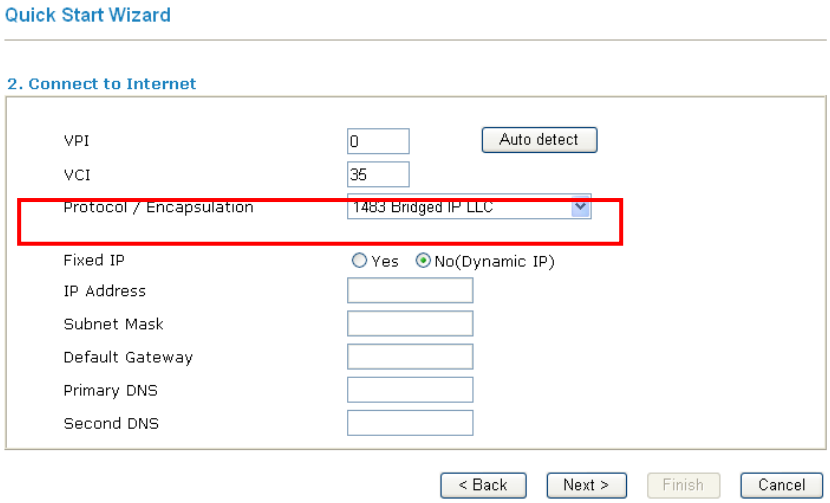


Click **Finish.** The online status of this protocol will be shown as below.

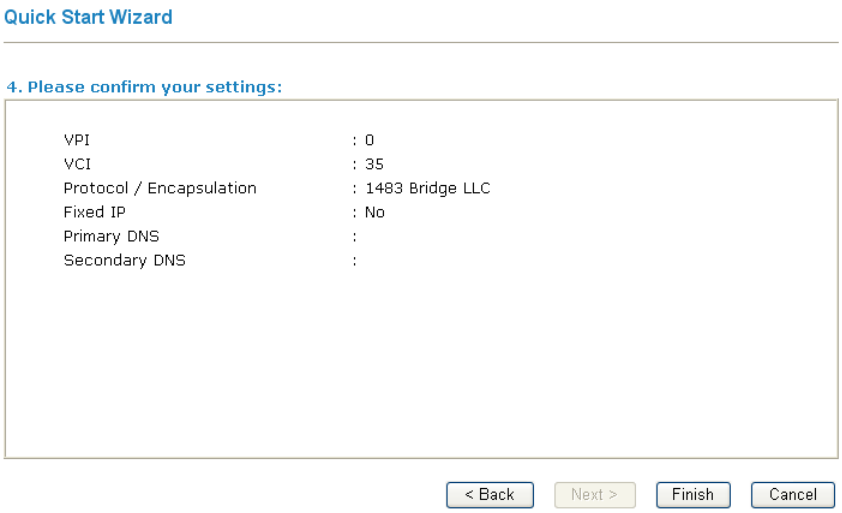



## 2.2.3 Bridged IP

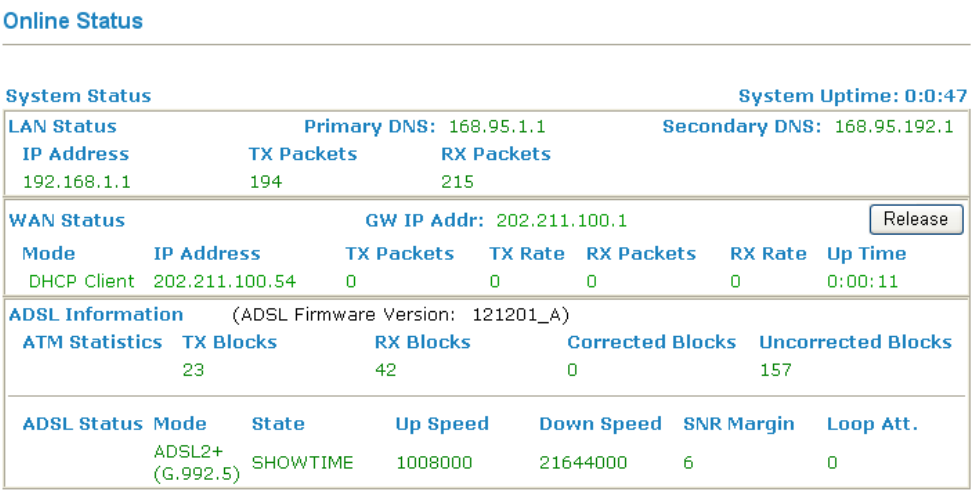
Click **1483 Bridged IP** as the protocol. Type in all the information that your ISP provides for this protocol.




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

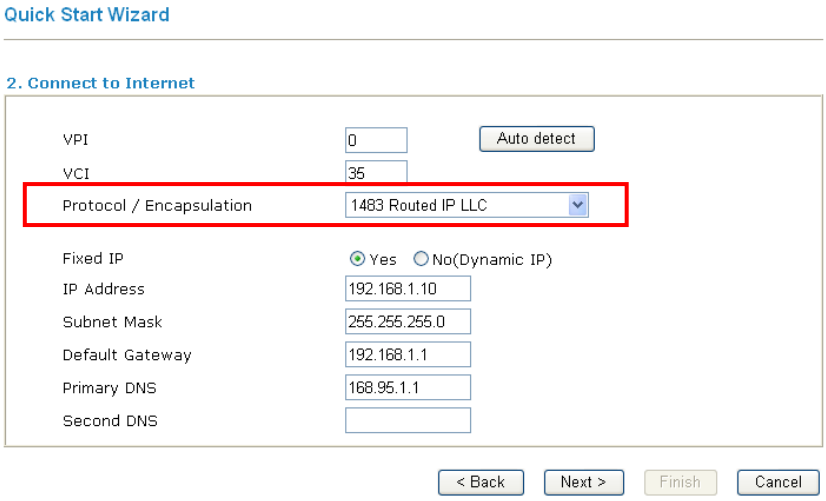


Click **Finish.** The online status of this protocol will be shown as below.

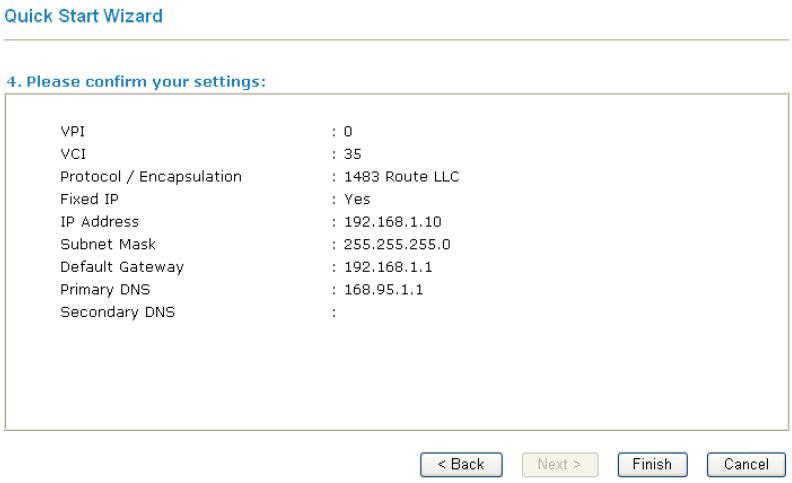



## 2.2.4 Routed IP

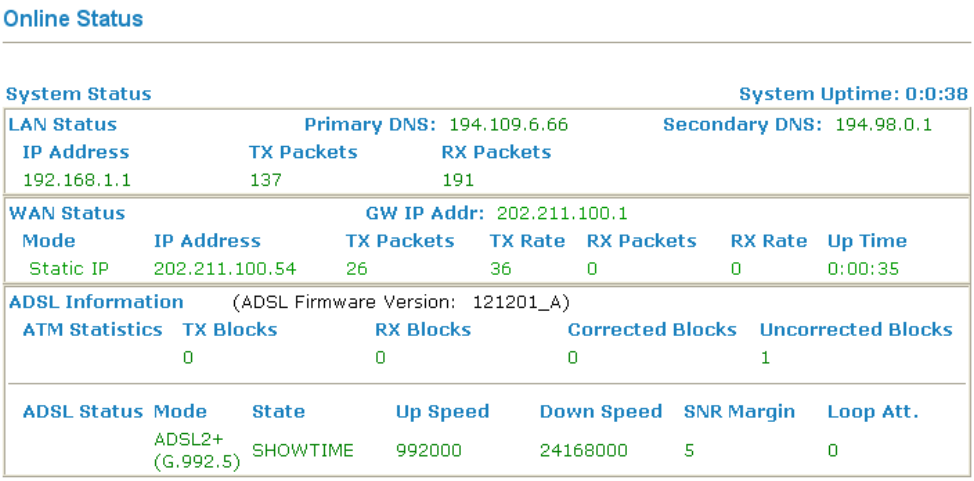
Click **1483 Routed IP** as the protocol. Type in all the information that your ISP provides for this protocol.




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



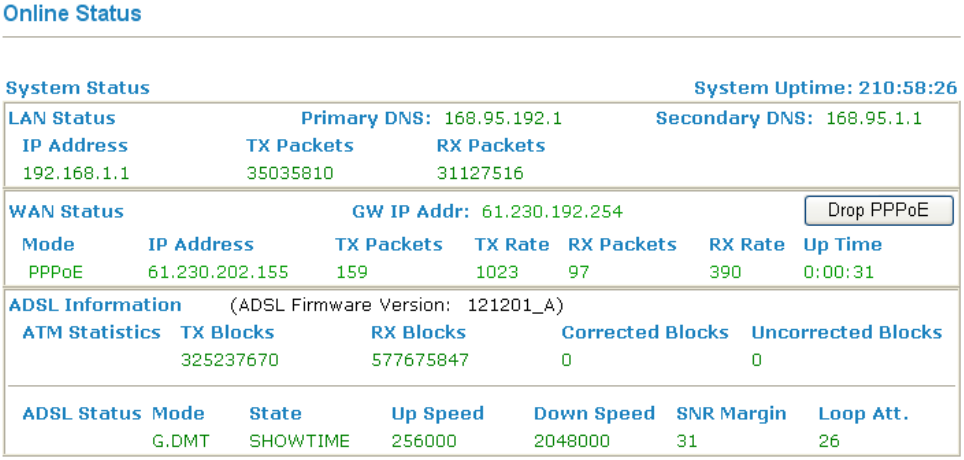
Click **Finish.** The online status of this protocol will be shown as below.




## 2.3 Online Status for Each Protocol

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

**Online status for PPPoA/PPPoE**



**Online status for Bridge**

Online Status

System Status — System Uptime: 0:0:47

LAN Status — Primary DNS: 168.95.1.1 — Secondary DNS: 168.95.192.1

| IP Address | TX Packets | RX Packets |
|---|---|---|
| 192.168.1.1 | 194 | 215 |

WAN Status — GW IP Addr: 202.211.100.1 — Release

| Mode | IP Address | TX Packets | TX Rate | RX Packets | RX Rate | Up Time |
|---|---|---|---|---|---|---|
| DHCP Client | 202.211.100.54 | 0 | 0 | 0 | 0 | 0:00:11 |

ADSL Information (ADSL Firmware Version: 121201_A)

| ATM Statistics | TX Blocks | RX Blocks | Corrected Blocks | Uncorrected Blocks |
|---|---|---|---|---|
| | 23 | 42 | 0 | 157 |

| ADSL Status | Mode | State | Up Speed | Down Speed | SNR Margin | Loop Att. |
|---|---|---|---|---|---|---|
| | ADSL2+ (G.992.5) | SHOWTIME | 1008000 | 21644000 | 6 | 0 |

**Online status for Routed IP**

Online Status

System Status — System Uptime: 0:0:38

LAN Status — Primary DNS: 194.109.6.66 — Secondary DNS: 194.98.0.1

| IP Address | TX Packets | RX Packets |
|---|---|---|
| 192.168.1.1 | 137 | 191 |

WAN Status — GW IP Addr: 202.211.100.1

| Mode | IP Address | TX Packets | TX Rate | RX Packets | RX Rate | Up Time |
|---|---|---|---|---|---|---|
| Static IP | 202.211.100.54 | 26 | 36 | 0 | 0 | 0:00:35 |

ADSL Information (ADSL Firmware Version: 121201_A)

| ATM Statistics | TX Blocks | RX Blocks | Corrected Blocks | Uncorrected Blocks |
|---|---|---|---|---|
| | 0 | 0 | 0 | 1 |

| ADSL Status | Mode | State | Up Speed | Down Speed | SNR Margin | Loop Att. |
|---|---|---|---|---|---|---|
| | ADSL2+ (G.992.5) | SHOWTIME | 992000 | 24168000 | 5 | 0 |

| | |
|---|---|
| **Primary DNS** | Displays the assigned IP address of the primary DNS. |
| **Secondary DNS** | Displays the assigned IP address of the secondary DNS. |
| **IP Address (in LAN)** | Displays the IP address of the LAN interface. |
| **TX Packets** | Displays the total transmitted packets at the LAN interface. |
| **RX Packets** | Displays the total number of received packets at the LAN interface. |
| **GW IP Addr:** | Displays the assigned IP address of the default gateway. |
| **IP Address (in WAN)** | Displays the IP address of the WAN interface. |
| **TX Rate** | Displays the speed of transmitted packets at the WAN interface. |
| **RX Rate** | Displays the speed of received packets at the WAN interface. |
| **Up Time** | Displays the total system uptime of the interface. |
| **TX Blocks** | Displays the total number of transmitted ATM Blocks. |
| **RX Blocks** | Displays the total number of received ATM Blocks. |
| **Corrected Blocks** | Displays the total l number of received ATM Blocks corrupted but corrected. |

| | |
|---|---|
| **Uncorrected Blocks** | Displays the total number of received ATM Blocks corrupted but uncorrected. |
| **Mode** | Displays the modulation mode used: G.DMT, G.Lite, or T1.413. |
| **State** | Displays the DSL line status. |
| **Up Speed** | Displays the upstream speed (bits/ second). |
| **Down Speed** | Displays the downstream speed (bits/ second). |
| **SNR Margin** | Displays the value of Signal Noise Ratio Margin (dB). The higher value has better signal quality. |
| **Loop Att.** | Displays the value of subscribed Loop Attenuation. |

## 2.4 Status Bar

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


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

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

# 3 Advanced Web Configuration

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

## 3.1 Internet Access

### 3.1.1 Basics of Internet Protocol (IP) Network

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

**From 10.0.0.0 to 10.255.255.255**
**From 172.16.0.0 to 172.31.255.255**
**From 192.168.0.0 to 192.168.255.255**

#### What are Public IP Address and Private IP Address

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

#### Get Your Public IP Address from ISP

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

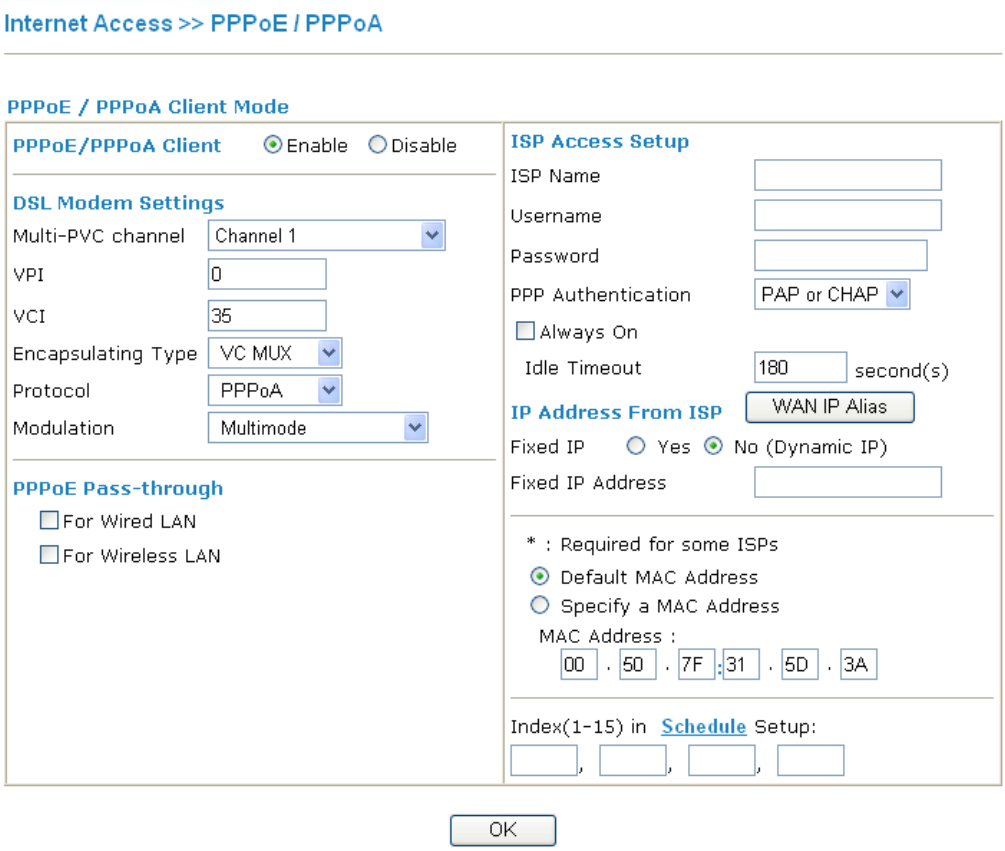
In ADSL deployment, the PPP (Point to Point)-style authentication and authorization is required for bridging customer premises equipment (CPE). Point to Point Protocol over Ethernet (PPPoE) connects a network of hosts via an access device to a remote access concentrator or aggregation concentrator. This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

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

## 3.1.2 PPPoE/PPPoA

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

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




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

**DSL Modem Settings** Set up the DSL parameters required by your ISP. These are vital for building DSL connection to your ISP.
**Multi-PVC channel** – The selections displayed here are determined by the page of **Internet Access** – **Multi PVCs**. **Select M-PVCs Channel** means no selection will be chosen.
**VPI** - Type in the value provided by ISP.
**VCI** - Type in the value provided by ISP.
**Encapsulating Type** - Drop down the list to choose the type provided by ISP.
**Protocol** - Drop down the list to choose the one provided by ISP.
If you have already used **Quick Start Wizard** to set the protocol, then it is not necessary for you to change any settings in this group.

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

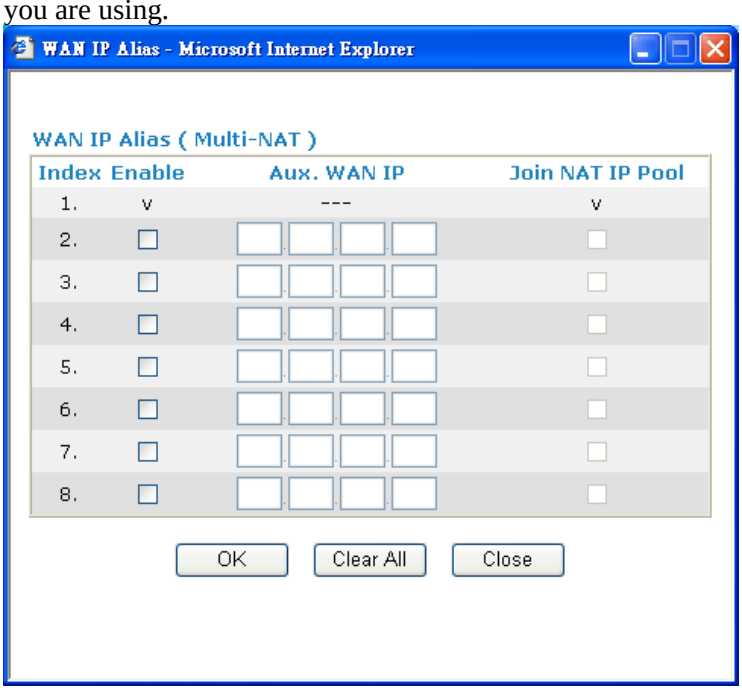
**For Wired LAN** – If you check this box, PCs on the same network can use another set of PPPoE session (different with the Host PC) to access into Internet.
**For Wireless LAN** – If you check this box, PCs on the same network through wireless connection can use another set of PPPoE session (different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

**ISP Access Setup**

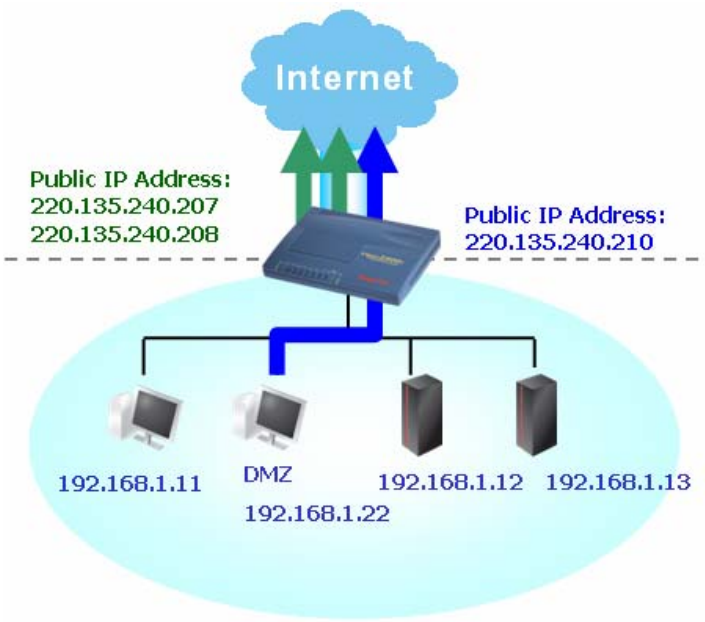
Enter your allocated username, password and authentication parameters according to the information provided by your ISP. If you want to connect to Internet all the time, you can check **Always On**.
**ISP Name** – Type in the ISP Name provided by ISP in this field.
**Username** – Type in the username provided by ISP in this field.
**Password** – Type in the password provided by ISP in this field.
**PPP Authentication** – Select **PAP only** or **PAP or CHAP** for PPP.
**Always On** – Check this box if you want the router keeping connecting to Internet forever.
**Idle Timeout** – Set the timeout for breaking down the Internet after passing through the time without any action.

**IP Address From ISP**

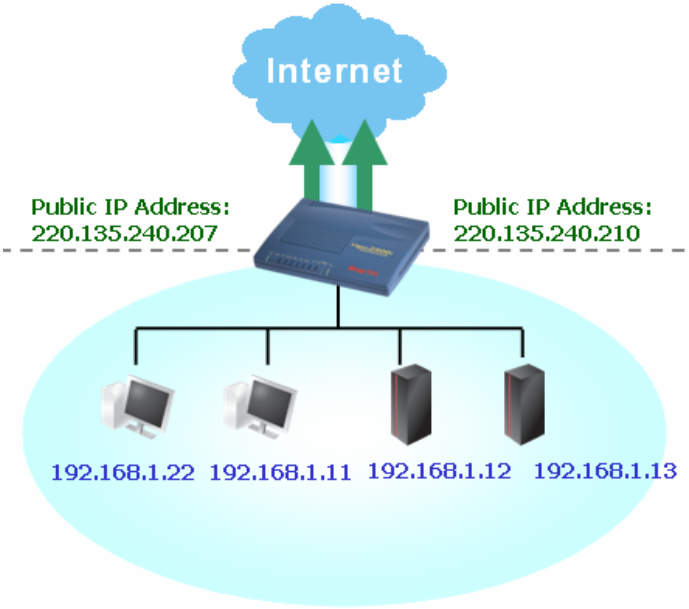
Usually ISP dynamically assigns IP address to you each time you connect to it and request. In some case, your ISP provides service to assign you the same IP address whenever you request. In this case, you can fill in this IP address in the Fixed IP field. Please contact your ISP before you want to use this function.
**Fixed IP** – Click **Yes** to use this function and type in a fixed IP address in the box.
**WAN IP Alias** - If you have multiple public IP addresses and would like to utilize them on the WAN interface, please use WAN IP Alias. You can set up to 8 public IP addresses other than the current one you are using.




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




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



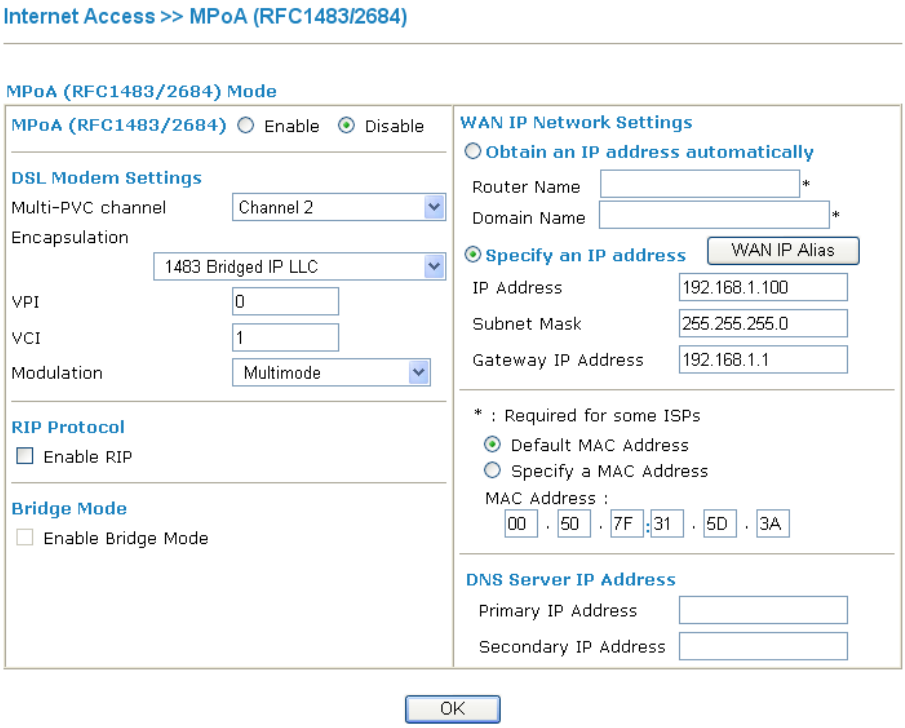

| | |
|---|---|
| **Default MAC Address** | Type in MAC address for the router. You can use **Default MAC Address** or specify another MAC address for your necessity.<br>MAC Address – Type in the MAC address for the router manually. |
| **Index (1-15) in Schedule Setup** | You can type in four sets of time schedule for your request. All the schedules can be set previously in **Application – Schedule** web page and you can use the number that you have set in that web page. |

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

### 3.1.3 MPoA

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

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




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

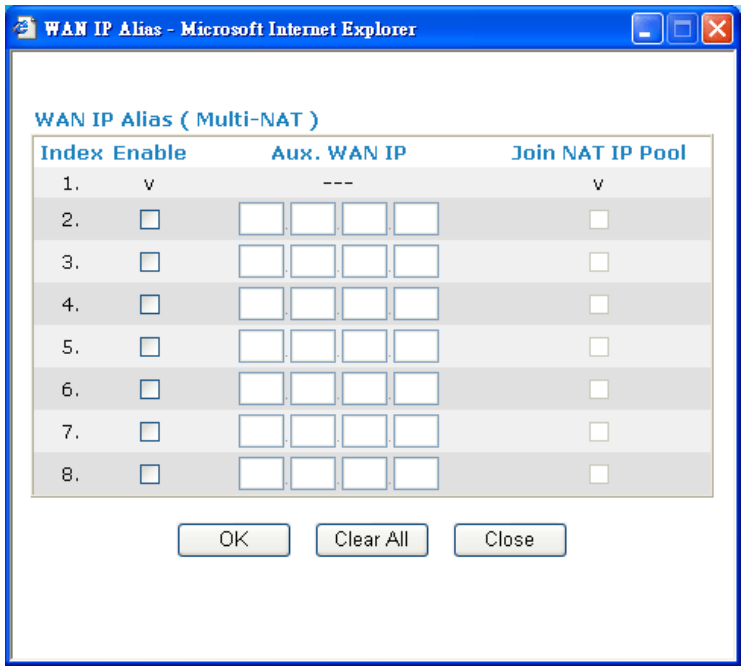
**DSL Modem Settings** Set up the DSL parameters required by your ISP. These are vital for building DSL connection to your ISP.
**Multi-PVC channel** - The selections displayed here are determined by the page of **Internet Access** – **Multi PVCs**. **Select M-PVCs Channel** means no selection will be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

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

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

**WAN IP Network Settings** This group allows you to obtain an IP address automatically and allows you type in IP address manually.

**Obtain an IP address automatically** – Click this button to obtain the IP address automatically.
**Router Name** – Type in the router name provided by ISP.
**Domain Name** – Type in the domain name that you have assigned.
**WAN IP Alias** - If you have multiple public IP addresses and would like to utilize them on the WAN interface, please use WAN IP Alias. You can set up to 8 public IP addresses other than the current one you are using.




**Specify an IP address** – Click this radio button to specify some data.
**IP Address** – Type in the private IP address.
**Subnet Mask** – Type in the subnet mask.
**Gateway IP Address** – Type in gateway IP address.

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

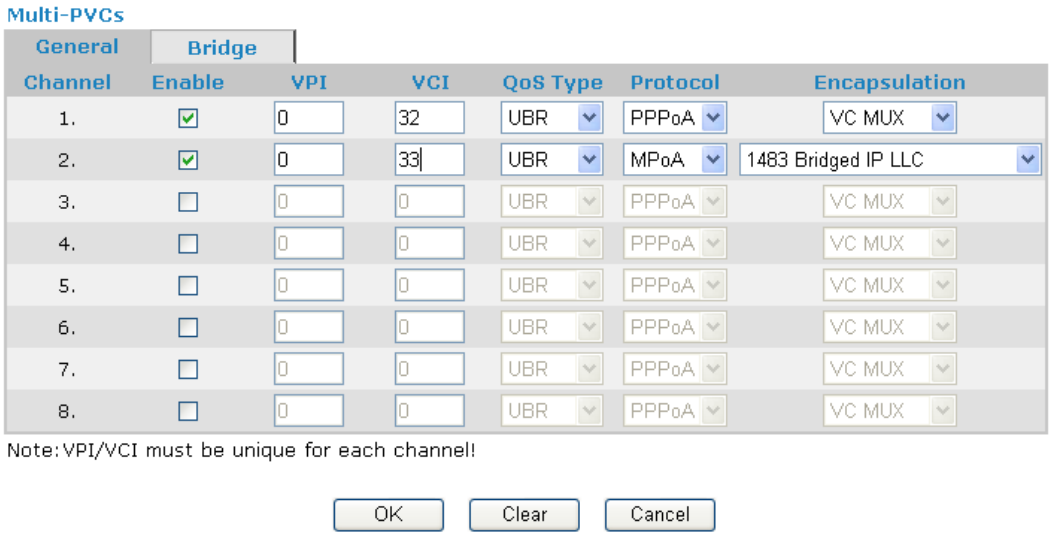
**DNS Server IP Address** — Type in the primary IP address for the router. If necessary, type in secondary IP address for necessity in the future.

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

## 3.1.4 Multi-PVCs

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

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

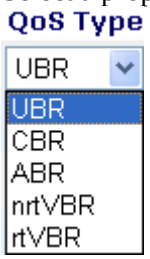



**Enable** Check this box to enable that channel. The channels that you enabled here will be shown in the **Multi-PVC channel** drop down list on the web page of **Internet Access**. Though you can enable eight channels in this page, yet only one channel can be chosen on the web page of **Internet Access**.

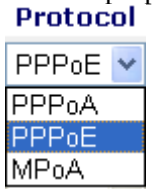
**VPI** Type in the value provided by your ISP.

**VCI** Type in the value provided by your ISP.

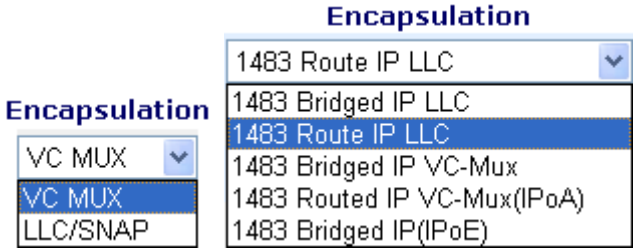
**QoS Type** Select a proper QoS type for the channel.



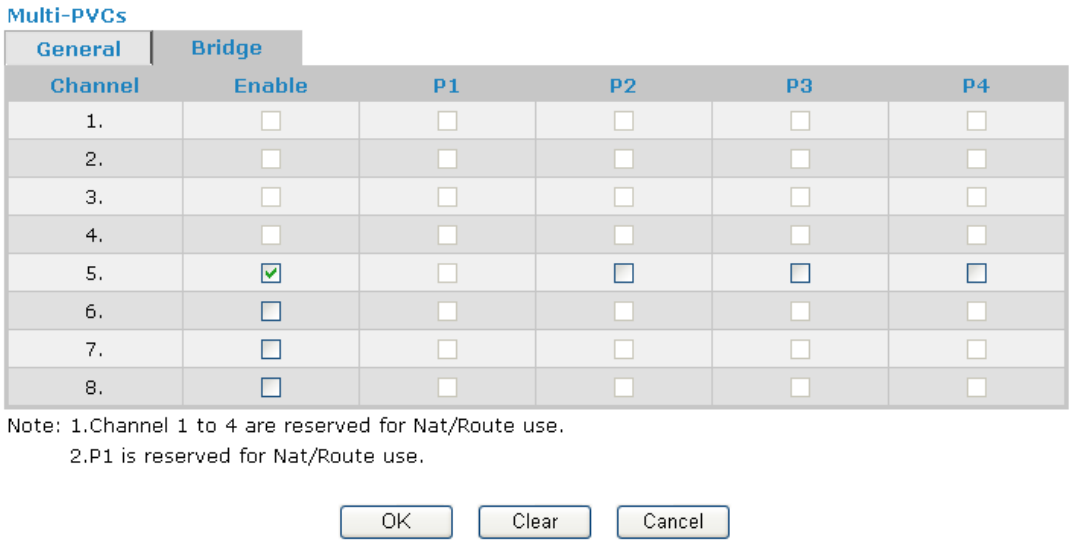

**Protocol** Select a proper protocol for this channel.



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




General page lets you set the first PVC. As to set the second PVC line, please click the **Bridge** tab to open Bridge configuration page.




**Enable** Check this box to enable that channel. Only channel 5 to 8 can be set in this page, for channel 1 to 4 are reserved for NAT using.

**P1 to P4** It means the LAN port 1 to 4. Check the box to designate the LAN port for channel 5 to 8.

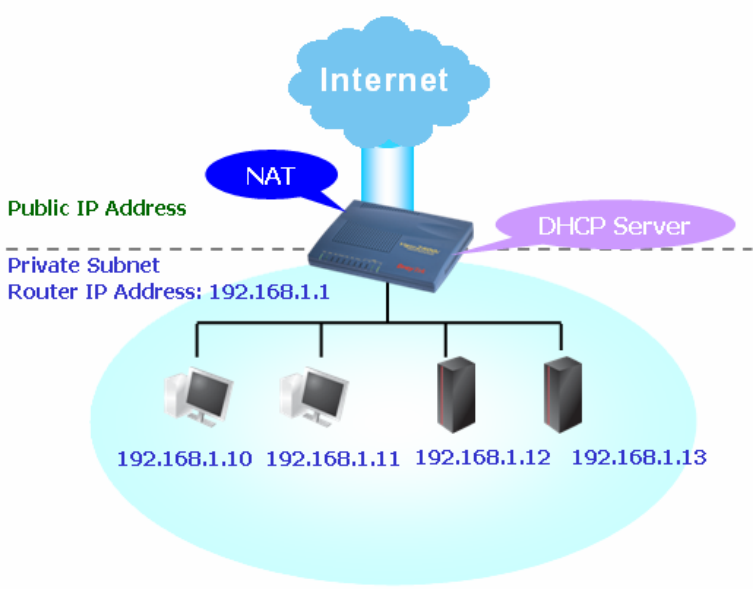
Click **Clear** to remove all the configurations in this page if you do not satisfy it. When you finish the configuration, please click **OK** to save and exit this page. Or click Cancel to abort the configuration and exit this page.

## 3.2 LAN

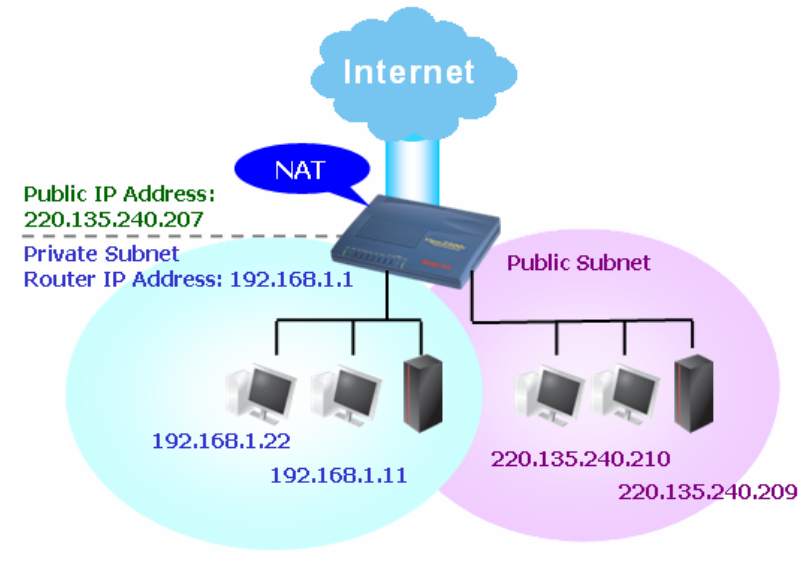
Local Area Network (LAN) is a group of subnets regulated and ruled by router. The design of network structure is related to what type of public IP addresses coming from your ISP.

### 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)

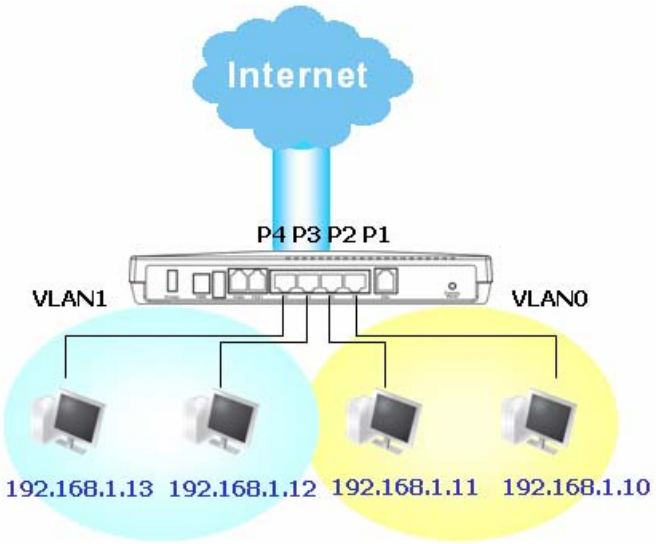
Vigor router will exchange routing information with neighboring routers using the RIP to accomplish IP routing. This allows users to change the information of the router such as IP address and the routers will automatically inform for each other.

### 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

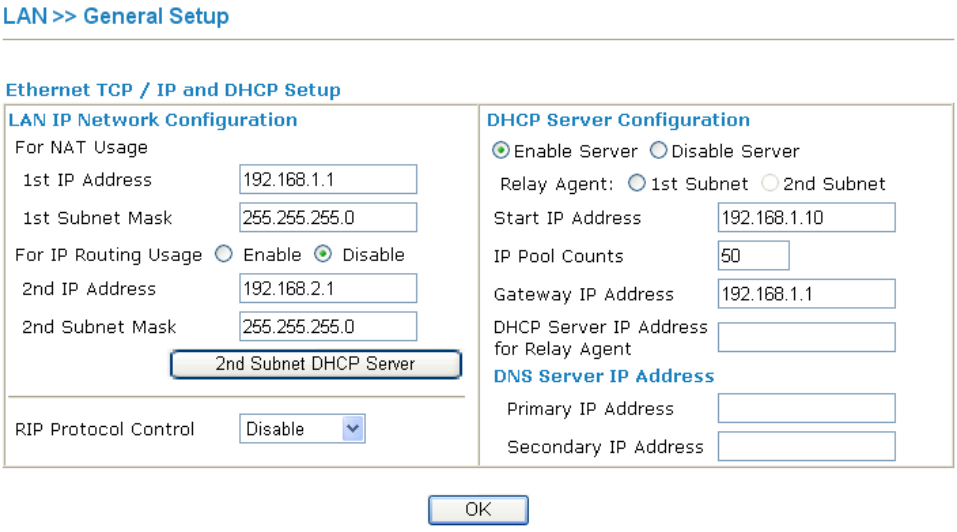
You can group local hosts by physical ports and create up to 4 virtual LANs. To manage the communication between different groups, please set up rules in Virtual LAN (VLAN) function and the rate of each.




## 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**.



**1st IP Address** Type in private IP address for connecting to a local private network (Default: 192.168.1.1).

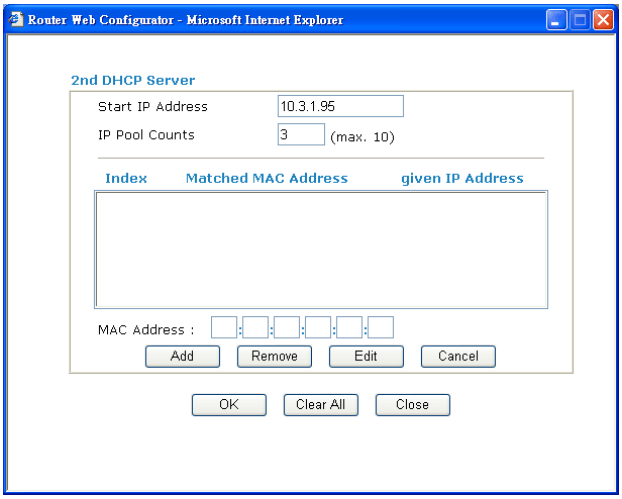
**1st Subnet Mask** Type in an address code that determines the size of the network. (Default: 255.255.255.0/ 24)

**For IP Routing Usage** Click **Enable** to invoke this function. The default setting is **Disable**.

**2nd IP Address** Type in secondary IP address for connecting to a subnet. (Default: 192.168.2.1/ 24)

**2nd Subnet Mask** An address code that determines the size of the network. (Default: 255.255.255.0/ 24)

**2nd DHCP Server** You can configure the router to serve as a DHCP server for the 2nd subnet.




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

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

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

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


**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.

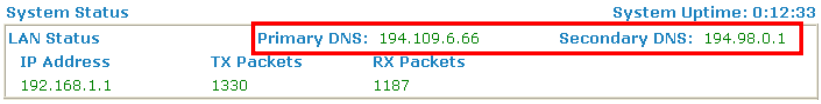
If you want to use another DHCP server in the network other than Vigor Router's, you can let Relay Agent help you to redirect the DHCP request to the specified location.
**Enable Server -** Let the router assign IP address to every host in the LAN.
**Disable Server –** Let you manually assign IP address 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.

**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:



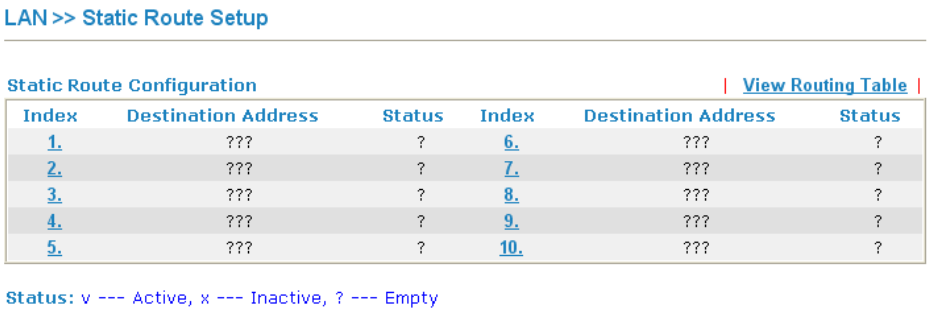
If both the Primary IP and Secondary IP Address fields are left empty, the router will assign its own IP address to local users as a DNS proxy server and maintain a DNS cache.

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**.

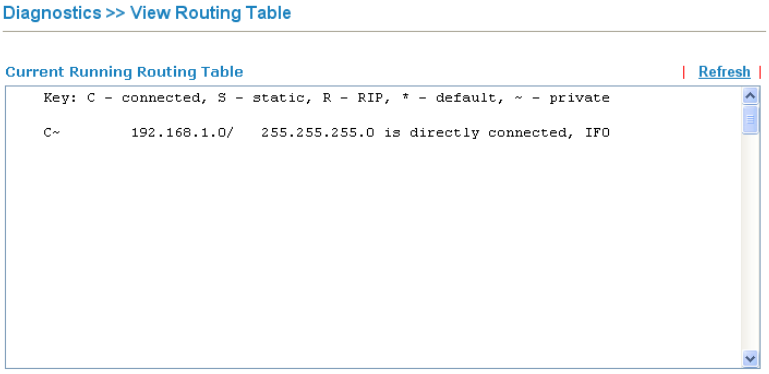



**Index** The number (1 to 10) under Index allows you to open next page to setup static route.

**Destination Address** Displays the destination address of the static route.

**Status** Displays the status of the static route.

**Viewing Routing Table** Displays the routing table for your reference.



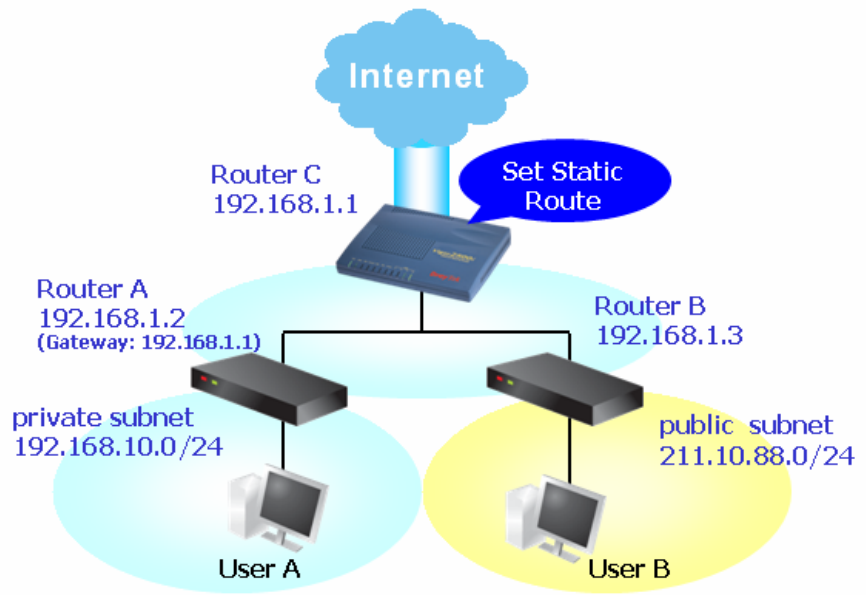

### Add Static Routes to Private and Public Networks

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

- use the Main Router to surf the Internet.
- create a private subnet 192.168.10.0 using an internal Router A (192.168.1.2)
- create a public subnet 211.100.88.0 via an internal Router B (192.168.1.3).

- have set Main Router 192.168.1.1 as the default gateway for the Router A 192.168.1.2.

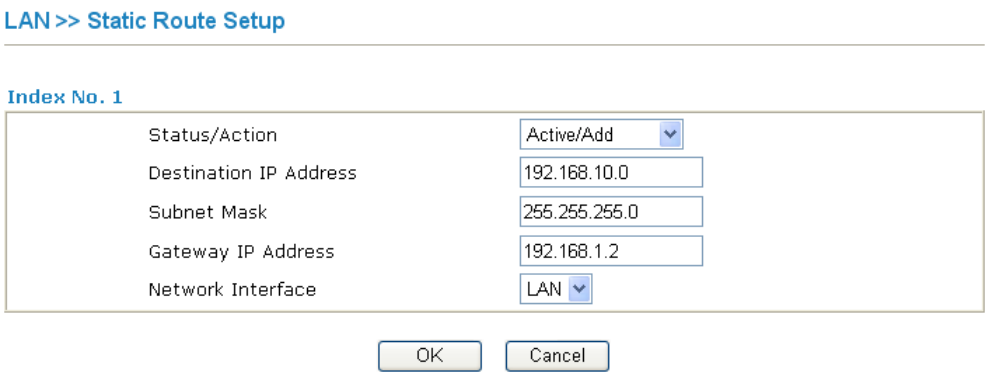
Before setting Static Route, user A cannot talk to user B for Router A can only forward recognized packets to its default gateway Main Router.



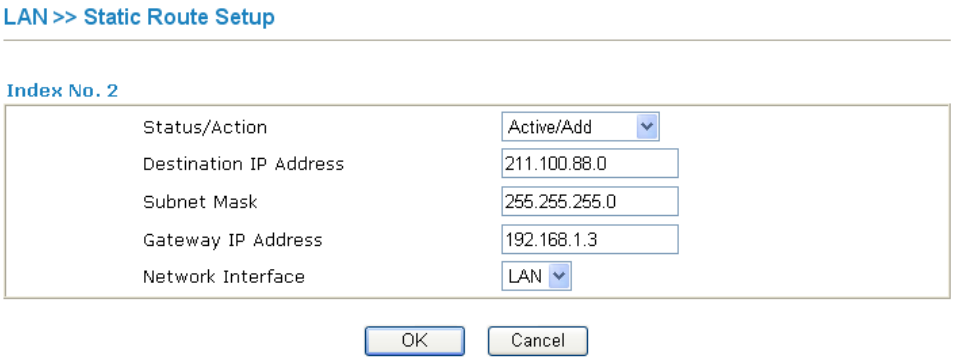

1. Go to **LAN** page and click **General Setup**, select 1st Subnet as the **RIP Protocol Control.** Then click the **OK** button.

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

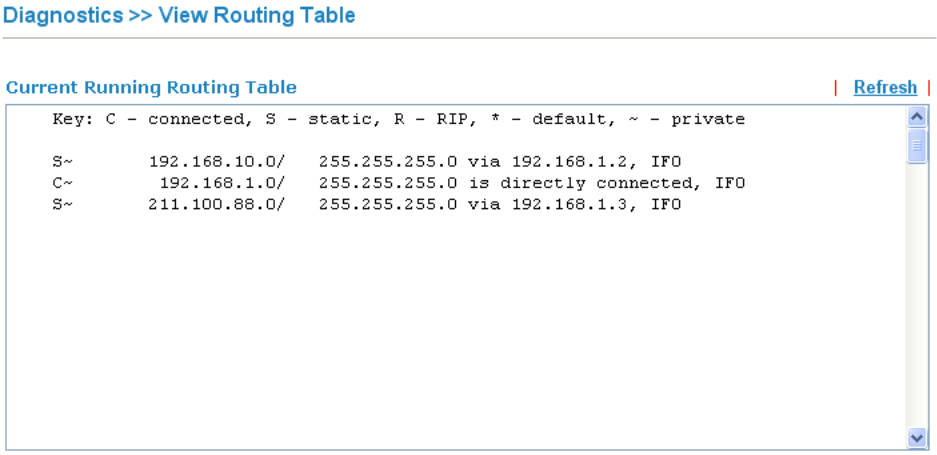
2. Click the **LAN - Static Route** and click on the **Index Number 1.** Please add a static route as shown below, which regulates all packets destined to 192.168.10.0 will be forwarded to 192.168.1.2. Click **OK**.




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

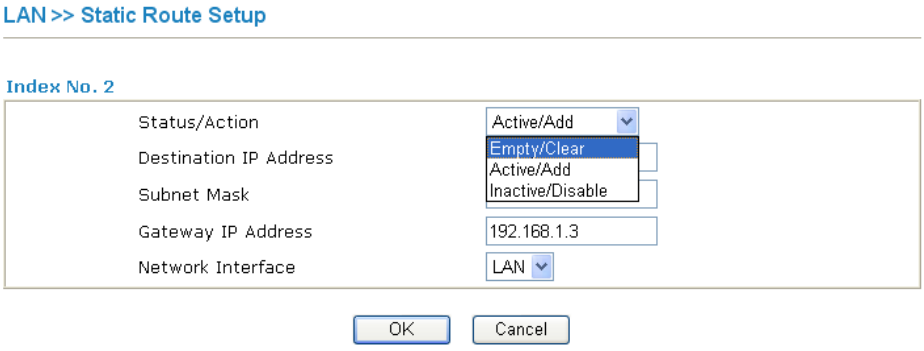



4. Go to **Diagnostics** and choose **Routing Table** to verify current routing table.



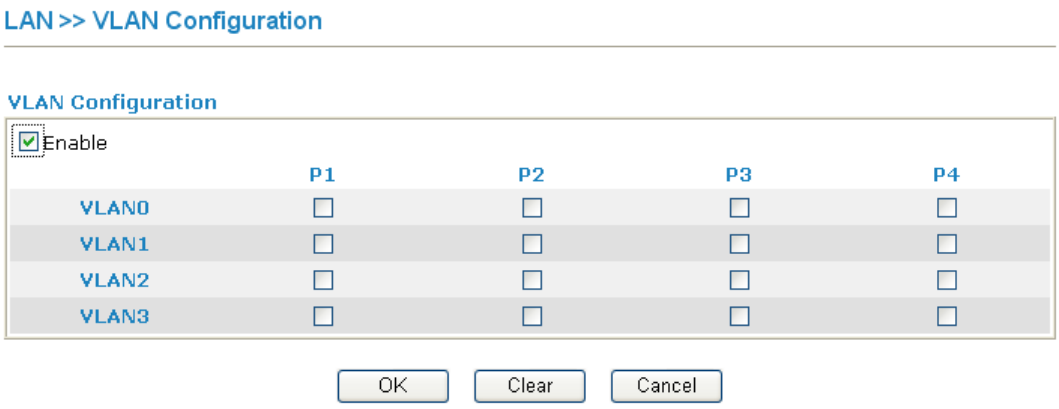

## Disable Static Route

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



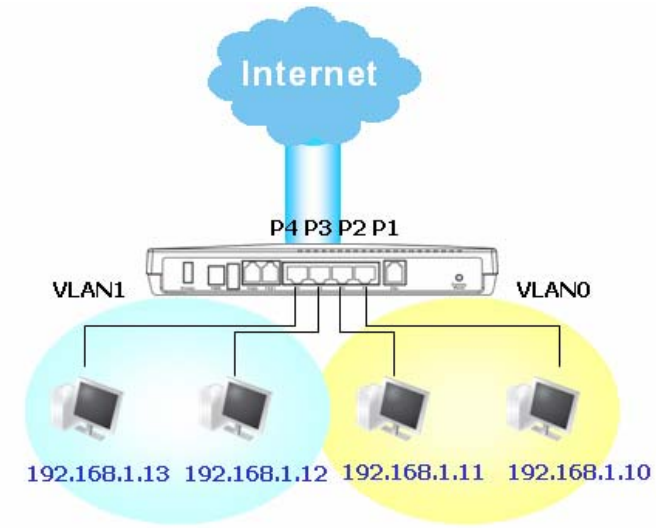
## 3.2.4 VLAN

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

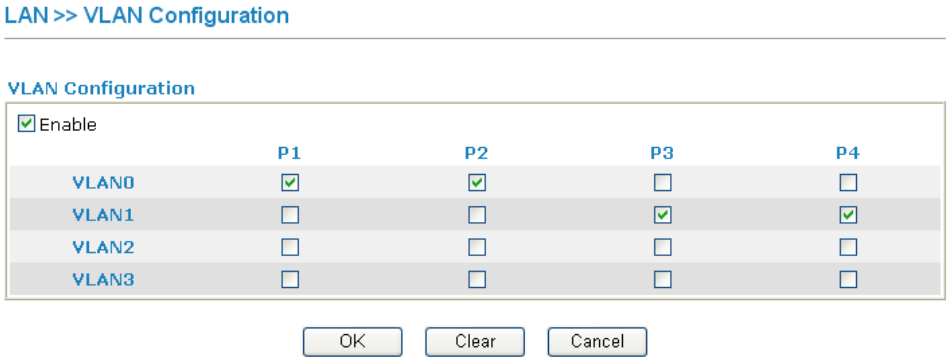



To add or remove a VLAN, please refer to the following example.

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




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




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

## 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.

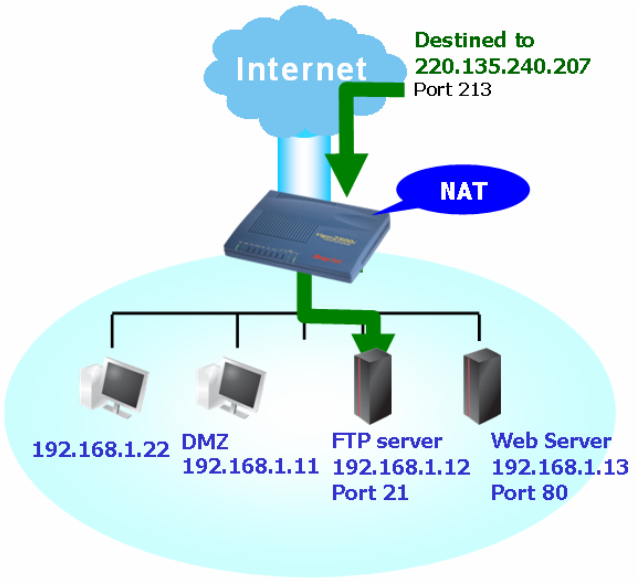
The benefit of the NAT includes:

- **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.

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.

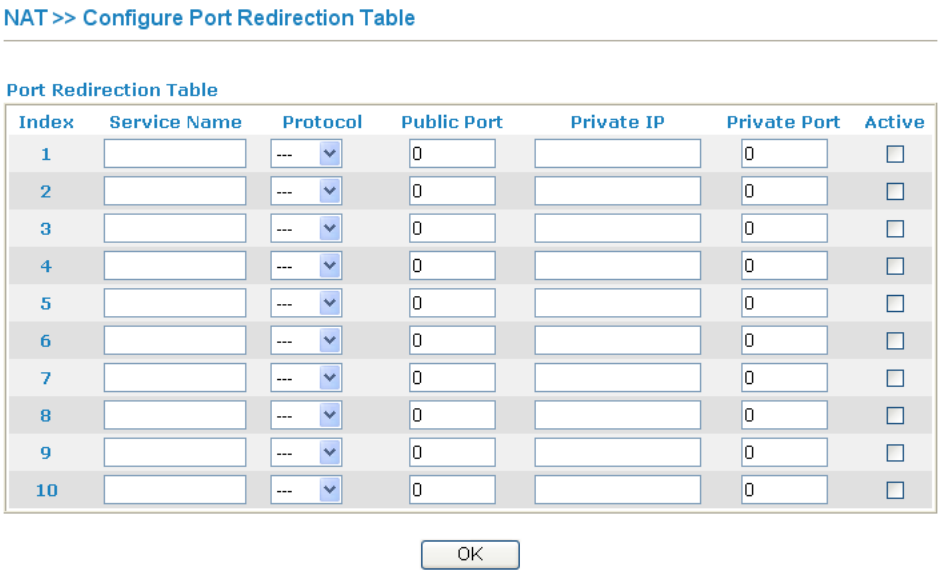
### 3.3.1 Port Redirection

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 10 port-mapping entries for the internal hosts.




**Service Name** Enter the description of the specific network service.

**Protocol** Select the transport layer protocol (TCP or UDP).

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

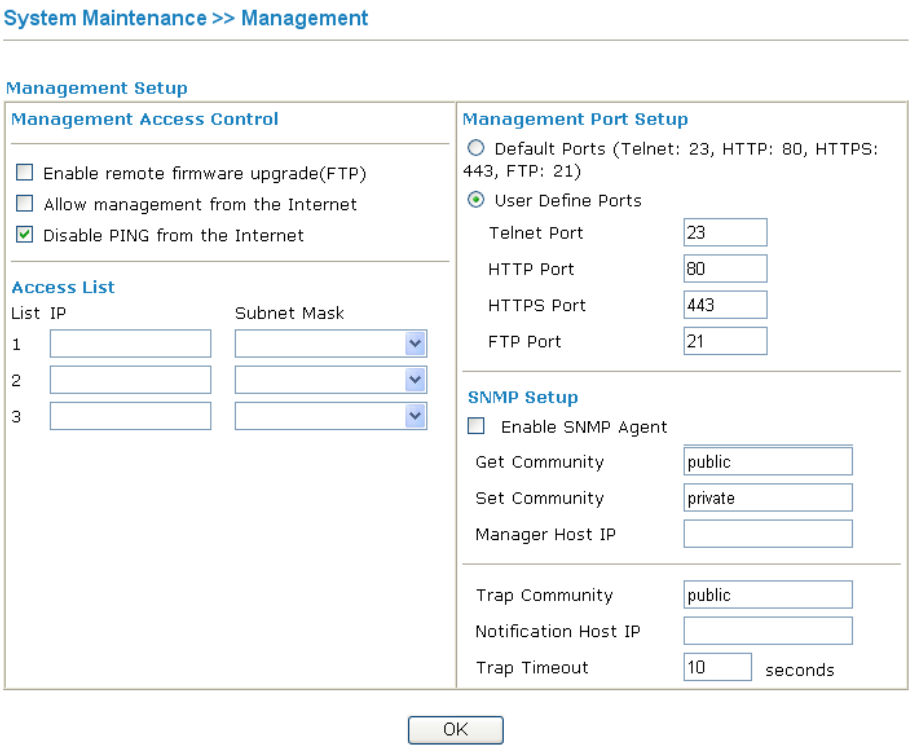
**Private IP** Specify the private IP address of the internal host providing the service.

**Private Port** Specify the private port number of the service offered by the internal host.

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

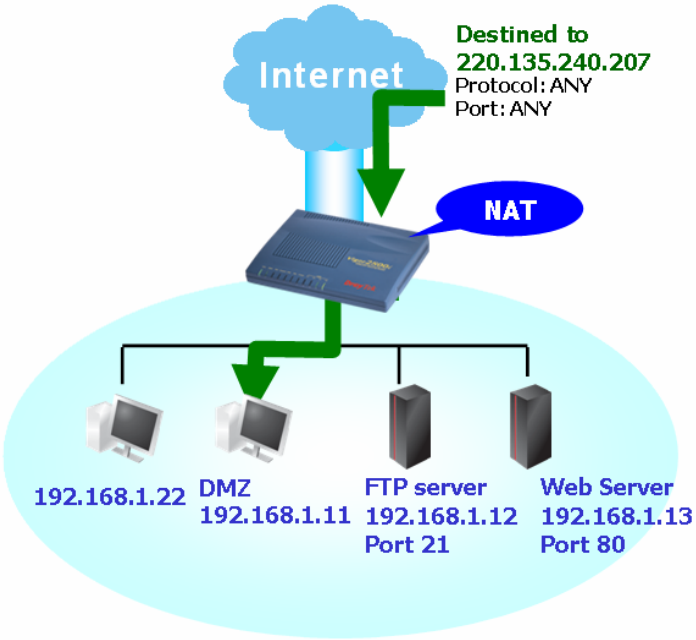
Note that the router has its own built-in services (servers) such as Telnet, HTTP and FTP etc. Since the common port numbers of these services (servers) are all the same, you may need to reset the router's in order to avoid confliction.

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



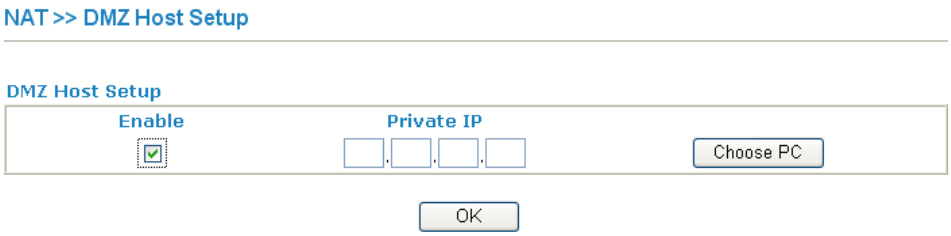

## 3.3.2 DMZ Host

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

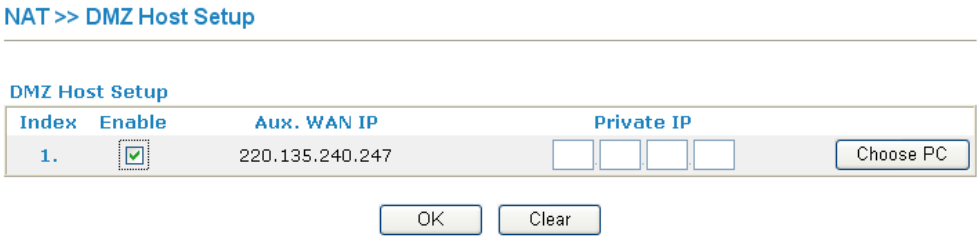


**Note:** The inherent security properties of NAT are somewhat bypassed if you set up DMZ host. We suggest you to add additional filter rules or a secondary firewall.

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



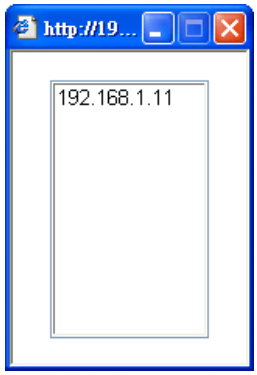

If you previously have set up **WAN Alias** in **Internet Access>>PPPoE/PPPoA** or **Internet Access>>MPoA,** you will find them in **Aux. WAN IP list** for your selection.



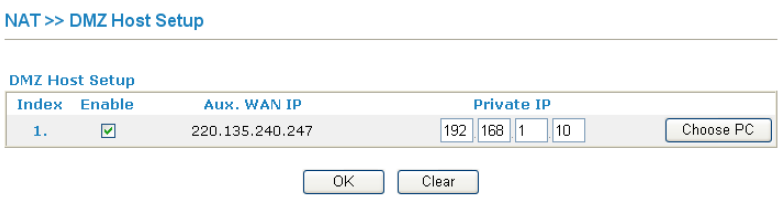

**Enable** Check to enable the DMZ Host function.

**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.



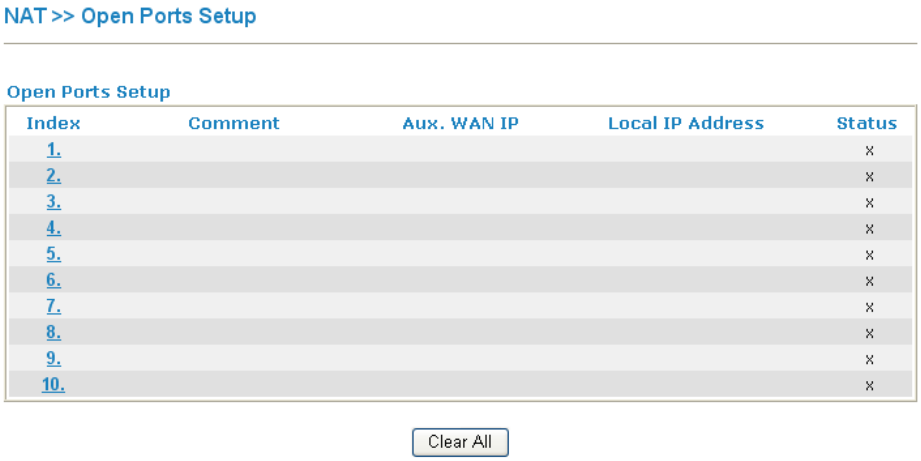

When you have selected one private IP from the above dialog, the IP address will be shown on the following screen. Click OK to save the setting.



## 3.3.3 Open Ports

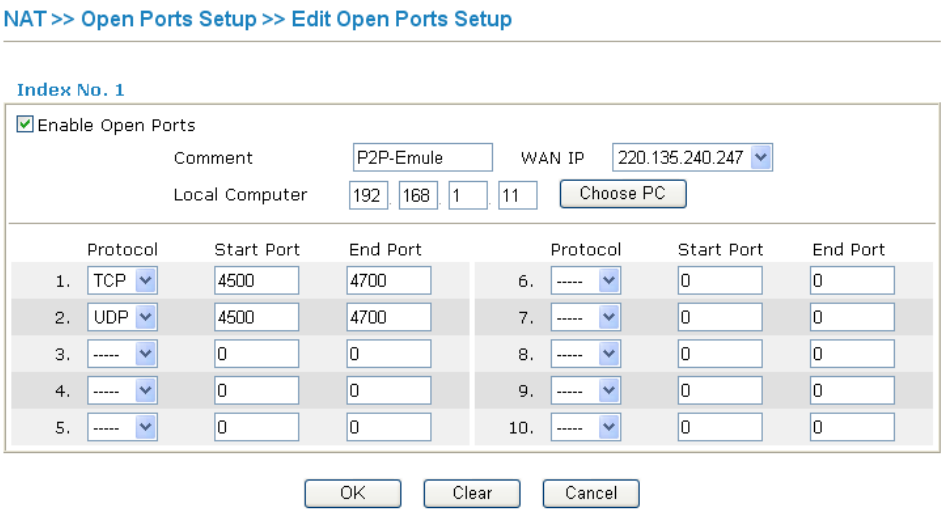
**Open Ports** allows you to open a range of ports for the traffic of special applications. Common application of Open Ports includes P2P application (e.g., BT, KaZaA, Gnutella, WinMX, eMule and others), Internet Camera etc. Ensure that you keep the application involved up-to-date to avoid falling victim to any security exploits.

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



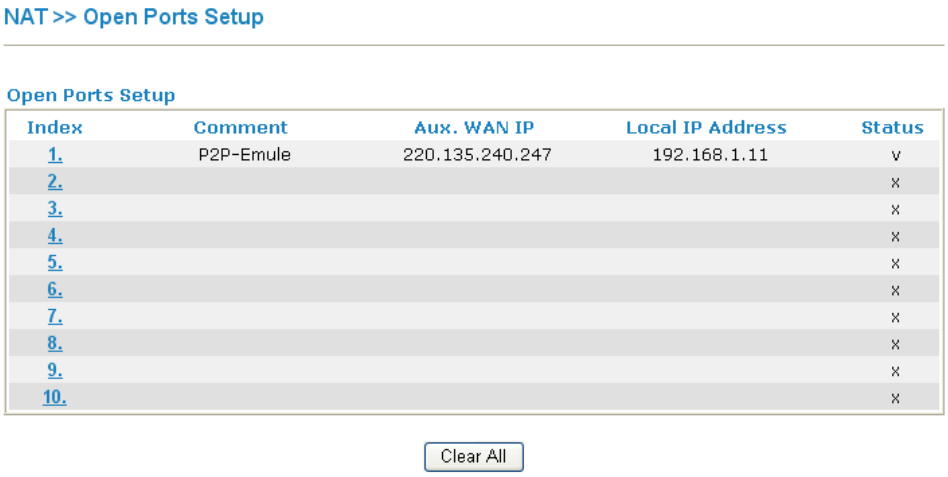

| | |
|---|---|
| **Index** | Indicate the relative number for the particular entry that you want to offer service in a local host. You should click the appropriate index number to edit or clear the corresponding entry. |
| **Comment** | Specify the name for the defined network service. |
| **Aux. WAN IP** | Display the private IP address of the local host that you specify in WAN Alias. This field will not appear if you did not specify any WAN IP in the WAN Alias page. |
| **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.



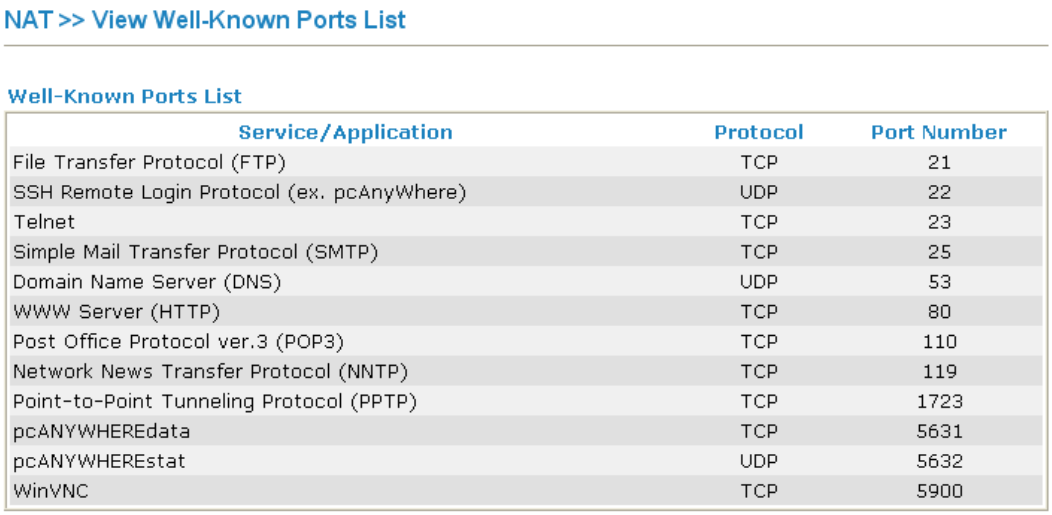
However, if you previously have set up **WAN Alias** in **Internet Access>>PPPoE/PPPoA** or **Internet Access>>MPoA**, you will find that **WAN IP** appeared for your selection.

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



### 3.3.4 Well-Known Ports List

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



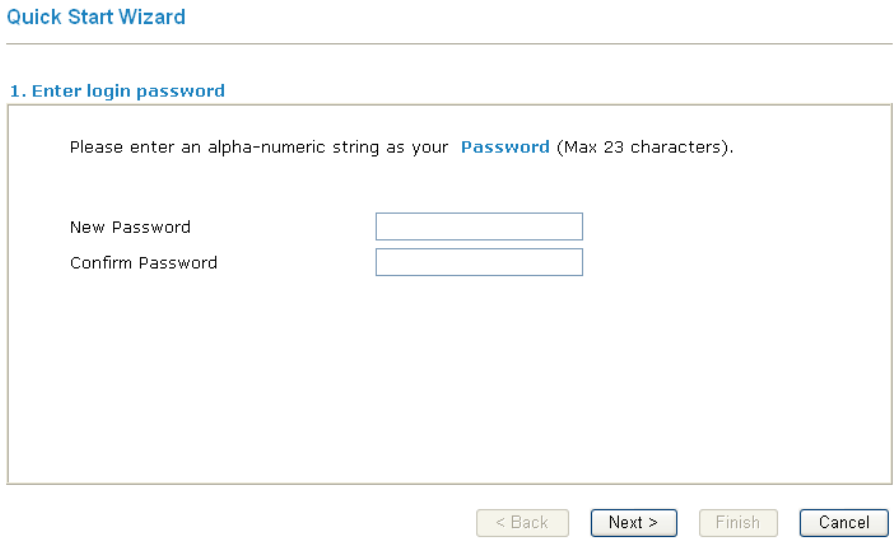

| Service/Application | Protocol | Port Number |
|---|---|---|
| File Transfer Protocol (FTP) | TCP | 21 |
| SSH Remote Login Protocol (ex. pcAnyWhere) | UDP | 22 |
| Telnet | TCP | 23 |
| Simple Mail Transfer Protocol (SMTP) | TCP | 25 |
| Domain Name Server (DNS) | UDP | 53 |
| WWW Server (HTTP) |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

## 3.4 Firewall

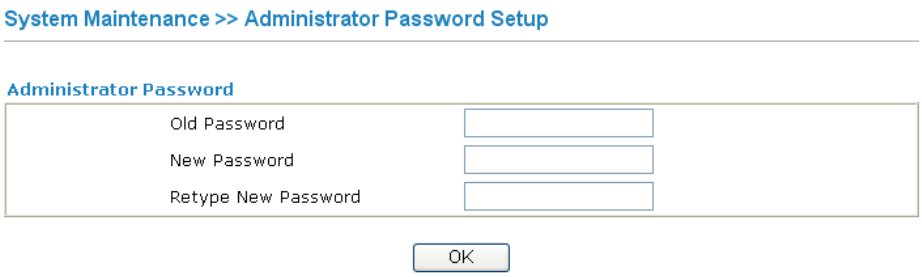
### 3.4.1 Basics for Firewall

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

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




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




## Firewall Facilities

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

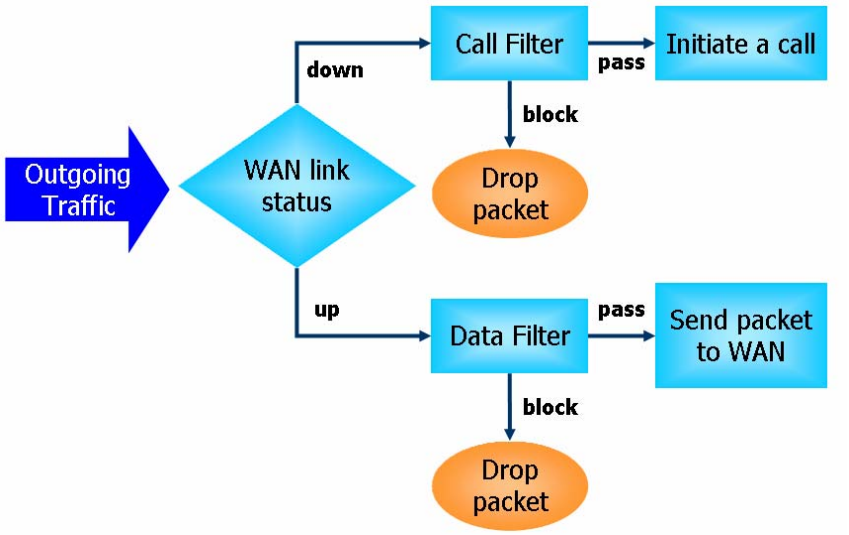
- User-configurable IP filter (Call Filter/ Data Filter).
- Stateful Packet Inspection (SPI): tracks packets and denies unsolicited incoming data
- Selectable Denial of Service (DoS) /Distributed DoS (DDoS) attacks protection
- URL Content Filter

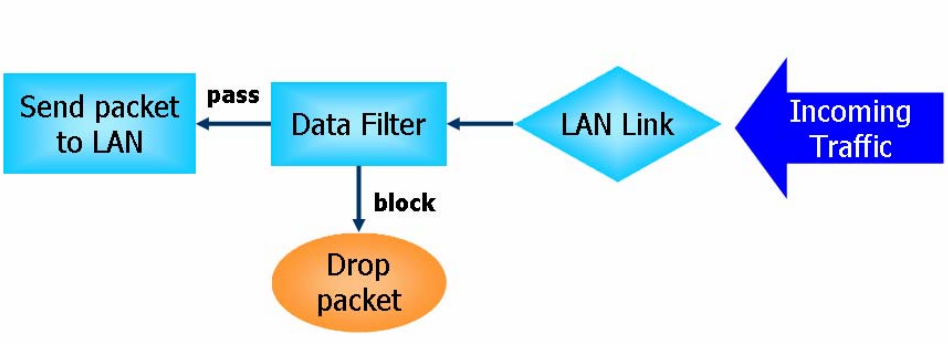
## IP Filters

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.

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

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

## Denial of Service (DoS) Defense

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

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

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

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

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

### Content Filtering

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

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

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

### Web Filtering

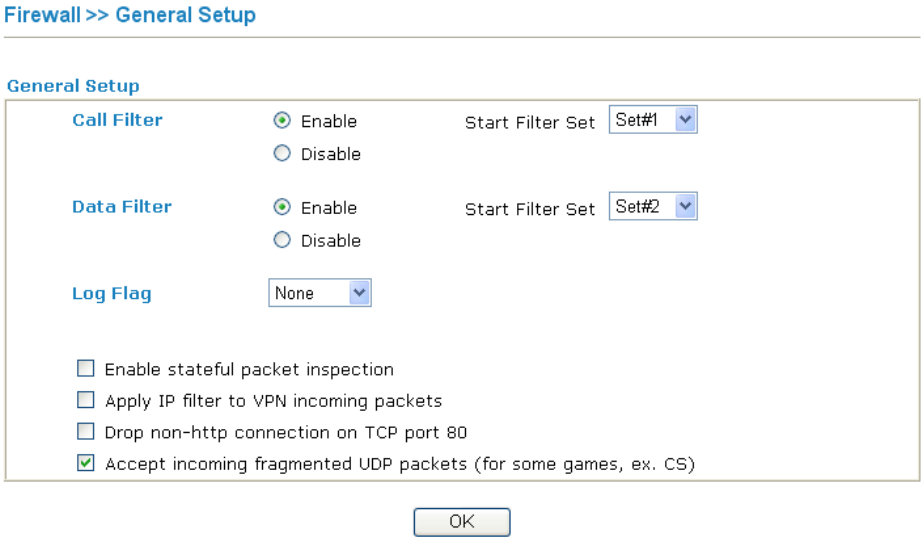
We all know that the content on the Internet just like other types of media may be inappropriate sometimes. As a responsible parent or employer, you should protect those in your trust against the hazards. With Web filtering service of the Vigor router, you can protect your business from common primary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

Once you have activated your Web Filtering service in Vigor router and chosen the categories of website you wish to restrict, each URL address requested (e.g.www.bbc.co.uk) will be checked against our server database, powered by SurfControl. The database covering over 70 languages and 200 countries, over 1 billion Web pages divided into 40 easy-to-understand categories. 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.

## 3.4.2 General Setup

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

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




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

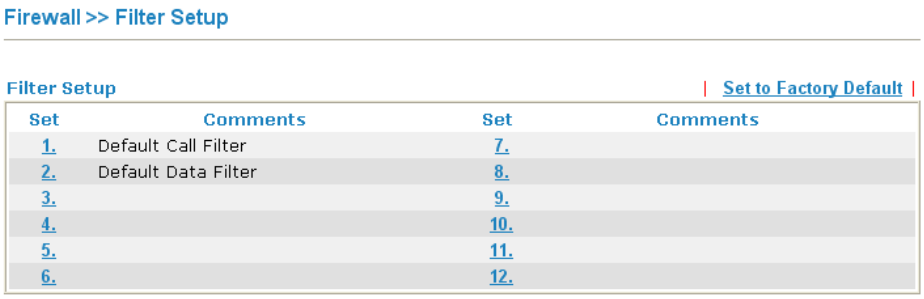
**Data Filter** Check **Enable** to activate the Data Filter function. Assign a start filter set for the Data Filter.

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

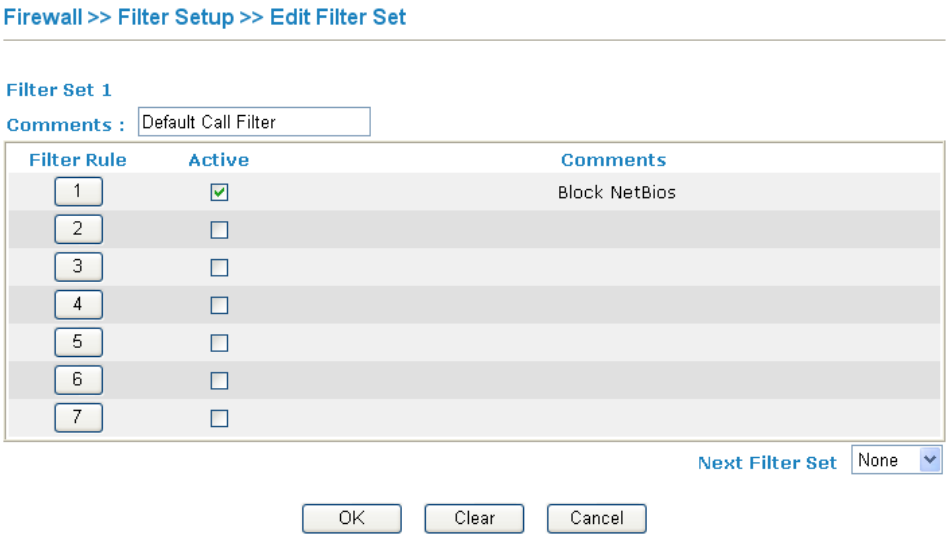
Some on-line games (for example: Half Life) will use lots of fragmented UDP packets to transfer game data. Instinctively as a secure firewall, Vigor router will reject these fragmented packets to prevent attack unless you enable **Accept Incoming Fragmented UDP Packets**. By checking this box, you can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

## 3.4.3 Filter Setup

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




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.



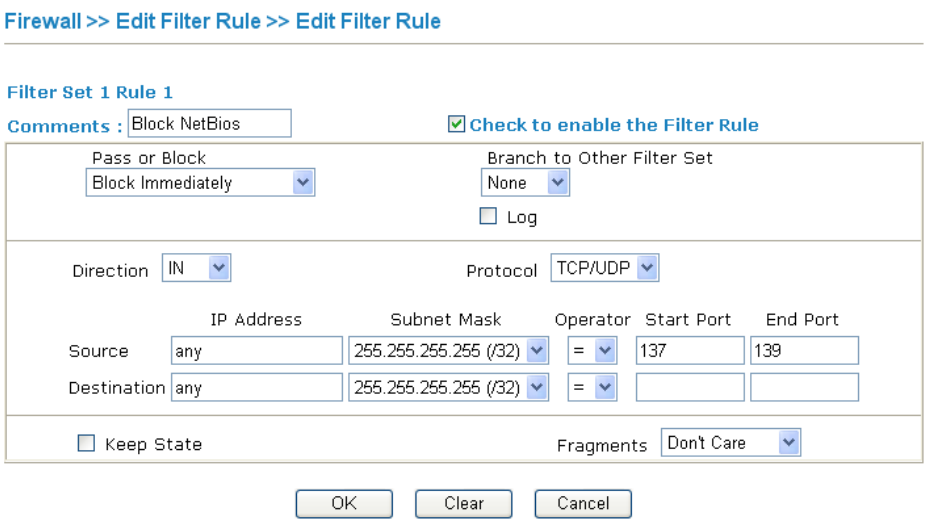

**Filter Rule** — Click a button numbered (1 ~ 7) to edit the filter rule. Click the button will open Edit Filter Rule web page. For the detailed information, refer to the following page.

**Active** — Enable or disable the filter rule.

**Comment** — Enter filter set comments/description. Maximum length is 23–character long

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

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




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

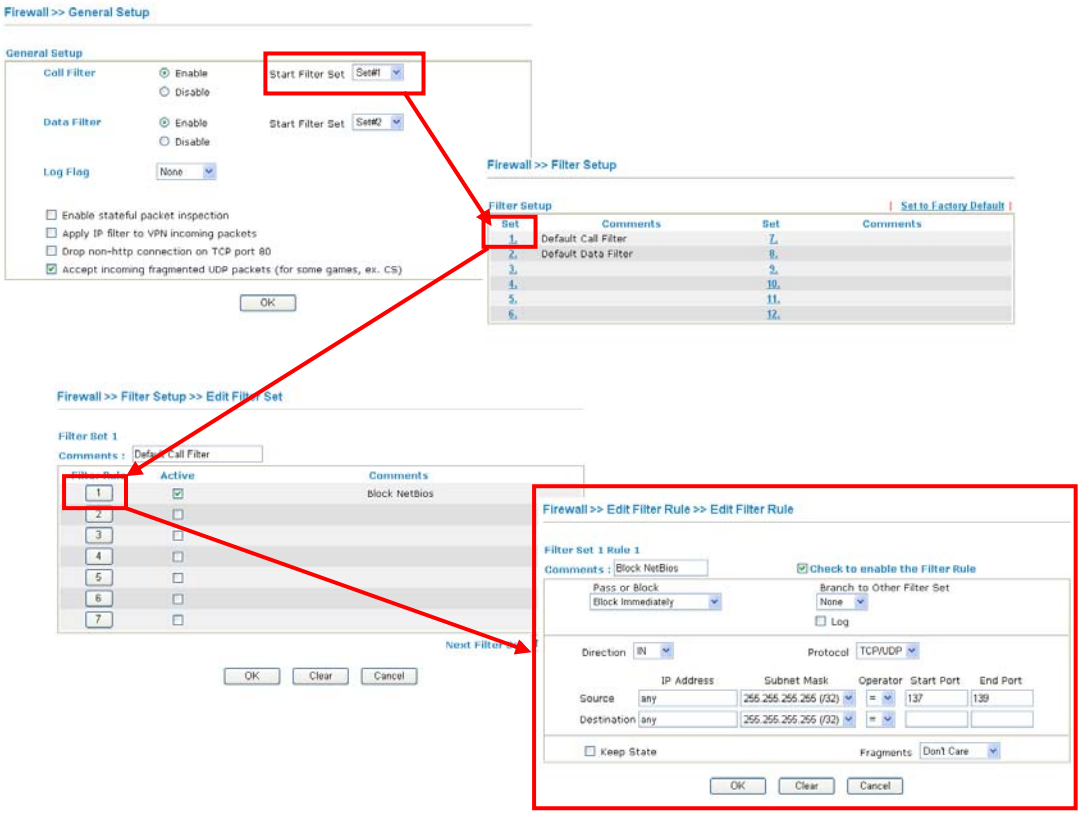
**Check to enable the Filter Rule** — Check this box to enable the filter rule.

**Pass or Block** — Specifies the action to be taken when packets match the rule.
**Pass Immediately** - Packets matching the rule will be passed immediately.
**Block Immediately** - Packets matching the rule will be dropped immediately.

| | |
|---|---|
| | **Pass If No Further Match -** A packet matching the rule, and that does not match further rules, will be passed through.<br>**Block If No Further Match -** A packet matching the rule, and that does not match further rules, will be dropped. |
| **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. |
| **Log** | Check this box to enable the log function. Use the Telnet command ***log-f*** to view the logs. |
| **Direction** | Set the direction of packet flow. It is for **Data Filter** only. For the **Call Filter**, this setting is not available since **Call Filter** is only applied to outgoing traffic. |
| **Protocol** | Specify the protocol(s) which this filter rule will apply to. |
| **IP Address** | Specify the source and destination IP addresses for this filter rule to apply to. Place the symbol "!" before a specific IP Address will prevent this rule from being applied to that IP address. To apply the rule to all IP address, enter **any** or leave the field blank. |
| **Subnet Mask** | Select the **Subnet Mask** for the IP Address column for this filter rule to apply from the drop-down menu. |
| **Operator, Start Port and End Port** | The operator column specifies the port number settings. If the **Start Port** is empty, the **Start Port** and the **End Port** column will be ignored. The filter rule will filter out any port number.<br>***(=)*** If the End Port is empty, the filter rule will set the port number to be the value of the Start Port. Otherwise, the port number ranges between the Start Port and the End Port (including the Start Port and the End Port).<br>***(!=)***If the End Port is empty, the port number is not equal to the value of the Start Port. Otherwise, this port number is not between the Start Port and the End Port (including the Start Port and End Port).<br>***(>)*** Specify the port number is larger than the Start Port (includes the Start Port).<br>***(<)*** Specify the port number is less than the Start Port (includes the Start Port). |
| **Keep State** | This function should work along with Direction, Protocol, IP address, Subnet Mask, Operator, Start Port and End Port settings. It is used for Data Filter only.<br><br>Keep State is in the same nature of modern term Stateful Packet Inspection. It tracks packets, and accept the packets with appropriate characteristics showing its state is legal as the protocol defines. It will deny unsolicited incoming data. You may select protocols from any, TCP, UDP, TCP/UDP, ICMP and IGMP. |
| **Fragments** | Specify the action for fragmented packets. And it is used for **Data Filter** only.<br>***Don't care -***No action will be taken towards fragmented packets.<br>***Unfragmented -***Apply the rule to unfragmented packets.<br>***Fragmented -*** Apply the rule to fragmented packets.<br>***Too Short -*** Apply the rule only to packets that are too short to contain a complete header. |

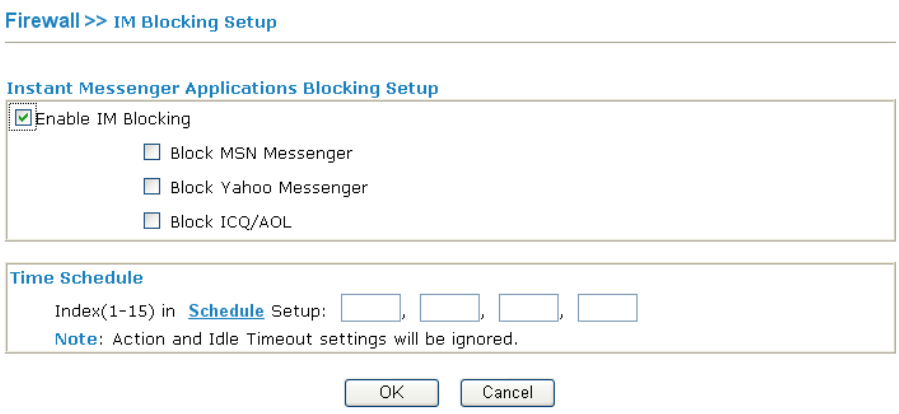
### Example

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



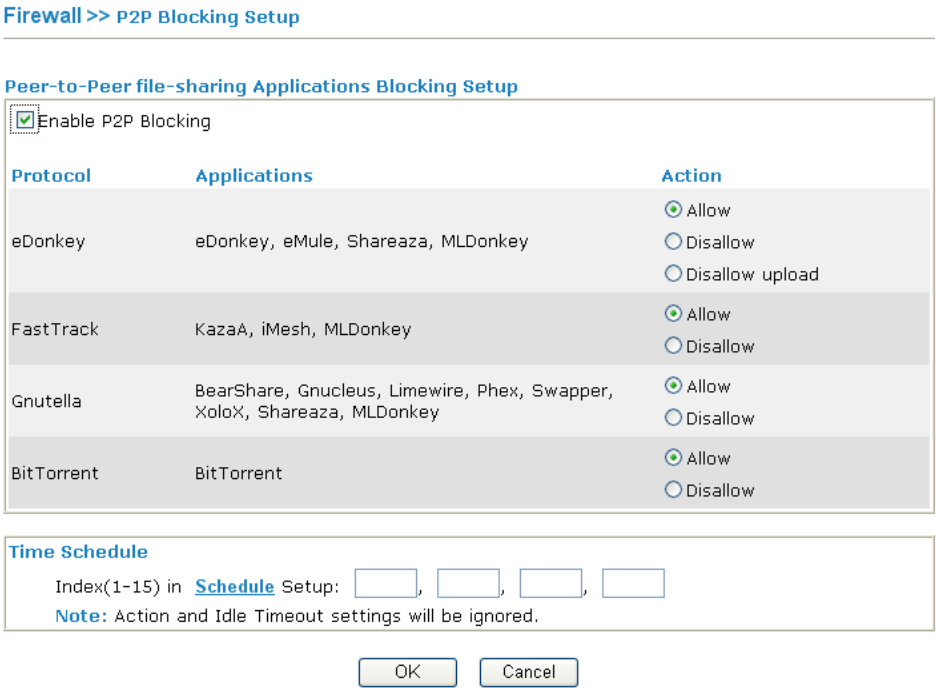

## 3.4.4 IM Blocking

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



## 3.4.5 P2P Blocking

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

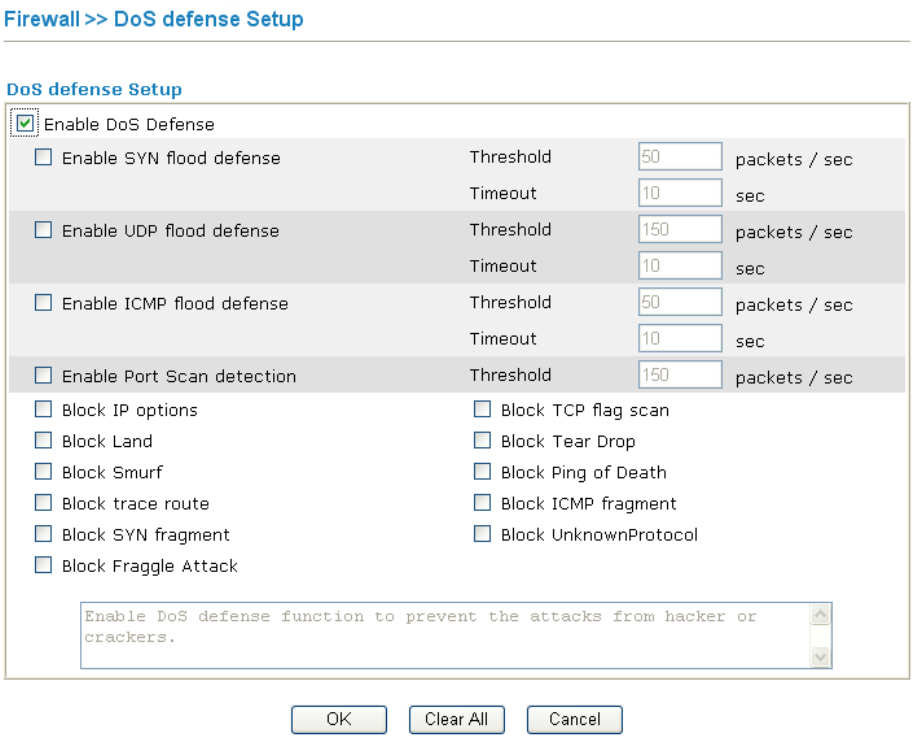



**Action** Specify the action for each protocol.
**Allow –** Allow the client to access into the application through the specified protocol.
**Disallow –** Forbid the client to access into the application through the specified protocol.
**Disallow upload –** Forbid the client to access into the application through the specified protocol for downloading. Yet uploading is allowed.

## 3.4.6 DoS Defense

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

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




| | |
|---|---|
| **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.

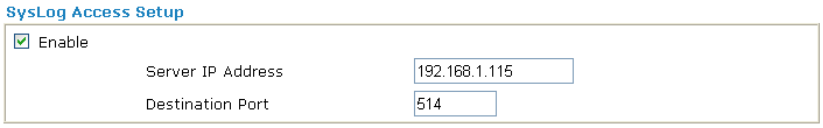
**Block Unknown Protocol**

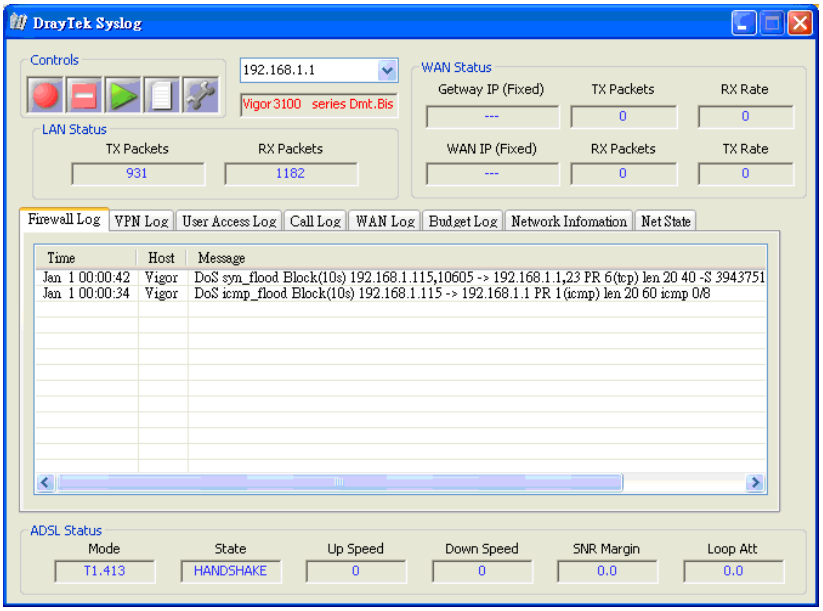
Check the box to activate the Block Unknown Protocol function. Individual IP packet has a protocol field in the datagram header to indicate the protocol type running over the upper layer. However, the protocol types greater than 100 are reserved and undefined at this time. Therefore, the router should 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. (Refer to **System Maintenance >> Syslog/Mail Alert** for detail information.)

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



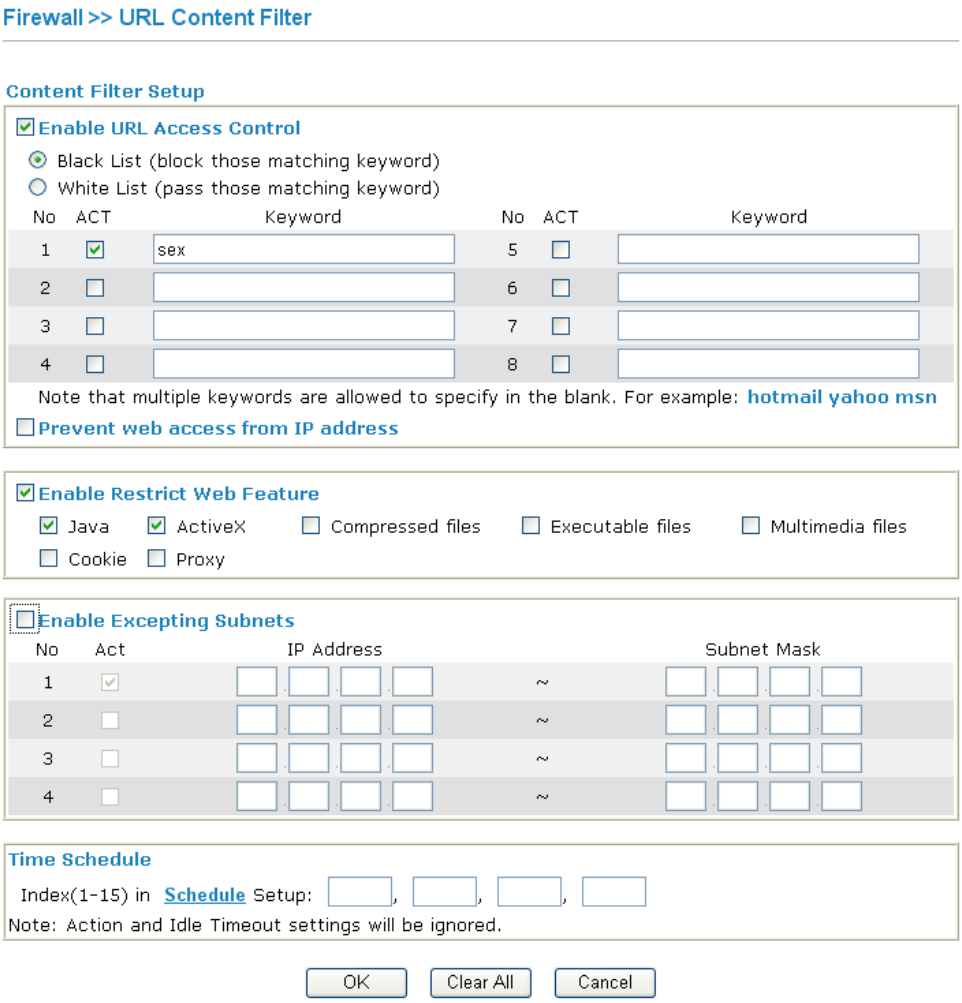

## 3.4.7 URL Content Filter

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

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

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

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




| | |
|---|---|
| **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.<br><br>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.<br>***Java*** - Check the checkbox to activate the Block Java object function. The Vigor router will discard the Java objects from the Internet.<br><br>***ActiveX*** - Check the box to activate the Block ActiveX object function. Any ActiveX object from the Internet will be refused.<br>***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.<br>**zip, rar, .arj, .ace, .cab, .sit**<br>***Executable file*** - Check the box to reject any downloading behavior of the executable file from the Internet.<br>**.exe, .com, .scr, .pif, .bas, .bat, .inf, .reg**<br>***Cookie*** - Check the box to filter out the cookie transmission from inside to outside world to protect the local user's privacy.<br>***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.<br>**.mov .mp3 .rm .ra .au .wmv**<br>**.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. |

### 3.4.8 Web Content Filter

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

For this section, please refer to **Web Content Filter** user’s guide for detailed information.

# 3.5 Applications

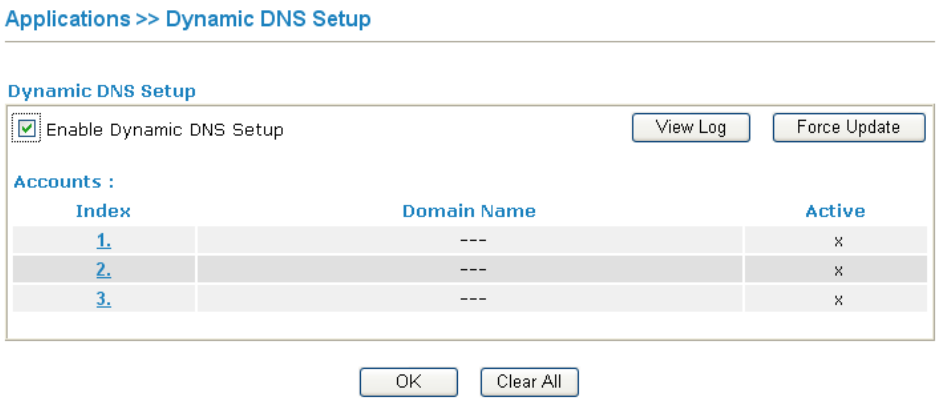
## 3.5.1 Dynamic DNS

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

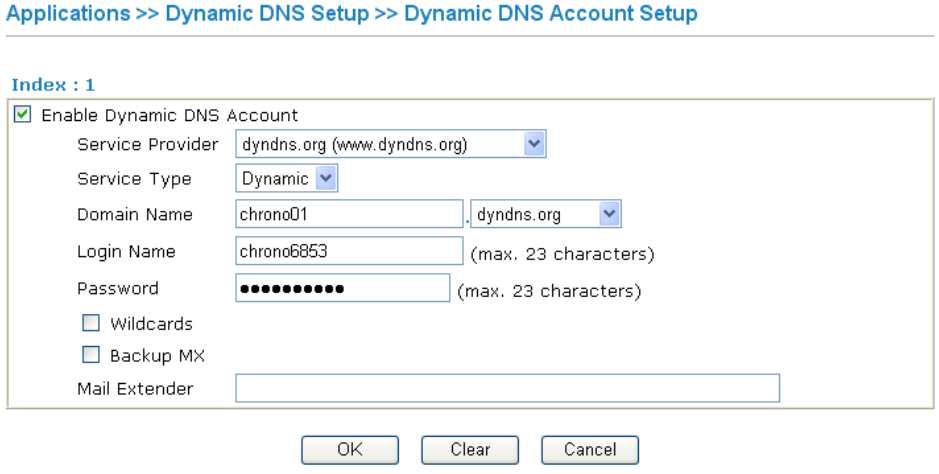
Before you use the Dynamic DNS feature, you have to apply for free DDNS service to the DDNS service providers. The router provides up to three accounts from three different DDNS service providers. Basically, Vigor routers are compatible with the DDNS services supplied by most popular DDNS service providers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

**Enable the Function and Add a Dynamic DNS Account**

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




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*.



| | |
|---|---|
| **Service Provider** | Select the service provider for the DDNS account. |
| **Service Type** | Select a service type (Dynamic, Custom, Static). |
| **Domain Name** | Type in a domain name that you applied previously. |
| **Login Name** | Type in the login name that you set for applying domain. |
| **Password** | Type in the password that you set for applying domain. |

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

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

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

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

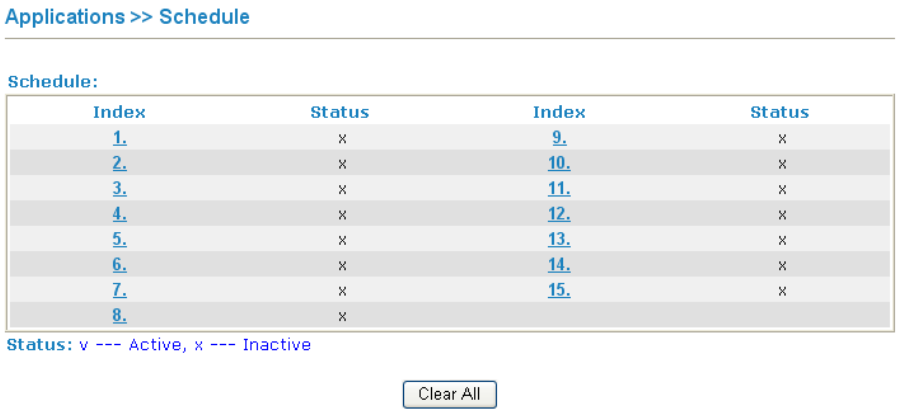
**Delete a Dynamic DNS Account**

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

## 3.5.2 Schedule

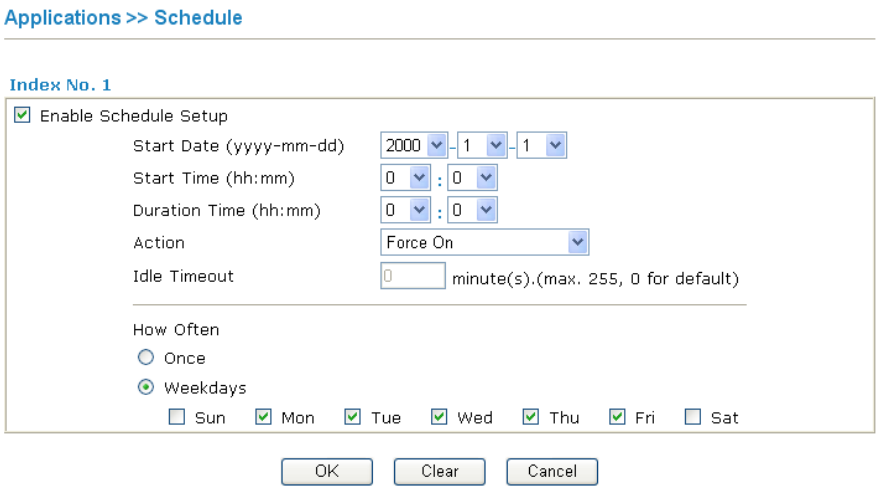
The Vigor router has a built-in real time clock which can update itself manually or automatically by means of Network Time Protocols (NTP). As a result, you can not only schedule the router to dialup to the Internet at a specified time, but also restrict Internet access to certain hours so that users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

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




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

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




| | |
|---|---|
| **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.<br>**Force On** -Force the connection to be always on.<br>**Force Down** -Force the connection to be always down.<br>**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.<br>**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.<br>**How often** -Specify how often the schedule will be applied<br>**Once** -The schedule will be applied just once<br>**Weekdays** -Specify which days in one week should perform the schedule. |

**Example**

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

**Office Hour:**

**(Force On)**

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

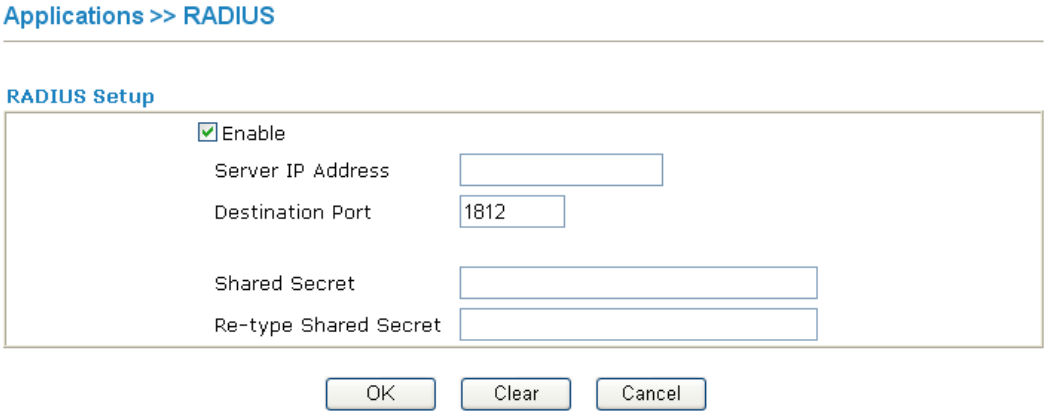
1. Make sure the PPPoE connection and **Time Setup** is working properly.
2. Configure the PPPoE always on from 9:00 to 18:00 for whole week.
3. Configure the **Force Down** from 18:00 to next day 9:00 for whole week.

4. Assign these two profiles to the PPPoE Internet access profile. Now, the PPPoE Internet connection will follow the schedule order to perform **Force On** or **Force Down** action according to the time plan that has been pre-defined in the schedule profiles.

## 3.5.3 RADIUS

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.

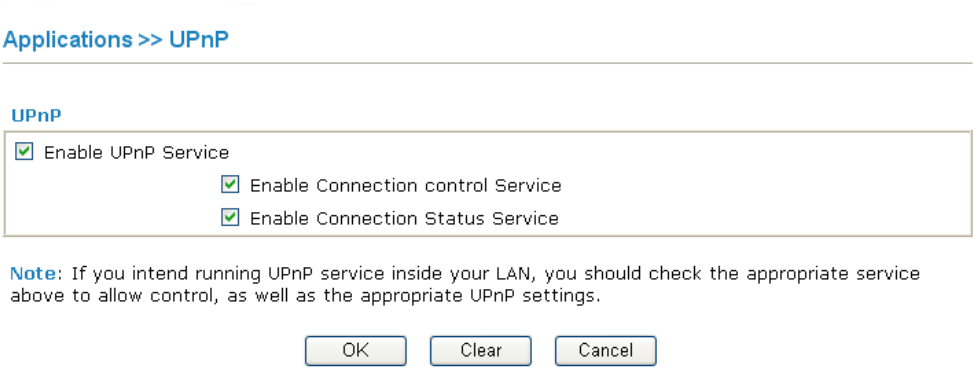
The built-in RADIUS client feature enables the router to assist the remote dial-in user or a wireless station and the RADIUS server in performing mutual authentication. It enables centralized remote access authentication for network management.




| | |
|---|---|
| **Enable** | Check to enable RADIUS client feature |
| **Server IP Address** | Enter the IP address of RADIUS server |
| **Destination Port** | The UDP port number that the RADIUS server is using. The default value is 1812 , based on RFC 2138. |
| **Shared Secret** | The RADIUS server and client share a secret that is used to authenticate the messages sent between them. Both sides must be configured to use the same shared secret. |
| **Re-type Shared Secret** | Re-type the Shared Secret for confirmation. |

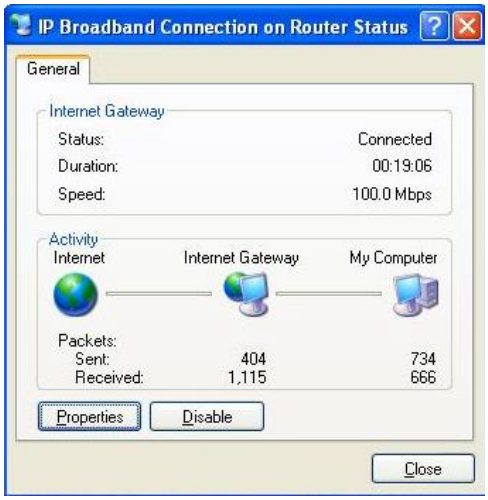
## 3.5.4 UPnP

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.

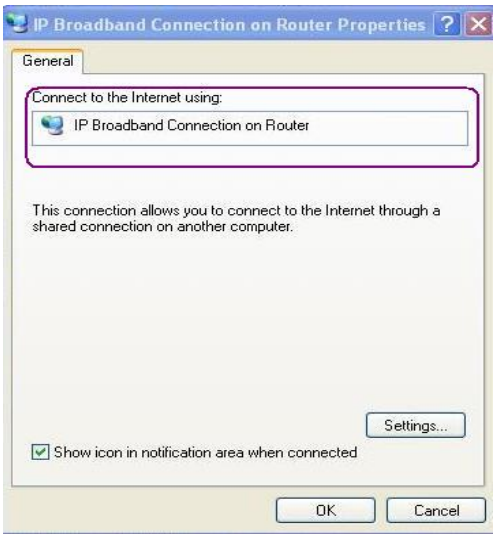


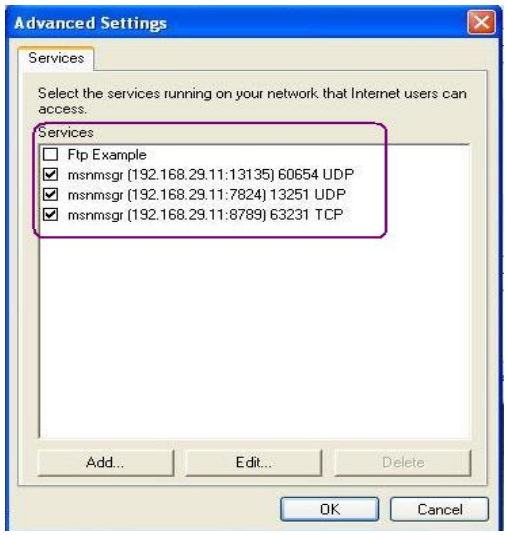

**Enable UPNP Service** Accordingly, you can enable either the **Connection Control Service** or **Connection Status Service**.

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


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




The reminder as regards concern about Firewall and UPnP:

**Can't work with Firewall Software**

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

**Security Considerations**

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

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

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

## 3.5.5 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), such as voice over IP, videoconferencing, streaming video or data.

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?

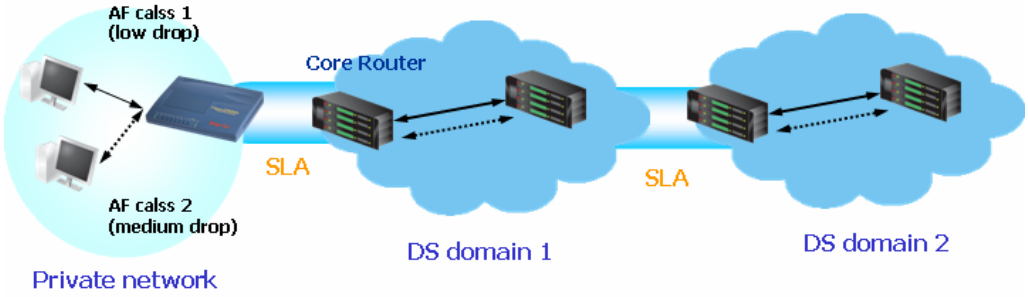
There are two components within Primary configuration of QoS deployment:

- 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.

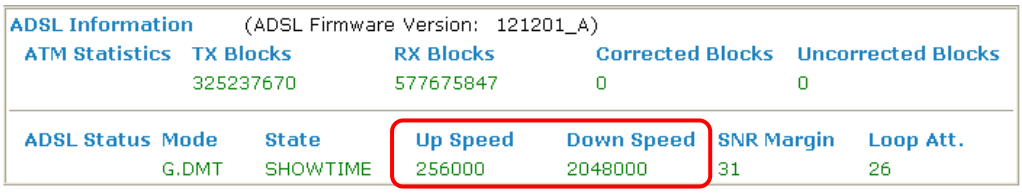
One more larger-scale implementation of QoS network is to apply DSCP (Differentiated Service Code Point) and IP Precedence disciplines at Layer 3. Compared with legacy IP Precedence that uses Type of Service (ToS) field in the IP header to define 8 service classes, DSCP is a successor creating 64 classes 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.



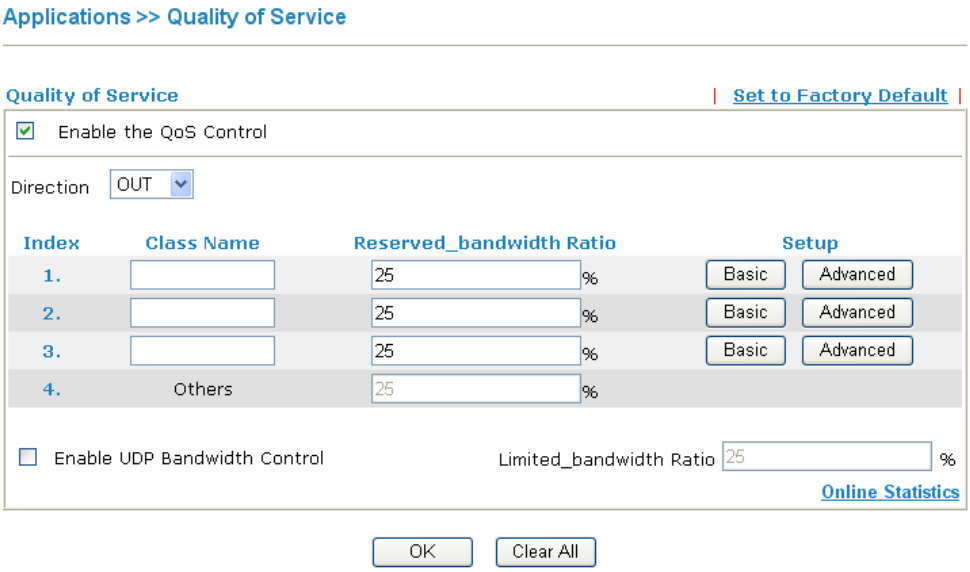

However, each node may take different attitude toward packets with high priority marking since it may bind with the business deal of SLA among different DS domain owners. It's not easy to achieve deterministic and consistent high-priority QoS traffic throughout the whole network with merely Vigor router's effort.

For more effective QoS deployment, you should check the available ADSL upstream and downstream speed in **Online Status** as indicated below before you configure the QoS setting.

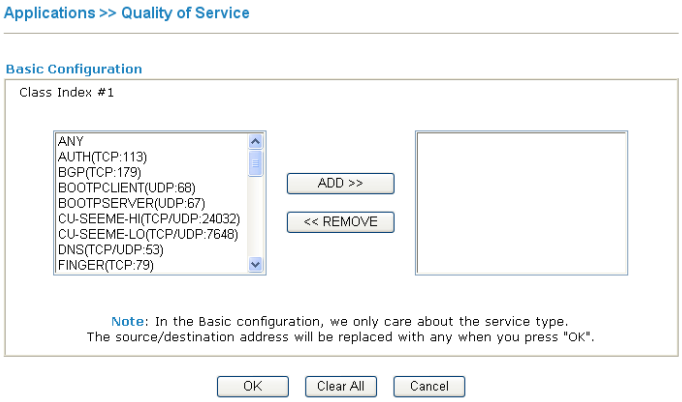



The following QoS policies will be defined in the form of ratio of upstream/downstream speed. We will also provide application QoS requirement as reference to help you accomplish this task. The setting values will vary depending on the network condition.

Click on **Application >>QoS Control**. The following screen will appear.



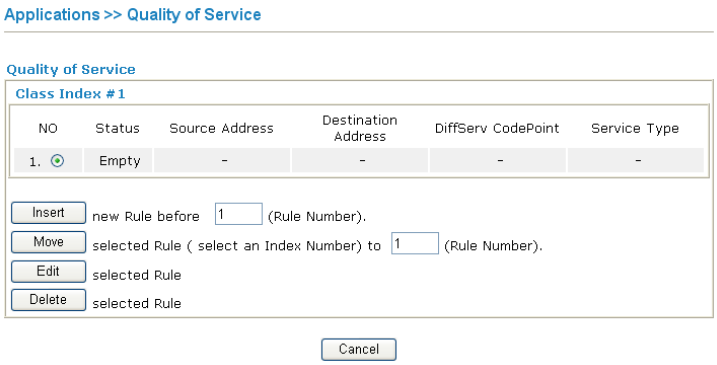

| | |
|---|---|
| **Enable the QoS Control** | For V models, the factory default for this is checked to enable. |
| **Direction** | Define which traffic the QoS Control settings apply to.<br>**IN-** apply to incoming traffic only.<br>**OUT**-apply to outgoing traffic only.<br>**BOTH-** apply to both incoming and outgoing traffic. |
| **Index** | The group index number of QoS Control settings. There are total 4 groups. |
| **Class Name** | Define the name for the group index. |
| **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**. |
| **Setup** | There are two-level of settings:<br>**Basic** - setup Reserved Bandwidth Ratio according to the traffic service type. We provide a list of common service types.<br>**Advance** - custom setting of Reserved Bandwidth Ratio based on the source address, destination address, DiffServ CodePoint, and service type. |
| **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 used to limit the total bandwidth of UDP application. |
| **Basic button** | Click this button to open basic configuration for each index number. |



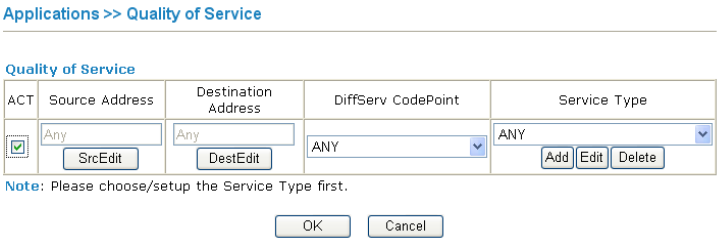

Choose one of the items from the left box and click **ADD>>**. The selected one will be shown on the right box. To remove the selected on from the right box, simply choose the one again and click **<<Remove.**

**Advanced button**

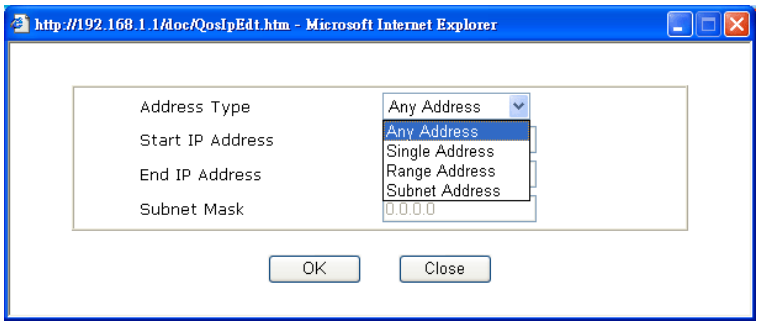
Click this button to open advanced configuration for each index number**.** You can insert, move, edit or delete select rule in this page.




For inserting a rule, click **Insert** to open the following page.

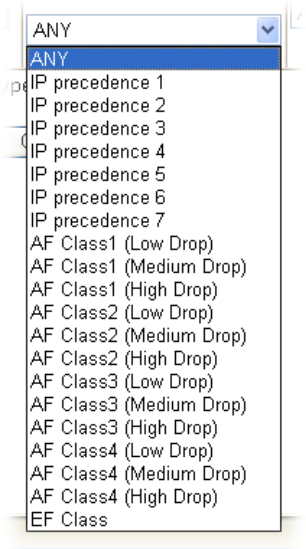



**SrcEdit** - allows you to edit source address information.
**DestEdit** - allows you to edit destination address information. If you click one of the buttons, you will see the following dialog.

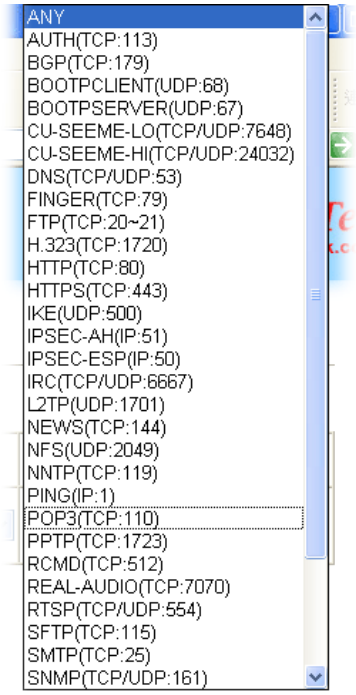


From the Address Type drop-down list, please choose one of the selections as the address type. And type in start IP and end IP address and Subnet Mask.

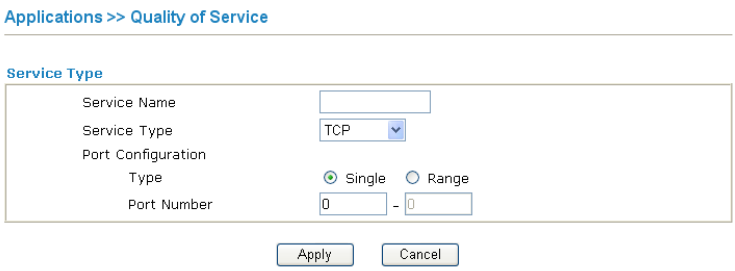
**DiffServ CodePoint** – all the packets of data will be divided with different levels and will be processed according to the level type by the system. Please assign one of the levels of the data for processing with QoS control.




**Service Type** – It determines the service type of the data for processing with QoS control. It can also be edited. Simply click **Add/Edd/Delete** button to access into the following page.



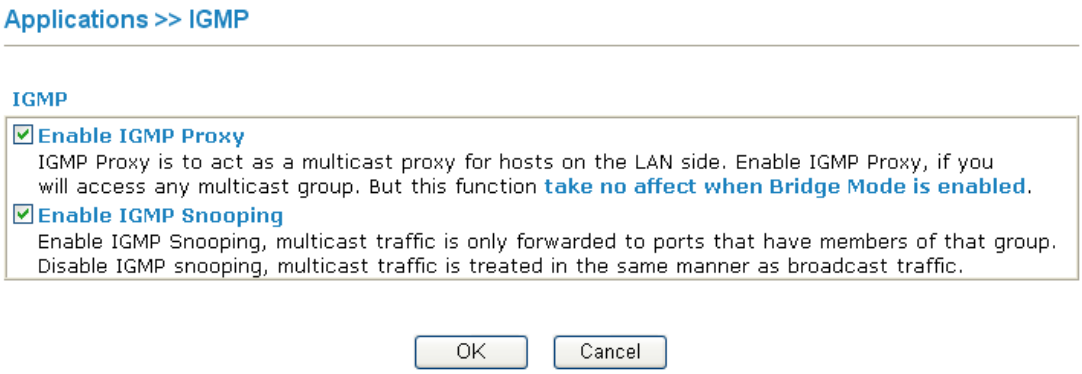

You can add a new service name for your necessity. Also, you can **Edit/Delete** to change the one that you added before.

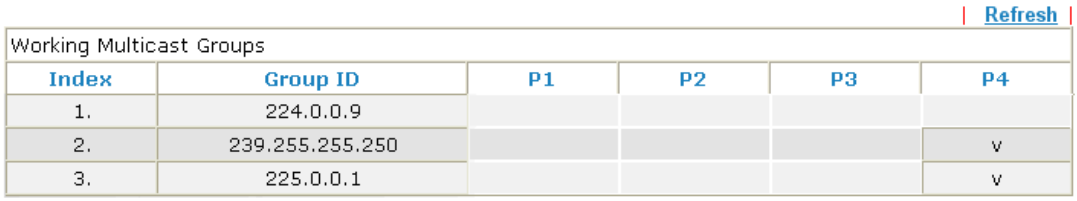



Please type in the service name, select **Service typ**e (TCP/UDP and both). Next choose either one of the port configuration type (Single or Range) and type in the range for the **Port Number**.

## 3.5.6 IGMP

IGMP is the abbreviation of Internet Group Management Protocol. It is a communication protocol which is mainly used for managing the membership of Internet Protocol multicast groups. For invoking IGMP Snooping function, you have to check the Enable IGMP Proxy box first for activating the IGMP proxy function.




**Enable IGMP Proxy** — Check this box to enable this function. The application of multicast will be executed through WAN port.

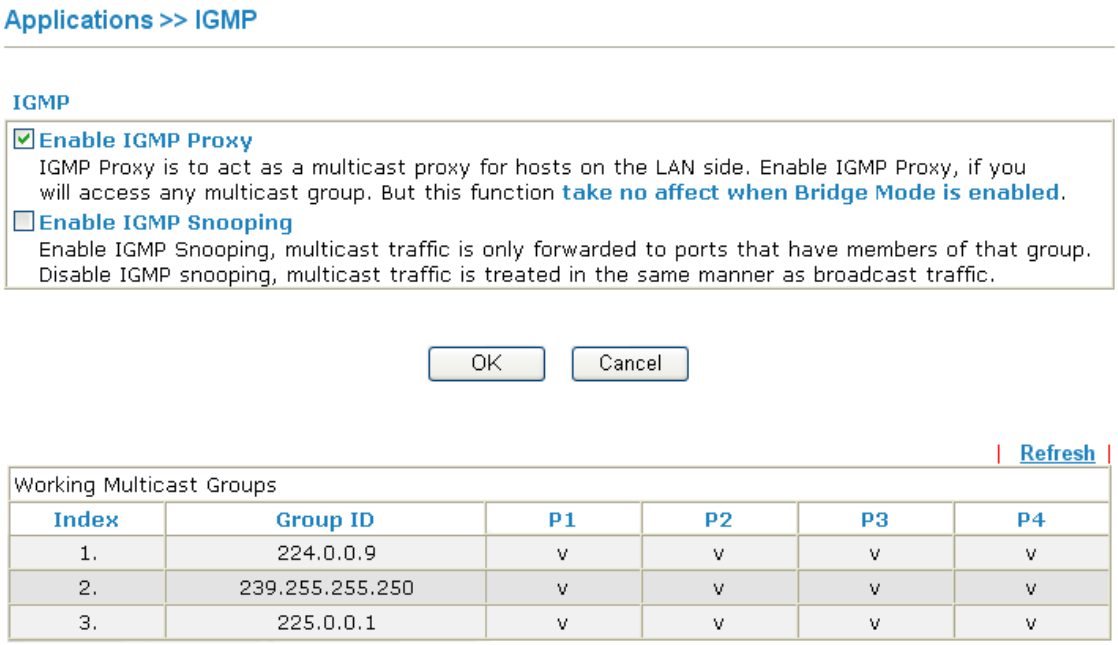
**Enable IGMP Snooping** — Check this box to enable this function. The application of multicast will be executed for the clients in LAN.

**Group ID** — This field displays the ID port for the multicast group. The available range for IGMP starts from 224.0.0.0 to 239.255.255.254.

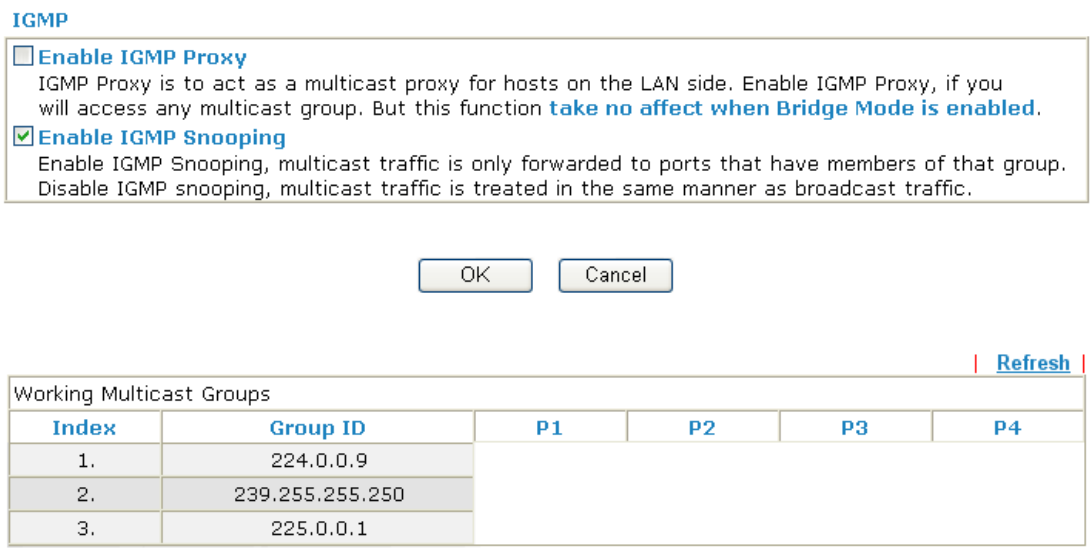
**P1 to P4** — It indicates the LAN port used for the multicast group.

**Refresh** — Click this link to renew the working multicast group status.

If you check Enable IGMP Proxy only, you will get the following page. All the multicast groups will be listed and all the LAN ports (P1 to P4) are available for use.




If you check Enable IGMP Snooping only, you will get the following page. Though all the multicast groups are listed, yet all the LAN ports (P1 to P4) are not available for use.

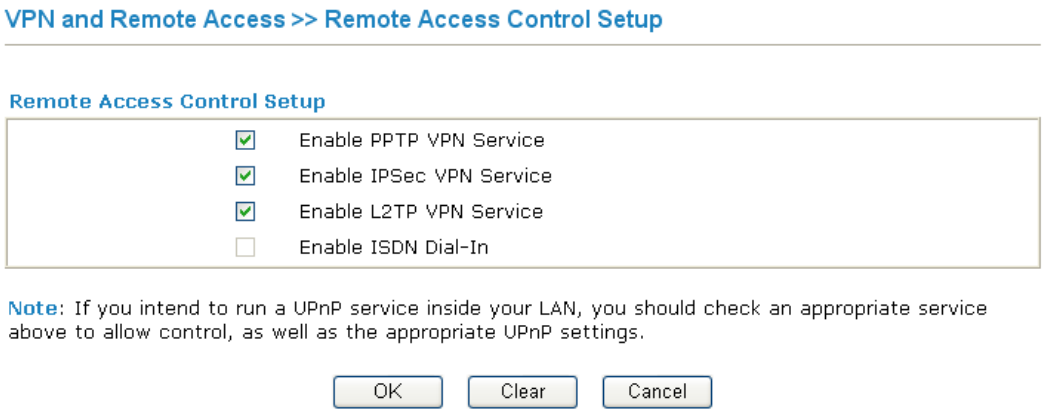


## 3.6 VPN and Remote Access

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.

### 3.6.1 Remote Access Control

Enable the necessary VPN service as you need. If you intend to run a VPN server inside your LAN, you should disable the VPN service of Vigor Router to allow VPN tunnel pass through, as well as the appropriate NAT settings, such as DMZ or open port.




**Enable PPTP VPN Service** Check this box to activate the VPN service through PPTP protocol.

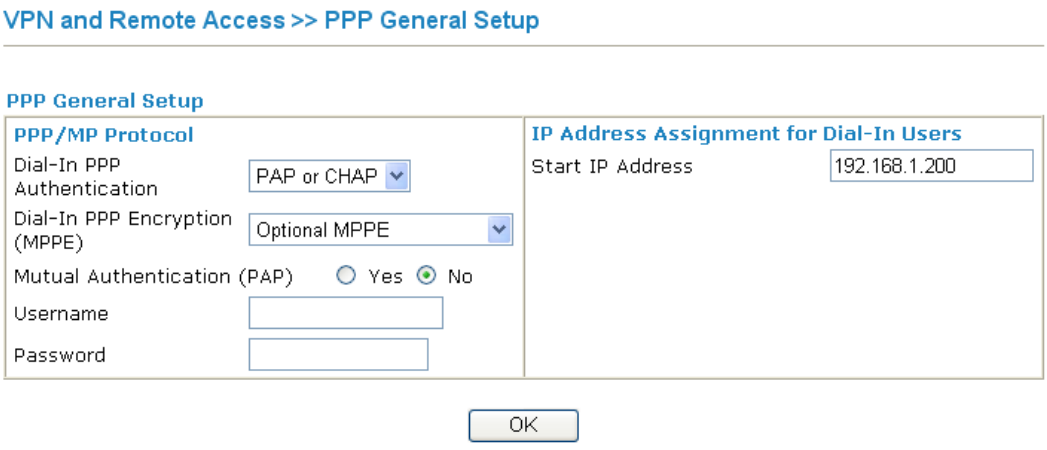
**Enable IPSec VPN Service** Check this box to activate the VPN service through IPSec protocol.

**Enable L2TP VPN Service** Check this box to activate the VPN service through L2TP protocol.

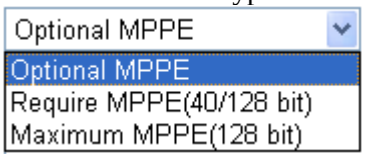
**Enable ISDN Dial-IN** This box will be valuable for the router with ISDN interface.

### 3.6.2 PPP General Setup

This submenu only applies to PPP-related VPN connections, such as PPTP, L2TP, L2TP over IPSec.




**Dial-In PPP** Select this option to force the router to authenticate dial-in

| | |
|---|---|
| **Authentication PAP Only** | users with the PAP protocol. |
| **PAP or CHAP** | Selecting this option means the router will attempt to authenticate dial-in users with the CHAP protocol first. If the dial-in user does not support this protocol, it will fall back to use the PAP protocol for authentication. |
| **Dial-In PPP Encryption (MPPE Optional MPPE** | This option represents that the MPPE encryption method will be optionally employed in the router for the remote dial-in user. If the remote dial-in user does not support the MPPE encryption algorithm, the router will transmit "no MPPE encrypted packets". Otherwise, the MPPE encryption scheme will be used to encrypt the data.<br>  <br>**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 128-bit to perform encryption prior to using 40-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.<br>**Maximum MPPE -** This option indicates that the router will only use the MPPE encryption scheme with maximum bits (128 bits) 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. |

### 3.6.3 IPSec General Setup

In **IPSec General Setup,** there are two major parts of configuration.

There are two phases of IPSec.

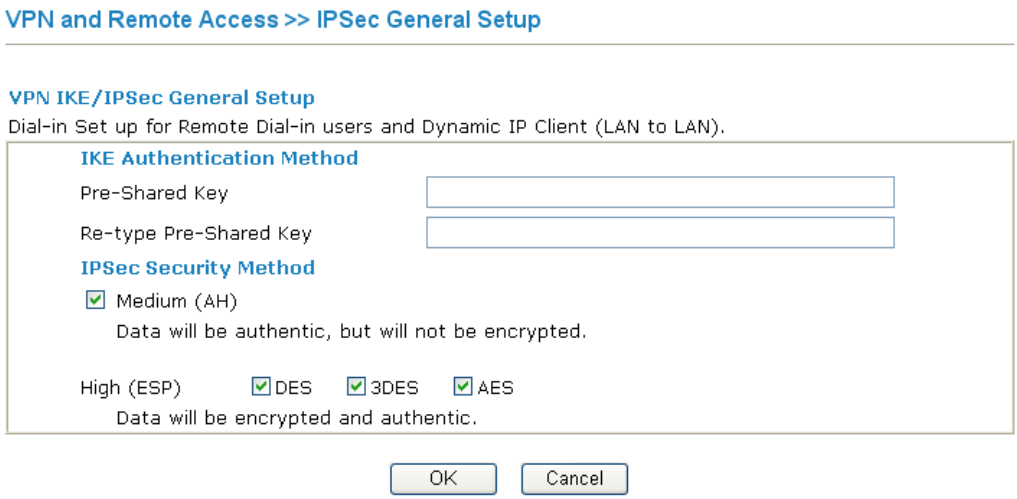
- Phase 1: negotiation of IKE parameters including encryption, hash, Diffie-Hellman parameter values, and lifetime to protect the following IKE exchange, authentication of both peers using either a Pre-Shared Key or Digital Signature (x.509). The peer that starts the negotiation proposes all its policies to the remote peer and then remote peer tries to find a highest-priority match with its policies. Eventually to set up a secure tunnel for IKE Phase 2.

- Phase 2: negotiation IPSec security methods including Authentication Header (AH) or Encapsulating Security Payload (ESP) for the following IKE exchange and mutual examination of the secure tunnel establishment.

There are two encapsulation methods used in IPSec, **Transport** and **Tunnel**. The **Transport** mode will add the AH/ESP payload and use original IP header to encapsulate the data payload only. It can just apply to local packet, e.g., L2TP over IPSec. The **Tunnel** mode will not only add the AH/ESP payload but also use a new IP header (Tunneled IP header) to encapsulate the whole original IP packet.

Authentication Header (AH) provides data authentication and integrity for IP packets passed between VPN peers. This is achieved by a keyed one-way hash function to the packet to create a message digest. This digest will be put in the AH and transmitted along with packets. On the receiving side, the peer will perform the same one-way hash on the packet and compare the value with the one in the AH it receives.

Encapsulating Security Payload (ESP) is a security protocol that provides data confidentiality and protection with optional authentication and replay detection service.

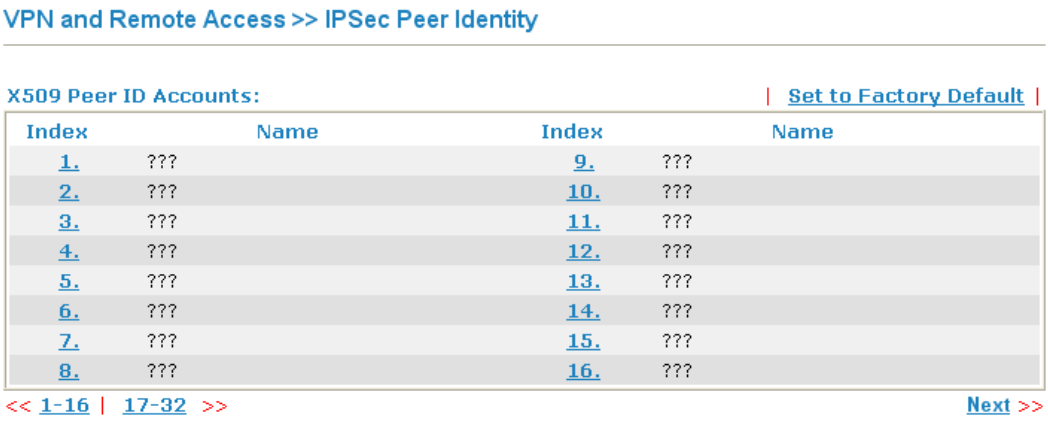



**IKE Authentication Method** This usually applies to those are remote dial-in user or node (LAN-to-LAN) which uses dynamic IP address and IPSec-related VPN connections such as L2TP over IPSec and IPSec tunnel.
**Pre-Shared Key-** Specify a key for IKE authentication
**Re-type Pre-Shared Key-**Confirm 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.

## 3.6.4 IPSec Peer Identity

To use digital certificate for peer authentication in either LAN-to-LAN connection or Remote User Dial-In connection, here you may edit a table of peer certificate for selection. As shown below, the router provides 32 entries of digital certificates for peer dial-in users.



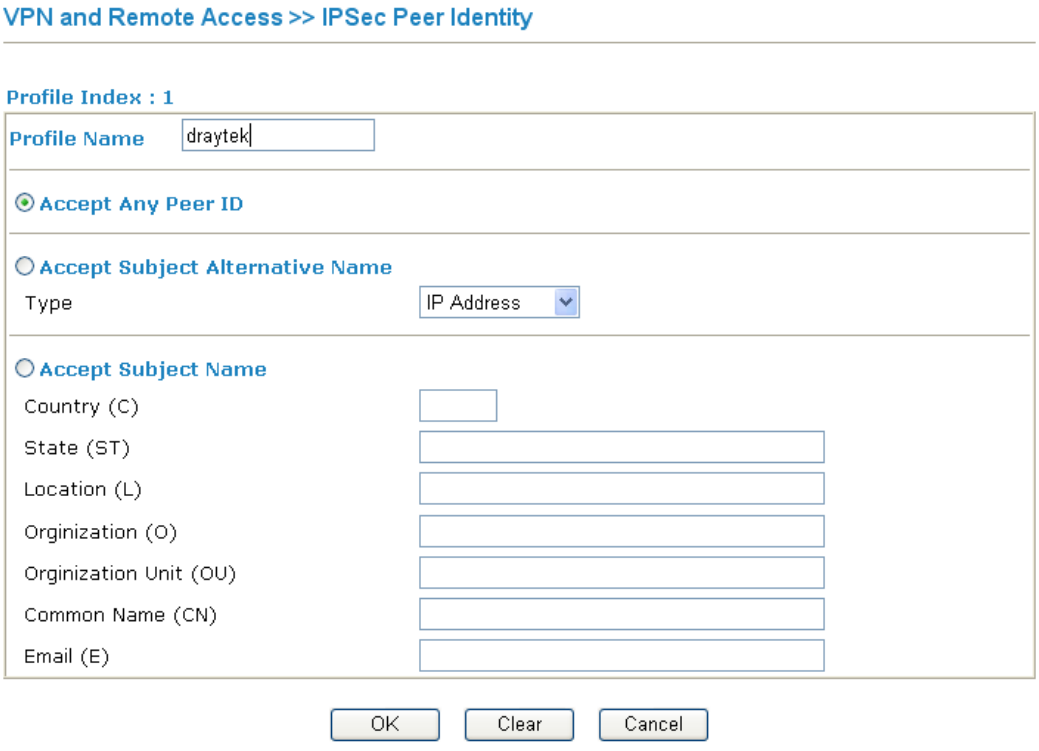

**Set to Factory Default** Click it to clear all indexes.

**Index** Click the number below Index to access into the setting page of IPSec Peer Identity.

**Name** Display the profile name of that index.

**Next** Click this link to access into next page for setting more accounts.

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.



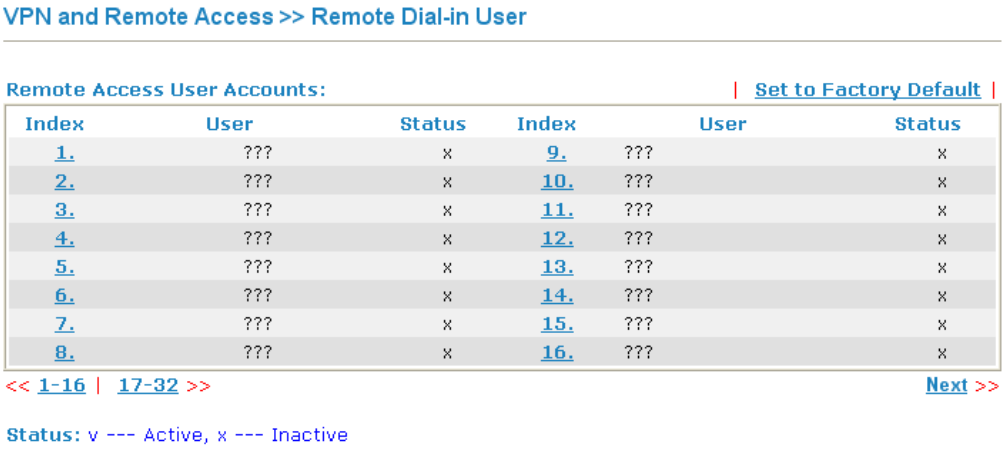

**Profile Name** Type in a name in this file.

| | |
|---|---|
| **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 Name,** or **E-Mail**. 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)**. |

## 3.6.5 Remote User Profiles

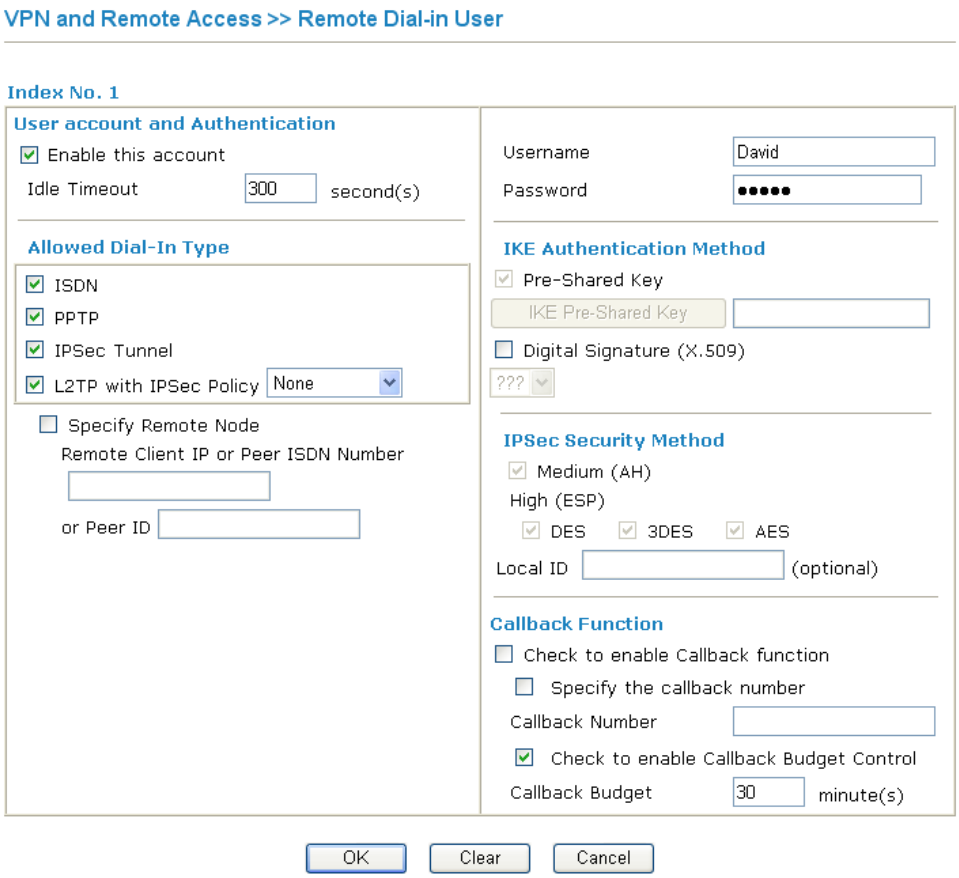
You can manage remote access by maintaining a table of remote user profile, so that users can be authenticated to dial-in or build the VPN connection. You may set parameters including specified connection peer ID, connection type (VPN including PPTP, IPSec Tunnel, and L2TP by itself or over IPSec) and corresponding security methods, etc.

The router provides 32 access accounts for dial-in users. Besides, you can extend the user accounts to the RADIUS server through the built-in RADIUS client function. The following figure shows the summary table.




| | |
|---|---|
| **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. |
| **Next** | Click this link to access into next page for setting more accounts. |

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.




**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 trigger a 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.
N**ice 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 Remote Node**

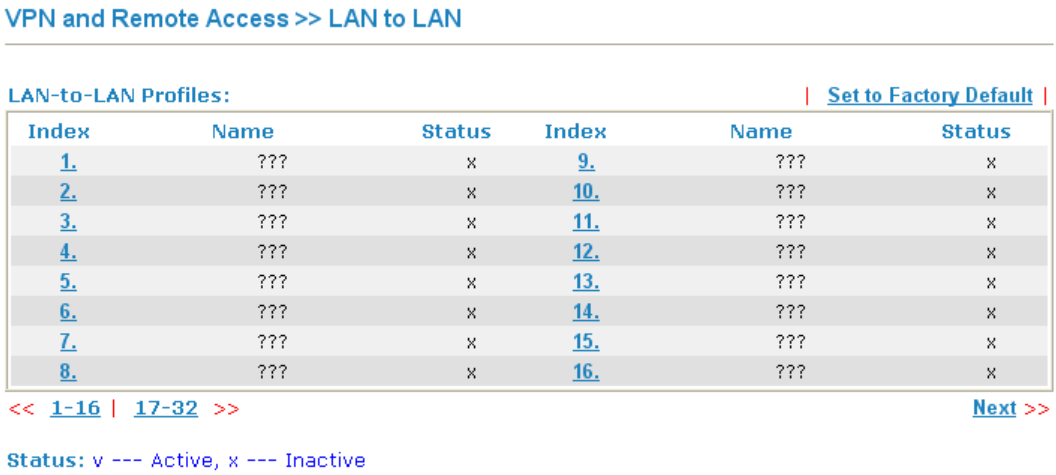
**Check the checkbox-**You can specify the IP address of the remote dial-in user or peer ID (used in IKE aggressive mode).

| | |
|---|---|
| | **Uncheck the checkbox**-This means the connection type you select above will apply the authentication methods and security methods in the **general settings**. |
| **User Name** | This field is applicable when you select PPTP or L2TP with or without IPSec policy above. |
| **Password** | This field is applicable when you select 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.<br>**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.<br>**Digital Signature (X.509) –** Check the box of Digital Signature to invoke this function and select one predefined in the X.509 Peer ID Profiles. |
| **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.<br>**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.<br>**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.<br>**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 router owner will be charged the connection fee by the telecom.<br>**Check to enable Callback function**-Enables the callback function.<br>**Specify the callback number**-The option is for extra security. Once enabled, the router will ONLY call back to the specified Callback Number.<br>**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.<br>**Callback Budget (Unit: minutes)**- Specify the time budget for the dial-in user. The budget will be decreased automatically per callback connection. |

## 3.6.6 LAN to LAN Profiles

Here you can manage LAN-to-LAN connections by maintaining a table of connection profiles. You may set parameters including specified connection direction (dial-in or dial-out), connection peer ID, connection type (VPN including PPTP, IPSec Tunnel, and L2TP by itself or over IPSec) and corresponding security methods, etc.

The router provides up to 32 profiles, which also means supporting 32 VPN tunnels simultaneously. The following figure shows the summary table.



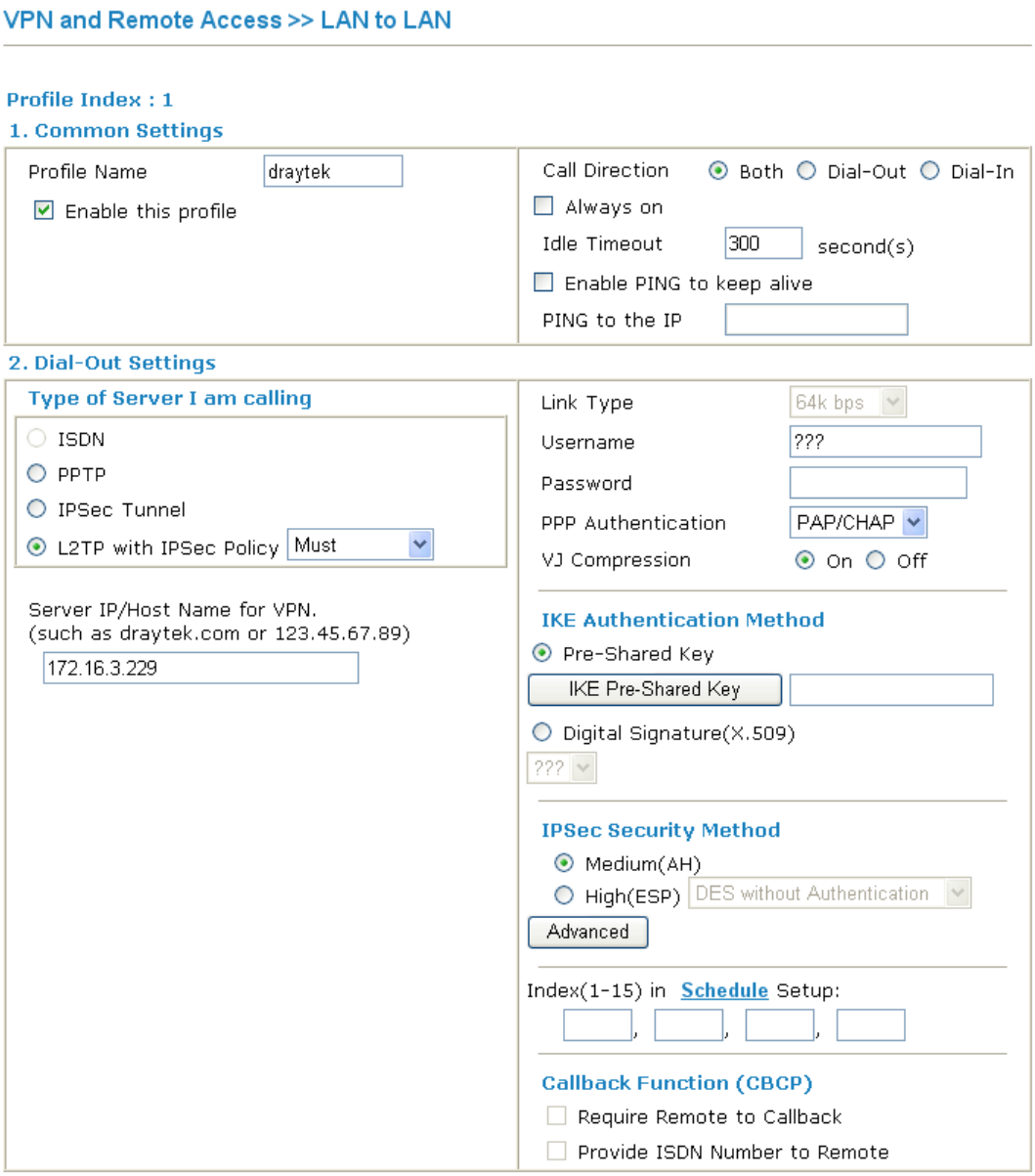

**Set to Factory Default** Click to clear all indexes.

**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 Name** | Specify a name for the profile of the LAN-to-LAN connection. |
| **Enable this profile** | Check here to activate this profile. |
| **Call Direction** | Specify the allowed call direction of this LAN-to-LAN profile:<br>**Both**- initiator/responder<br>**Dial-Out**- initiator only<br>**Dial-In**- responder only |
| **Always On or Idle Timeout** | **Always On**-Check to enable router always keep VPN connection.<br>**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. |

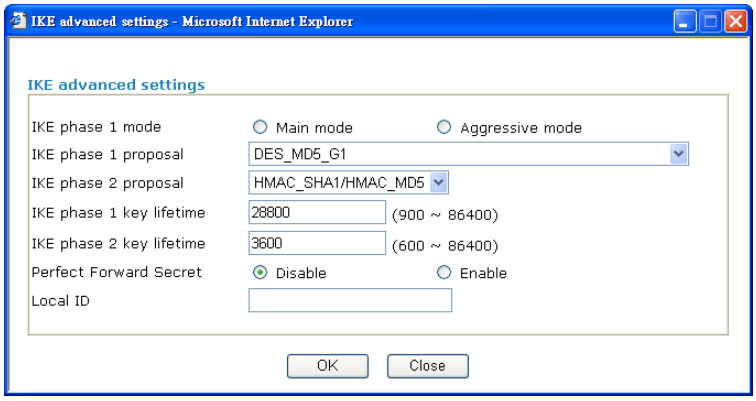
| | |
|---|---|
| **PING to the IP** | Enter the IP address of the remote host that located at the other-end of the VPN tunnel. |
| | **Enable PING to Keep Alive** is used to handle abnormal IPSec VPN connection disruption. It will help to provide the state of a VPN connection for router's judgment of redial.<br>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 dial-out connection to the server. 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 a 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:<br>**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.<br>**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.<br>**Must:** Specify the IPSec policy to be definitely applied on the L2TP connection. |
| **User Name** | This field is applicable when you select PPTP or L2TP w/ or w/out IPSec policy above. |
| **Password** | This field is applicable when you select PPTP or L2TP w/ or w/out IPSec policy above. |
| **PPP Authentication** | This field is applicable when you select PPTP or L2TP w/ or w/out IPSec policy above. PAP/CHAP is the most common selection due to wild compatibility. |
| **VJ compression** | This field is applicable when you select PPTP or L2TP w/ or w/out 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.<br>**Pre-Shared Key**-Input 1-63 characters as pre-shared key.<br>**Digital Signature (X.509)** - Select one predefined in the X.509 Peer ID Profiles. |

**IPSec Security Method** This group of fields is a must for IPSec Tunnels and L2TP with IPSec Policy.

**Medium** **Authentication Header (AH)** means data will be authenticated, but not be encrypted. By default, this option is active.

**High (ESP-Encapsulating Security Payload)-** means payload (data) will be encrypted and authenticated. Select from below:
**DES without Authentication** -Use DES encryption algorithm and not apply any authentication scheme.
**DES with Authentication**-Use DES encryption algorithm and apply MD5 or SHA-1 authentication algorithm.
**3DES without Authentication**-Use triple DES encryption algorithm and not apply any authentication scheme.
**3DES with Authentication**-Use triple DES encryption algorithm and apply MD5 or SHA-1 authentication algorithm.
**AES without Authentication**-Use AES encryption algorithm and not apply any authentication scheme.
**AES with Authentication**-Use AES encryption algorithm and apply MD5 or SHA-1 authentication algorithm.

**Advanced** Specify mode, proposal and key life of each IKE phase, Gateway etc.
The window of advance setup is shown as below:

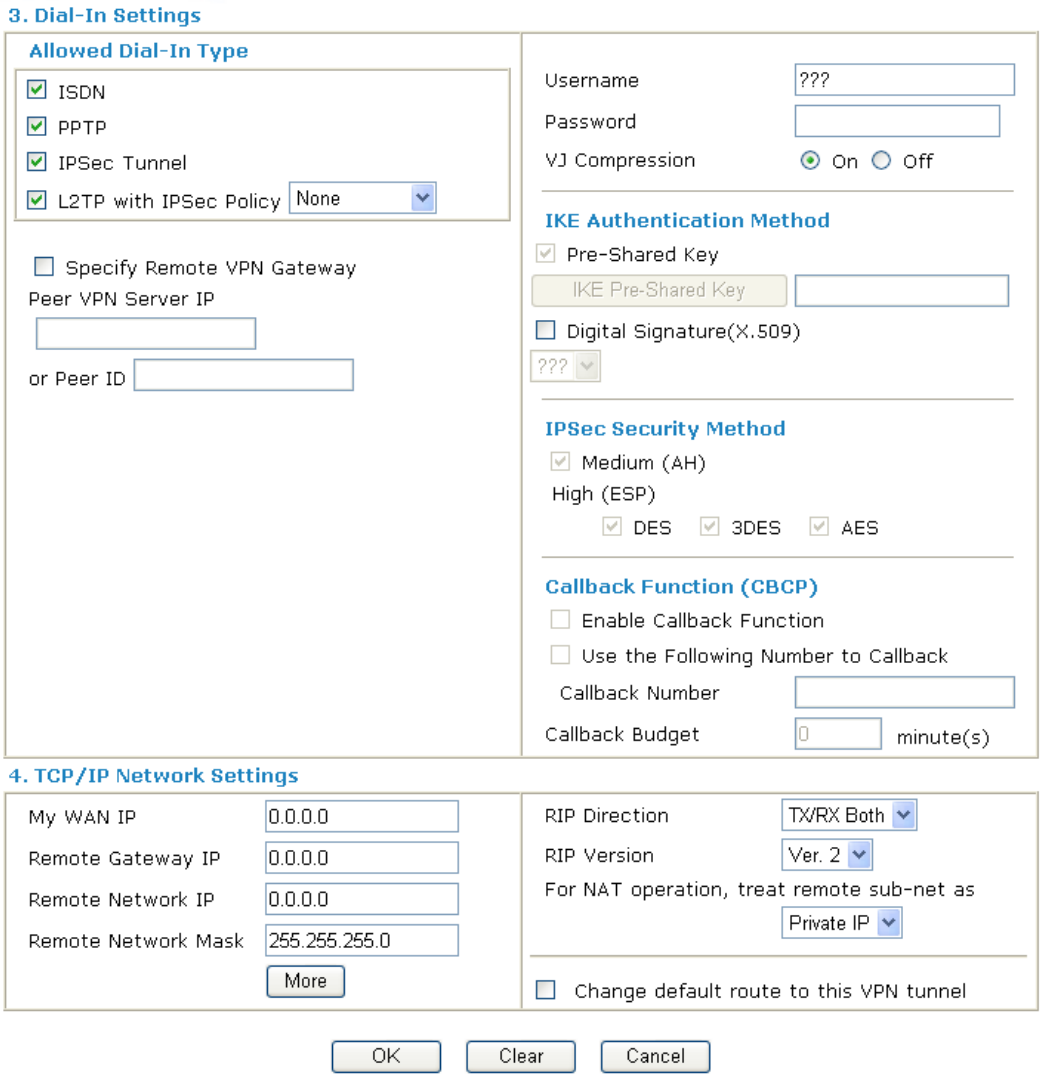



**IKE phase 1 mode** -Select from **Main** mode and **Aggressive** mode. The ultimate outcome is to exchange security proposals to create a protected secure channel. **Main** mode is more secure than **Aggressive** mode since more exchanges are done in a secure channel to set up the IPSec session. However, the **Aggressive** mode is faster. The default value in Vigor router is Main mode.
**IKE phase 1 proposal**-To propose the local available authentication schemes and encryption algorithms to the VPN peers, and get its feedback to find a match. Two combinations are available for Aggressive mode and nine for **Main** mode. We suggest you select the combination that covers the most schemes.
**IKE phase 2 proposal**-To propose the local available algorithms to the VPN peers, and get its feedback to find a match. Three combinations are available for both modes. We suggest you select the combination that covers the most algorithms.
**IKE phase 1 key lifetime**-For security reason, the lifetime of

key should be defined. The default value is 28800 seconds. You may specify a value in between 900 and 86400 seconds.
**IKE phase 2 key lifetime-**For security reason, the lifetime of key should be defined. The default value is 3600 seconds. You may specify a value in between 600 and 86400 seconds.
**Perfect Forward Secret (PFS)-**The IKE Phase 1 key will be reused to avoid the computation complexity in phase 2. The default value is inactive this function.
**Local ID -** In **Aggressive** mode, Local ID is on behalf of the IP address while identity authenticating with remote VPN server. The length of the ID is limited to 47 characters.

**Callback Function (for I models only)**

The callback function provides a callback service as a part of PPP suite only for the ISDN dial-in user. The router owner will be charged the connection fee by the telecom.
**Require Remote to Callback-**Enable this to let the router to require the remote peer to callback for the connection afterwards.
**Provide ISDN Number to Remote-**In the case that the remote peer requires the Vigor router to callback, the local ISDN number will be provided to the remote peer. Check here to allow the Vigor router to send the ISDN number to the remote router. **This feature is useful for *i* model only.**



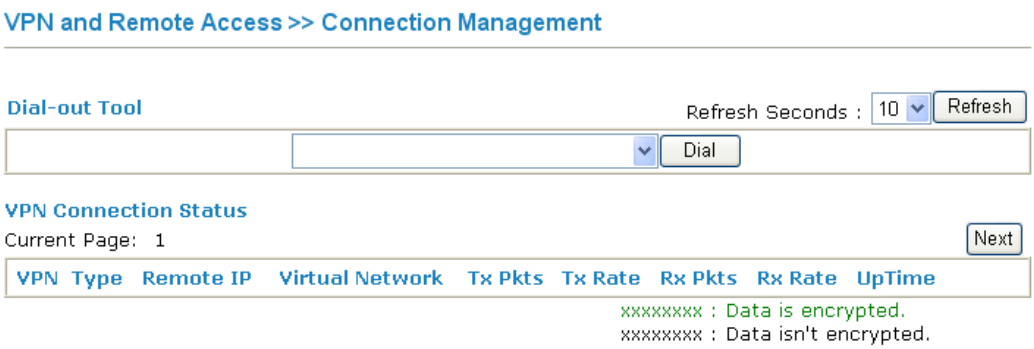

| | |
|---|---|
| **Allowed Dial-In Type** | Determine the dial-in connection with different types. |
| **ISDN** | Allow the remote ISDN dial-in connection. You can further set up Callback function below. You should set the User Name and Password of remote dial-in user below. This feature is useful for *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 trigger a 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:<br>**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.<br>**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.<br><br>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 PPTP or L2TP w/ or w/out IPSec policy above. |
| **Password** | This field is applicable when you select PPTP or L2TP w/ or w/out IPSec policy above. |
| **VJ Compression** | VJ Compression is used for TCP/IP protocol header compression. This field is applicable when you select PPTP or L2TP w/ or w/out IPSec policy above. |
| **IKE Authentication Method** | This group of fields is applicable for IPSec Tunnels and L2TP with IPSec Policy when you Specify ISDN CLID (for *i* model only) or Remote VPN Gateway Peer ISDN Number (for *i* model only) or Peer VPN Server IP. The only exception is Digital Signature (X.509) can be set when you select IPSec tunnel either w/ or w/o specify the CLID or IP address of the remote node.<br>**Pre-Shared Key -** Input 1-63 characters as pre-shared key.<br>**Digital Signature (X.509) -** Select one predefined in the X.509 Peer ID Profiles. |
| **IPSec Security Method** | This group of fields is a must for IPSec Tunnels and L2TP with IPSec Policy when you specify the remote node.<br>**Medium-** Authentication Header (AH) means data will be authenticated, but not be encrypted. By default, this option is active.<br>**High-** Encapsulating Security Payload (ESP) means payload (data) will be encrypted and authenticated. You may select encryption algorithm from Data Encryption Standard (DES), Triple DES (3DES), and AES. |
| **Callback Function** | The callback function provides a callback service only for the ISDN dial-in user (this feature is useful for *i* model only). The router owner will be charged the connection fee by the telecom.<br>**Check to enable Callback function**-Enables the callback function.<br>**Callback number**-The option is for extra security. Once enabled, the router will ONLY call back to the specified Callback Number.<br>**Callback budget**- By default, the callback function has limitation of callback period. Once the callback budget is exhausted, the function will be disabled automatically.<br>**Callback Budget (Unit: minutes)-** 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. |
| **My WAN IP** | This field is only applicable when you select PPTP or L2TP w/ or w/out 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. |
| **Remote Gateway IP** | This field is only applicable when you select PPTP or L2TP w/ or w/out 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. |
| **Remote Network IP/ Remote Network Mask** | Add a static router 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 router 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. |
| **RIP Version** | Select the RIP protocol version. Specify Ver. 2 for greatest compatibility. |
| **For NAT operation, treat remote sub-net as** | While communicating with remote subnet, the router can treat it as private subnet by sending packets with the router's private IP address, or treat it as public subnet by sending packets with the router's public IP address. |

## 3.6.7 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.




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

| | |
|---|---|
| **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. |

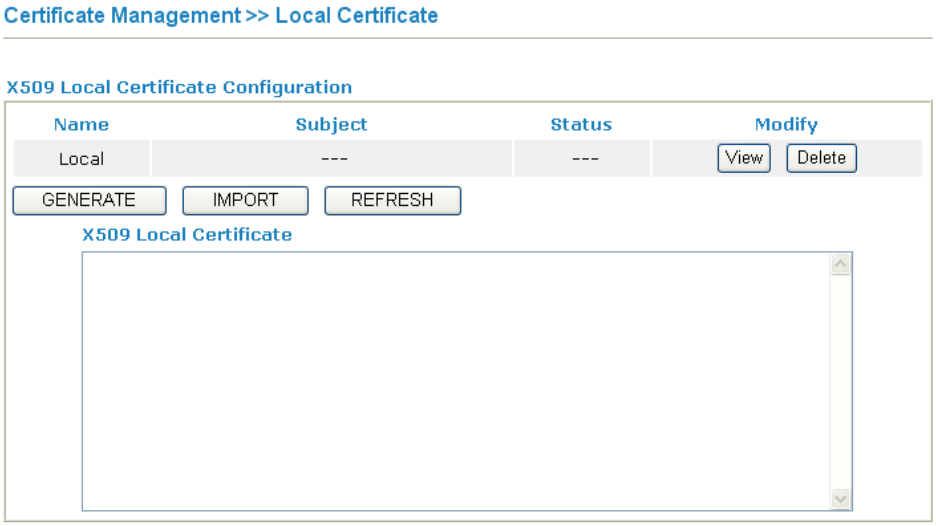
## 3.7 Certificate Management

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.

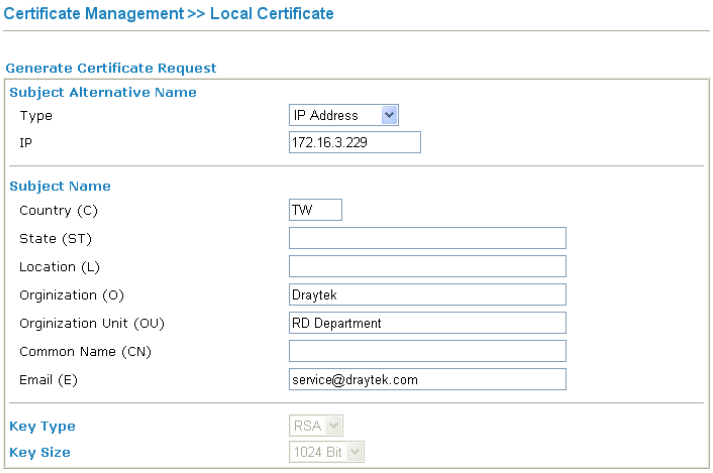
Any entity wants to utilize digital certificates should first request a certificate issued by a CA server. It should also retrieve certificates of other trusted CA servers so it can authenticate the peer with certificates issued by those trusted CA servers.

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.

## 3.7.1 Local Certificate




**Generate** Click this button to open **Generate Certificate Request** window.



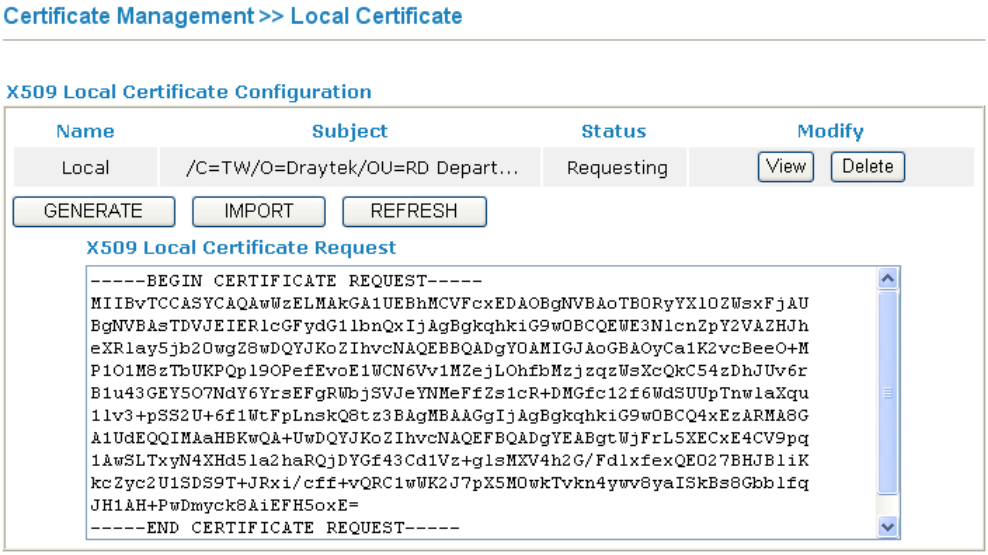

Type in all the information that the window request. Then click **Generate** again.

**Import** Click this button to import a saved file as the certification information.

**Refresh** Click this button to refresh the information listed below.

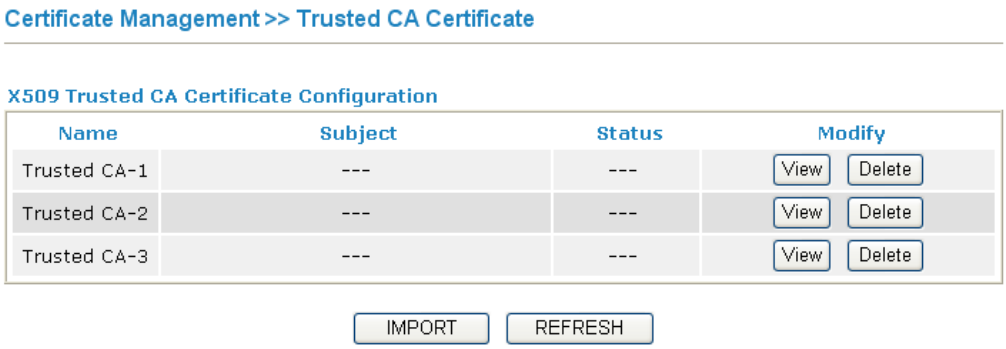
**View** Click this button to view the detailed settings for certificate request.

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

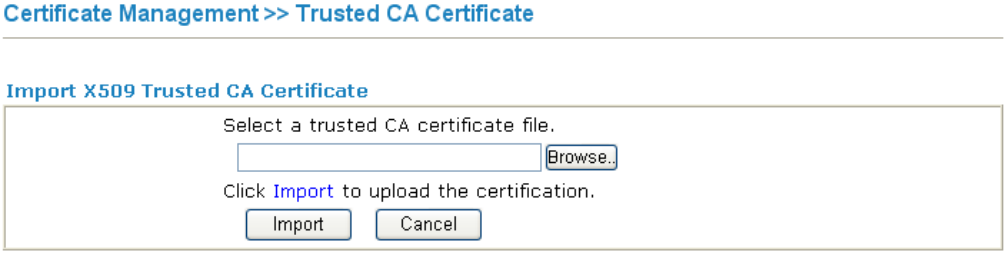



## 3.7.2 Trusted CA Certificate

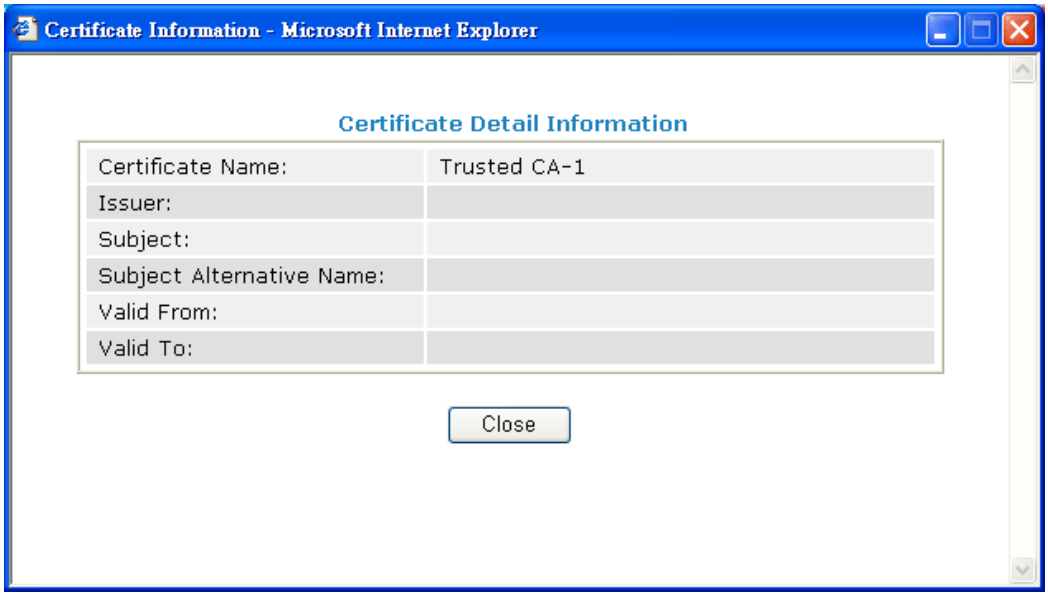
Trusted CA certificate lists three sets of trusted CA certificate.




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.




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.




## 3.8 VoIP

Voice over IP network (VoIP) enables you to use your broadband Internet connection to make toll quality voice calls over the Internet.

There are many different call signaling protocols, methods by which VoIP devices can talk to each other. The most popular protocols are SIP, MGCP, Megaco and H.323. These protocols are not all compatible with each other (except via a soft-switch server).

The Vigor V models support the SIP protocol as this is an ideal and convenient deployment for the ITSP (Internet Telephony Service Provider) and softphone and is widely supported. SIP is an end-to-end, signaling protocol that establishes user presence and mobility in VoIP structure. Every one who wants to talk using his/her SIP Uniform Resource Identifier, “SIP Address”. The standard format of SIP URI is

**sip: user:password @ host: port**

Some fields may be optional in different use. In general, "host” refers to a domain. The “userinfo” includes the user field, the password field and the @ sign following them. This is very similar to a URL so some may call it “SIP URL”. SIP supports peer-to-peer direct calling and also calling via a SIP proxy server (a role similar to the gatekeeper in H.323 networks), while the MGCP protocol uses client-server architecture, the calling scenario being very similar to the current PSTN network.

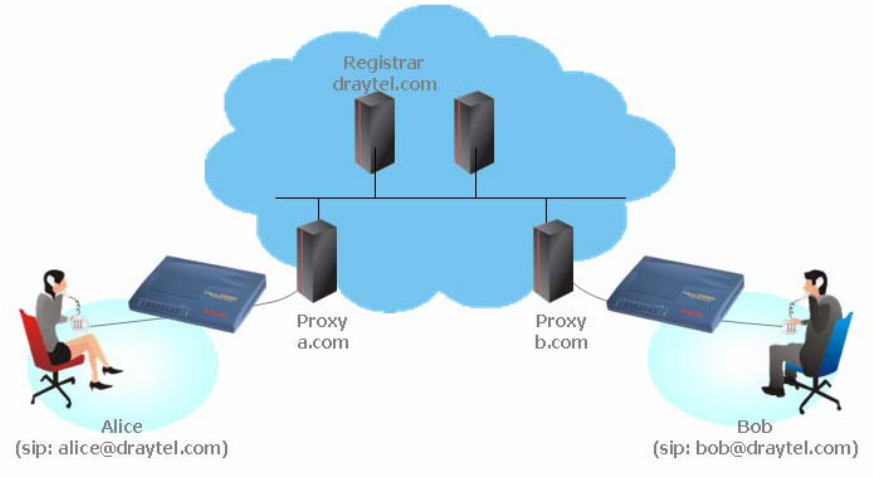
After a call is setup, the voice streams transmit via RTP (Real-Time Transport Protocol). Different codecs (methods to compress and encode the voice) can be embedded into RTP packets. Vigor V models provide various codecs, including G.711 A/μ-law, G.723, G.726 and G.729 A & B. Each codec uses a different bandwidth and hence provides different levels of voice quality. The more bandwidth a codec uses the better the voice quality, however the codec used must be appropriate for your Internet bandwidth.

Usually there will be two types of calling scenario, as illustrated below:

- **Calling via SIP Servers**

  First, the Vigor V models of yours will have to register to a SIP Registrar by sending registration messages to validate. Then, both parties’ SIP proxies will forward the sequence of messages to caller to establish the session.

  If you both register to the same SIP Registrar, then it will be illustrated as below:




The major benefit of this mode is that you don't have to memorize your friend's IP address, which might change very frequently if it's dynamic. Instead of that, you will only have to using **dial plan** or directly dial your friend's **account name** if you are with the same SIP Registrar. Please refer to the **Example 1 and 2 in the Calling Scenario.**

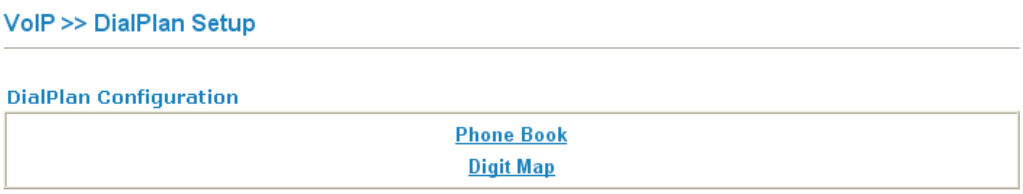
- **Peer-to-Peer**

  Before calling, you have to know your friend's IP Address. The Vigor VoIP Routers will build connection between each other. Please refer to the **Example 3 in the Calling Scenario.**


Our Vigor V models firstly apply efficient codecs designed to make the best use of available bandwidth, but Vigor V models also equip with automatic QoS assurance. QoS Assurance assists to assign high priority to voice traffic via Internet. You will always have the required inbound and outbound bandwidth that is prioritized exclusively for Voice traffic over Internet but you just get your data a little slower and it is tolerable for data traffic.

## 3.8.1 DialPlan

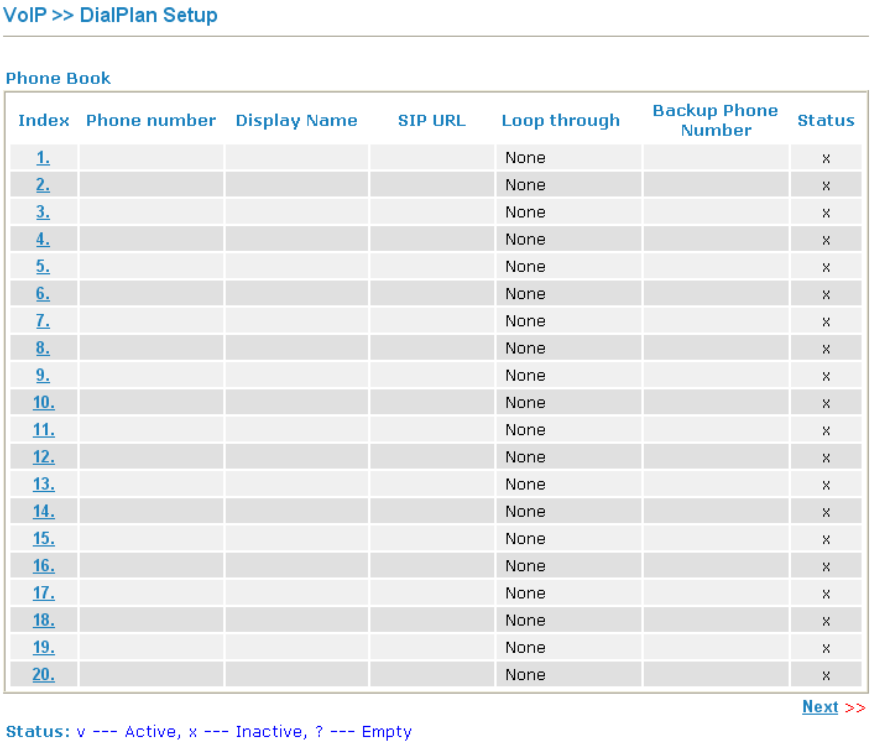
This page allows you to set phone book and digit map for the VoIP function. Click the **Phone Book** and **Digit Map** links on the page to access into next pages for dialplan settings.



## Phone Book

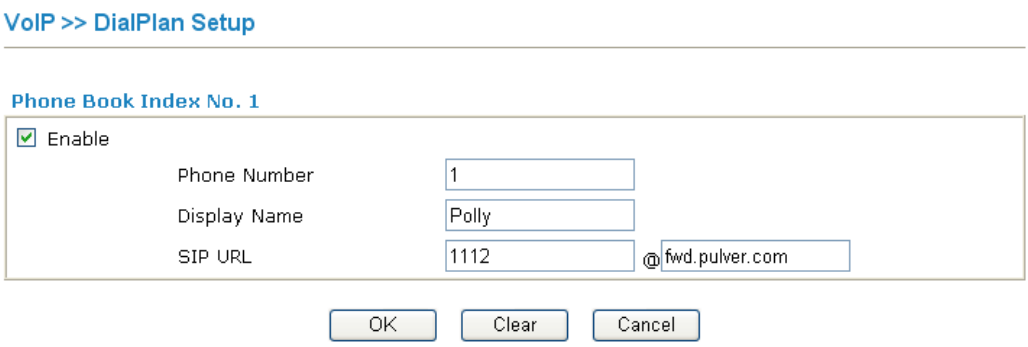
In this section, you can set your VoIP contacts in the “phonebook”, called DialPlan. It can help you to make calls quickly and easily by using “speed-dial” **Phone Number**. There are total 60 index entries in the DialPlan for you to store all your friends and family members’ SIP addresses.

For the models of Vigor 2700VGi/2700V (MODULE: 2S1L)/2700VG (MODULE: 2S1L), the phone book settings should be the same as the following:



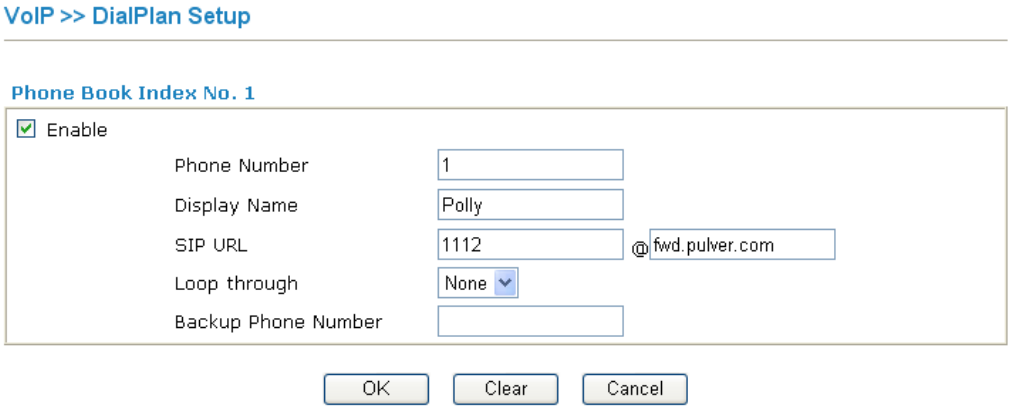

For the models of Vigor2700V (MODULE: 2S)/ 2700VG (MODULE: 2S), the phone book settings should be the same as the following:


Click any index number to display the dial plan setup page. Below is a sample page obtained from Vigor 2700V.



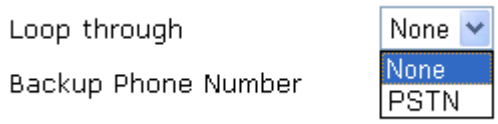

| | |
|---|---|
| **Enable** | Click this to enable this entry. |
| **Phone Number** | The speed-dial number of this index. This can be any number you choose, using digits **0-9** and ***** . |
| **Display Name** | The Caller-ID that you want to be displayed on your friend's screen. This let your friend can easily know who's calling without memorizing lots of SIP URL Address. |
| **SIP URL** | Enter your friend's SIP Address |

This page will differ for different models. Below is a sample page obtained from Vigor 2700VGi. The selection for **Loop through** differs slightly in Vigor 2700VGi and Vigor 2700V(MODULE: 2S1L)/VG (MODULE: 2S1L).




| | |
|---|---|
| **Enable** | Click this to enable this entry. |
| **Phone Number** | The speed-dial number of this index. This can be any number you choose, using digits **0-9** and ***** . |
| **Display Name** | The Caller-ID that you want to be displayed on your friend's screen. This let your friend can easily know who's calling without memorizing lots of SIP URL Address. |
| **SIP URL** | Enter your friend's SIP Address |
| **Loop through** | For the model of Vigor 2700V (MODULE: 2S1L)/ Vigor 2700VG (MODULE: 2S1L), the selection should be as the |

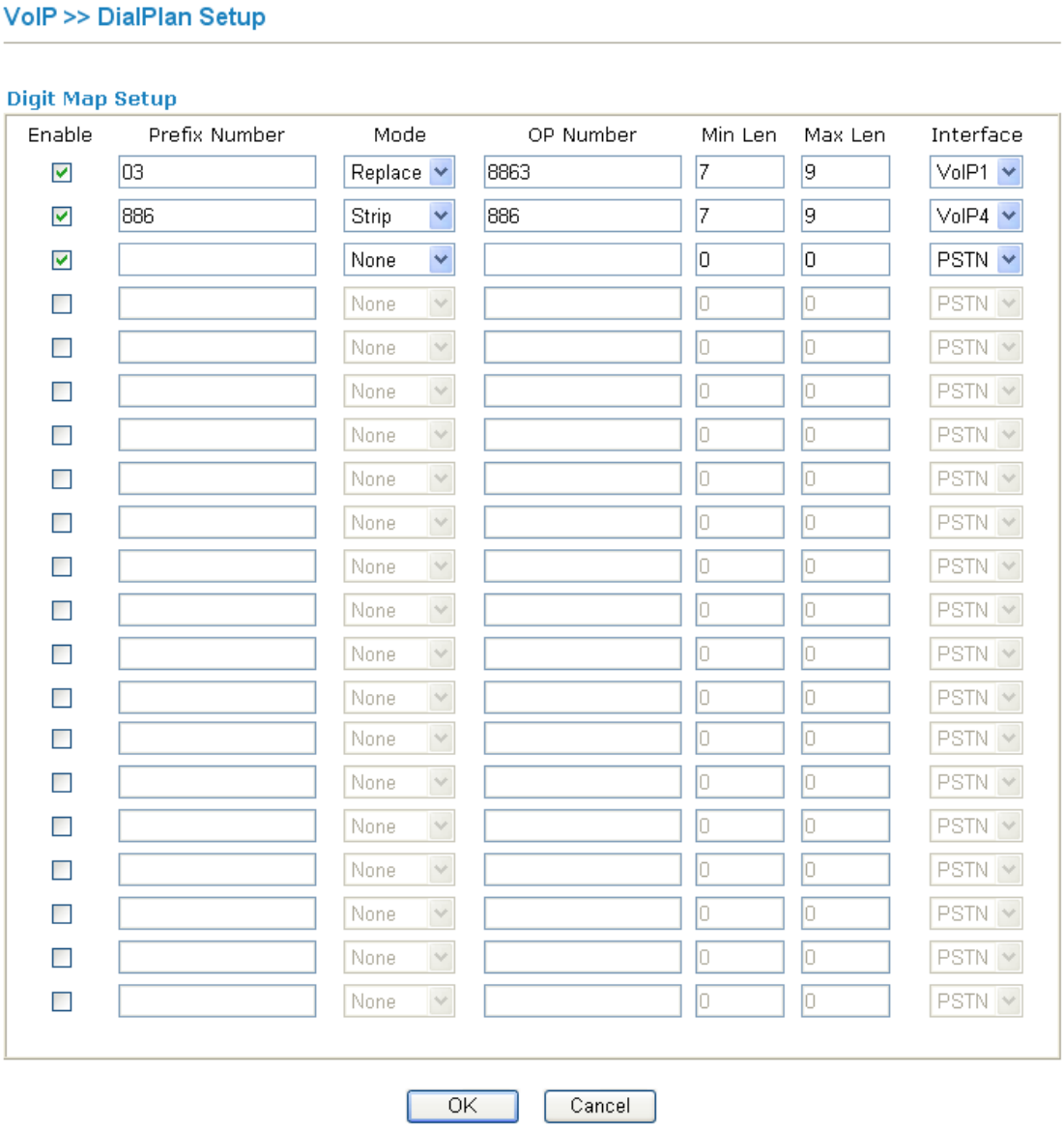
following:




**Backup Phone Number** When the VoIP phone is obstructs or the Internet breaks down for some reasons, the backup phone will be dialed out to replace the VoIP phone number. At this time, the phone call will be changed from VoIP phone into PSTN call according to the loop through direction chosen. Note that, during the phone switch, the blare of phone will appear for a short time. And when the VoIP phone is switched into the PSTN phone, the telecom co. might charge you for the connection fee. Please type in backup phone number (PSTN number) for this VoIP phone setting.

## Digit Map

For the convenience of user, this page allows users to edit prefix number for the SIP account with adding number, stripping number or replacing number. It is used to help user having a quick and easy way to dial out through VoIP interface.

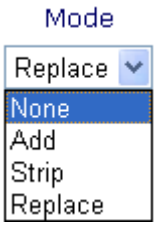



**Enable** — Check this box to invoke this setting.

**Prefix Number** — The phone number set here is used to add, strip, or replace the OP number.

**Mode** — **None** - No action.
**Add** - When you choose this mode, the OP number will be added with the prefix number for calling out through the specific VoIP interface.
**Strip** - When you choose this mode, the OP number will be deleted by the prefix number for calling out through the specific VoIP interface. Take the above picture (Prefix Table Setup web page) as an example, the OP number of *886* will be deleted completely for the prefix number is set with *886*.
**Replace** - When you choose this mode, the OP number will be

replaced by the prefix number for calling out through the specific VoIP interface. Take the above picture (Prefix Table Setup web page) as an example, the OP number of *8863* will be replaced completely by 03 for the prefix number is set with *03*.




**OP Number** The front number you type here is the first part of the account number that you want to execute special function (according to the chosen mode) by using the prefix number.

**Min Len** Set the minimal length of the dial number for applying the prefix number settings. Take the above picture (Prefix Table Setup web page) as an example, if the dial number between 7 and 9, that number can apply the prefix number settings here.

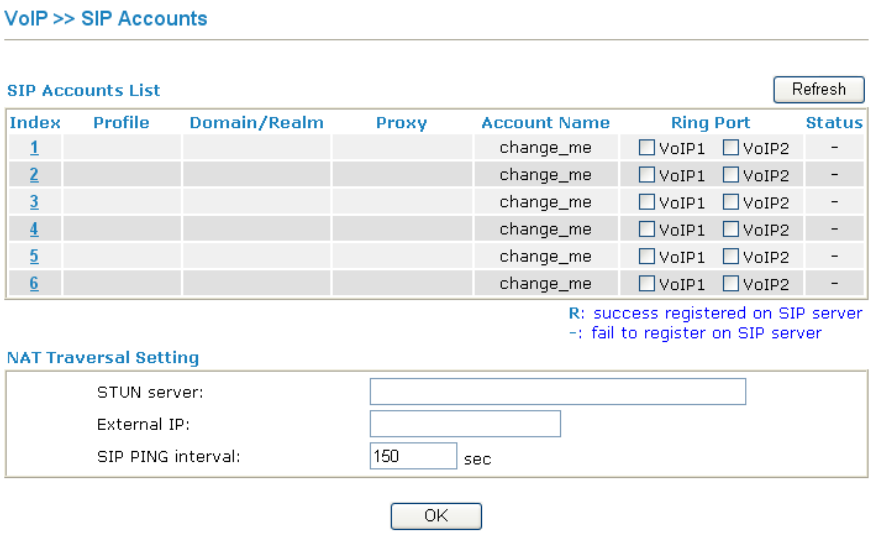
**Max Len** Set the maximum length of the dail number for applying the prefix number settings.

**Interface** Choose the one that you want to enable the prefix number settings from the seven pre-saved SIP accounts (including PSTN). The PSTN interface is available for 2700V (MODULE: 2S1L)/ Vigor 2700VG (MODULE: 2S1L) only.

## 3.8.2 SIP Accounts

In this section, you set up your own SIP settings. When you apply for an account, your SIP service provider will give you an **Account Name** or user name, **SIP Registrar, Proxy,** and **Domain name**. (The last three might be the same in some case). Then you can tell your folks your SIP Address as in **Account Name@ Domain name**

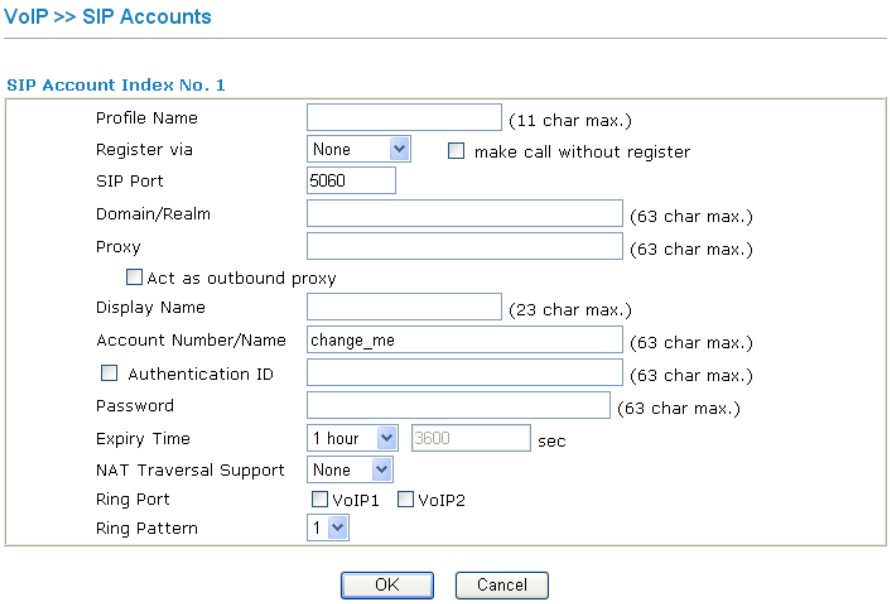
As Vigor VoIP Router is turned on, it will first register with Registrar using AuthorizationUser@Domain/Realm. After that, your call will be bypassed by SIP Proxy to the destination using AccountName@Domain/Realm as identity.



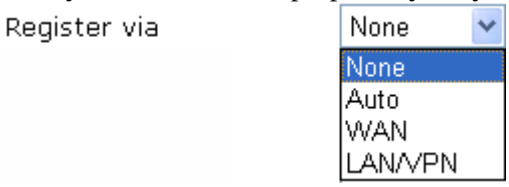

**Index** Click this link to access into next page for setting SIP account.

**Profile** Display the profile name of the account.

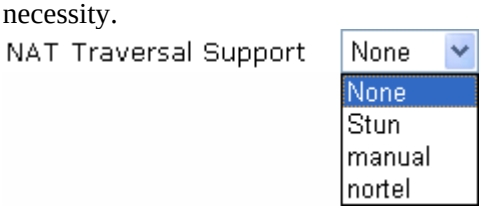
| | |
|---|---|
| **Domain/Realm** | Display the domain name or IP address of the SIP registrar server. |
| **Proxy** | Display the domain name or IP address of the SIP proxy server. |
| **Account Name** | Display the account name of SIP address before @. |
| **Ring Port** | Specify which port will ring when receiving a phone call. |
| **STUN Server** | Type in the IP address of the STUN server. |
| **External IP** | Type in the gateway IP address. |
| **SIP PING interval** | The default value is 150sec. It is useful for a Nortel server NAT Traversal Support. |
| **Status** | Show the status for the corresponding SIP account. **R** means such account is registered on SIP server successfully. **–** means the account is failed to register on SIP server. |



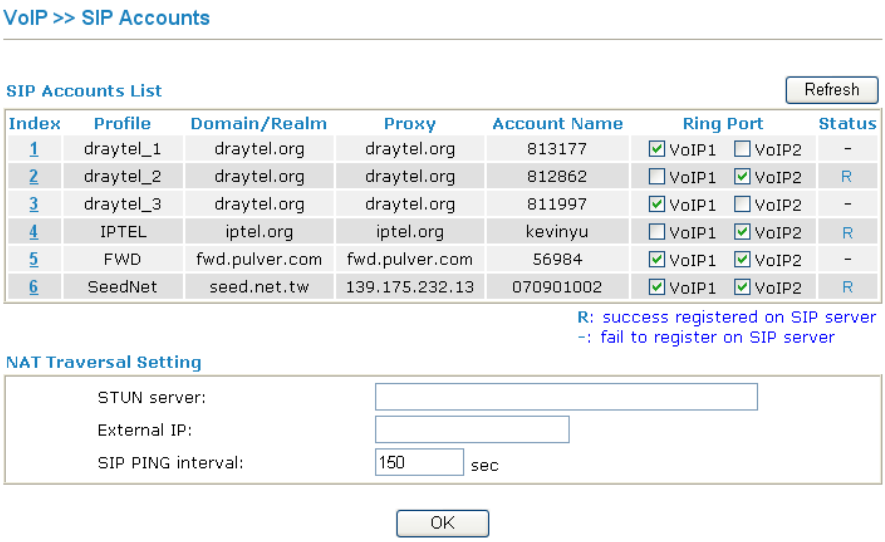

| | |
|---|---|
| **Profile Name** | Assign a name for this profile for identifying. You can type similar name with the domain. For example, if the domain name is *draytel.org*, then you might set *draytel-1* in this field. |
| **Register via** | If you want to make VoIP call without register personal information, please choose **None** and check the box to achieve the goal. Some SIP server allows user to use VoIP function without registering. For such server, please check the box of **make call without register**. Choosing **Auto** is recommended. The system will select a proper way for your VoIP call. |




| | |
|---|---|
| **SIP Port** | Set the port number for sending/receiving SIP message for building a session. The default value is **5060.** Your peer must set the same value in his/her Registrar. |
| **Domain/Realm** | Set the domain name or IP address of the SIP Registrar server. |

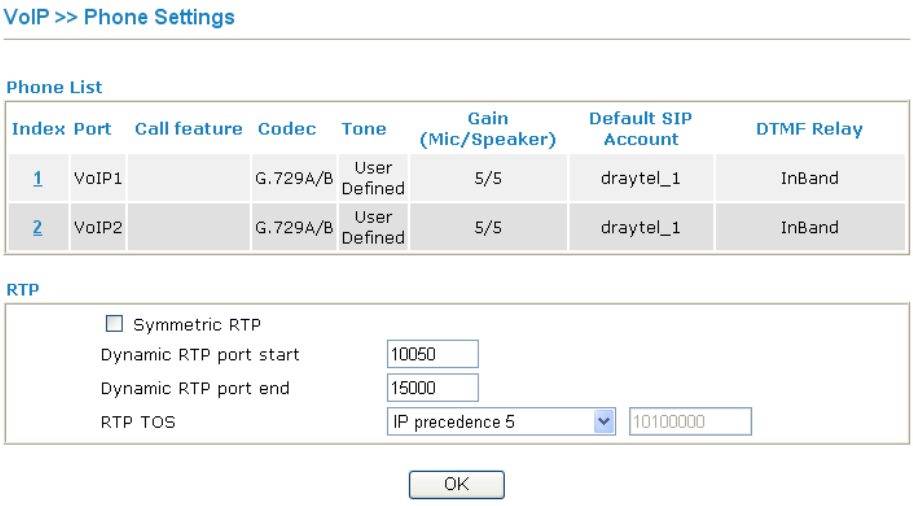
| | |
|---|---|
| **Proxy** | Set domain name or IP address of SIP proxy server. By the time you can type**:port** number after the domain name to specify that port as the destination of data transmission (e.g., nat.draytel.org**:5065**) |
| **Act as Outbound Proxy** | Check this box to make the proxy acting as outbound proxy. |
| **Display Name** | The caller-ID that you want to be displayed on your friend's screen. |
| **Account Number/Name** | Enter your account name of SIP Address, e.g. every text before @. |
| **Authentication ID** | Check the box to invoke this function and enter the name or number used for SIP Authorization with SIP Registrar. If this setting value is the same as Account Name, it is not necessary for you to check the box and set any value in this field. |
| **Password** | The password provided to you when you registered with a SIP service. |
| **Expiry Time** | The time duration that your SIP Registrar server keeps your registration record. Before the time expires, the router will send another register request to SIP Registrar again. |
| **NAT Traversal Support** | If the router (e.g.**,** broadband router) you use connects to internet by other device, you have to set this function for your necessity.<br>  <br>**None –** Disable this function.<br>**Stun** – Choose this option if there is Stun server provided for your router.<br>**Manual** – Choose this option if you want to specify an external IP address as the NAT transversal support.<br>**Nortel** – If the soft-switch that you use supports nortel solution, you can choose this option. |
| **Ring Port** | Set VoIP 1 or VoIP 2 as the default ring port. |
| **Ring Pattern** | Choose a ring tone type for the VoIP phone call.<br>  |

Below shows successful SIP accounts for your reference.




## 3.8.3 Phone Settings

This page allows user to set phone settings for VoIP 1 and VoIP 2 respectively.




**RTP**

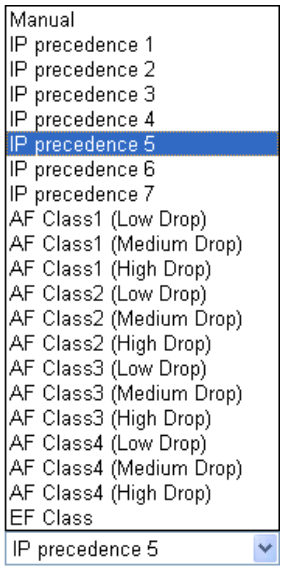
**Symmetric RTP** – Check this box to invoke the function. To make the data transmission going through on both ends of local router and remote router not misleading due to IP lost (for example, sending data from the public IP of remote router to the private IP of local router), you can check this box to solve this problem.

**Dynamic RTP port start** - Specifies the start port for RTP stream. The default value is 10050.

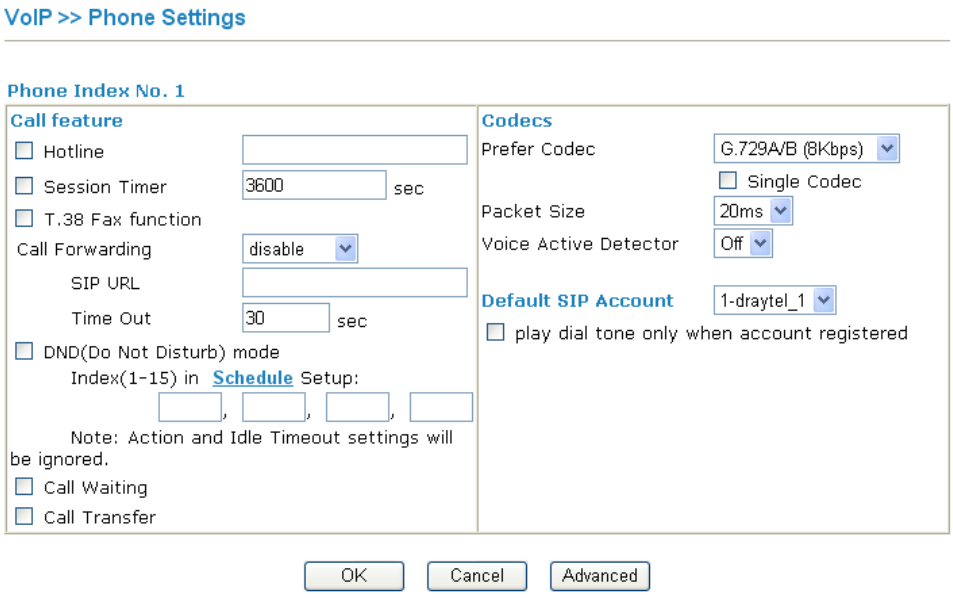
**Dynamic RTP port end** - Specifies the end port for RTP stream. The default value is 15000.

**RTP TOS** – It decides the level of VoIP package. Use the drop

down list to choose any one of them.




Click the number **1** or **2** link under Index column, you can access into the following page for configuring Phone settings.

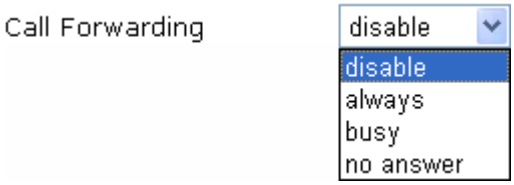



**Hotline** Check the box to enable it. Type in the SIP URL in the field for dialing automatically when you pick up the phone set.

**Session Timer** Check the box to enable the function. In the limited time that you set in this field, if there is no response, the connecting call will be closed automatically.

**T.38 Fax function** If the remote end also supports FAX function, you can check this box to enable this function.

**Call Forwarding** There are four options for you to choose. **Disable** is to close call forwarding function. **Always** means all the incoming calls will be forwarded into SIP URL without any reason. **Busy** means the incoming calls will be forwarded into SIP URL only when the local system is busy. **No answer** means if the incoming calls do not receive any response, they will be forwarded to the SIP URL by the time out.




**SIP URL** – Type in the SIP URL (e.g., aaa@draytel.org or abc@iptel.org) as the site for call forwarded.
**Time Out** – Set the time out for the call forwarding. The default setting is 30 sec.

**DND (Do Not Disturb) mode**

Set a period of peace time without disturbing by VoIP phone call. During the period, the one who dial in will listen busy tone, yet the local user will not listen any ring tone.

**Schedule -** Enter the index of schedule profiles to control the DND mode according to the preconfigured schedules. Refer to section **3.5.2 Schedule** for detailed configuration.

**Call Waiting**

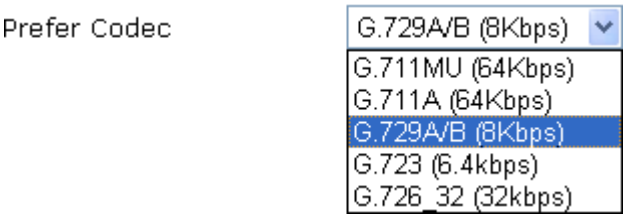
Check this box to invoke this function. A notice sound will appear to tell the user new phone call is waiting for your response. Click hook flash to pick up the waiting phone call.

**Call Transfer**

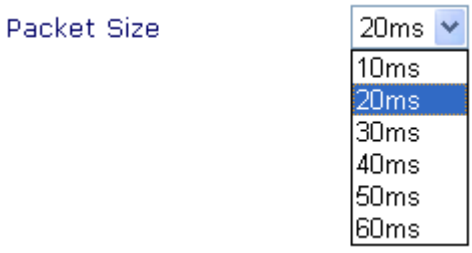
Check this box to invoke this function. Click hook flash to initiate another phone call. When the phone call connection succeeds, hang up the phone. The other two sides can communicate, then.

**Prefer Codec**

Select one of five codecs as the default for your VoIP calls. The codec used for each call will be negotiated with the peer party before each session, and so many not be your default choice. The default codec is G.729A/B; it occupies little bandwidth while maintaining good voice quality.
If your upstream speed is only 64Kbps, do not use G.711 codec. It is better for you to have at least 256Kbps upstream if you would like to use G.711.

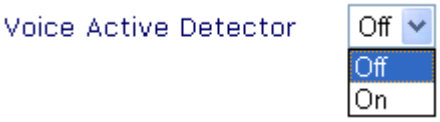



**Single Codec** – If the box is checked, only the selected Codec will be applied.
**Packet Size**-The amount of data contained in a single packet. The default value is 20 ms, which means the data packet will contain 20 ms voice information.




**Voice Active Detector -** This function can detect if the voice on both sides is active or not. If not, the router will do something to save the bandwidth for other using. Click On to

invoke this function; click off to close the function.

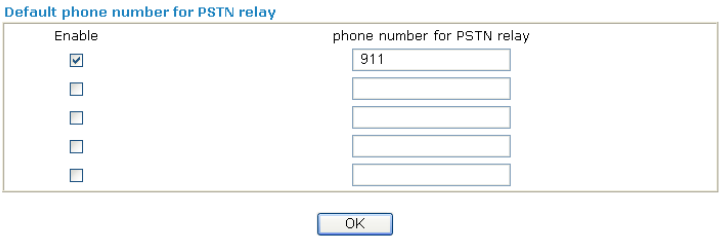



**Default SIP Account** — There are six groups of SIP accounts that you can set. Use the drop down list to choose the profile name of the account as the default one.

**Play dial tone only when account registered** — Check this box to invoke the function.

## 3.8.4 PSTN Setup

Some emergency phone (e.g., 911) or special phone cannot be dialed out by using VoIP and can be called out through PSTN line only. To solve this problem, this page allows you to set five sets of PSTN number for dialing without passing through Internet. Please type the number in the field of **phone number for PSTN relay**.

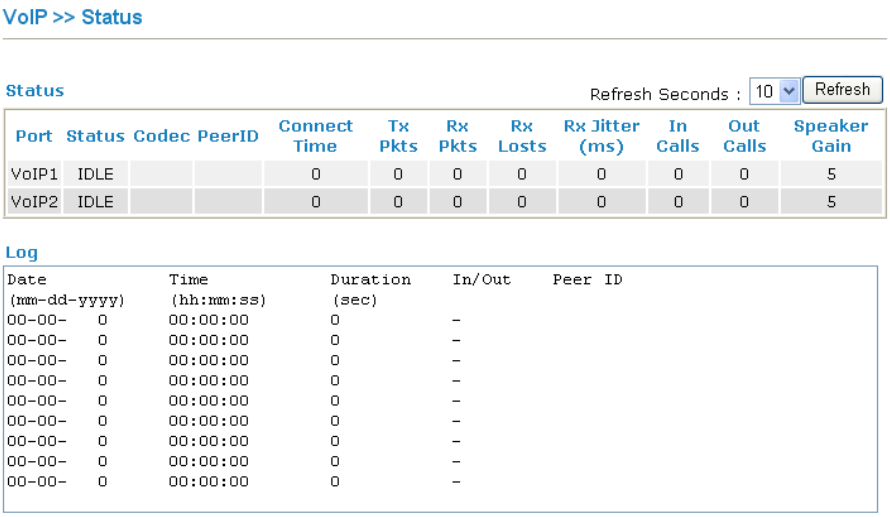



Then, check the **Enable** box to make the PSTN number available for dial whenever you need.

**Note:** This function is available for Vigor2700V/2700VG (MODULE 2S1L) only.

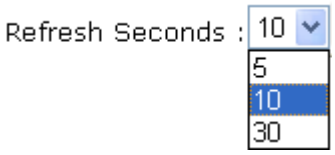
## 3.8.5 Status

On VoIP call status, you can find codec, connection and other important call status for both VoIP 1 and 2 ports.




**Refresh Seconds** — Specify the interval of refresh time to obtain the latest VoIP calling information. The information will update immediately

when the Refresh button is clicked.



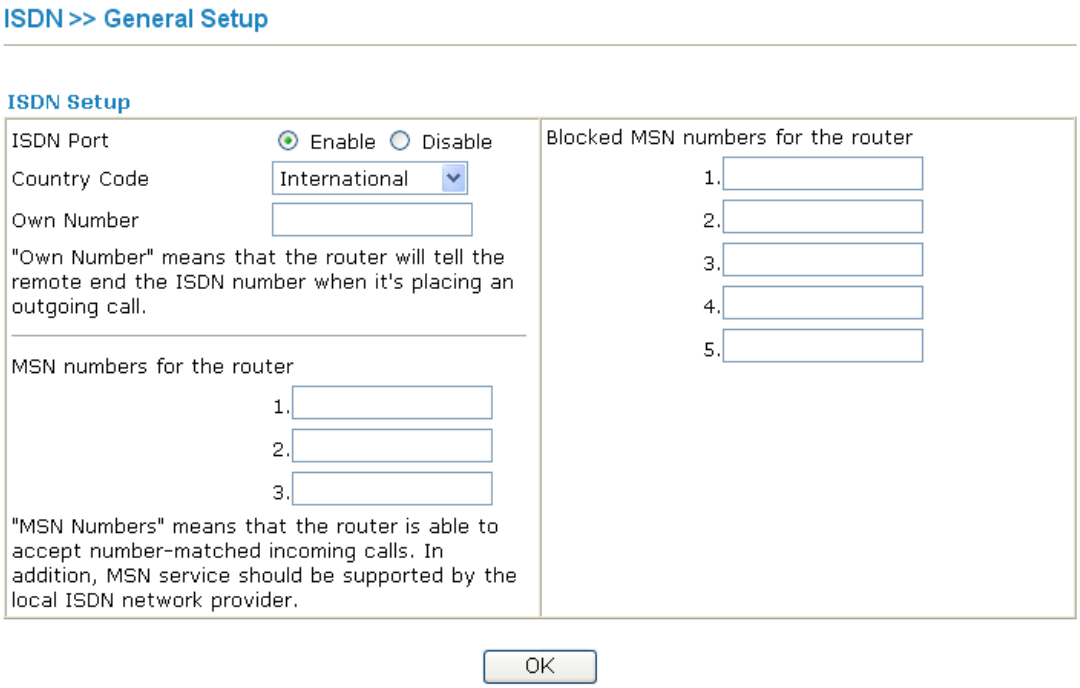

| | |
|---|---|
| **Port** | It shows current connection status for the port of VoIP1 and VoIP2. |
| **Status** | It shows the VoIP connection status.<br>**IDLE -** Indicates that the VoIP function is idle.<br>**HANG_UP -** Indicates that the connection is not established (busy tone).<br>**CONNECTING -** Indicates that the user is calling out.<br>**WAIT_ANS -** Indicates that a connection is launched and waiting for remote user's answer.<br>**ALERTING -** Indicates that a call is coming.<br>**ACTIVE-**Indicates that the VoIP connection is launched. |
| **Codec** | Indicates the voice codec employed by present channel. |
| **PeerID** | The present in-call or out-call peer ID (the format may be IP or Domain). |
| **Connect Time** | The format is represented as seconds. |
| **Tx Pkts** | Total number of transmitted voice packets during this connection session. |
| **Rx Pkts** | Total number of received voice packets during this connection session. |
| **Rx Losts** | Total number of lost packets during this connection session. |
| **Rx Jitter** | The jitter of received voice packets. |
| **In Calls** | The accumulating times of in-call. |
| **Out Calls** | The accumulating times of out-call. |
| **Speaker Gain** | The volume of present call. |
| **Log** | Display logs of VoIP calls. |

## 3.9 ISDN

ISDN stands for Integrated Services Digital Network. It is an international communications standard for sending voice, video, and data over digital telephone lines.

> Note: The feature is available for ***i*** models only.

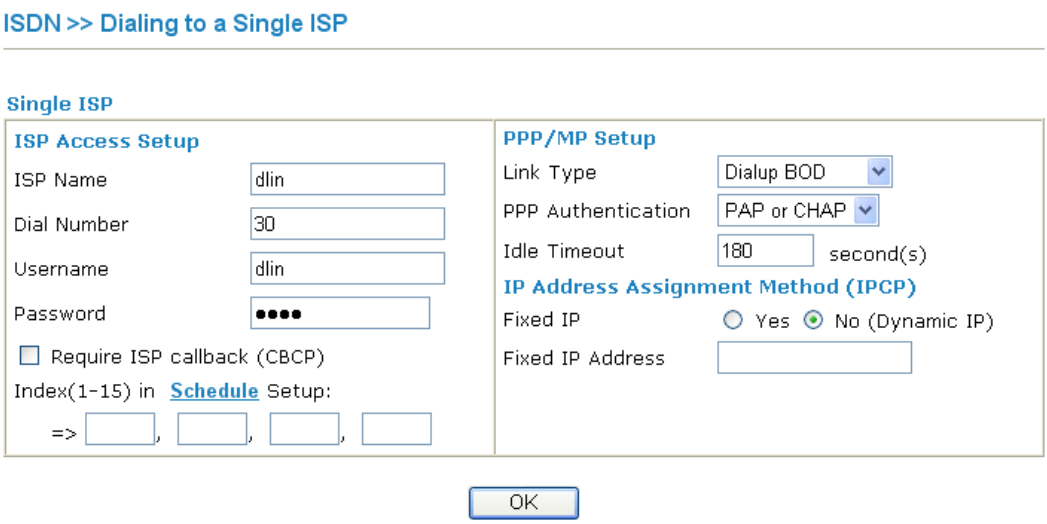
### 3.9.1 General Setup




| | |
|---|---|
| **ISDN Port** | Click **Enable** to open the ISDN port and **Disable** to close it. |
| **Country Code** | For proper operation on your local ISDN network, you should choose the correct country code. |
| **Own Number** | Enter your ISDN number. Every outgoing call will carry the number to the receiver. |
| **MSN Numbers for the Router** | **MSN Numbers** mean that the router is able to accept only number-matched incoming calls. In addition, MSN services should be supported by local ISDN network provider. The router provides three fields for MSN numbers. Note that MSN services must be acquired from your local telecommunication operators. By default, MSN function is disabled. If you leave the fields blank, all incoming calls will be accepted without number matching. |
| **Blocked MSN Numbers for the router** | Enter the specified MSN number into the fields to prevent the router from dialing the specific MSN number. |

### 3.9.2 Dialing to a Single ISP

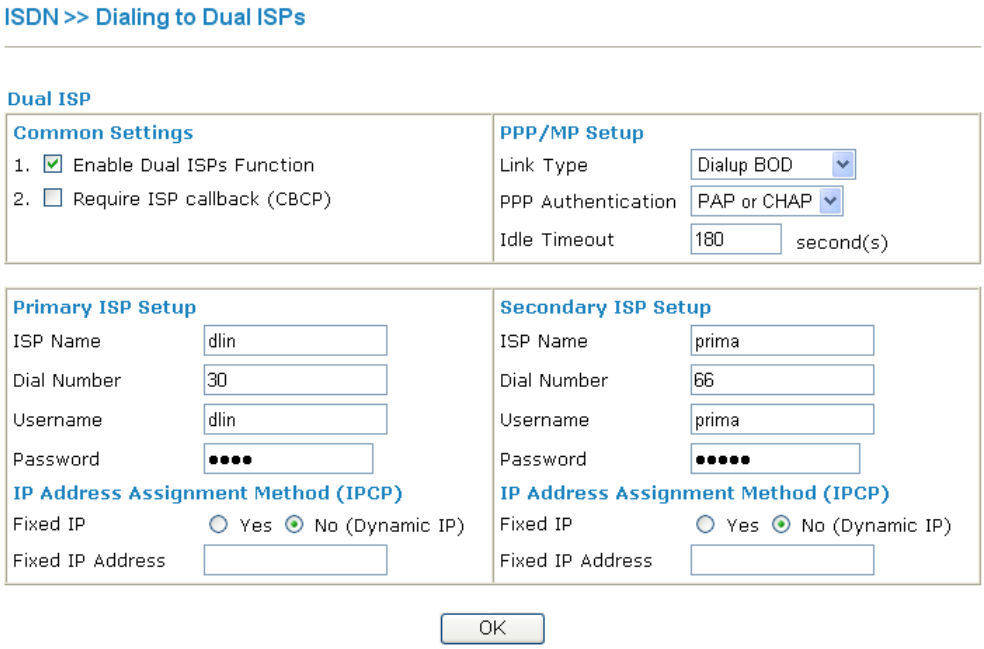
If you access the Internet via a single ISP, press this link.




| | |
|---|---|
| **ISP Name** | Enter your ISP name. |
| **Dial Number** | Enter the ISDN access number provided by your ISP. |
| **Username** | Enter the username provided by your ISP. |
| **Password** | Enter the password provided by your ISP. |
| **Require ISP Callback (CBCP)** | If your ISP supports the callback function, check this box to activate the Callback Control Protocol during the PPP negotiation. |
| **Scheduler (1-15)** | Enter the index of schedule profiles to control the Internet access according to the preconfigured schedules. |
| **Link Type** | There are four link types: Link Disable, Dialup 64 Kbps, Dialup 128 Kbps, and Dialup BOD.<br>**Link Disable** - Disable the ISDN dial-out function.<br>**Dialup 64Kbps** - Use one ISDN B channel for Internet access.<br>**Dialup 128Kbps** - Use both ISDN B channels for Internet access.<br>**Dialup BOD** - BOD stands for bandwidth-on-demand. The router will use only one B channel in low traffic situations. Once the single B channel bandwidth is fully used, the other B channel will be activated automatically through the dialup. For more detailed BOD parameter settings, please refer to the **Advanced Setup** field > **Call Control and PPP/MP Setup**. |
| **PPP Authentication** | **PAP Only** - Configure the PPP session to use the PAP protocol to negotiate the username and password with the ISP.<br>**PAP or CHAP** - Configure the PPP session to use the PAP or CHAP protocols to negotiate the username and password with the ISP. |
| **Idle Timeout** | Idle timeout means the router will be disconnect after being idle for a preset amount of time. The default is 180 seconds. If you set the time to 0, the ISDN connection to the ISP will always remain on. |
| **Fixed IP** | In most environments, you should not change these settings as most ISPs provide a dynamic IP address for the router when it connects to the ISP. If your ISP provides a fixed IP address, check **Yes t**o invoke this function and enter the IP address in the field of **Fixed IP Address**. |
| **Fixed IP Address** | Type the IP address. |

## 3.9.3 Dialing to Dual ISPs

If you have more than one ISP, press this link to configure two ISP dialup profiles. You will be able to dial to both ISPs at the same time. This is mainly for those ISPs that do not support Multiple-Link PPP (ML-PPP) function. In such cases, dialing to two ISPs can increase the bandwidth utilization of the ISDN channels to 128kbps data speed.

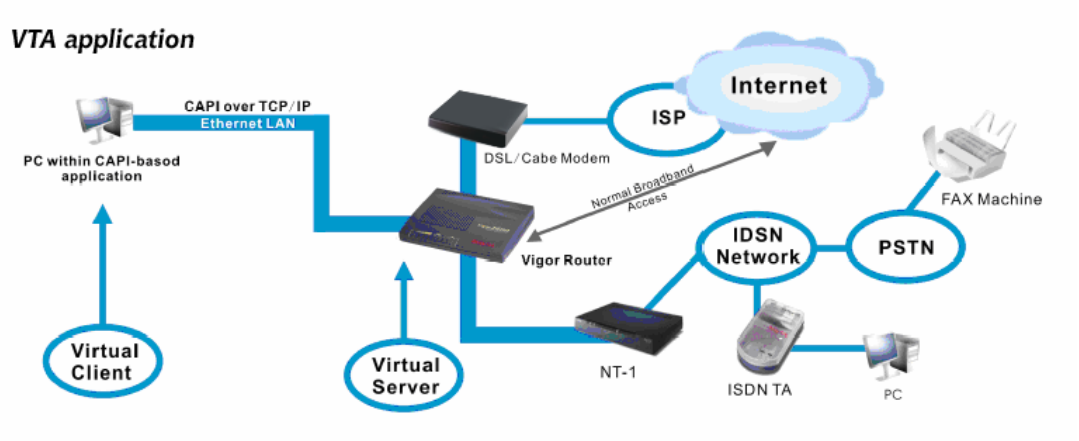



Most configuration parameters are the same as those of the previous part. This screen provides a checkbox to enable the Dual ISPs function and adds the secondary ISP Setup section field. Check the corresponding box and enter the second ISP information. About the details please refer to the descriptions of the previous part.

## 3.9.4 Virtual TA

**Virtual TA** means the local hosts or PCs in the network that uses popular CAPI-based software such as RVS-COM or BVRP to access the router as a local ISDN TA for sending or receiving FAX messages over the ISDN line. Basically, it is a client/server network model. The built-in Virtual TA server handles the establishment and release of connections. The Virtual TA client, which is installed on the local hosts or PCs, creates a CAPI-based driver to relay all CAPI messages between the applications and the router CAPI module. Before describing the configuration of **Virtual TA** in the Vigor routers, please notice the following limitations.

- The Virtual TA client only supports Microsoft™ Windows 95 OSR2.1/98/98SE/Me/2000 platforms.
- The Virtual TA client only supports the CAPI 2.0 protocol and has no built-in FAX engine.
- One ISDN BRI interface has two B channels. The maximum number of active clients is also two.
- Before you configure the Virtual TA, you must set the correct country code.




As depicted in the above application scenario, the Virtual TA client can make an outgoing call or accept an incoming call to/from a peer FAX machine or ISDN TA, etc.

Before you configure the Virtual TA (Remote CAPI) Setup, please install the virtual TA client first. Simply insert the CD bundled with your Vigor router, or directly double-click one of the installer files. In which **Vsetup95.exe** is for Windows 95 OSR2.1 or higher; **Vsetup98.exe** is for Windows 98, 98SE and Me; and **Vsetup2k.exe** is for Windows 2000. Follow the on-screen instructions of the installer. The last step will ask you to restart your computer. Click **OK** to restart your computer.

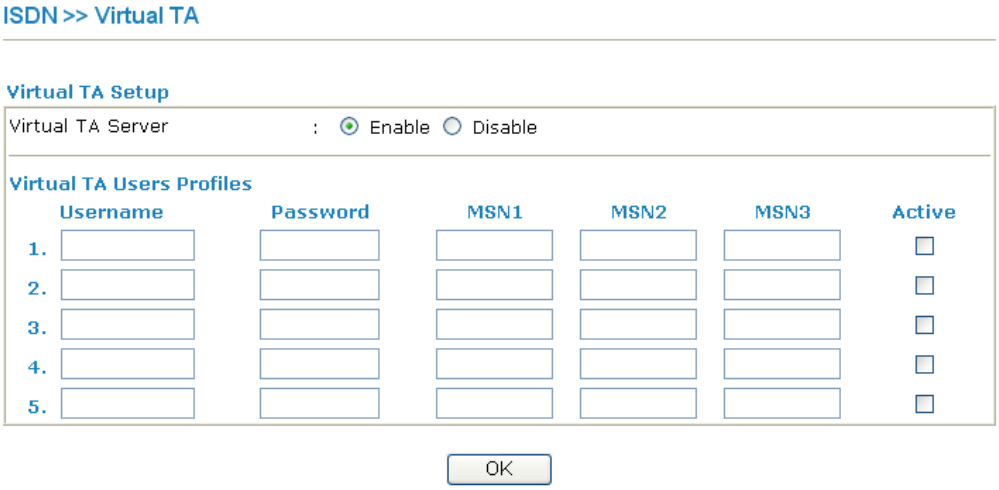
After the computer restarts, you will see a VT icon in the taskbar (usually in the bottom-right of the screen, near the clock) as shown below.


When the icon text is GREEN, the Virtual TA client is connected to the Virtual TA server and you can launch your CAPI-based software to use the client to access the router. Please read your software user guide for detailed configuration. If the icon text is RED, it means the client has lost the connection to the server. In such condition, please check the physical Ethernet connection.


Next, click the **Virtual TA (Remote CAPI) Setup** link in the **Quick Setup** group to configure the Virtual TA features.

Since the Virtual TA application is a client/server network model, you must configure it on both ends to run properly your Virtual TA application.

By default, the Virtual TA server is enabled and the Username/Password fields are left blank. Any Virtual TA client may login to the server. Once a single Username/Password field has been filled in, the Virtual TA server will only allow clients with a valid Username/Password to login. The screen of Virtual TA configuration is presented below.




| | |
|---|---|
| **Virtual TA Server** | **Enable:** Select it to activate the server.<br>**Disable:** Select it to deactivate the server. All Virtual TA applications will be terminated. |
| **Username** | Enter the username of a specific client. |
| **Password** | Enter the password of a specific client. |
| **MSN1/ MSN2/MSN3** | MSN stands for **Multiple Subscriber Number**. It means you can apply to more than one ISDN lines number over a single subscribed line. Note that the service must be acquired from your telecom. Specify the MSN numbers for a specific client. If you have no MSN services, leave this field blank. |
| **Active** | Check it to enable the client to access the server. |

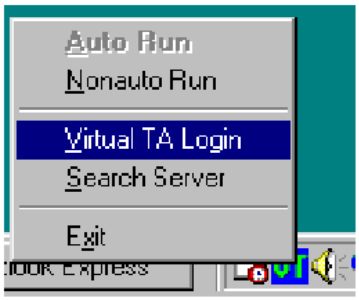
## User Profile

Note that creating a single user access account will limit the access to the Virtual TA server to only the specified account holders.

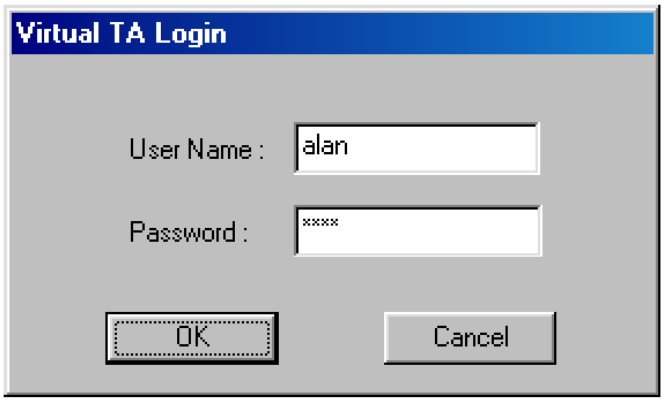
Assume you did not acquire any MSN service from your ISDN network provider.

**On the server** - Click **Virtual TA (Remote CAPI) Setup** link, and fill in the Username and Password fields. Check the **Active** box to enable the account.


**On the client** - Right-click the mouse on the VT icon. The following pop-up menu will be shown.



Click the **Virtual TA Login** tab to launch the login box.

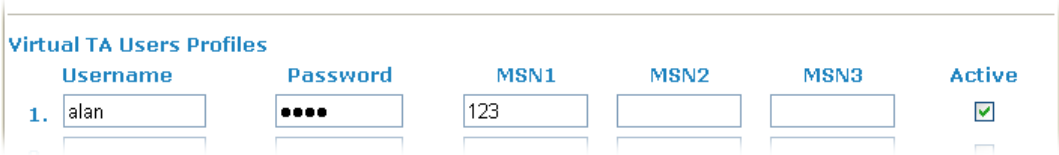



Enter the Username/Password and then click **OK**. After a short time, the VT icon text will turn green.

## MSN Configuration

If you have applied to an MSN number service, the Virtual TA server can assign which client has the specified MSN number. When an incoming call arrives, the server will inform the appropriate client. Now we set an example to describe the configuration of the MSN number.

Suppose that you could assign the MSN number **123** to the client “alan”.



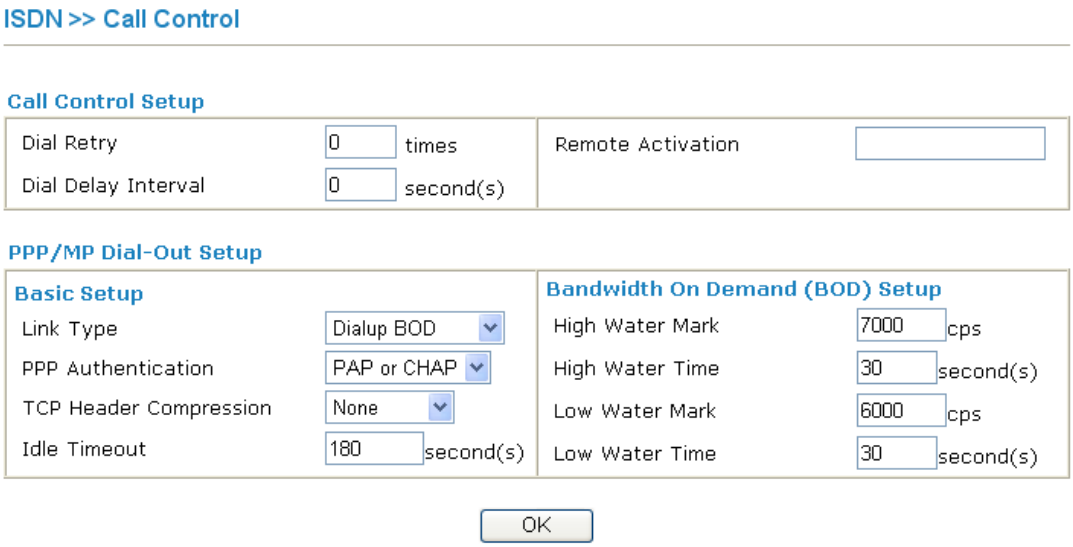

Type the specified MSN number in the CAPI-based software. When the Virtual TA server sends an alert signal to the specified Virtual TA client, the CAPI-based software will also receive the action, the software will not accept the incoming call.

## 3.9.5 Call Control

Some applications require that the router (only for *i* models) be remotely activated, or be able to dial up to the ISP via the ISDN interface. Vigor routers provide this feature which allows you to make a phone call to the router and then ask it to dial up to the ISP.

**Note:** Call Control is only available for *i* models equipped with the ISDN interface.

Please set **Dialing to a Single ISP** first before configuring this web page.

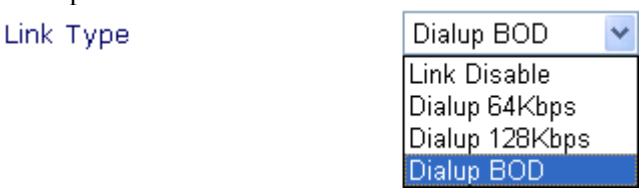



**Dial Retry** — It specifies the dial retry counts per triggered packet. A triggered packet is the packet whose destination is outside the local network. The default setting is no dial retry. If set to 5, for each triggered packet, the router will dial 5 times until it is connected to the ISP or remote access router.

**Dial Delay Interval** — It specifies the interval between dialup retries. By default, the interval is 0 second.

**Remote Activation** — It specifies a phone number in the **Remote Activation** field to enable the remote activation function. If the router accepts a call from the number 12345678, it will terminate the incoming call immediately and dial to the ISP.

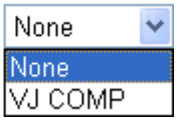
**Link Type** — Because ISDN has two B channels (64Kbps/per channel), you can specify whether you would like to have single B channel, two B channels or BOD (Bandwidth on Demand). Four options are available: Link Disable, Dialup 64Kbps, Dialup 128Kbps, Dialup BOD.




**PPP Authentication** — It specifies the PPP authentication method for PPP/MP connections. Normally you can set it to **PAP/CHAP** for better compatibility.

**TCP Header Compression** — **VJ Compression** - It is used for TCP/IP protocol header compression. Normally it is set to **None** to improve bandwidth

utilization.

TCP Header Compression 


| | |
|---|---|
| **Idle Timeout** | Because our ISDN link type is “Dial On Demand”, the connection will be initiated only when needed. |
| **High Water Mark and High Water Time** | BOD stands for bandwidth-on-demand for Multiple-Link PPP (ML-PPP or MP). **High Water Mark/ High Water Time/ Low Water Mark/Low Water Time** parameters are applied when you set the **Link Type** to **Dialup BOD**. The ISDN usually uses one B channel to access the Internet or remote network when you choose the Dialup BOD link type. The router will use the parameters here to decide on when you activate/drop the additional B channel. Note that **cps** (characters-per-second) measures the total link utilization.<br><br>These parameters specify the situation in which the second channel will be activated. With the first connected channel, if its utilization exceeds the High Water Mark and such a channel is being used over the High Water Time, the additional channel will be activated. Thus, the total link speed will be 128kbps (two B channels). |
| **Low Water Mark and Low Water Time** | These parameters specify the situation in which the second channel will be dropped. In terms of the two B channels, if their utilization is under the Low Water Mark and these two channels are being used over the High Water Time, the additional channel will be dropped. As a result, the total link speed will be 64kbps (one B channel). |

**Note:** If you are not sure whether your ISP can support BOD and/or ML-PPP’s features, please seek assistance from your ISP, local dealers or our website: **support@draytek.com**.

## 3.10 Wireless LAN

Note: This function is used for G models only.

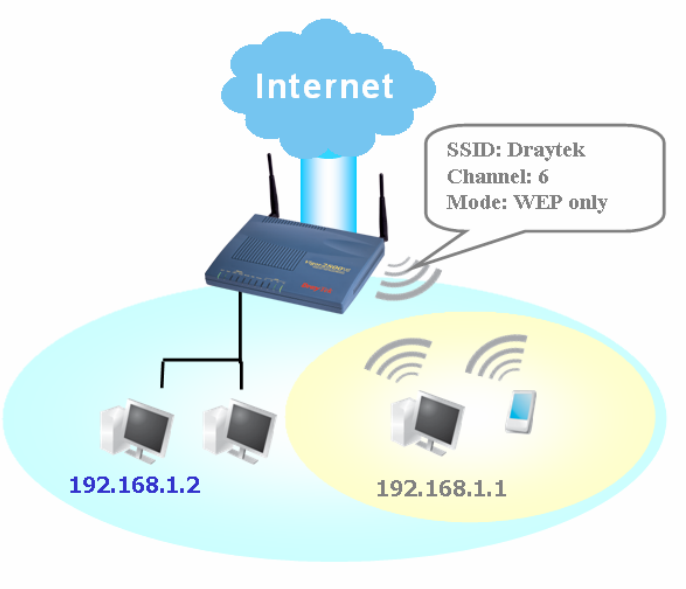
Over recent years, the market for wireless communications has enjoyed tremendous growth. Wireless technology now reaches or is capable of reaching virtually every location on the surface of the earth. Hundreds of millions of people exchange information every day via wireless communication products. The Vigor G model, a.k.a. Vigor wireless router, is designed for maximum flexibility and efficiency of a small office/home. Any authorized staff can bring a built-in WLAN client PDA or notebook into a meeting room for conference without laying a clot of LAN cable or drilling holes everywhere. Wireless LAN enables high mobility so WLAN users can simultaneously access all LAN facilities just like on a wired LAN as well as Internet access.

The Vigor wireless routers are equipped with a wireless LAN interface compliant with the standard IEEE 802.11g protocol. To boost its performance further, the Vigor Router is also loaded with advanced wireless technology Super G ™ to lift up data rate up to 108 Mbps*. Hence, you can finally smoothly enjoy stream music and video.

Note: * The actual data throughput will vary according to the network conditions and environmental factors, including volume of network traffic, network overhead and building materials.

## 3.10.1 Basic Concept

In an Infrastructure Mode of wireless network, Vigor wireless router plays a role as an Access Point (AP) connecting to lots of wireless clients or Stations (STA). All the STAs will share the same Internet connection with other wired hosts via Vigor wireless router. The **General Settings** will set up the information of this wireless network, including its SSID as identification, located channel etc.




### Security Overview

**Real-time Hardware Encryption:** Vigor Router is equipped with a hardware AES encryption engine so it can apply the highest protection to your data without influencing user experience.

**Complete Security Standard Selection:** To ensure the security and privacy of your wireless communication, we provide several prevailing standards on market.

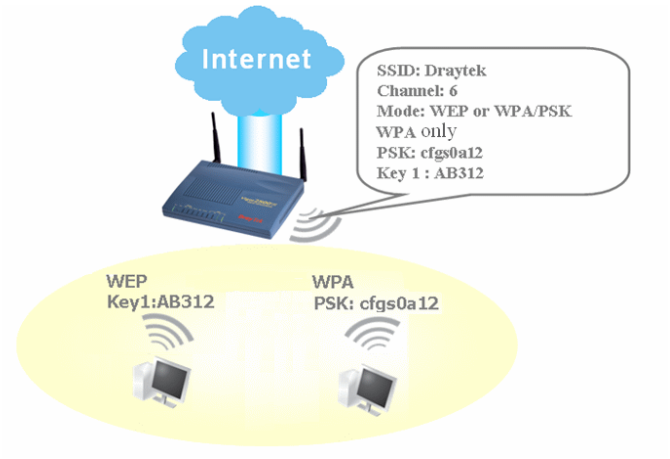
WEP (Wired Equivalent Privacy) is a legacy method to encrypt each frame transmitted via radio using either a 64-bit or128-bit key. Usually access point will preset a set of four keys and it will communicate with each station using only one out of the four keys.

WPA(Wi-Fi Protected Access), the most dominating security mechanism in industry, is separated into two categories: WPA-personal or called WPA Pre-Share Key (WPA/PSK), and WPA-Enterprise or called WPA/802.1x.

In WPA-Personal, a pre-defined key is used for encryption during data transmission. WPA applies Temporal Key Integrity Protocol (TKIP) for data encryption while WPA2 applies AES. The WPA-Enterprise combines not only encryption but also authentication.

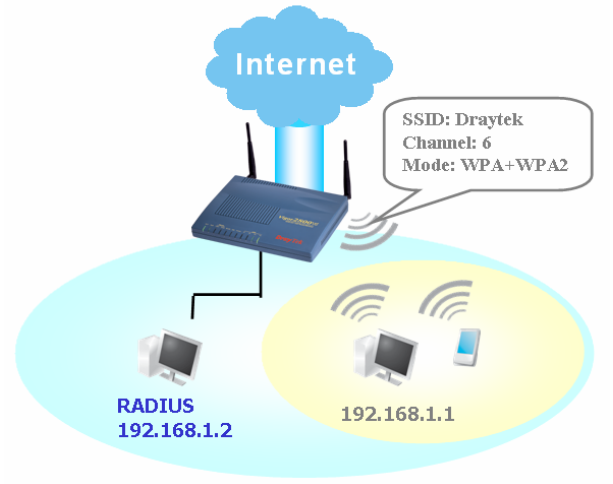
Since WEP has been proved vulnerable, you may consider using WPA for the most secure connection. You should select the appropriate security mechanism according to your needs. No matter which security suite you select, they all will enhance the over-the-air data protection and /or privacy on your wireless network. The Vigor wireless router is very flexible and can support multiple secure connections with both WEP and WPA at the same time.

***Example 1***




***Example 2***


***Example 3***

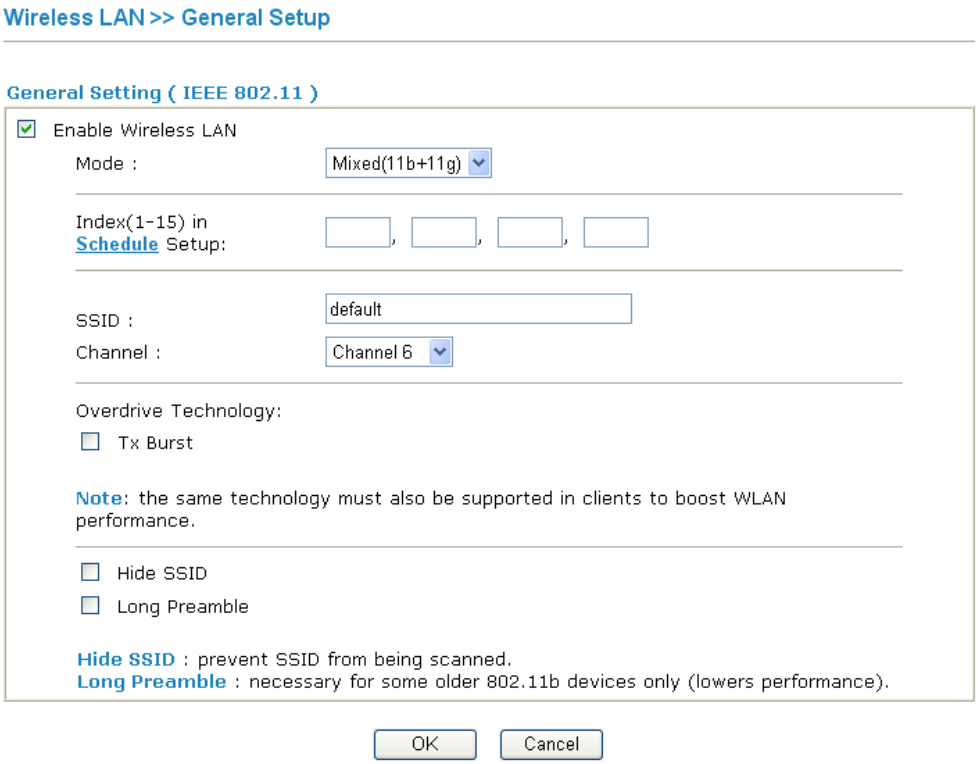



**Separate the Wireless and the Wired LAN- WLAN Isolation** enables you to isolate your wireless LAN from wired LAN for either quarantine or limit access reasons. To isolate means neither of the parties can access each other. To elaborate an example for business use, you may set up a wireless LAN for visitors only so they can connect to Internet without hassle of the confidential information leakage. For a more flexible deployment, you may add a filter of MAC address to isolate single user's access from wired LAN.

**Manage Wireless Stations - Station List** will display all the station in your wireless network and the status of their connection.

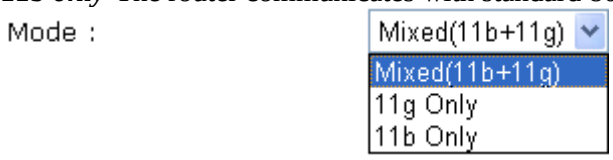
## 3.10.2 General Settings

By clicking the **General Settings**, a new web page will appear so that you could configure the SSID and the wireless channel. Please refer to the following figure for more information.




**Enable Wireless LAN** Check the box to enable wireless function.

**Mode** Select an appropriate wireless mode.
***Mixed (11b+11g)***-The router communicates with standard 802.11b and standard 802.11g STAs simultaneously.
***11g only***-The router communicates with standard 802.11b STAs.
***11b only***-The router communicates with standard 802.11b STAs.




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

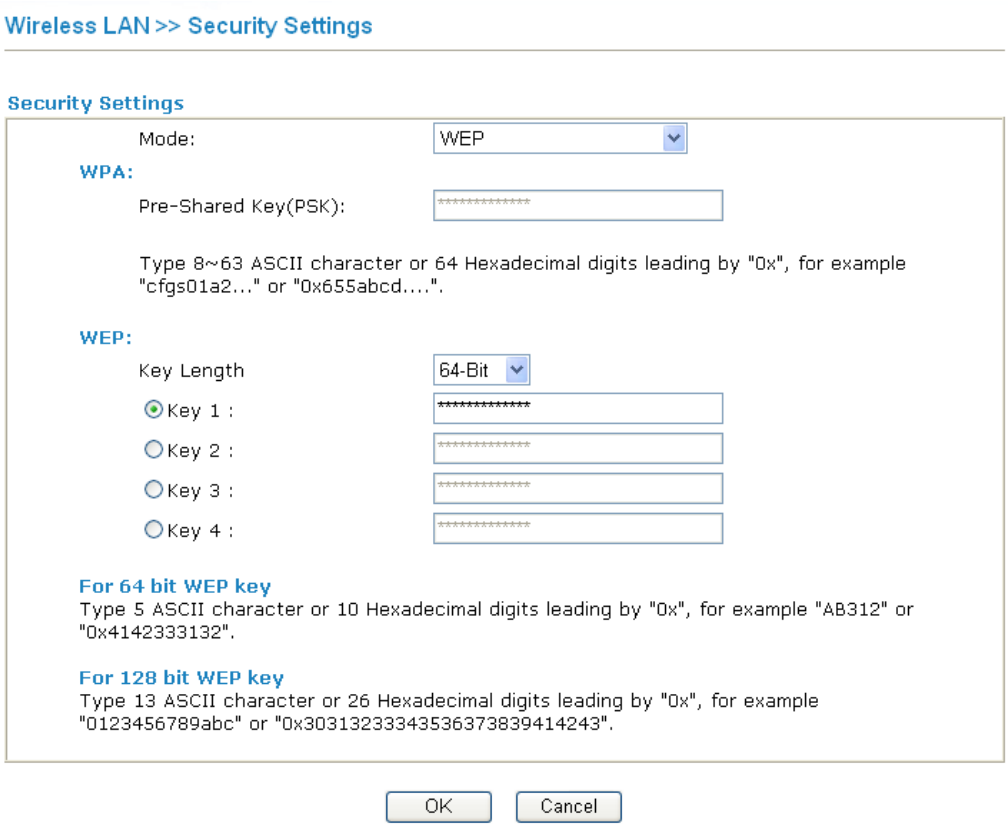
**SSID and Channel** The default SSID is "default". We suggest you to change it.
***SSID***- Means the identification of the wireless LAN. SSID can be any text numbers or various special characters.
***Channel***- Means the channel of frequency of the wireless LAN. The default channel is 6. You may switch channel if the selected channel is under serious interference.

**Hide SSID** Check it to prevent from wireless sniffing and make it harder for unauthorized clients or STAs to join your wireless LAN. Depending on the wireless utility, the user may only see the information except SSID or just cannot see any thing about Vigor wireless router while doing site survey

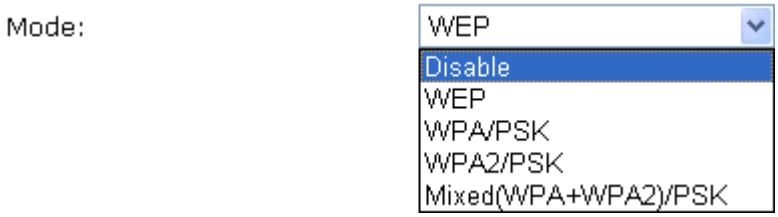
**Long Preamble** This option is to define the length of the sync field in an 802.11 packet. Most modern wireless network uses short preamble with 56 bit sync filed instead of long preamble with 128 bit sync field. However, some original 11b wireless network device only support long preamble. Check it to use **Long Preamble** if needed to communicate with this kind of devices.

## 3.10.3 Security

This page allows you to set security with different modes. After configuring the correct settings, please click **OK** to save and invoke it.




**Mode** **Disable**-Turn off the encryption mechanism. For the security of your router, please select any one of the encryption mode here.
**WEP**-Accepts only WEP clients and the encryption key should be entered in WEP Key.
**WPA/PSK**-Accepts only WPA clients and the encryption key should be entered in PSK.
**WPA2/PSK**-Accepts only WPA2 clients and the encryption key should be entered in PSK.
**Mixed (WPA+ WPA2)/PSK** - Accepts WPA and WPA2 clients simultaneously and the encryption key should be entered in PSK.




**WPA** The WPA encrypts each frame transmitted from the radio using the key, which either PSK (Pre-Shared Key) entered manually in this

field below or automatically negotiated via 802.1x authentication. Either **8~63** ASCII characters, such as 012345678(or 64 Hexadecimal digits leading by 0x, such as "0x321253abcde...").

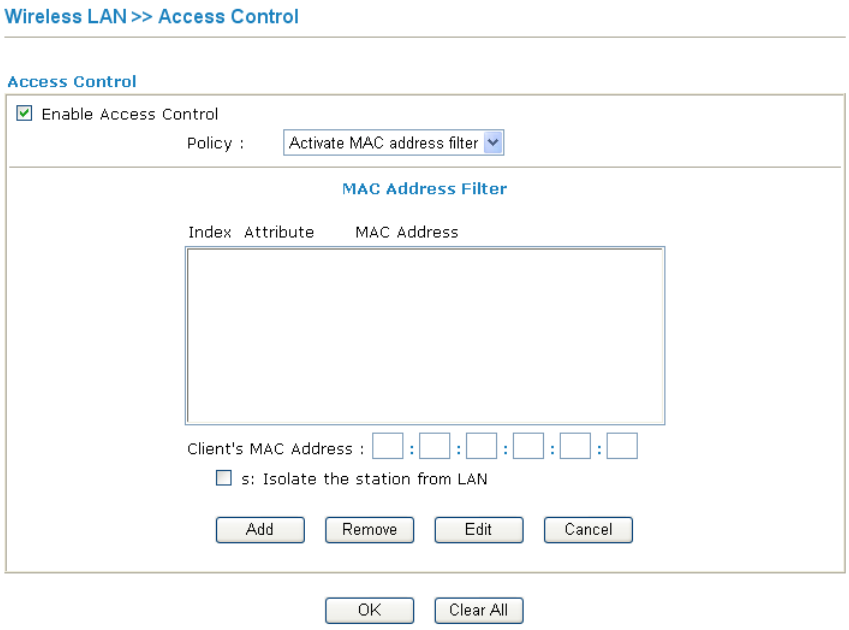
**WEP**

**For key length 64 bits** - For 64 bits WEP key, either **5** ASCII characters, such as 12345 (or 10 hexadecimal digitals leading by 0x, such as 0x4142434445.)
**For key length 128 bits** - For 128 bits WEP key, either **13** ASCII characters, such as ABCDEFGHIJKLM. (or 26 hexadecimal digits leading by 0x, such as 0x41424344454647484 94A4B4C4D)

All wireless devices must support the same WEP encryption bit size and have the same key. Four keys can be entered here, but only one key can be selected at a time. The keys can be entered in ASCII or Hexadecimal. Check the key you wish to use.

## 3.10.4 Access Control

For additional security of wireless access, the **Access Control** facility allows you to restrict the network access right by controlling the wireless LAN MAC address of client. Only the valid MAC address that has been configured can access the wireless LAN interface. By clicking the **Access Control**, a new web page will appear, as depicted below, so that you could edit the clients' MAC addresses to control their access rights.



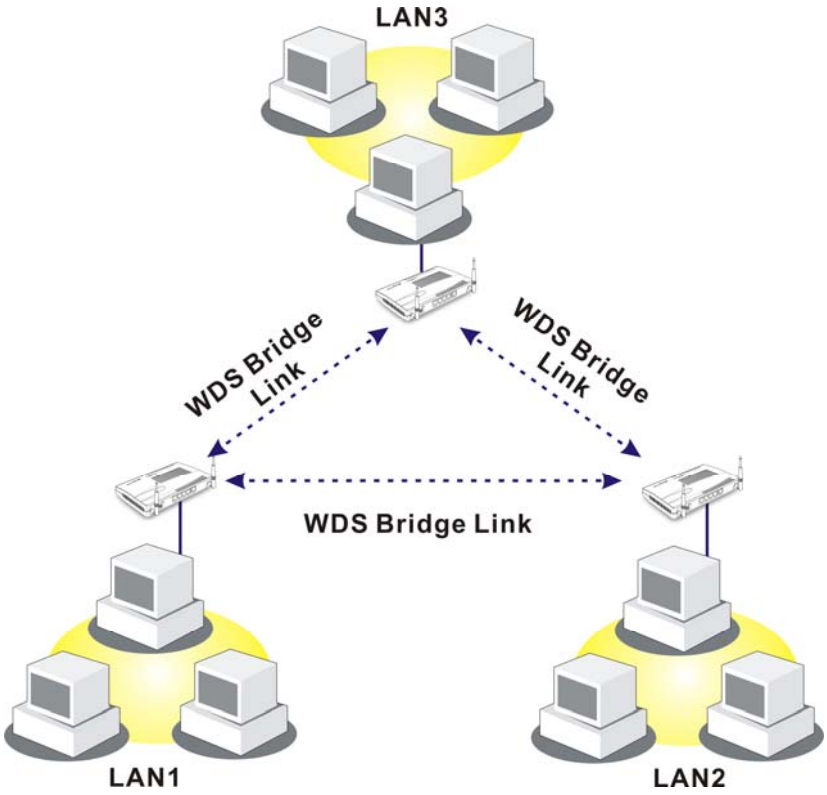

| | |
|---|---|
| **Enable Access Control** | Select to enable the MAC Address access control feature. |
| **Mac Address** | Manually enter the MAC address of wireless client. |
| **Add** | Add a new MAC address into the list. |
| **Remove** | Delete the selected MAC address in the list. |
| **Edit** | Edit the selected MAC address in the list. |
| **Cancel** | Give up the access control set up. |
| **OK** | Click it to save the access control list. |
| **Clear All** | Clean all entries in the MAC address list. |

### 3.10.5 WDS

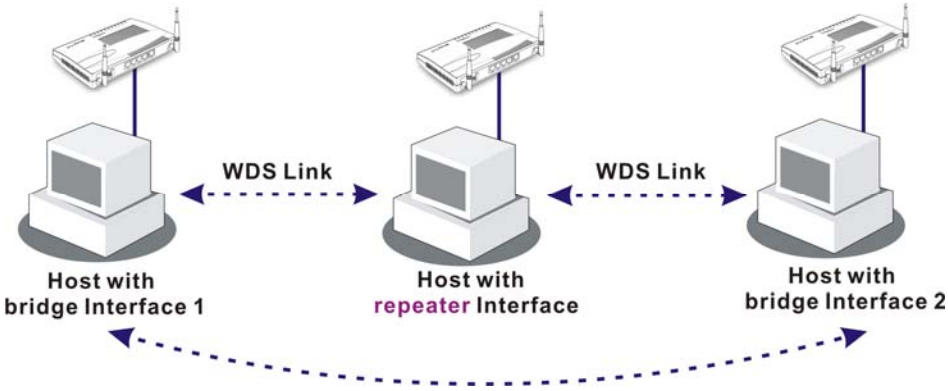
WDS means Wireless Distribution System. It is a protocol for connecting two access points (AP) wirelessly. Usually, it can be used for the following application:

- Provide bridge traffic between two LANs through the air.
- Extend the coverage range of a WLAN.

To meet the above requirement, two WDS modes are implemented in Vigor router. One is **Bridge**, the other is **Repeater**. Below shows the function of WDS-bridge interface:

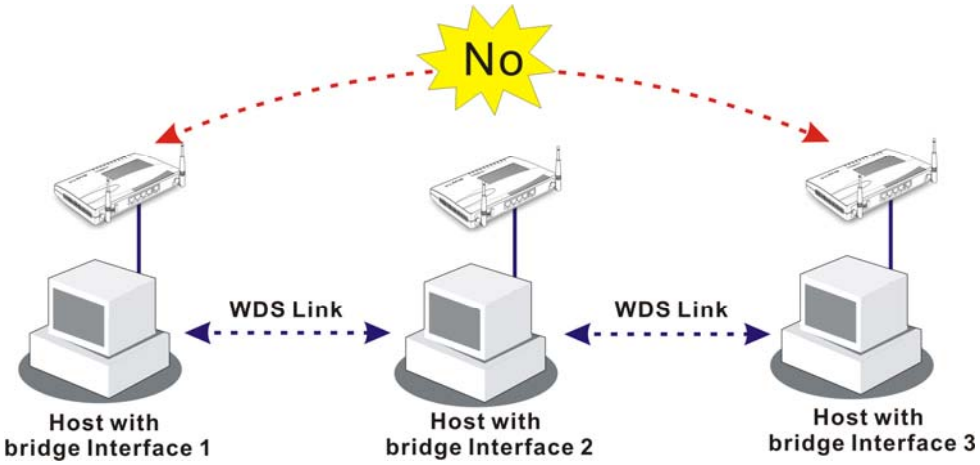



The application for the WDS-Repeater mode is depicted as below:

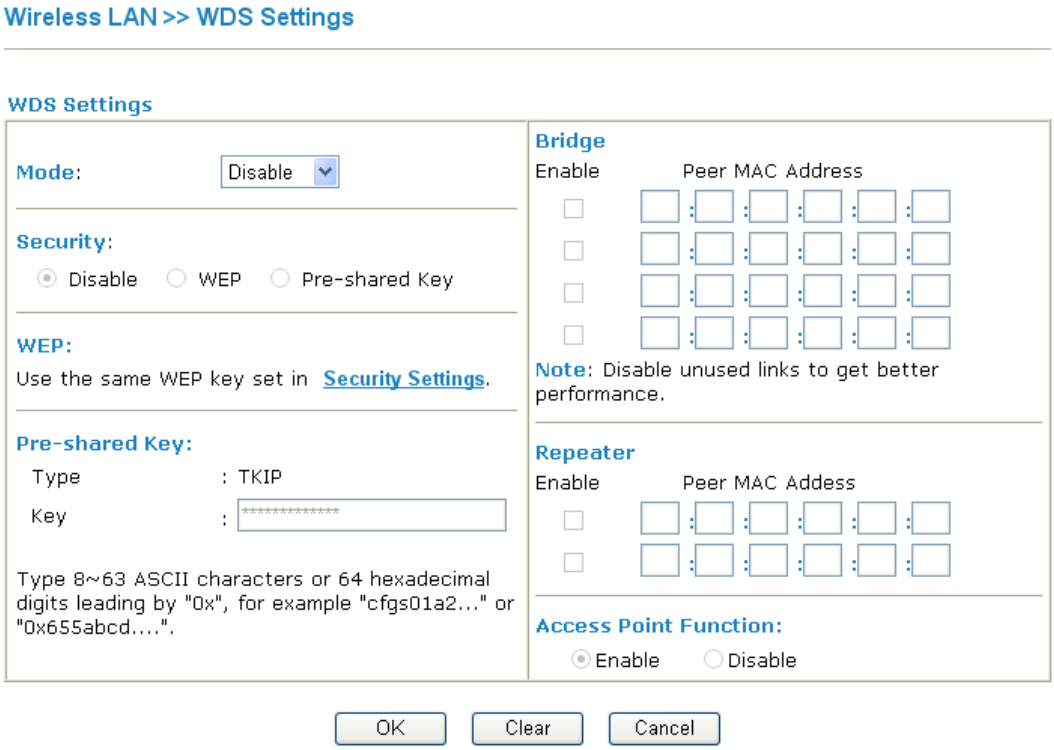



The major difference between these two modes is that: while in **Repeater** mode, the packets received from one peer AP can be repeated to another peer AP through WDS links. Yet in **Bridge** mode, packets received from a WDS link will only be forwarded to local wired or wireless hosts. In other words, only Repeater mode can do WDS-to-WDS packet forwarding.

In the following examples, hosts connected to Bridge 1 or 3 can communicate with hosts connected to Bridge 2 through WDS links. However, hosts connected to Bridge 1 CANNOT communicate with hosts connected to Bridge 3 through Bridge 2.




Click **WDS** from **Wireless LAN** menu. The following page will be shown.




**Mode** Choose the mode for WDS setting. **Disable** mode will not invoke any WDS setting. **Bridge** mode is designed to fulfill the first type of application. **Repeater** mode is for the second one.


**Security** There are three types for security, **Disable**, **WEP** and **Pre-shared key**. The setting you choose here will make the following WEP or Pre-shared key field valid or not. Choose one of the types for the router.

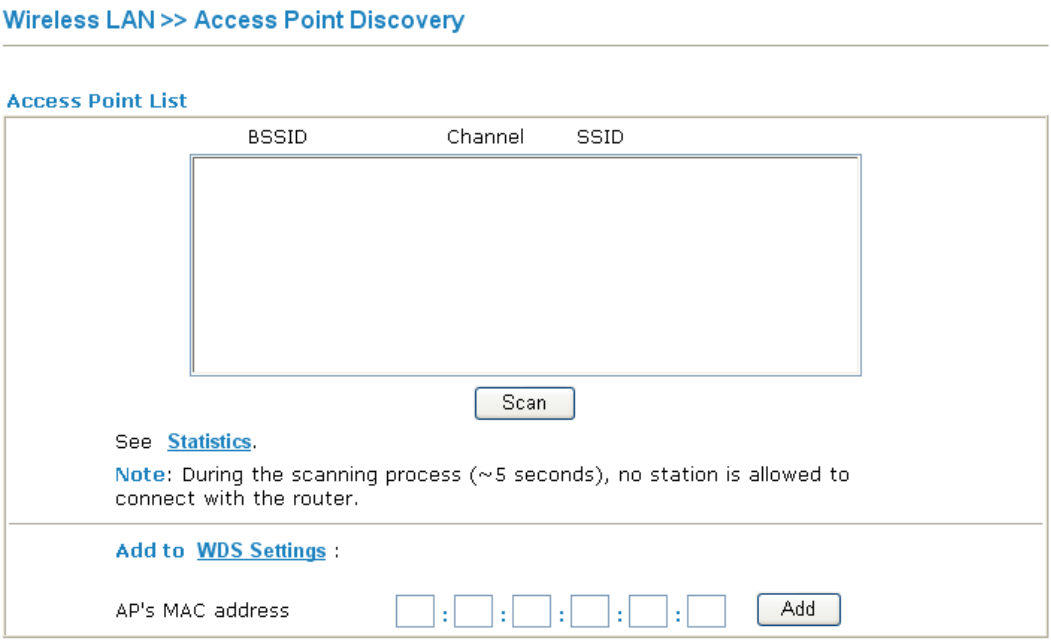
**WEP** Check this box to use the same key set in **Security Settings** page. If you did not set any key in **Security Settings** page, this check box will be dimmed.

| | |
|---|---|
| **Settings** | **Encryption Mode** - If you checked the box of **Use the same WEP key …**, you do not need to choose 64-bit or 128-bit as the Encryption Mode. If you do not check that box, you can set the WEP key now in this page.<br>**Key Index** - Choose the key that you want to use after selecting the proper encryption mode.<br>**Key** - Type the content for the key. |
| **Pre-shared Key** | Type 8 ~ 63 ASCII characters or 64 hexadecimal digits leading by “0x”. |
| **Bridge** | If you choose Bridge as the connecting mode, please type in the peer MAC address in these fields. **Six** peer MAC addresses are allowed to be entered in this page at one time. Yet please disable the unused link to get better performance. If you want to invoke the peer MAC address, remember to check **Enable** box in the front of the MAC address after typing. |
| **Repeater** | If you choose Repeater as the connecting mode, please type in the peer MAC address in these fields. Two peer MAC addresses are allowed to be entered in this page at one time. Similarly, if you want to invoke the peer MAC address, remember to check **Enable** box in the front of the MAC address after typing. |
| **Access Point Function** | Click **Enable** to make this router serving as an access point; click **Disable** to cancel this function. |
| **Status** | It allows user to send “hello” message to peers. Yet, it is valid only when the peer also supports this function. |

## 3.10.6 AP Discovery

Vigor router can scan all regulatory channels and find working APs in the neighborhood. Based on the scanning result, users will know which channel is clean for usage. Also, it can be used to facilitate finding an AP for a WDS link. Notice that during the scanning process (about 5 seconds), no client is allowed to connect to Vigor.

This page is used to scan the existence of the APs on the wireless LAN. Yet, only the AP which is in the same channel of this router can be found. Please click **Scan** to discover all the connected APs.

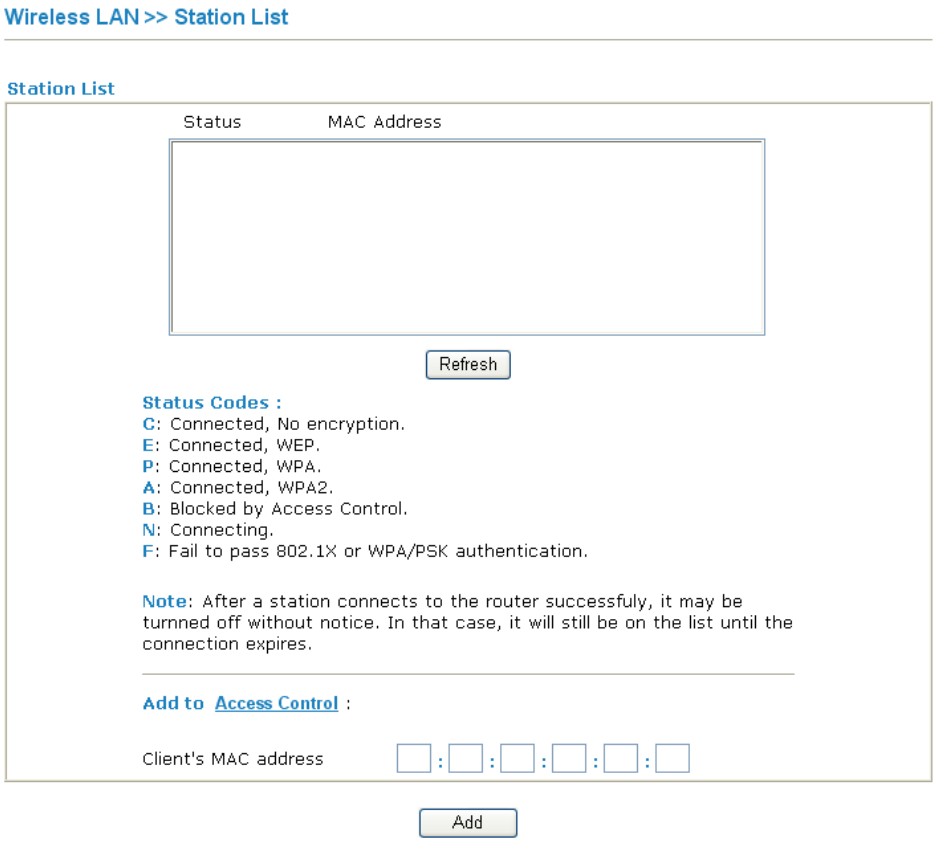



**Scan** It is used to discover all the connected AP. The results will be shown on the box above this button.

**Add** If you want the found AP applying the WDS settings, please type in the AP's MAC address on the bottom of the page and click **Add**. Later, the MAC address of the AP will be added to the page of WDS setting.

## 3.10.7 Station List

**Station List** provides the knowledge of connecting wireless clients now along with its status code. There is a code summary below for explanation. For convenient **Access Control**, you can select a WLAN station and click **Add to Access Control** below.



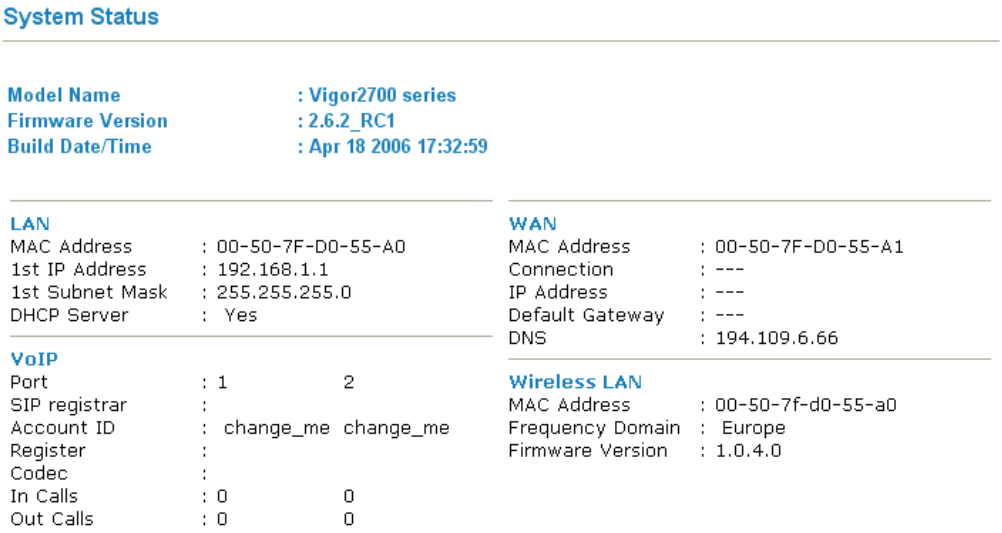

| | |
|---|---|
| **Refresh** | Click this button to refresh the status of station list. |
| **Add** | Click this button to add current selected MAC address into **Access Contro**l. |

## 3.11 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 and Date, Reboot System and Firmware Upgrade.

### 3.11.1 System Status

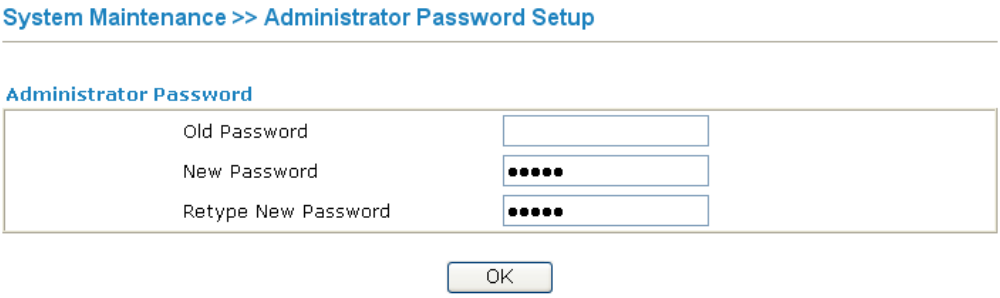
The **System Status** provides basic network settings of Vigor router. It includes LAN and WAN interface information. Also, you could get the current running firmware version or firmware related information from this presentation.




| | |
|---|---|
| **Model Name** | Displays the model name of the router. |
| **Firmware Version** | Displays the firmware version of the router. |
| **Build Date&Time** | Displays the date and time of the current firmware build. |
| **MAC Address** | Displays the MAC address of the LAN Interface. |
| **1st IP Address** | Displays the IP address of the LAN interface. |
| **1st Subnet Mask** | Displays the subnet mask address of the LAN interface. |
| **DHCP Server** | Displays the current status of DHCP server of the LAN interface. |
| **MAC Address** | Displays the MAC address of the WAN Interface. |
| **IP Address** | Displays the IP address of the WAN interface. |
| **Default Gateway** | Displays the assigned IP address of the default gateway. |
| **DNS** | Displays the assigned IP address of the primary DNS. |
| **MAC Address** | Displays the MAC address of the wireless Interface. |
| **Frequency Domain** | Displays the available channel supported by the wireless product. It varies in different country, Europe (13 usable channels), USA (11 usable channels). |
| **Firmware Version** | Displays information about equipped WLAN card driver. |

## 3.11.2 Administrator Password

This page allows you to set new password.




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

**New Password** Type in new password in this filed.

**Retype New Password** Type in the new password again.

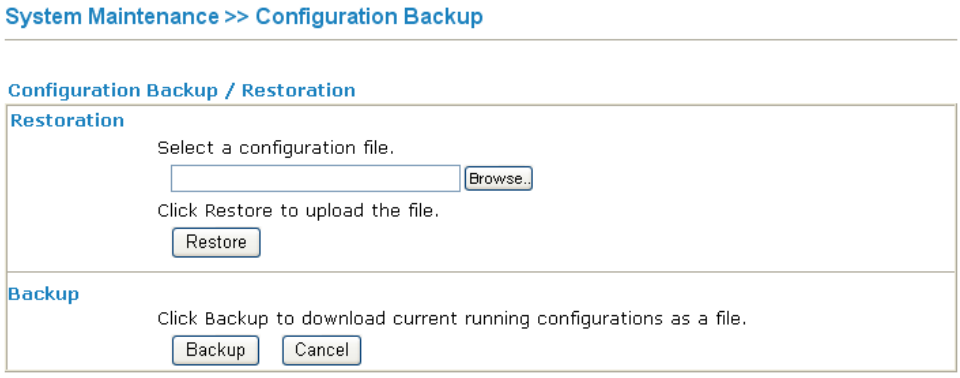
When you click OK, the login window will appear. Please use the new password to access into the web configurator again.

## 3.11.3 Configuration Backup

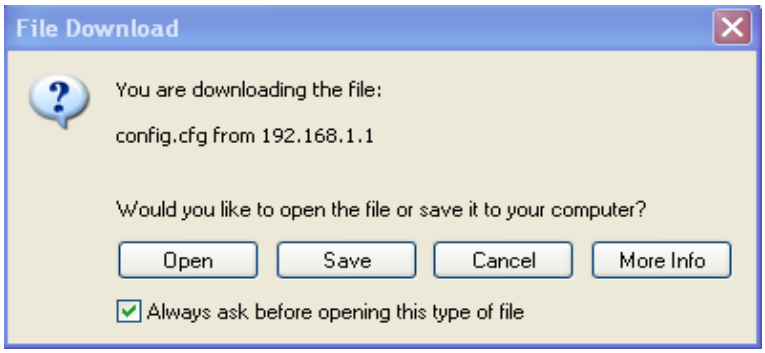
### Backup the Configuration

Follow the steps below to backup your configuration.

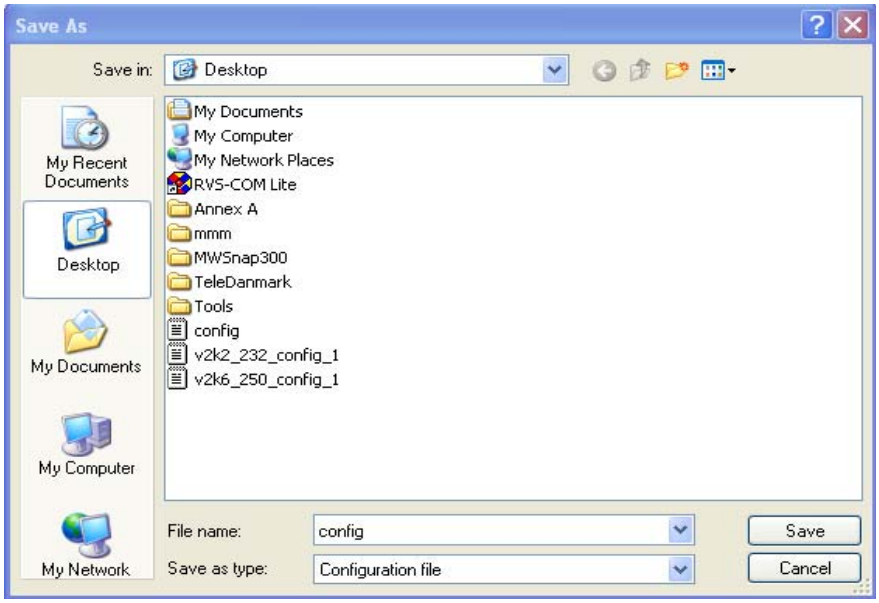
1. Go to **System Maintenance** >> **Configuration Backup**. The following windows will be popped-up, as shown below.




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




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

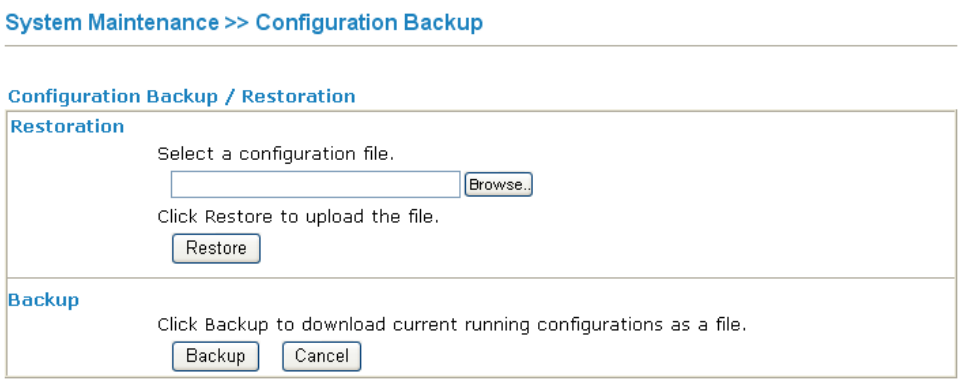



4. Click **Save** button, the configuration will download automatically to your computer as a file named **config.cfg**.

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

## Restore Configuration

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

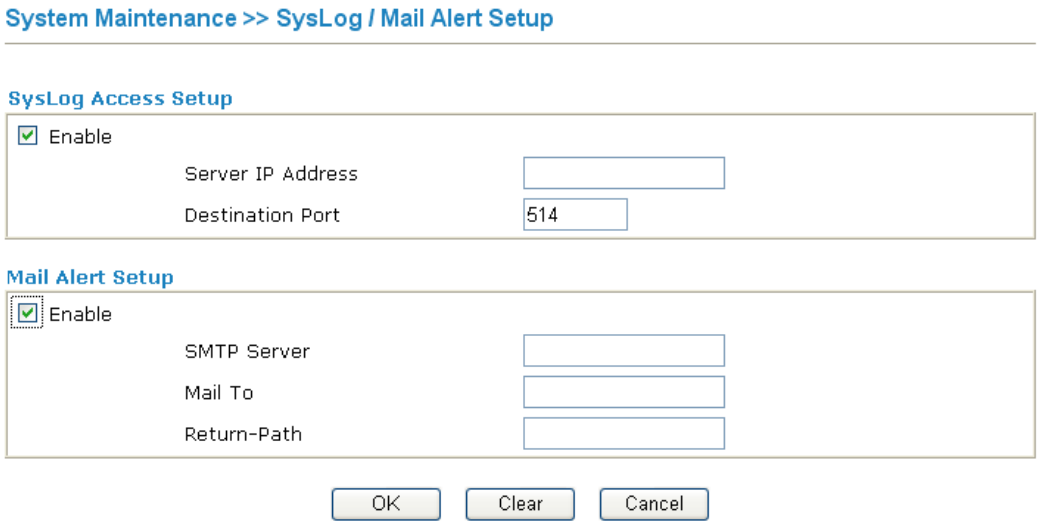



2. Click **Browse** button to choose the correct configuration file for uploading to the router.

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

## 3.11.4 Syslog/Mail Alert

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

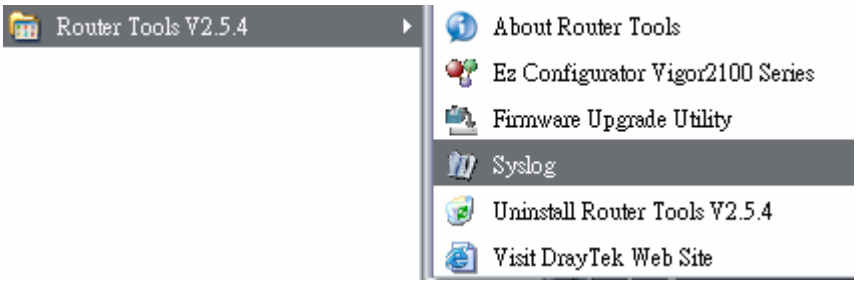



| | |
|---|---|
| **Enable** | Click "**Enable**" to activate this function. |
| **Syslog Server IP** | The IP address of the Syslog server. |
| **Destination Port** | Assign a port for the Syslog protocol. |
| **SMTP Server** | The IP address of the SMTP server. |
| **Mail To** | Assign a mail address for sending mails out. |
| **Return-Path** | Assign a path for receiving the mail from outside. |

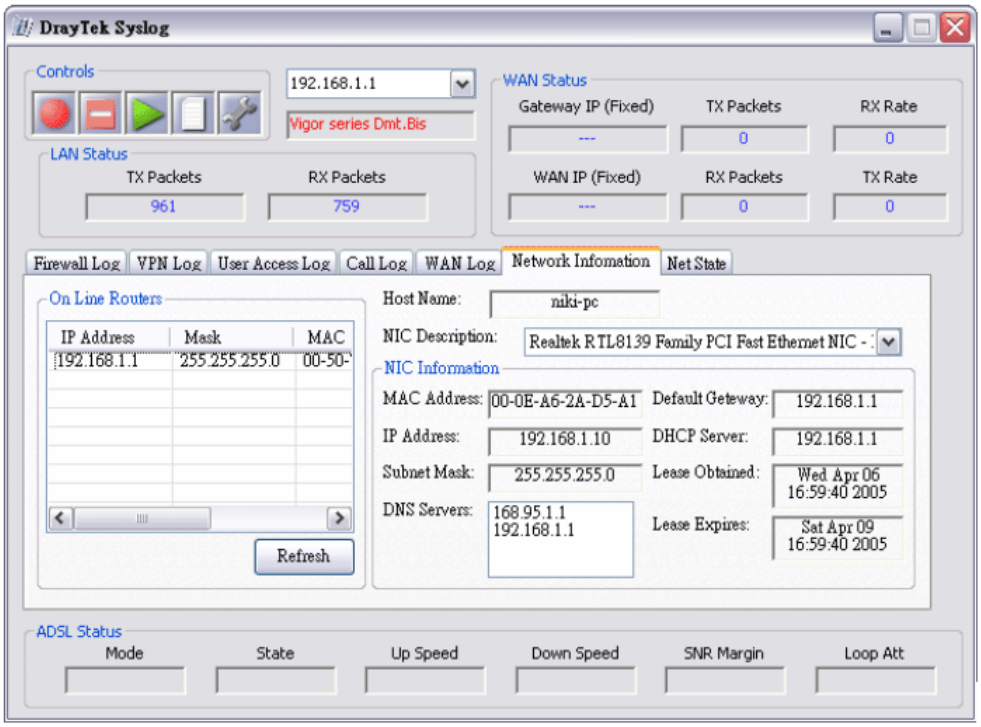
Click **OK** to save these settings.

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.

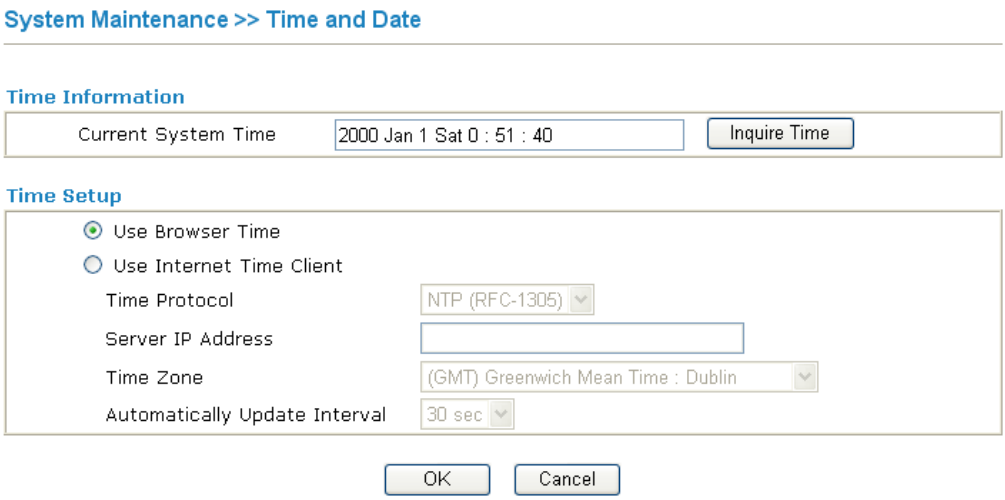



3. From the Syslog screen, select the router you want to monitor. Be reminded that in **Network Information**, select the network adapter used to connect to the router. Otherwise, you won't succeed in retrieving information from the router.




## 3.11.5 Time and Date

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

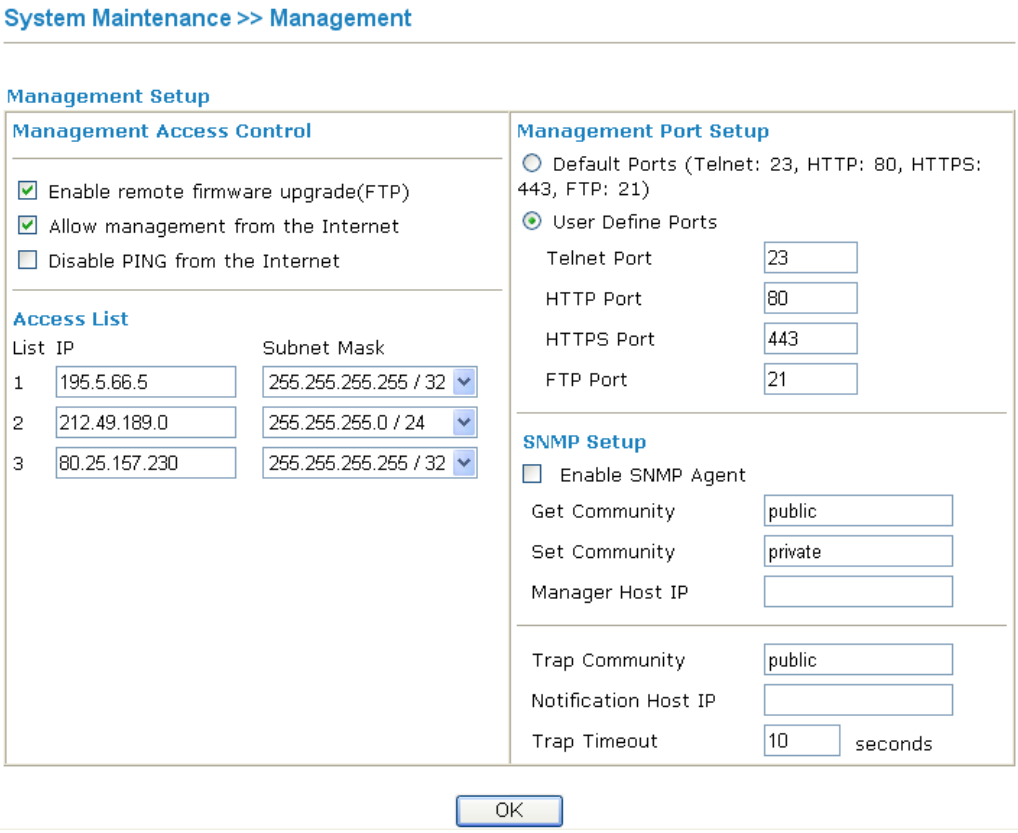



| | |
|---|---|
| **Current System Time** | Click **Inquire Time** to get the current time. |
| **Use Browser Time** | Select this option to use the browser time from the remote administrator PC host as router's system time. |
| **Use Internet Time Client** | Select to inquire time information from Time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

Click **OK** to save these settings.

## 3.11.6 Management

This page allows you to manage the settings for access control, access list, port setup, and SMP setup. For example, as to management access control, the port number is used to send/receive SIP message for building a session. The default value is 5060 and this must match with the peer Registrar when making VoIP calls.

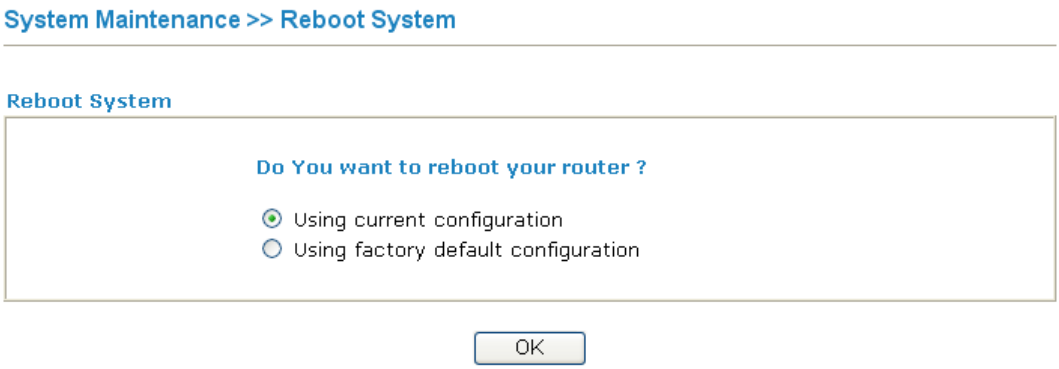



| | |
|---|---|
| **Enable remote firmware upgrade** | Chick the checkbox to allow remote firmware upgrade through FTP (File Transfer Protocol). |
| **Allow management from the Internet** | Enable the checkbox to allow system administrators to login from the Internet. By default, it is not allowed. |
| **Disable PING from the Internet** | Check the checkbox to reject all PING packets from the Internet. For security issue, this function is enabled by default. |
| **Access List** | You could specify that the system administrator can only login from a specific host or network defined in the list. A maximum of three IPs/subnet masks is allowed.<br>**List IP** - Indicate an IP address allowed to login to the router.<br>**Subnet Mask** - Represent a subnet mask allowed to login to the router. |
| **Default Ports** | Check to use standard port numbers for the Telnet and HTTP servers. |
| **User Defined Ports** | Check to specify user-defined port numbers for the Telnet 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. |

## 3.11.7 Reboot System

The Web Configurator may be used to restart your router. Click **Reboot System** from **System Maintenance** to open the following page.



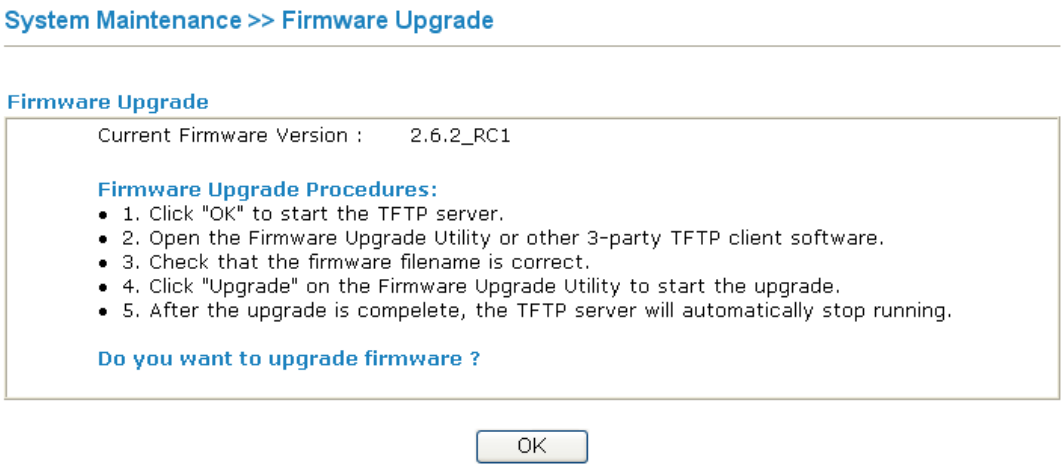

If you want to reboot the router using the current configuration, check **Using current configuration** and click **OK**. To reset the router settings to default values, check **Using factory default configuration** and click **OK**. The router will take 5 seconds to reboot the system.

## 3.11.8 Firmware Upgrade

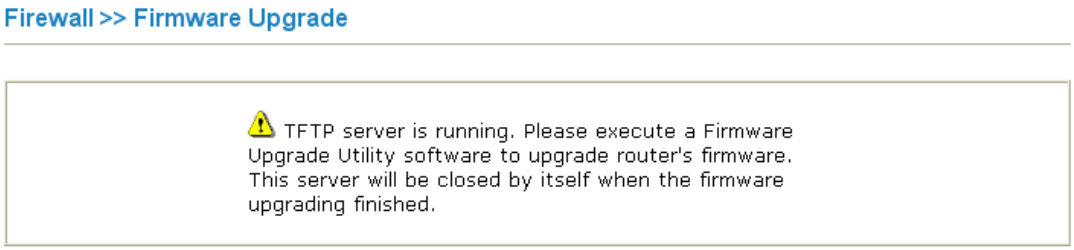
Before upgrading your router firmware, you need to install the Router Tools. The **Firmware Upgrade Utility** is included in the tools. The following web page will guide you to upgrade firmware by using an example. Note that this example is running over Windows OS (Operating System).

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

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




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



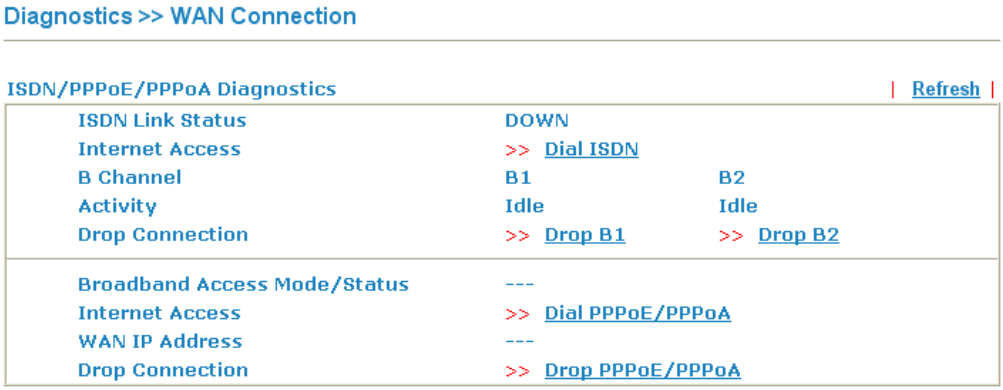

For the detailed information about firmware update, please go to Chapter 4.

## 3.12 Diagnostics

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

### 3.12.1 WAN Connection

Click **Diagnostics** and click **WAN Connection** to open the web page. According to the model you have, the WAN connection page will differ slightly. For example, ISDN Link Status appears only for *i* model.

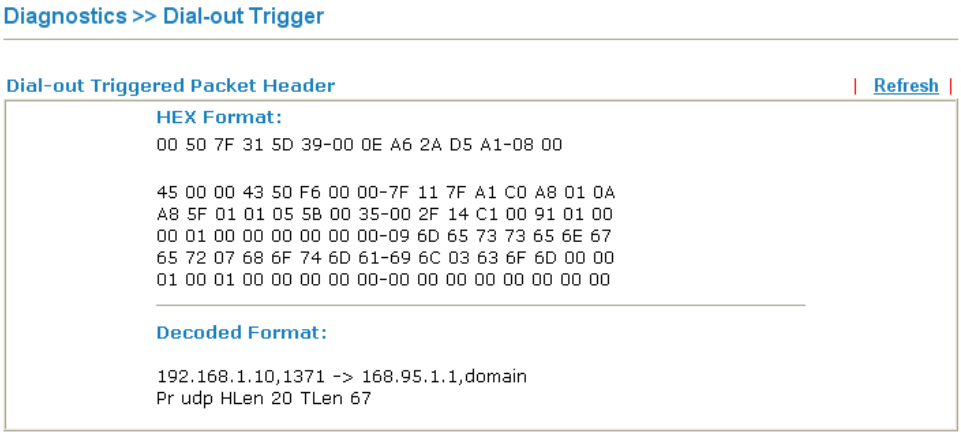



| | |
|---|---|
| **Refresh** | To obtain the latest information, click here to reload the page. |
| **Broadband Access Mode/Status** | Display the broadband access mode and status. If the broadband connection is active, it will show Internet access mode is enabled. If the connection is idle, it will show “**---**”. |

| | |
|---|---|
| **WAN IP Address** | The WAN IP address for the active connection. |
| **Dial PPPoE or PPPoA** | Click it to force the router to establish a PPPoE or PPPoA connection. |

## 3.12.2 Dial-out Trigger

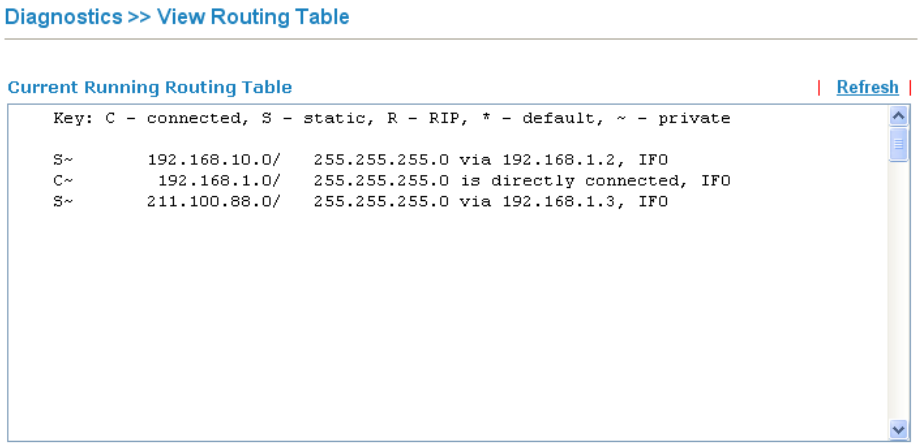
Click **Diagnostics** and click **Dial-out Trigger** to open the web page. The internet connection (e.g., ISDN, PPPoE, PPPoA, etc) is triggered by a package sending from the source IP address.




| | |
|---|---|
| **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. |

## 3.12.3 Routing Table

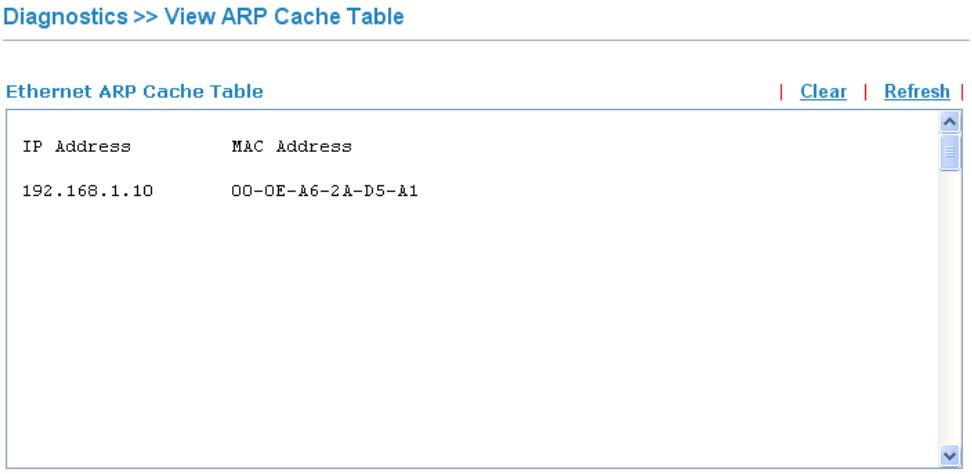
Click **Diagnostics** and click **Routing Table** to open the web page.




| | |
|---|---|
| **Refresh** | Click it to reload the page. |

## 3.12.4 ARP Cache Table

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



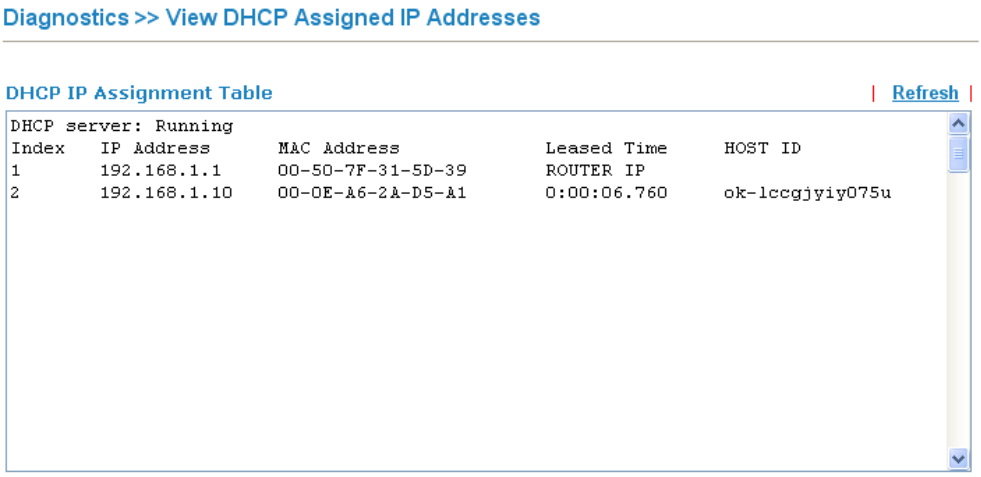

**Refresh** Click it to reload the page.

**Clear** Click it to clear the whole table.

## 3.12.5 DHCP Table

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

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




**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.

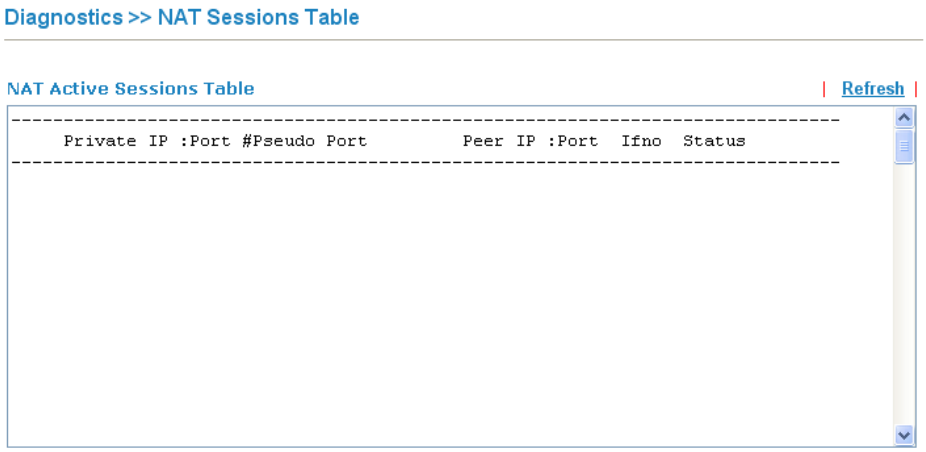
**Leased Time** It displays the leased time of the specified PC.

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

**Refresh** Click it to reload the page.

## 3.12.6 NAT Active Sessions Table

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




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

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

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

**Ifno** It displays the representing number for different interface.

| | |
|---|---|
| 0: | LAN |
| 1~2: | ISDN |
| 3: | WAN |
| 4 or above: | VPN |

**Status** The status values are defined as follows:

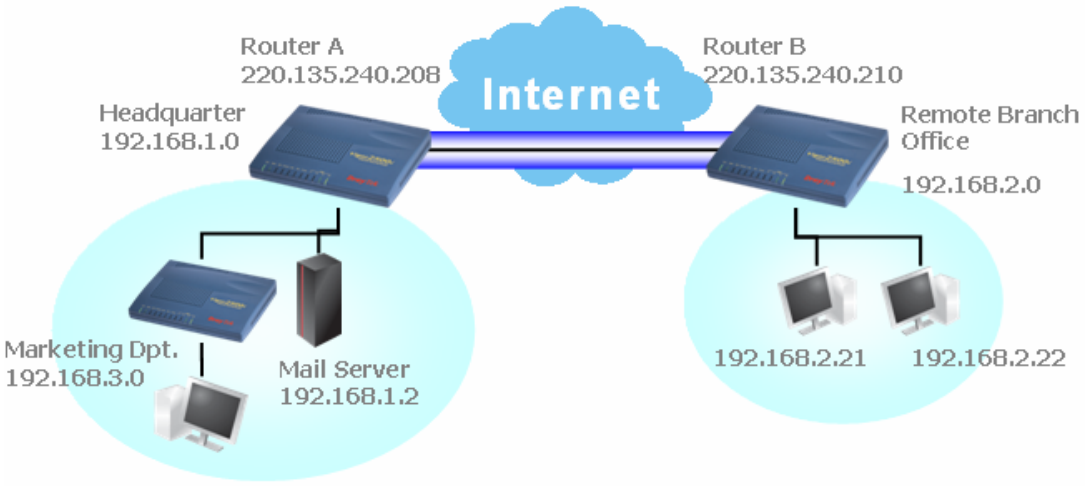
| | |
|---|---|
| 0: | other TCP status |
| 1: | TCP fin incoming |
| 2: | TCP fin out |
| 3: | TCP fin closing |
| 4: | TCP syn |
| 5: | TCP syn,ack |
| 6: | TCP ack |

**Refresh** Click it to reload the page.

# 4 Application and Examples

## 4.1 Create a LAN-to-LAN Connection Between Remote Office and Headquarter

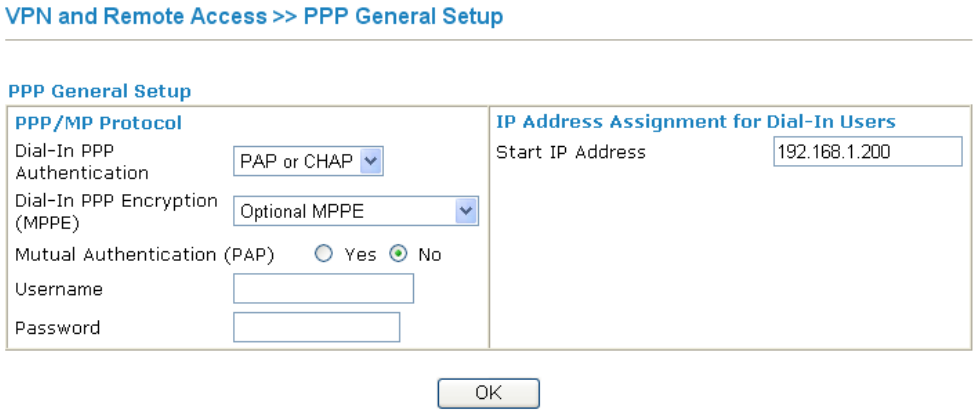
The most common case is that you may want to connect to network securely, such as the remote branch office and headquarter. According to the network structure as shown in the below illustration, you may follow the steps to create a LAN-to-LAN profile. These two networks (LANs) should NOT have the same network address.



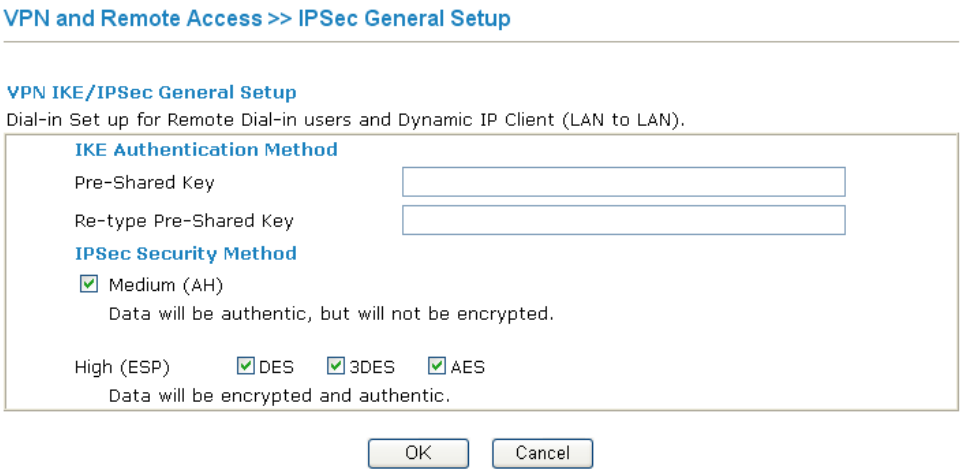

**Settings in Router A in headquarter:**

1. Go to **VPN and Remote Access** and select **Remote Access Control** to enable the necessary VPN service and click **OK**.

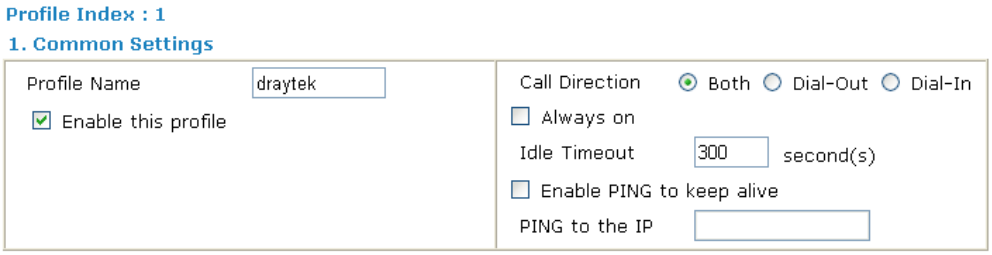
2. Then,
   For using **PPP** based services, such as PPTP, L2TP, you have to set general settings in **PPP General Setup**.



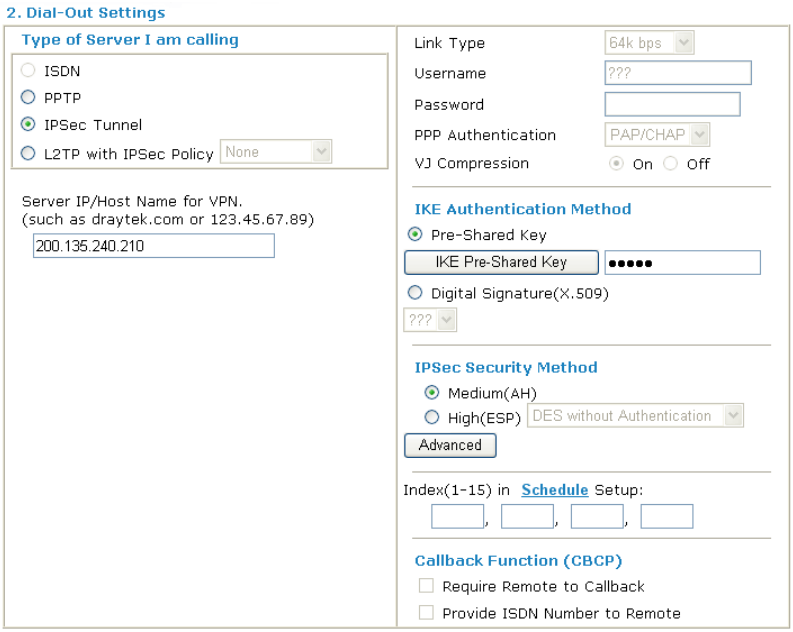
For using **IPSec**-based service, such as IPSec or L2TP with IPSec Policy, you have to set general settings in **IPSec General Setup**, such as the pre-shared key that both parties have known.



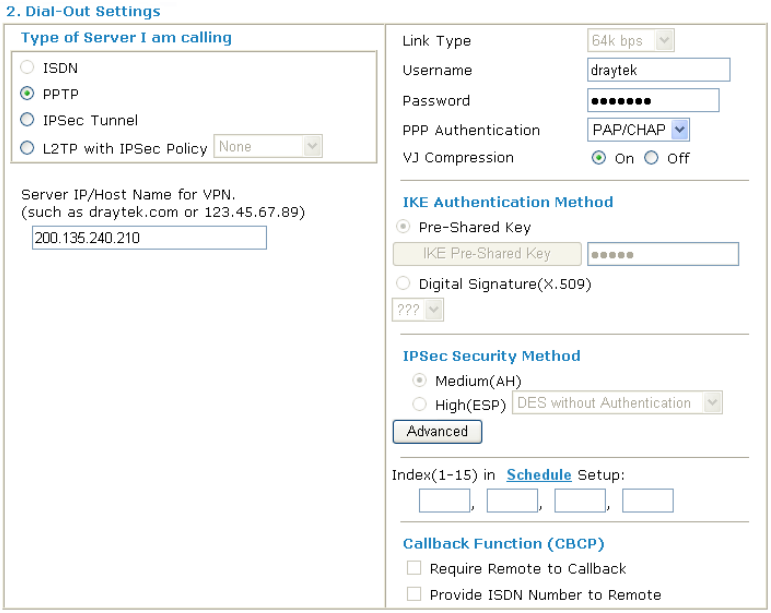

3. Go to **LAN-to-LAN**. Click on one index number to edit a profile.
4. Set **Common Settings** as shown below. You should enable both of VPN connections because any one of the parties may start the VPN connection.




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.

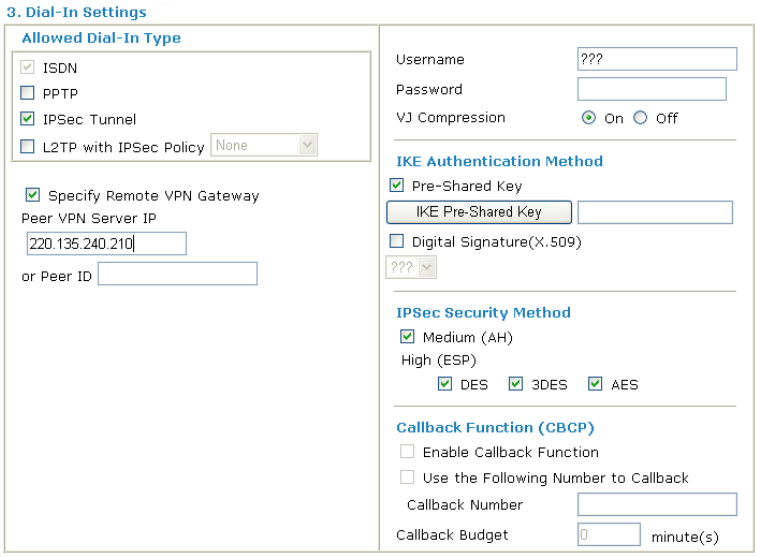



If a ***PPP-based service*** is selected, you should further specify the remote peer IP Address, Username, Password, PPP Authentication and VJ Compression for this Dial-Out connection.

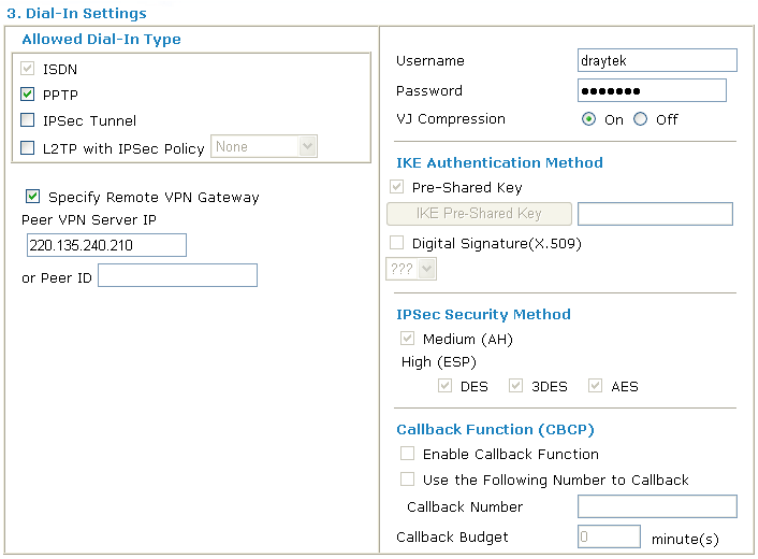



6. Set **Dial-In settings** to as shown below to allow Router B dial-in to build VPN connection.

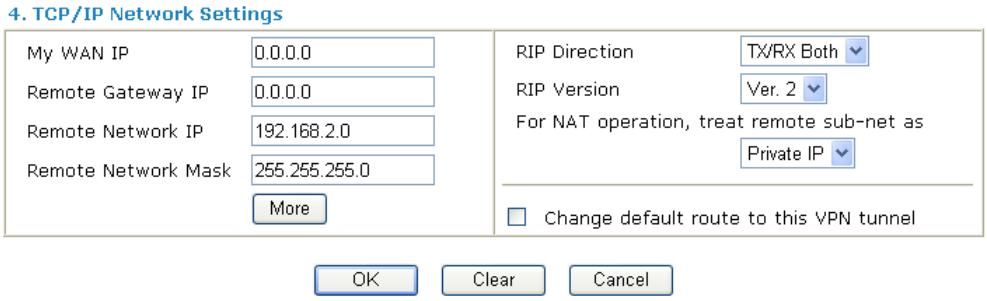
   If an ***IPSec-based*** service is selected, you may further specify the remote peer IP Address, IKE Authentication Method and IPSec Security Method for this Dial-In connection. Otherwise, it will apply the settings defined in **IPSec General Setup** above.




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.



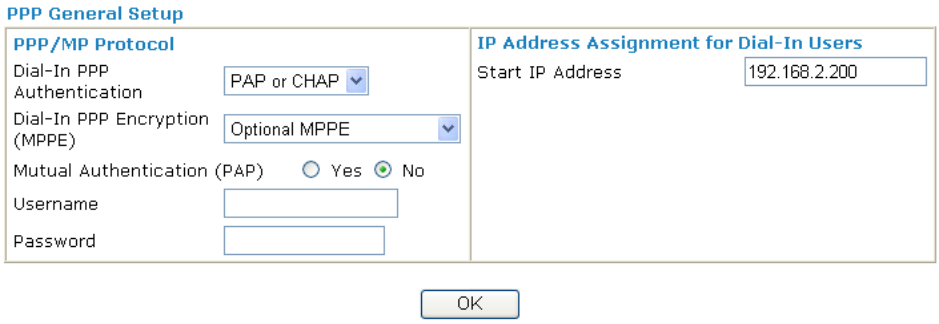

7. At last, set the remote network IP/subnet in **TCP/IP Network Settings** so that Router A can direct the packets destined to the remote network to Router B via the VPN connection.



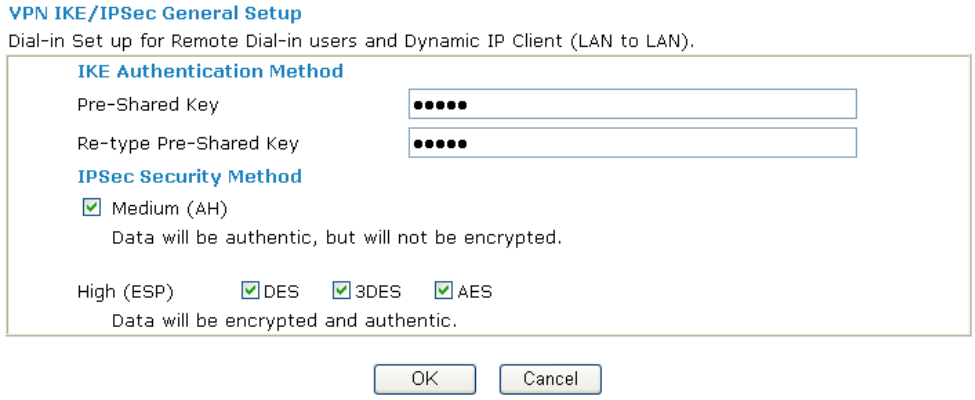

**Settings in Router B in the remote office:**

1. Go to **VPN and Remote Access** and select **Remote Access Control** to enable the necessary VPN service and click **OK**.

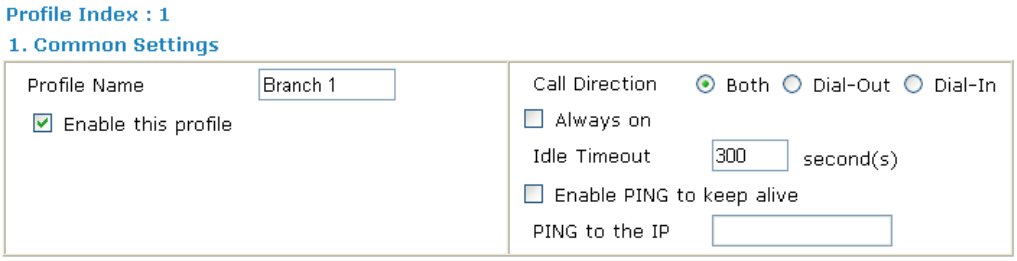
2. Then, for using **PPP based** services, such as PPTP, L2TP, you have to set general settings in **PPP General Setup**.




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.

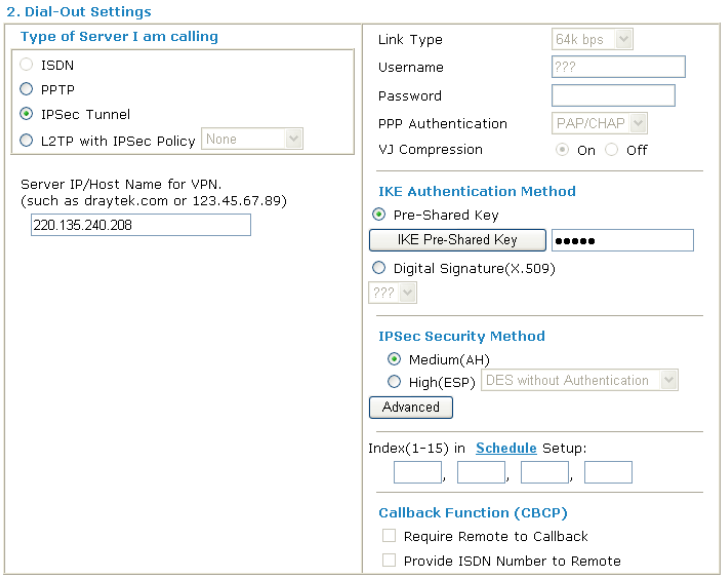



3. Go to **LAN-to-LAN**. Click on one index number to edit a profile.
4. Set **Common Settings** as shown below. You should enable both of VPN connections because any one of the parties may start the VPN connection.

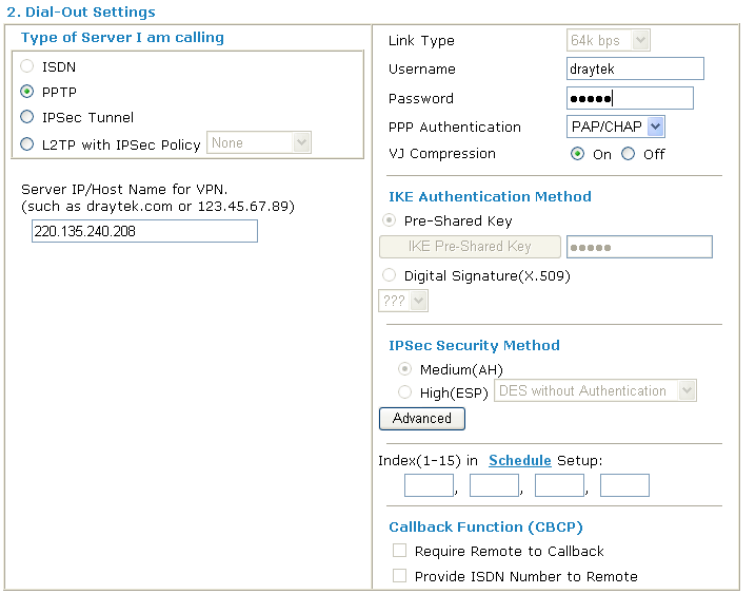



5. Set **Dial-Out Settings** as shown below to dial to connect to Router B aggressively with the selected Dial-Out method.

   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.

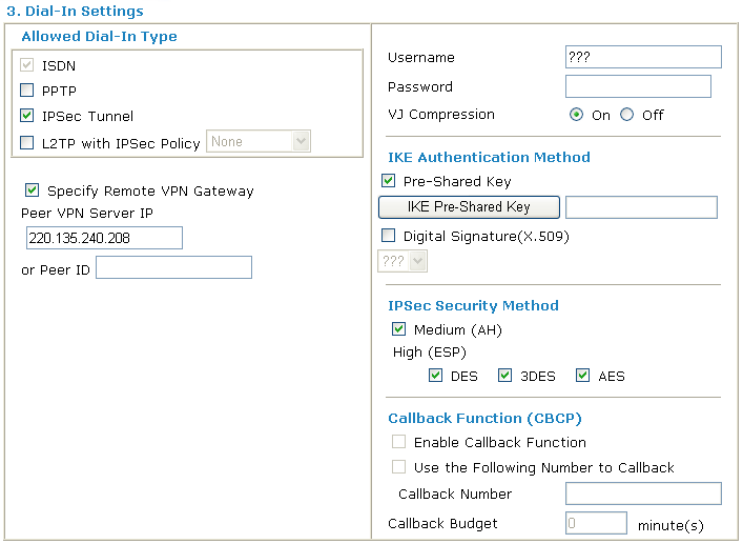



If a ***PPP-based*** service is selected, you should further specify the remote peer IP Address, Username, Password, PPP Authentication and VJ Compression for this Dial-Out connection.

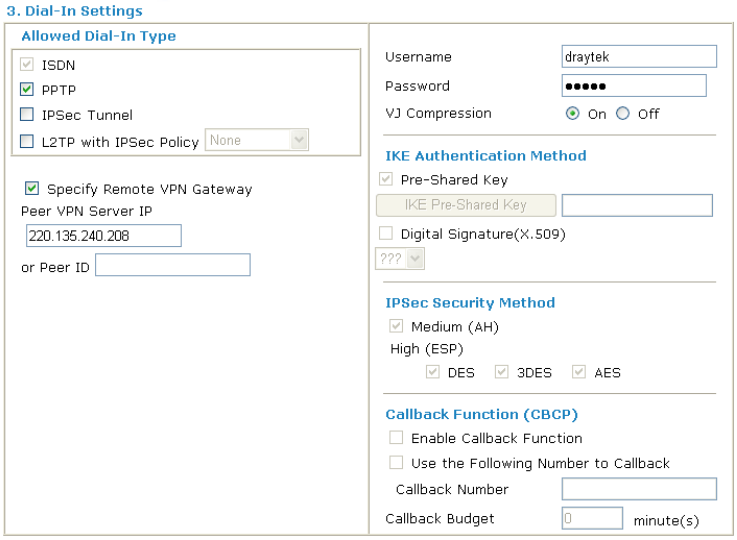



6. Set **Dial-In settings** to as shown below to allow Router A dial-in to build VPN connection.

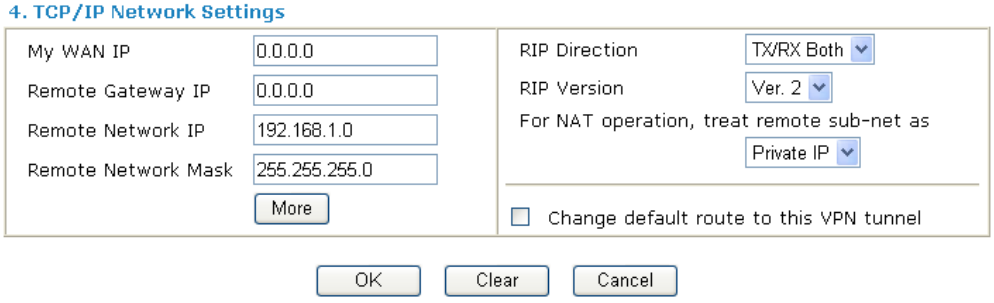
   If an ***IPSec-based*** service is selected, you may further specify the remote peer IP Address, IKE Authentication Method and IPSec Security Method for this Dial-In connection. Otherwise, it will apply the settings defined in **IPSec General Setup** above.




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.

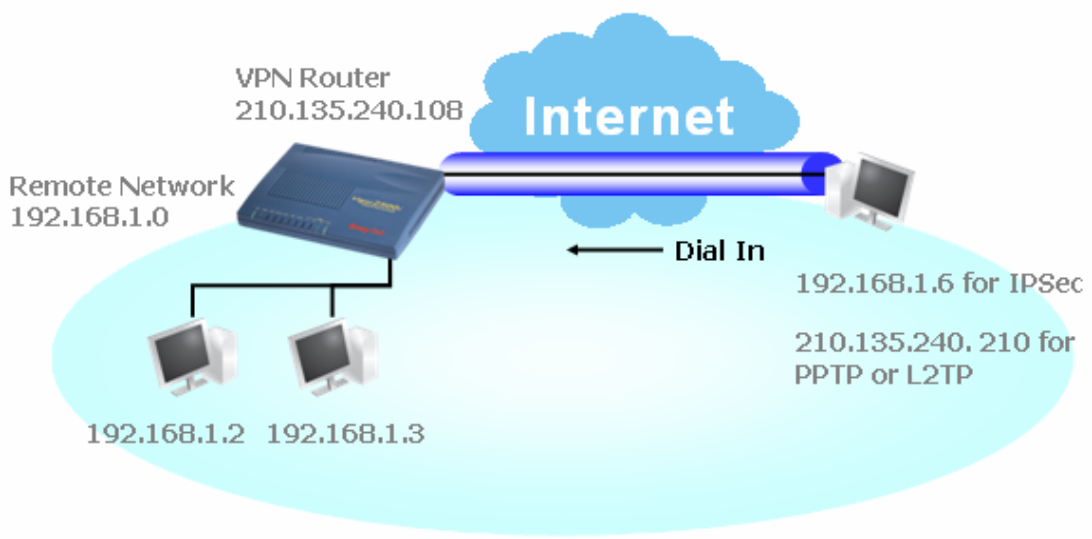



7. At last, set the remote network IP/subnet in **TCP/IP Network Settings** so that Router B can direct the packets destined to the remote network to Router A via the VPN connection.



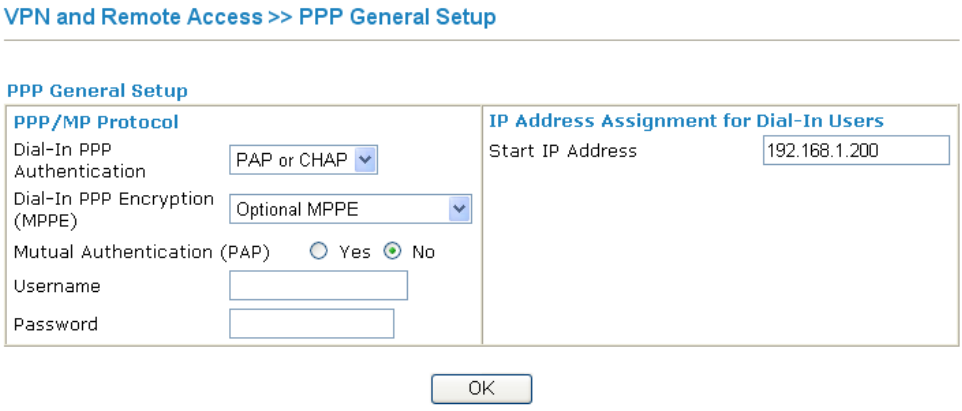
## 4.2 Create a Remote Dial-in User Connection Between the Teleworker and Headquarter

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.

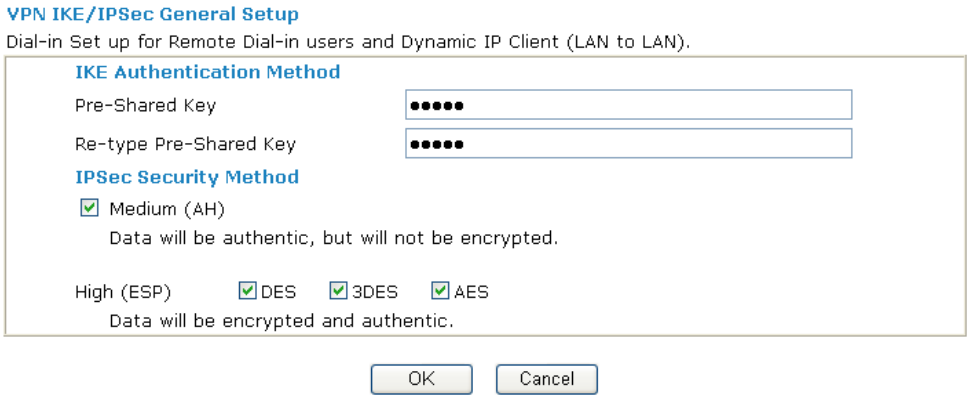



### Settings in VPN Router in the enterprise office:

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**.

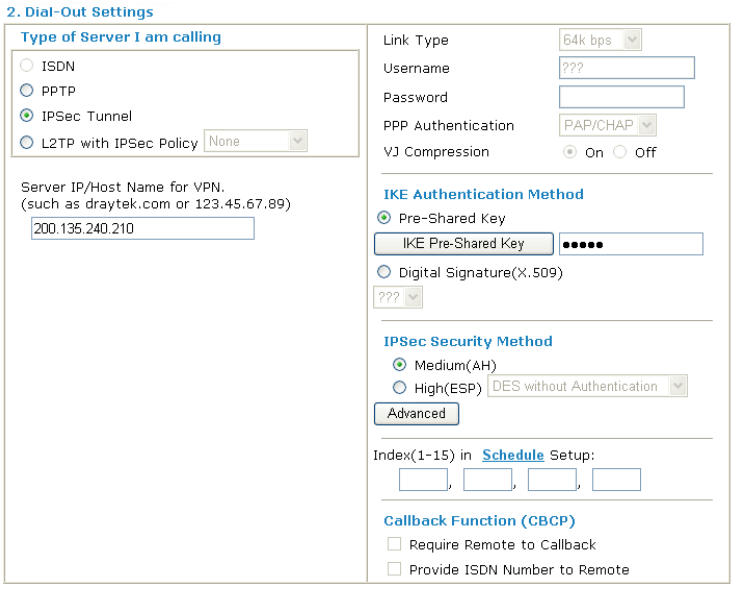



For using IPSec-based service, such as IPSec or L2TP with IPSec Policy, you have to set general settings in **IKE/IPSec General Setup**, such as the pre-shared key that both parties have known.

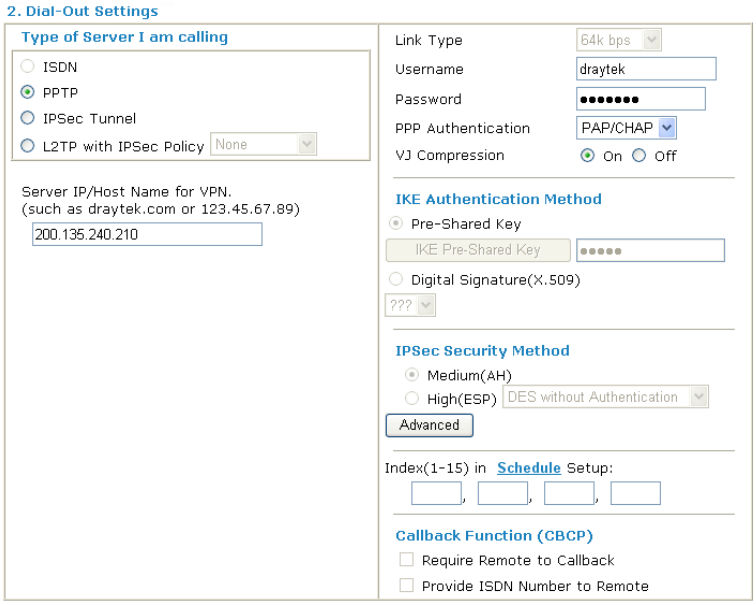



3. Go to **Remote Dial-In Users**. Click on one index number to edit a profile.
4. Set **Dial-In** settings to as shown below to allow the remote user dial-in to build VPN connection.

   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.



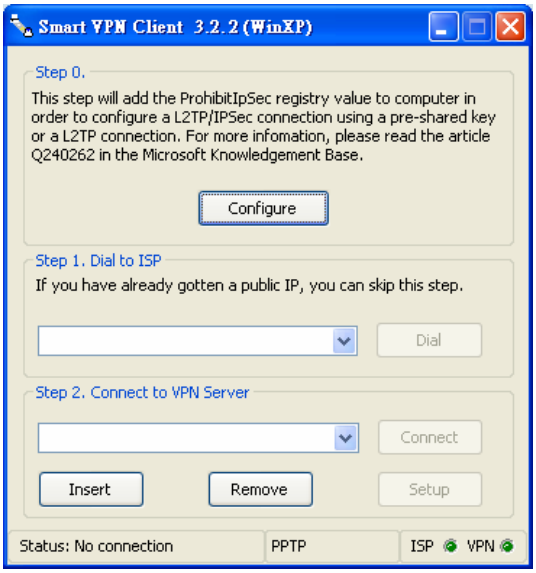

   If a ***PPP-based*** service is selected, you should further specify the remote peer IP Address, Username, Password, and VJ Compression for this Dial-In connection.




**Settings in the remote host:**

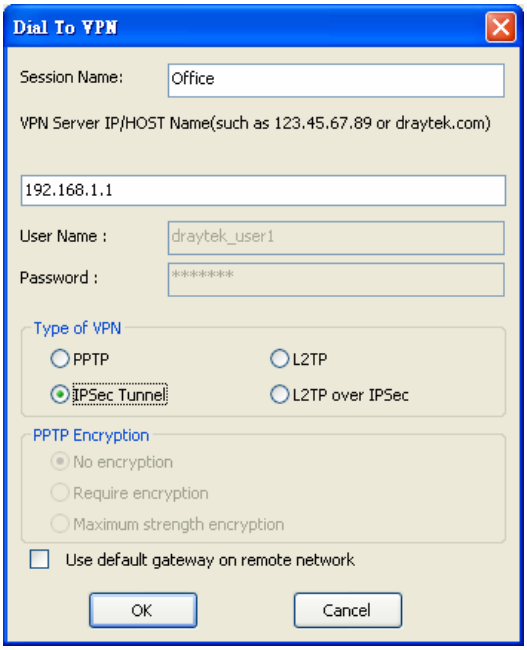
1. For Win98/ME, you may use "Dial-up Networking" to create the PPTP tunnel to Vigor router. For Win2000/XP, please use "Network and Dial-up connections" or “Smart VPN Client”, complimentary software to help you create PPTP, L2TP, and L2TP over IPSec tunnel. You can find it in CD-ROM in the package or 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.

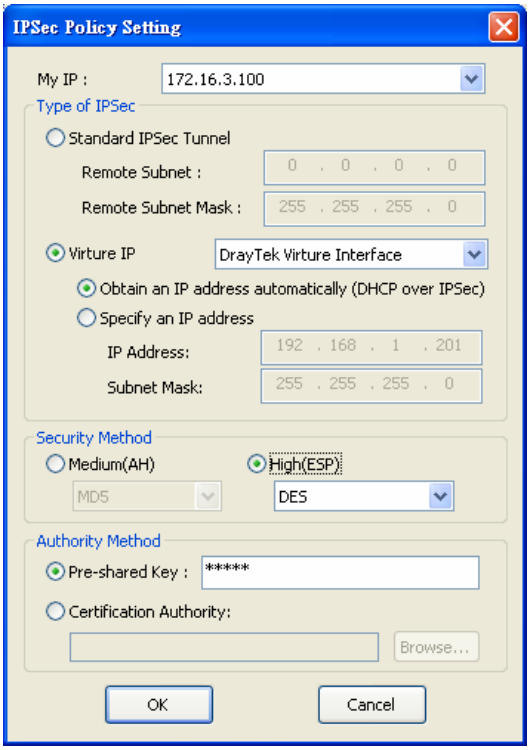



3. In **Step 2. Connect to VPN Server**, click **Insert** button to add a new entry.

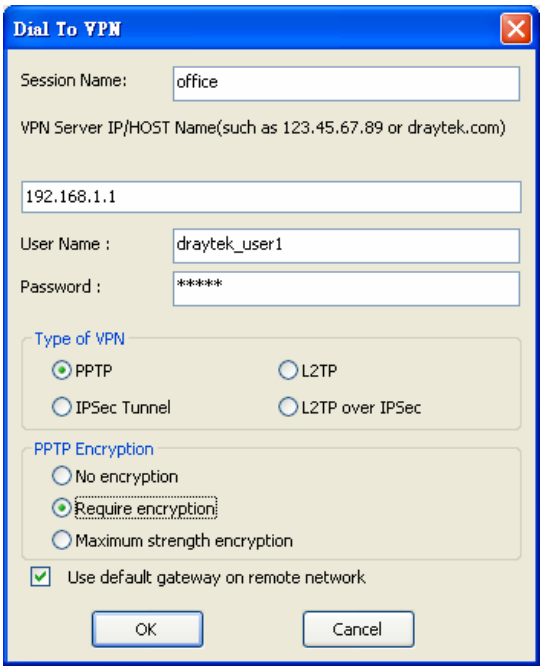
   If an IPSec-based service is selected as shown below,




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.

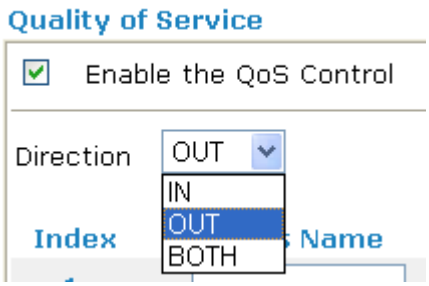



4. Click **Connect** button to build connection. When the connection is successful, you will find a green light on the right down corner.

## 4.3 QoS Setting Example

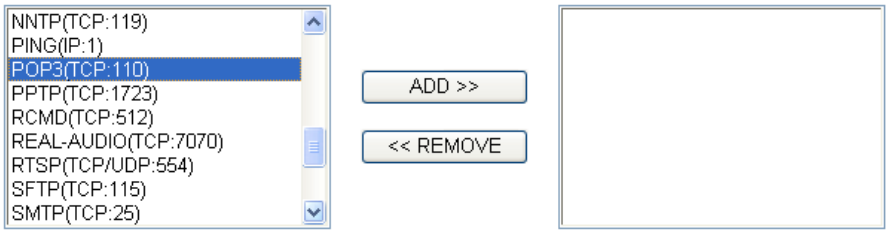
Assume a teleworker sometimes works at home and takes care of children. When working time, he would use Vigor router at home to connect to the server in the headquater office downtown via either HTTPS or VPN to check email and access internal database. Meanwhile, children may chat on VoIP or Skype in the restroom.

1. Click on **Application >>QoS Control**. Make sure you have checked the box of **Enable the QoS Control**. And select **BOTH** in **Direction**.




2. Enter the Class Name of Index 1. In this index, she will set reserve bandwidth for Email using protocol POP3 and SMTP. Click **Basic** button on the right.

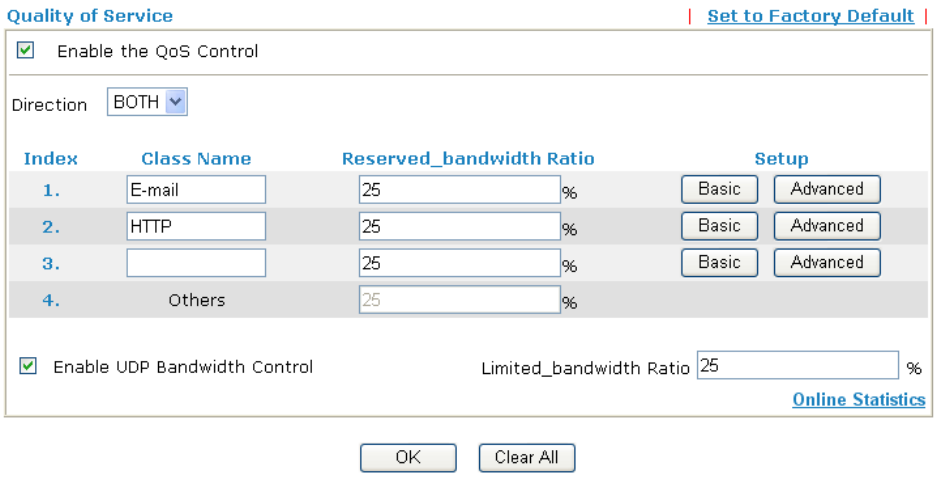
3. Select POP3 and SMTP on the left column and add to right column. Click **OK** to exit.




4. Enter the Class Name of Index 2. In this index, she will set reserve bandwidth for HTTP. And click **Basic** on the right.


5. Select HTTPS in the list on the left column and click on **ADD** to add to right column. Click **OK** to exit.

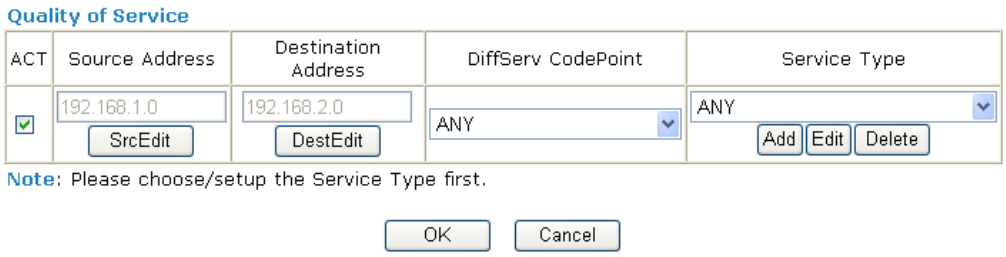

6. Check the Enable UDP Bandwidth Control on the bottom to prevent enormous UDP traffic of VoIP influent other application.




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

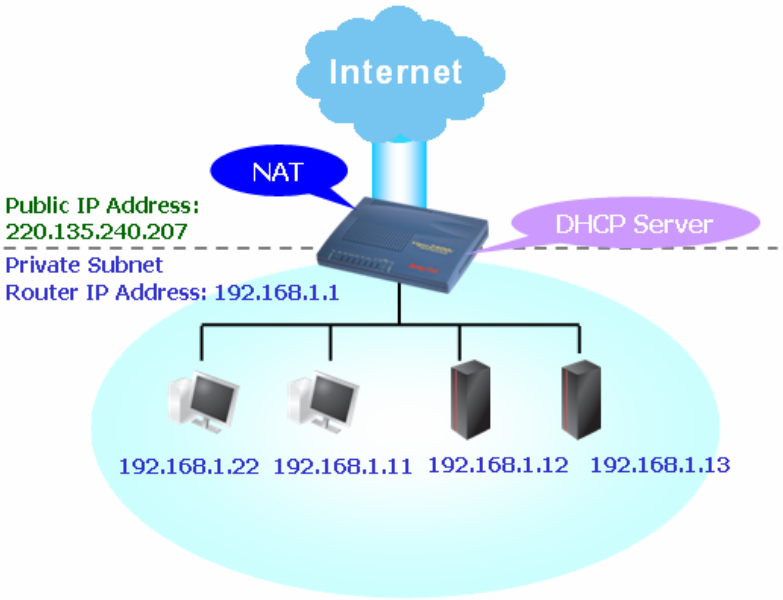
And click **Advanced** button on the right.


8. Click edit to open a new window. First, check the ACT box. Then click **SrcEdit t**o set a worker's subnet address. Click **DestEdit** to set headquarter's subnet address. Leave other fields and click OK.

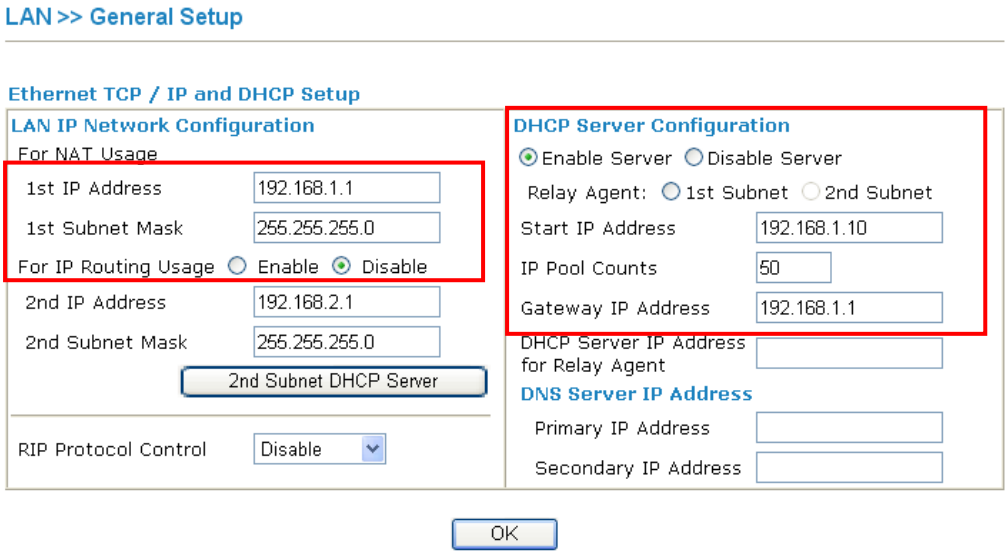



## 4.4 LAN – Created by Using NAT

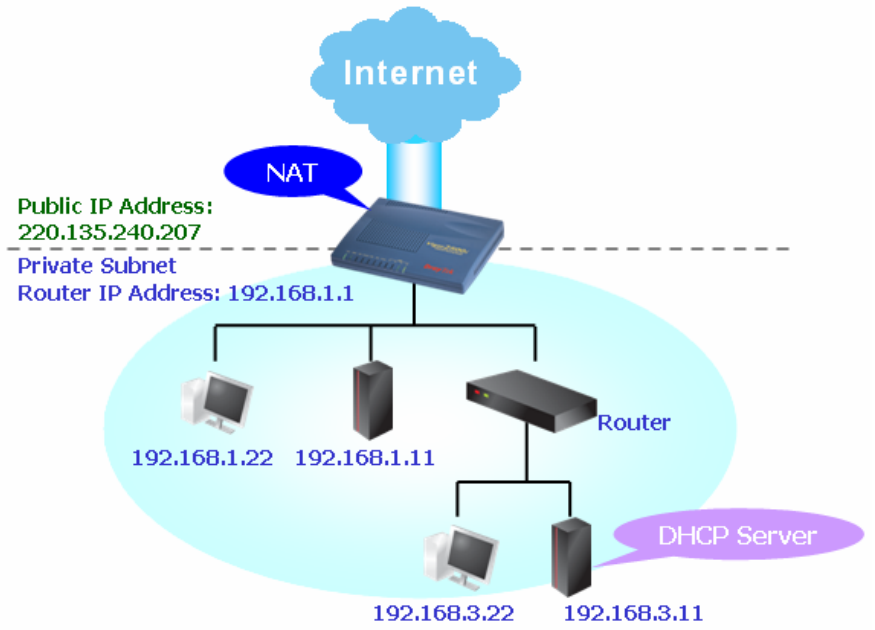
An example of default setting and the corresponding deployment are shown below. The default Vigor router private IP address/Subnet Mask is 192.168.1.1/255.255.255.0. The built-in DHCP server is enabled so it assigns every local NATed host an IP address of 192.168.1.x starting from 192.168.1.10.



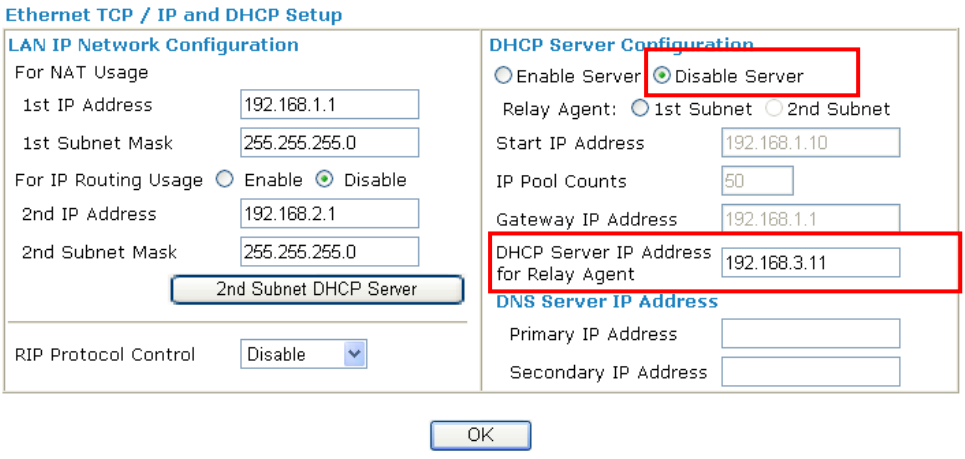

You can just set the settings wrapped inside the red rectangles to fit the request of NAT usage.




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




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



# 4.5 Calling Scenario for VoIP function

## 4.5.1 Calling via SIP Sever

**Example 1: Both John and David have SIP Addresses from different service providers.**

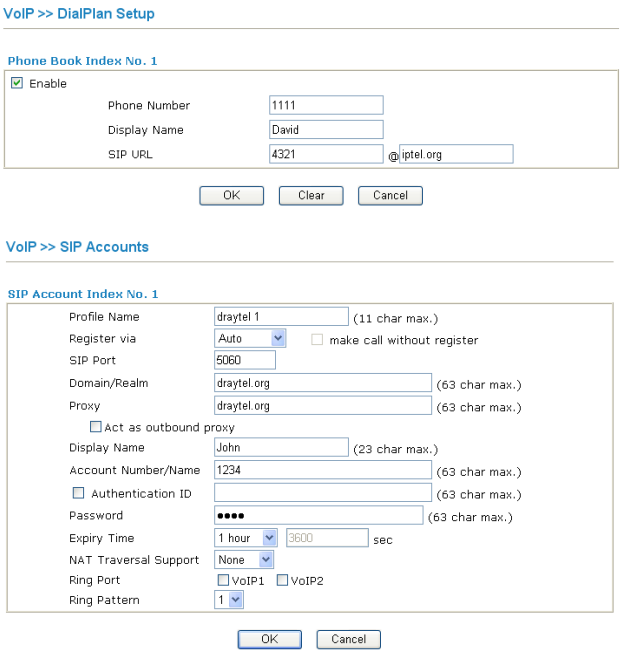
John's SIP URL: 1234@draytel.org, David's SIP URL: 4321@iptel.org

**Settings for John**
DialPlan index 1
Phone Number: 1111
Display Name: David
SIP URL: 4321@iptel.org

**SIP Accounts Settings ---**

Profile Name: draytel1
Register via: Auto
SIP Port: 5060 (default)
Domain/Realm: draytel.org
Proxy: draytel.org
Act as outbound proxy: unchecked
Display Name: John
Account Number/Name: 1234
Authentication ID: unchecked
Password: ****
Expiry Time: (use default value)

**CODEC/RTP/DTMF ---**
(Use default value)



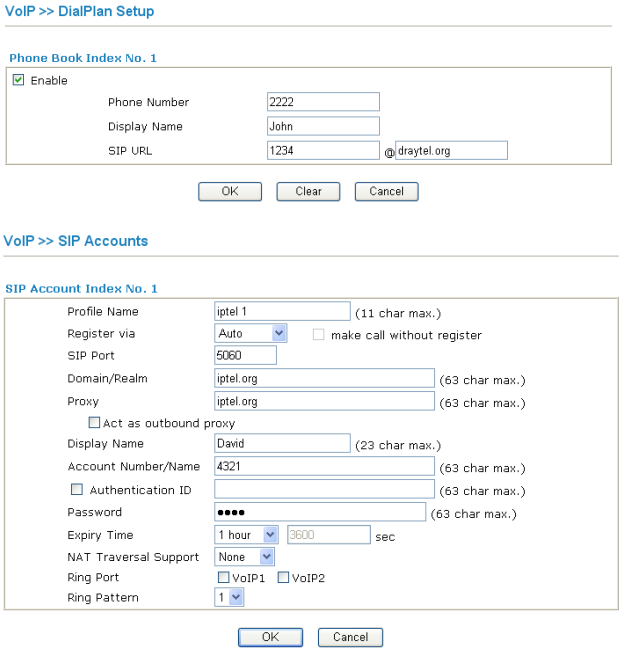

**John calls David ---**
He picks up the phone and dials 1111#. (DialPlan Phone Number for David)

---

**Settings for David**
DialPlan index 1
Phone Number:2222
Display Name: John
SIP URL:1234@draytel.org

**SIP Accounts Settings ---**
Profile Name: iptel 1
Register via: Auto
SIP Port: 5060(default)
Domain/Realm: iptel.org
Proxy: iptel.org
Act as outbound proxy: unchecked
Display Name: David
Account Name: 4321
Authentication ID: unchecked
Password: ****
Expiry Time: (use default value)

**CODEC/RTP/DTMF ---**
(Use default value)




**David calls John**
He picks up the phone and dials 2222# (DialPlan Phone Number for John)

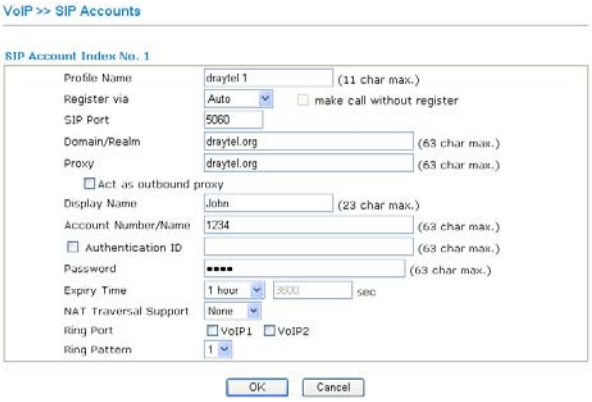
**Example 2: Both John and David have SIP Addresses from the same service provider.**

John's SIP URL: 1234@draytel.org , David's SIP URL: 4321@draytel.org

**Settings for John**
DialPlan index 1
Phone Number: 1111
Display Name: David
SIP URL: 4321@draytel.org


**SIP Accounts Settings ---**

Profile Name: draytel 1
Register via: Auto
SIP Port: 5060 (default)
Domain/Realm: draytel.org
Proxy: draytel.org
Act as outbound proxy: unchecked
Display Name: John
Account Number/Name: 1234
Authentication ID: unchecked
Password: ****
Expiry Time: (use default value)

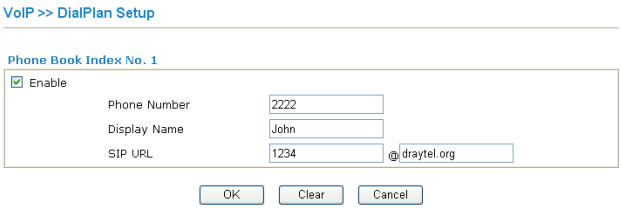



**CODEC/RTP/DTMF ---**
(Use default value)

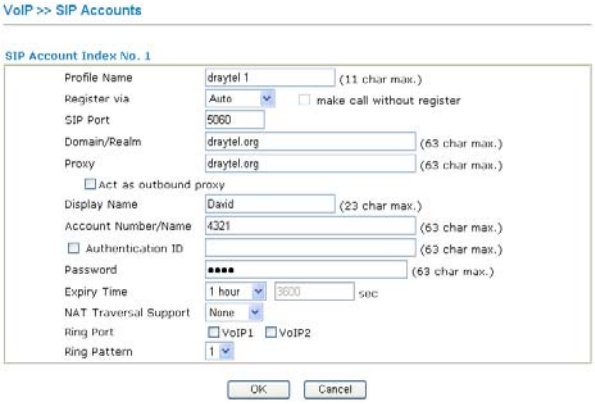
**John calls David**
He picks up the phone and dials 1111#. (DialPlan Phone Number for David) Or,
He picks up the phone and dials 4321#. (David's Account Name)

---

**Settings for David**
DialPlan index 1
Phone Number:2222
Display Name: John
SIP URL:1234@draytel.org




**SIP Accounts Settings ---**
Profile Name: John
Register via: Auto
SIP Port: 5060(default)
Domain/Realm: draytel.org
Proxy: iptel.org
Act as outbound proxy: unchecked
Display Name: David
Account Name: 4321
Authentication ID: unchecked
Password: ****
Expiry Time: (use default value)




**CODEC/RTP/DTMF---**
(Use default value)

**David calls John**
He picks up the phone and dials 2222# (DialPlan Phone Number for John) Or,
He picks up the phone and dials 1234# (John's Account Name)

## 4.5.2 Peer-to-Peer Calling

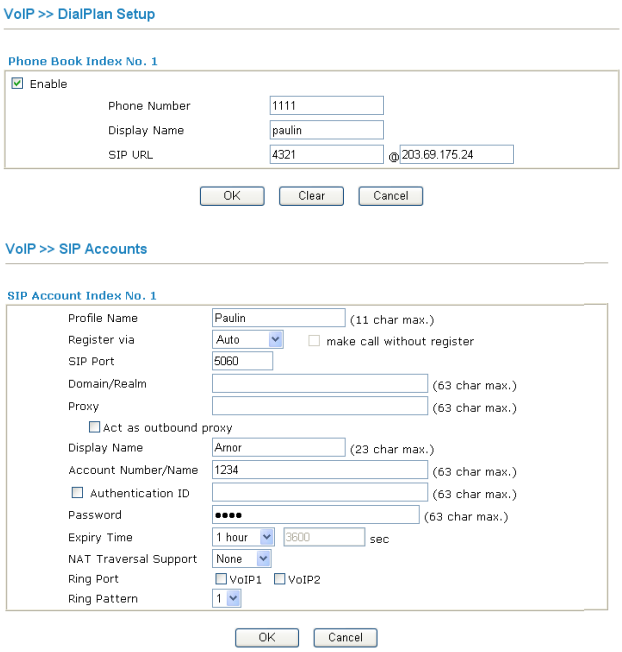
Example 3: Arnor and Paulin have Vigor routers respectively, they can call each other *without* SIP Registrar. First they must have each other's IP address and assign an Account Name for the port used for calling.

Arnor's SIP URL: 1234@214.61.172.53  Paulin's SIP URL: 4321@ 203.69.175.24

**Settings for Arnor**
DialPlan index 1
Phone Number: 1111
Display Name: paulin
SIP URL: 4321@ 203.69.175.24

**SIP Accounts Settings ---**
Profile Name: Paulin
Register via: None
SIP Port: 5060(default)
Domain/Realm: (blank)
Proxy: (blank)
Act as outbound proxy: unchecked
Display Name: Arnor
Account Name: 1234
Authentication ID: unchecked
Password: (blank)
Expiry Time: (use default value)

**CODEC/RTP/DTMF---**
(Use default value)



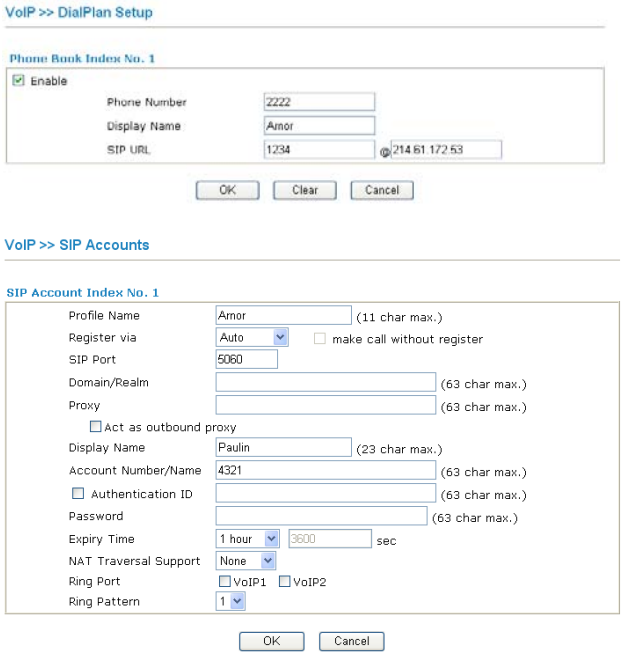

**Arnor calls Paulin**
He picks up the phone and dials **1111#**. (DialPlan Phone Number for Arnor)

---

**Settings for Paulin**
DialPlan index 1
Phone Number:2222
Display Name: Arnor
SIP URL: 1234@214.61.172.53

**SIP Accounts Settings ---**
Profile Name: Arnor
Register via: None
SIP Port: 5060(default)
Domain/Realm: (blank)
Proxy: (blank)
Act as outbound proxy: unchecked
Display Name: Paulin
Account Name: 4321
Authentication ID: unchecked
Password: (blank)
Expiry Time: (use default value)

**CODEC/RTP/DTMF---**
(Use default value)

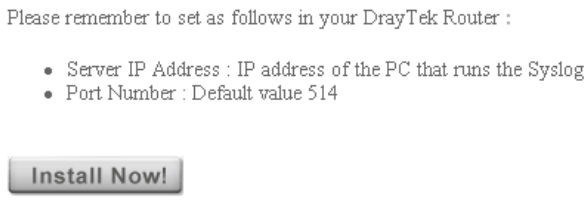



**Paulin calls Arnor**
He picks up the phone and dials **2222#** (DialPlan Phone Number for John)

## 4.6 Upgrade Firmware for Your Router

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

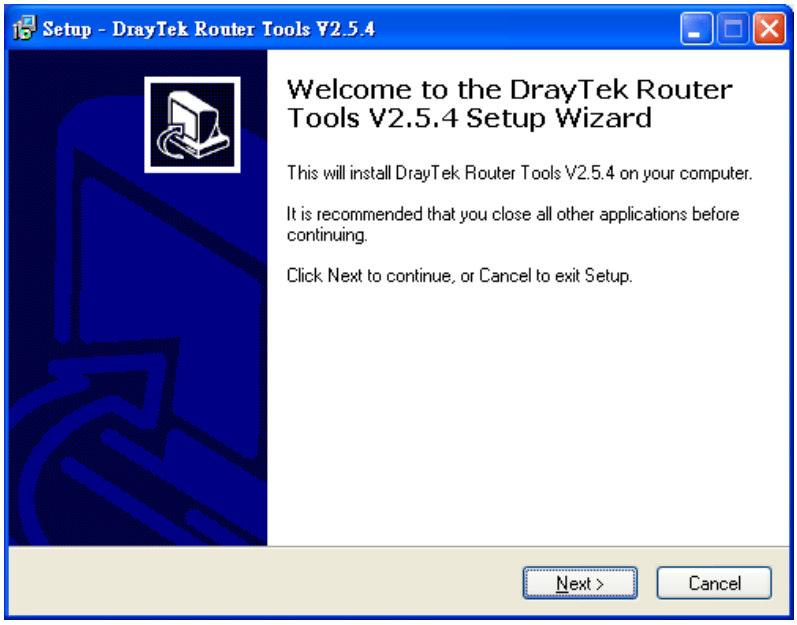
1. Insert CD of the router to your CD ROM.
2. From the webpage, please find out **Utility** menu and click it.
3. On the webpage of Utility, click **Install Now!** (under Syslog description) to install the corresponding program.



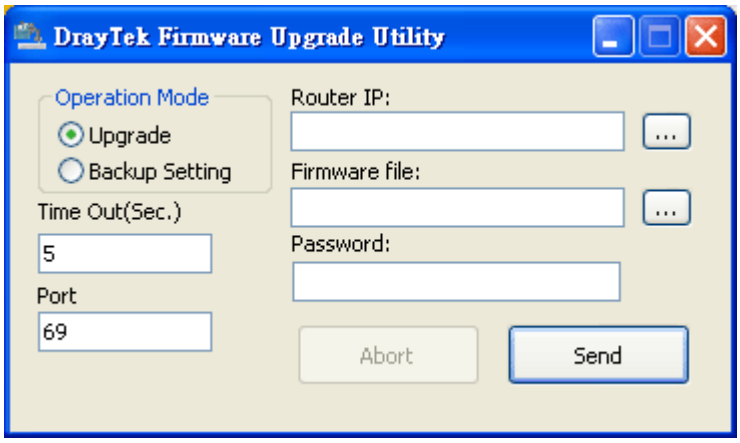

4. The file **RTSxxx.exe** will be asked to copy onto your computer. Remember the place of storing the execution file.
5. Go to **www.draytek.com** to find out the newly update firmware for your router.
6. Access into **Support Center >> Downloads**. Find out the model name of the router and click the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


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

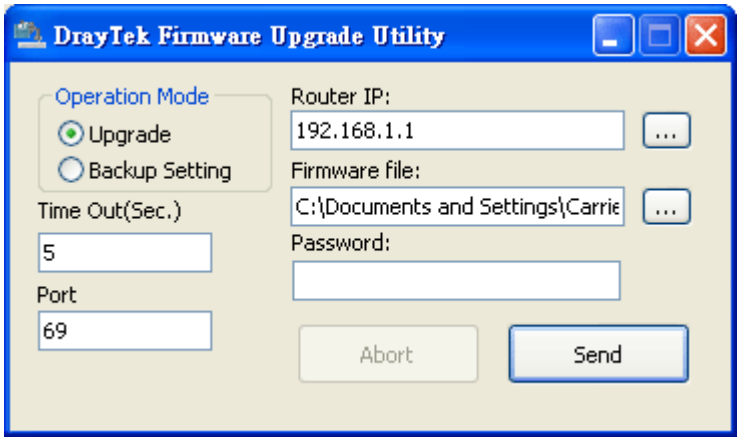
9. Double click on the icon of router tool. The setup wizard will appear.

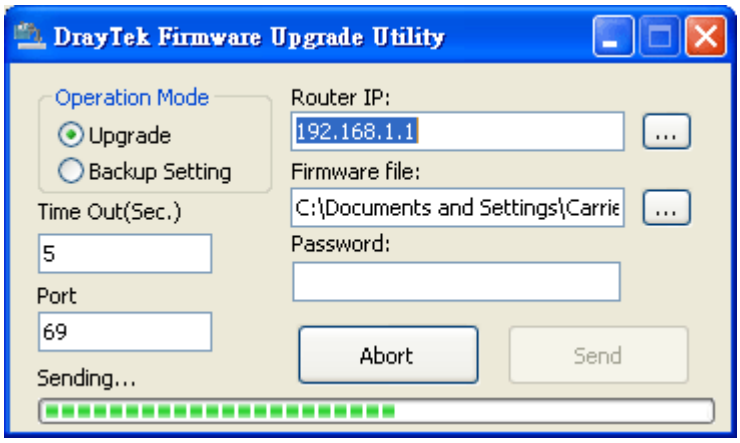

10. Follow the onscreen instructions to install the tool. Finally, click **Finish** to end the installation.
11. From the **Start** menu, open **Programs** and choose **Router Tools XXX** >> **Firmware Upgrade Utility**.




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

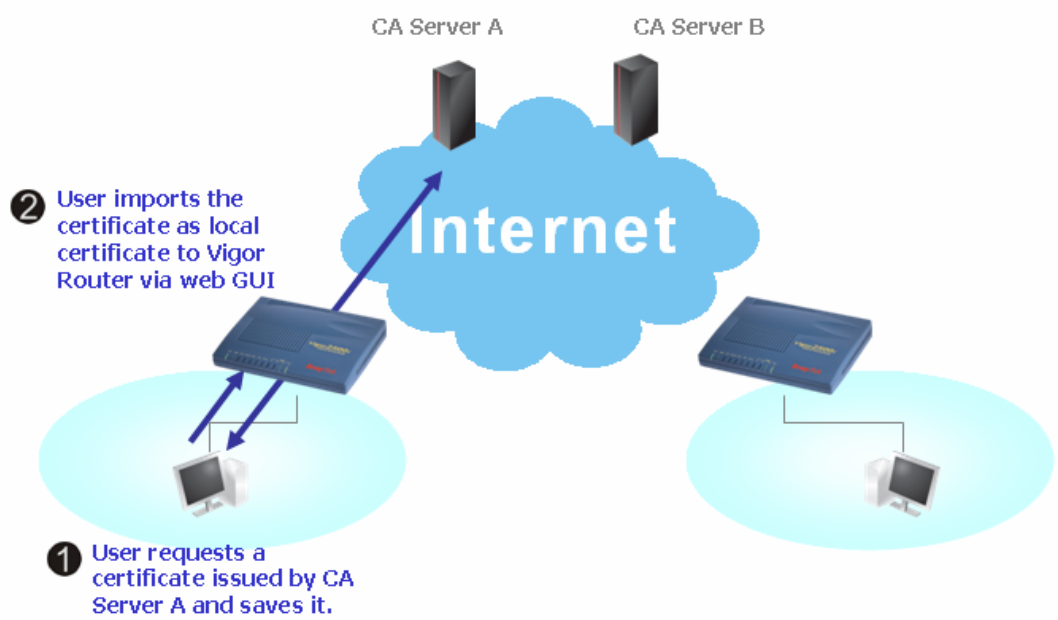



14. Click **Send**.

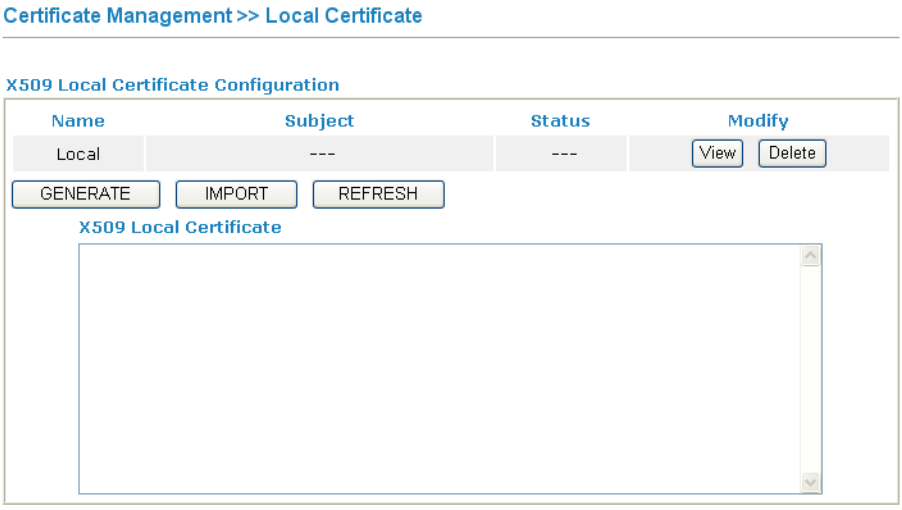



15. Now the firmware update is finished.

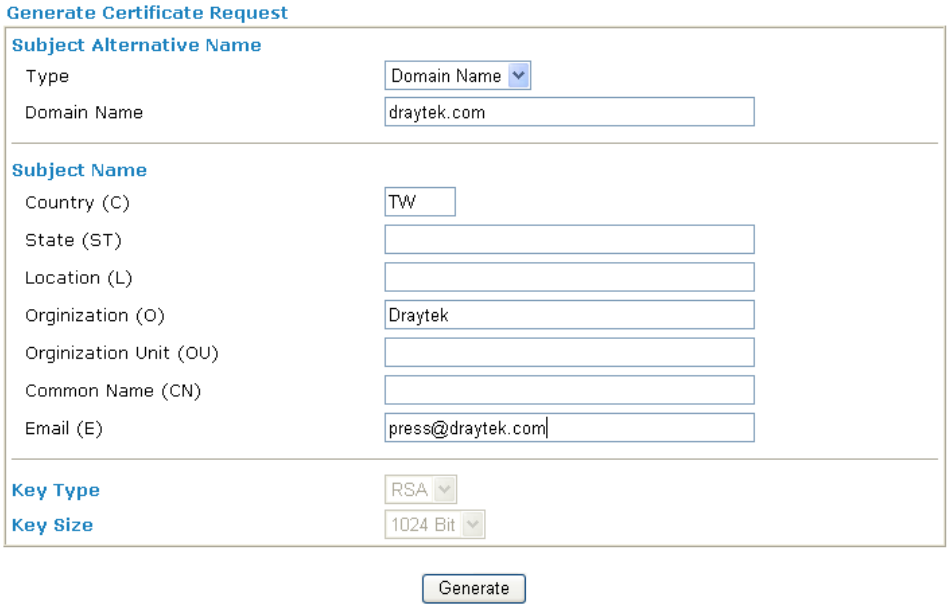
## 4.7 Request a Certificate from a CA Server on Windows CA Server



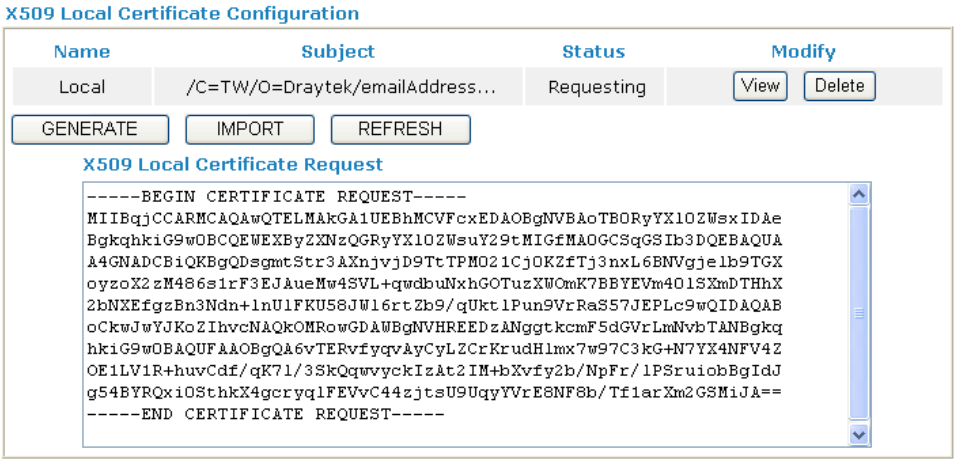

1. Go to **Certificate Management** and choose **Local Certificate**.



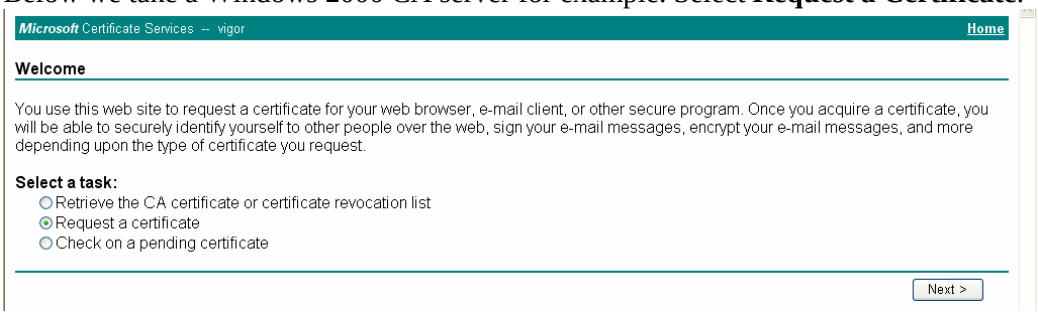

2. You can click **GENERATE** button to start to edit a certificate request. Enter the information in the certificate request.



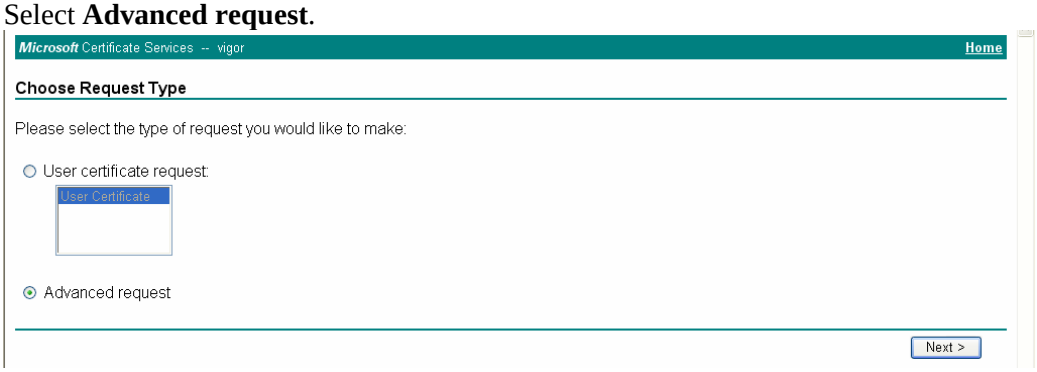

3. Copy and save the X509 Local Certificate Requet as a text file and save it for later use.



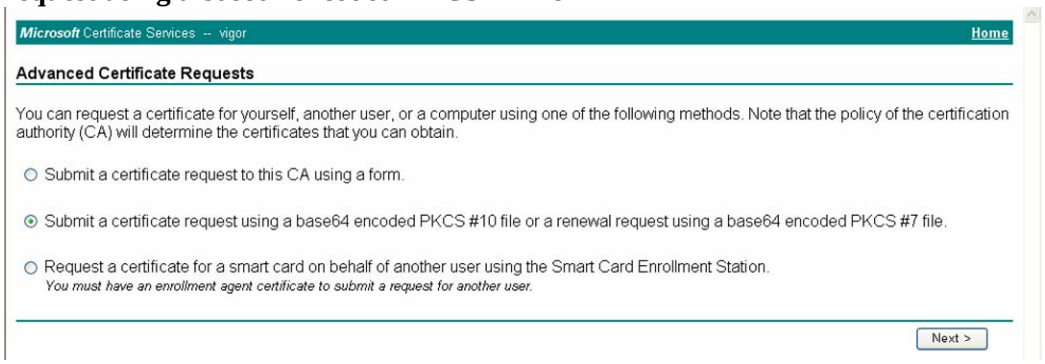

4. Connect to CA server via web browser. Follow the instruction to submit the request. Below we take a Windows 2000 CA server for example. Select **Request a Certificate**.



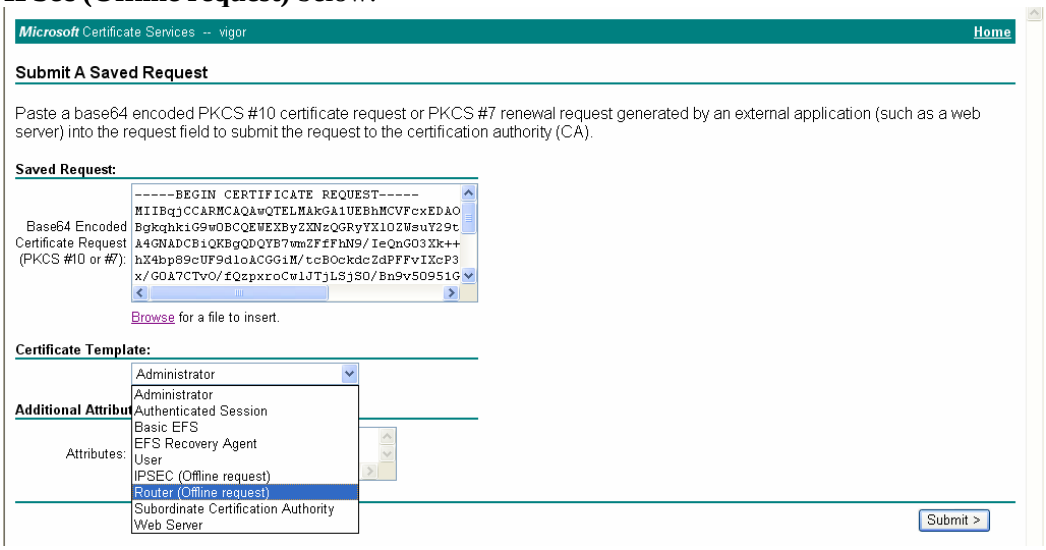
Select **Advanced request**.




Select **Submit a certificate request a base64 encoded PKCS #10 file or a renewal request using a base64 encoded PKCS #7 file**



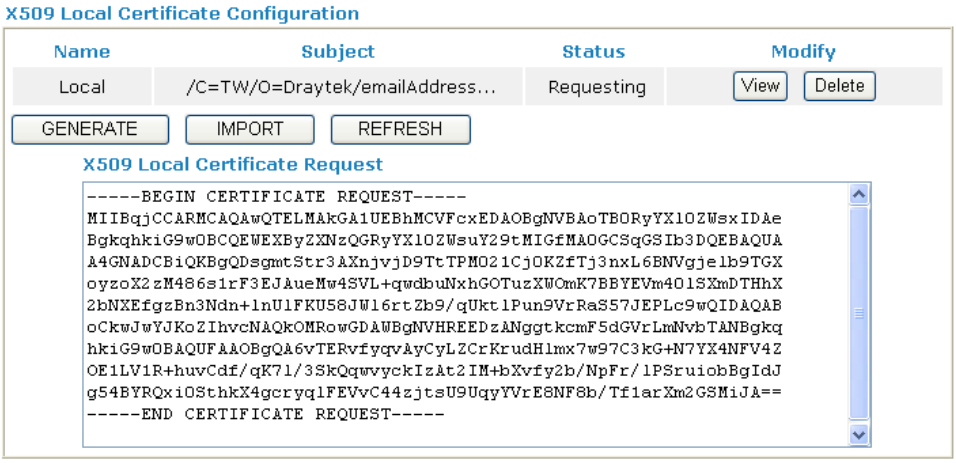

Import the X509 Local Certificate Request text file. Select **Router (Offline request)** or **IPSec (Offline request)** below.



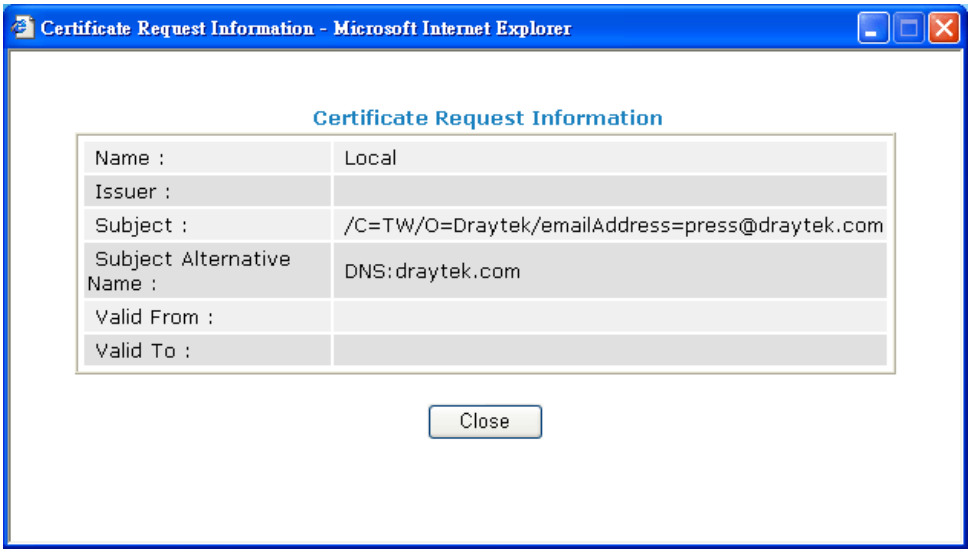

Then you have done the request and the server now issues you a certificate. Select **Base 64 encoded** certificate and **Download CA certificate**. Now you should get a certificate (.cer file) and save it.

5. 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

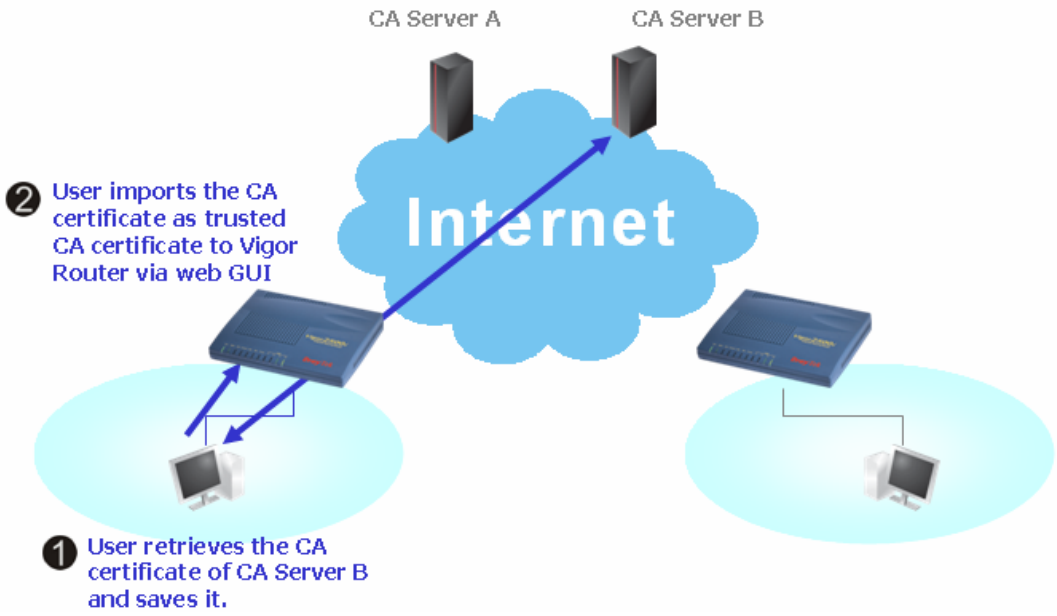
you will find the below window showing “------BEGIN CERTIFICATE------.....”



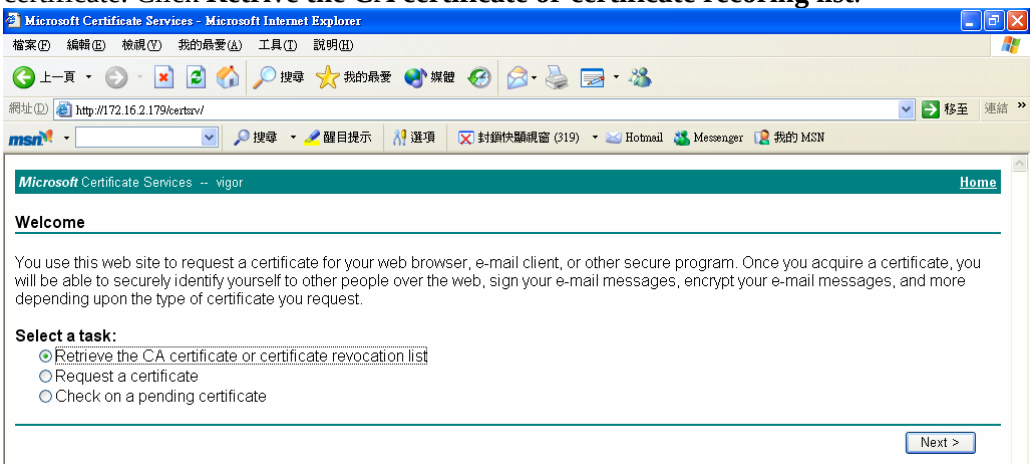

6. You may review the detail information of the certificate by clicking **View** button.



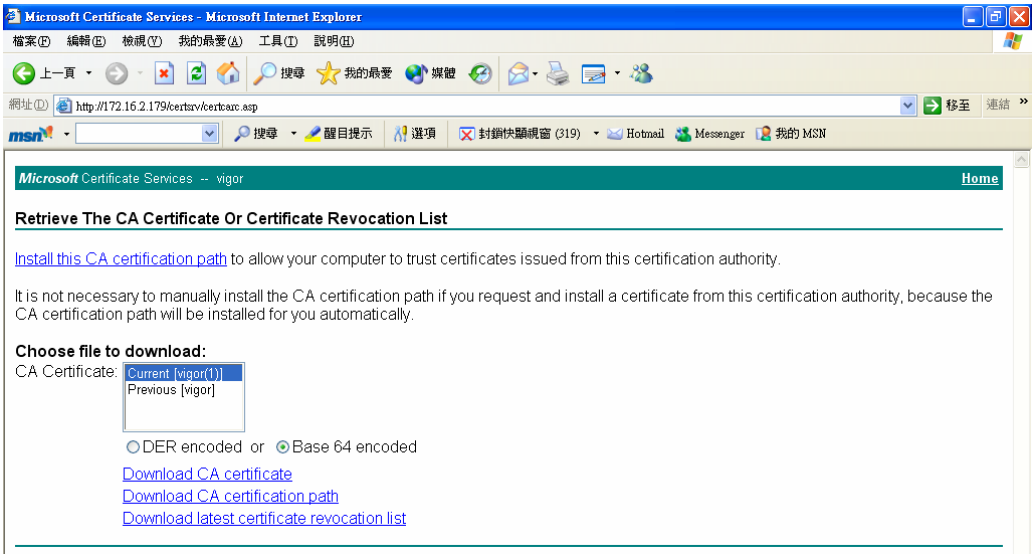
## 4.8 Request a CA Certificate and Set as Trusted on Windows CA Server



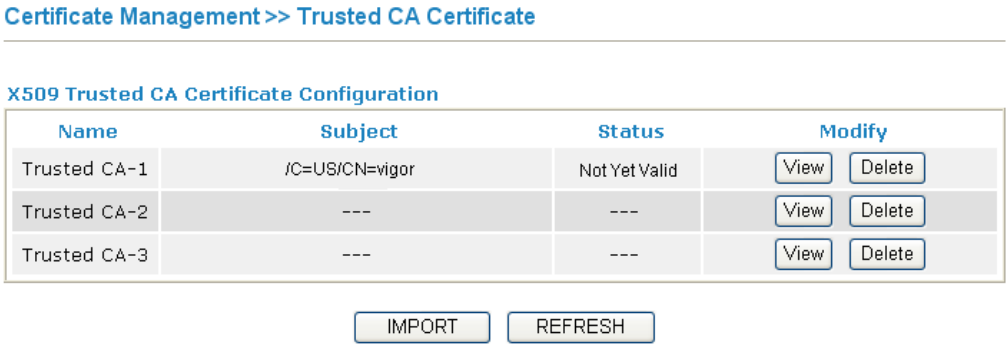

1. Use web browser connecting to the CA server that you would like to retrieve its CA certificate. Click **Retrive the CA certificate or certificate recoring list**.



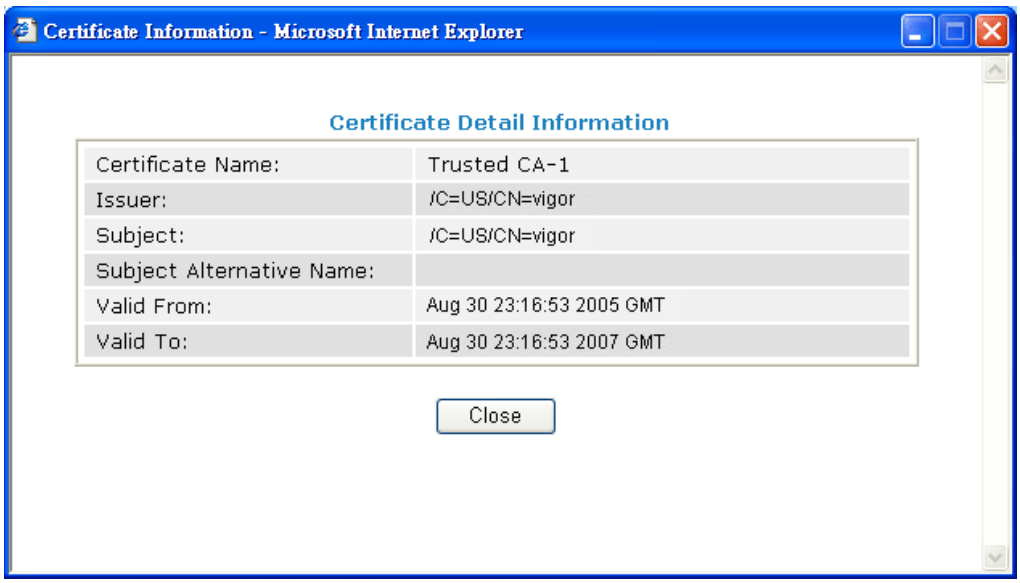
2. In **Choose file to download**, click CA Certificate **Current** and **Base 64 encoded,** and **Download CA certificate** to save the .cer. file.




3. 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.




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




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

# 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.

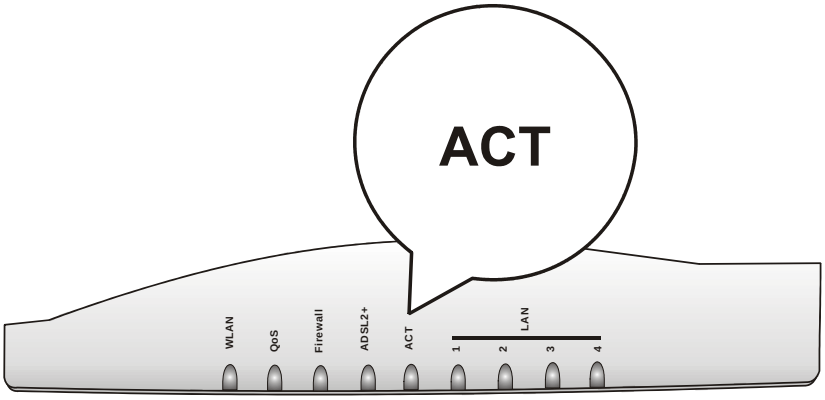
- Checking if the hardware status is OK or not.
- Checking if the network connection settings on your computer are OK or not.
- Pinging the router from your computer.
- Checking if the ISP settings are OK or not.
- Backing to factory default setting if necessary.

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 "**2.1 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 **"2.1 Hardware Installation"** to execute the hardware installation again. And then, try again.

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

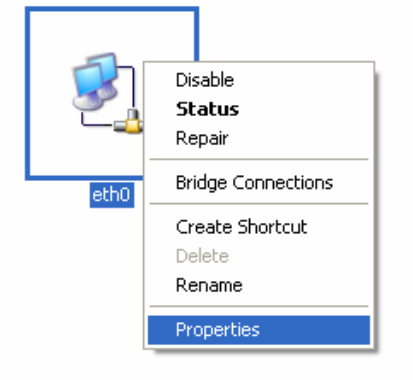
Sometimes the link failure occurs due to the wrong network connection settings. After trying the above section, if the link is stilled failed, please do the steps listed below to make sure the network connection settings is OK.

## For Windows

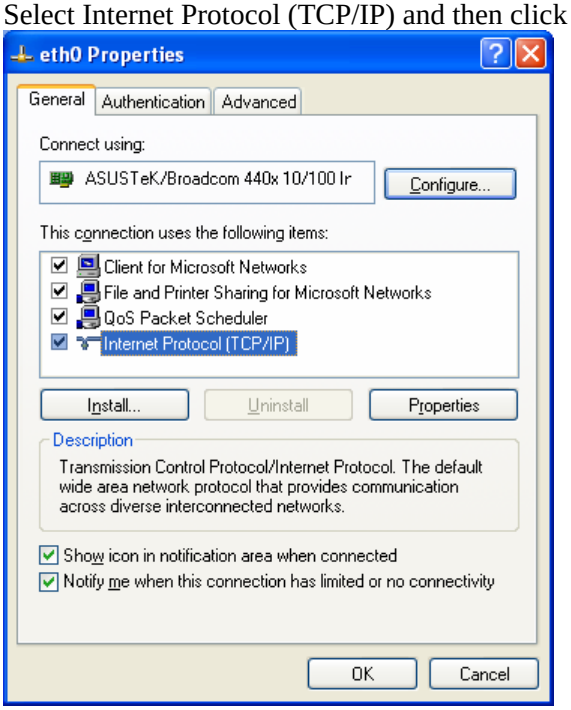
The example is based on Windows XP. As to the examples for other operation systems, please refer to the similar steps or find support notes in **www.draytek.com**.

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

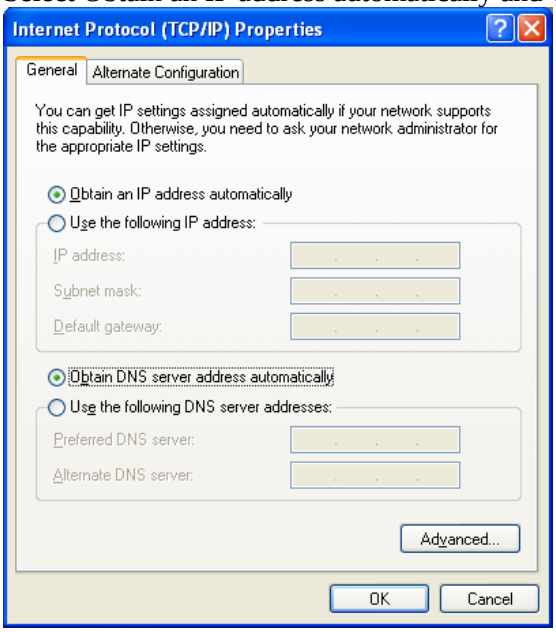

2. Right-click on Local Area Connection and click on Properties.




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

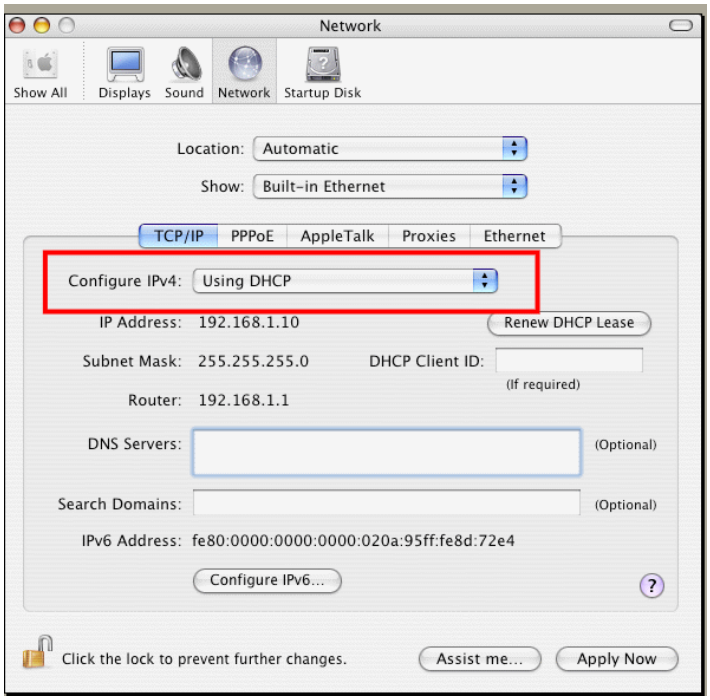


4. Select Obtain an IP address automatically and Obtain DNS server address automatically.




## 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.



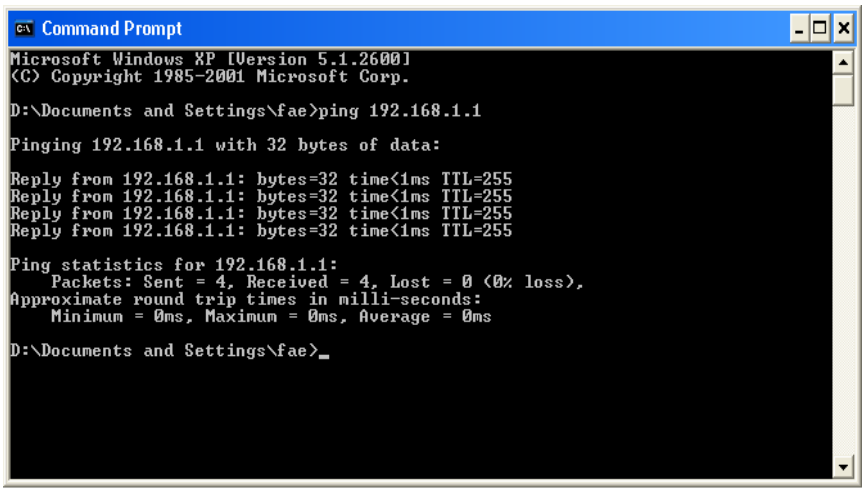
## 5.3 Pinging the Router from Your Computer

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 4.2)

Please follow the steps below to ping the router correctly.

### For Windows

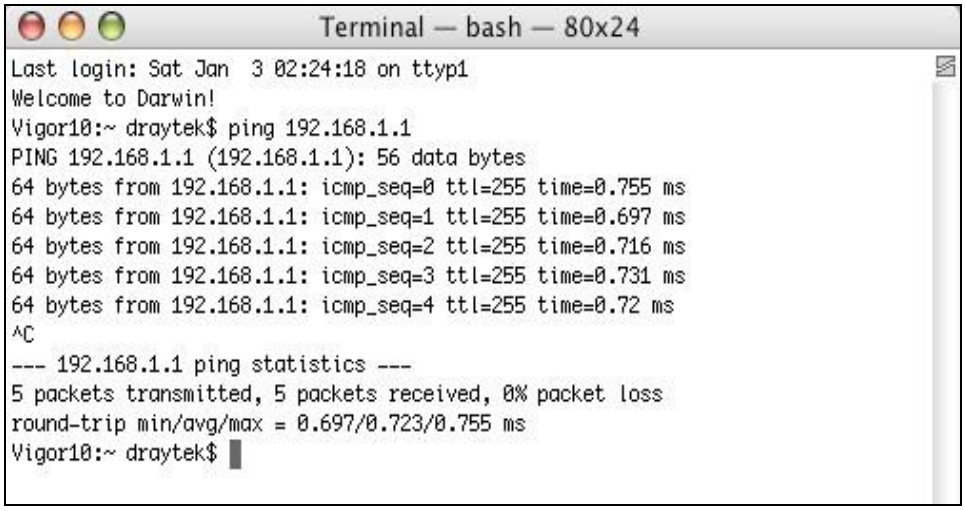
1. Open the **Command** Prompt window (from **Start menu> Run**).
2. Type **command** (for Windows 95/98/ME) or **cmd** (for Windows NT/ 2000/XP). The DOS command dialog will appear.




3. Type ping 192.168.1.1 and press [Enter]. It 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]. It the link is OK, the line of **“64 bytes from 192.168.1.1: icmp_seq=0 ttl=255 time=xxxx ms**” will appear.

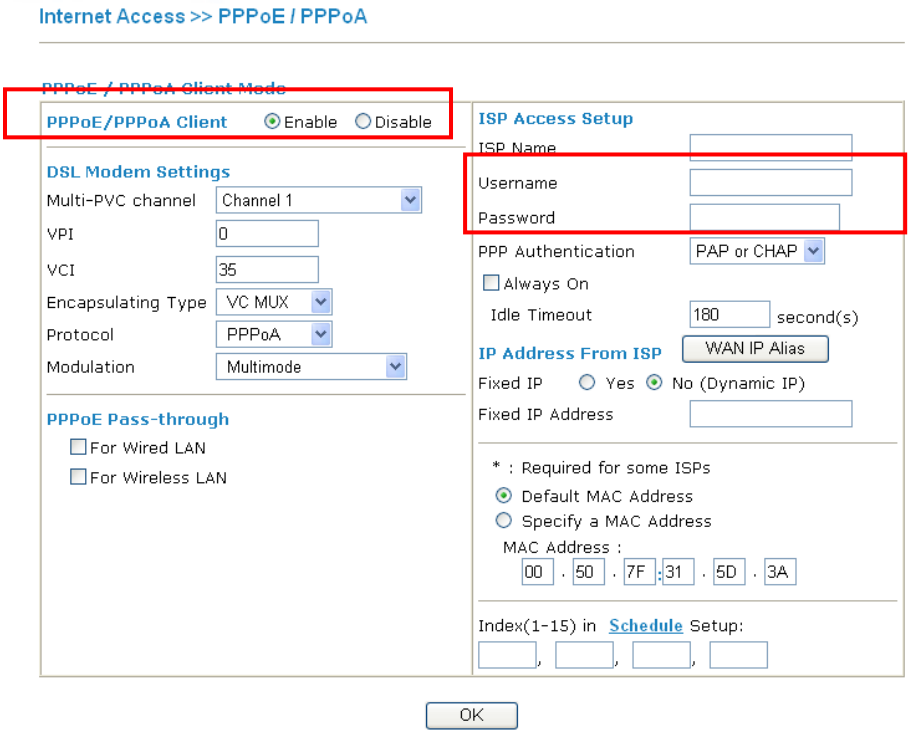

Terminal — bash — 80x24
Last login: Sat Jan 3 02:24:18 on ttyp1
Welcome to Darwin!
Vigor10:~ draytek$ ping 192.168.1.1
PING 192.168.1.1 (192.168.1.1): 56 data bytes
64 bytes from 192.168.1.1: icmp_seq=0 ttl=255 time=0.755 ms
64 bytes from 192.168.1.1: icmp_seq=1 ttl=255 time=0.697 ms
64 bytes from 192.168.1.1: icmp_seq=2 ttl=255 time=0.716 ms
64 bytes from 192.168.1.1: icmp_seq=3 ttl=255 time=0.731 ms
64 bytes from 192.168.1.1: icmp_seq=4 ttl=255 time=0.72 ms
^C
--- 192.168.1.1 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 0.697/0.723/0.755 ms
Vigor10:~ draytek$

## 5.4 Checking If the ISP Settings are OK or Not

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

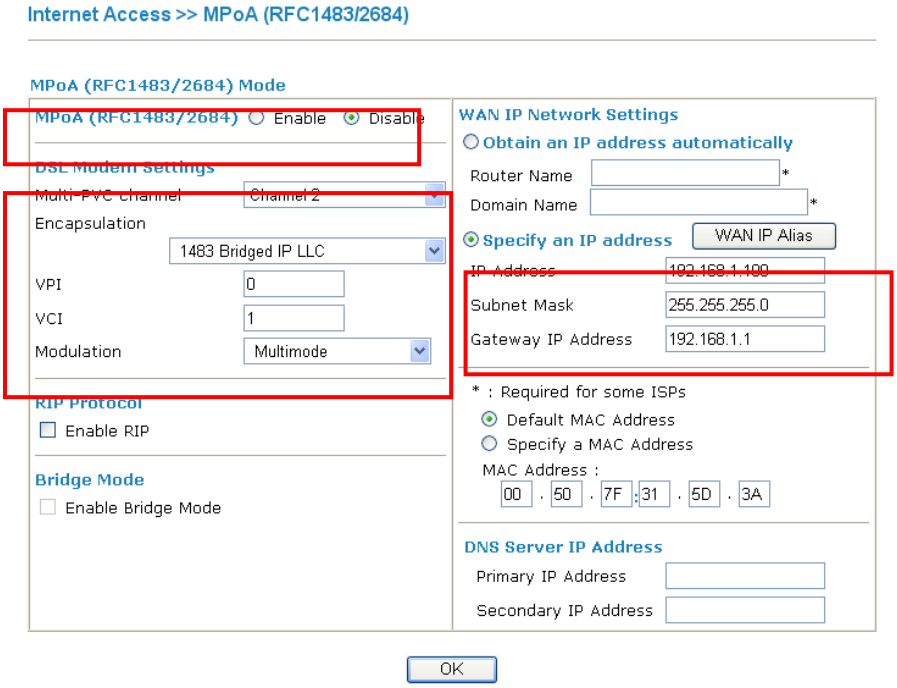

### For PPPoE/PPPoA Users

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



### For MPoA Users

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




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

## 5.5 Backing to Factory Default Setting If Necessary

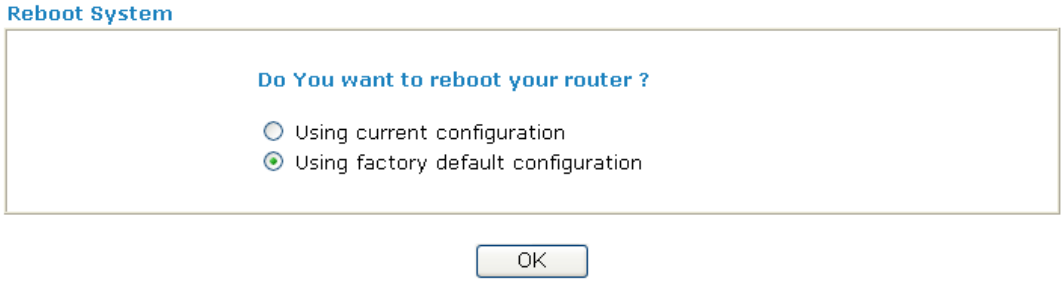
Sometimes, a wrong connection can be improved by returning to the default settings. Try to reset the router by software or hardware.

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

### Software Reset

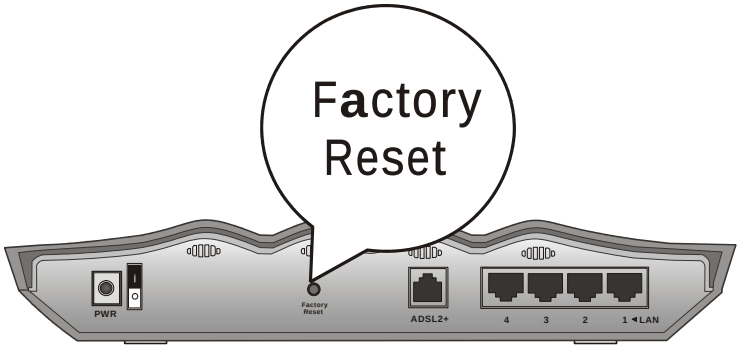
You can reset the router to factory default via Web page.

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




### 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.