DrayTek

Vigor2710 Series

ADSL2/2+ Firewall Router

Your reliable networking solutions partner

User's Guide

UK Version

V.1.0

Vigor2710 Series
ADSL2/2+ Firewall Router
User Guide

Version: 1.0(UK)

Date: 20/04/2009

Copyright Information

Copyright Declarations

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

Trademarks

The following trademarks are used in this document:

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

Safety Instructions and Approval

Safety Instructions

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

Warranty

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

Be a Registered Owner

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

Firmware & Tools Updates

Due to the continuous evolution of DrayTek technology, all routers may be regularly updated with new firmware. Please consult the DrayTek UK web site for more information on newest firmware, tools and documents. Please also check the UK web site for the full product specification and accessories as this can vary depending on your locality/market.

http://www.draytek.co.uk

European Community Declarations

Manufacturer: DrayTek Corp.
Address: No. 26, Fu Shing Road, HuKou County, HsinChu Industrial Park, Hsin-Chu, Taiwan 303
Product: Vigor2710 Series Router

DrayTek Corp. declares that Vigor2710 Series of routers are in compliance with the following essential requirements and other relevant provisions of R&TTE Directive 1999/5/EEC.

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

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

Regulatory Information

Federal Communication Commission Interference Statement

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

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

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

(1) This device may not cause harmful interference, and

(2) This device may accept any interference received, including interference that may cause undesired operation.

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

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

Table of Contents

1 **Preface 1**

1.1 Web Configuration Buttons Explanation 1

1.2 LED Indicators and Connectors 2

1.2.1 For Vigor2710 2
1.2.2 For Vigor2710n 4
1.2.3 For Vigor2710Vn 6

1.3 Hardware Installation 8

1.4 Printer Installation 9

2 **Configuring Basic Settings 15**

2.1 Two-Level Management 15

2.2 Accessing Web Page 15

2.3 Changing Password 16

2.4 Configuring Router for Internet Connectivity 18

2.5 Online Status 20

2.6 Saving Configuration 22

3 **User Mode Operation 23**

3.1 Internet Access 23

3.1.1 Basics of Internet Protocol (IP) Network 23
3.1.2 PPPoE/PPPoA 24
3.1.3 MPoA 26

3.2 LAN 28

3.2.1 Basics of LAN 28
3.2.2 General Setup 29

3.3 NAT 30

3.3.1 Port Redirection 31
3.3.2 DMZ Host 33
3.3.3 Open Ports 35

3.4 Applications 36

3.4.1 Dynamic DNS 36
3.4.2 UPnP 39

3.5 VoIP 40

3.5.1 DialPlan 42
3.5.2 SIP Accounts 50
3.5.3 Phone Settings 54
3.5.4 Status 59

3.6 Wireless LAN 60
3.6.1 Basic Concepts 60
3.6.2 General Setup 62
3.6.3 Security 64
3.6.4 Access Control 65
3.6.5 Station List 67
3.7 System Maintenance 67
3.7.1 System Status 67
3.7.2 User Password 69
3.7.3 Time and Date 69
3.7.4 Reboot System 70
3.8 Diagnostics 70
3.8.1 DHCP Table 71
3.8.2 Ping Diagnosis 71
3.8.3 Trace Route 72

Admin Mode Operation 73
4.1 Internet Access 73
4.1.1 Basics of Internet Protocol (IP) Network 73
4.1.2 PPPoE/PPPoA 74
4.1.3 MPoA 76
4.1.3 Multi-PVCs 78
4.2 LAN 83
4.2.1 Basics of LAN 83
4.2.2 General Setup 84
4.2.3 VLAN 86
4.2.4 Bind IP to MAC 87
4.3 NAT 88
4.3.1 Port Redirection 88
4.3.2 DMZ Host 91
4.3.3 Open Ports 93
4.4 Firewall 95
4.4.1 Basics for Firewall 95
4.4.2 General Setup 97
4.4.3 Filter Setup 99
4.4.4 DoS Defense 106
4.5 Objects Settings 109
4.5.1 IP Object 109
4.5.2 IP Group 111
4.5.3 Service Type Object 113
4.5.4 Service Type Group 114
4.5.5 Keyword Object 115
4.5.6 Keyword Group 116
4.5.7 File Extension Object 117
4.5.8 IM Object 119
4.5.9 P2P Object 120
4.5.9 P2P Object 120
4.5.10 Misc Object 121
4.6 CSM Profile 122

4.6.1 IM/P2P Filter Profile 123
4.6.2 URL Content Filter Profile 124
4.6.3 Web Content Filter Profile 128

4.7 Bandwidth Management 130

4.7.1 Sessions Limit 130
4.7.2 Bandwidth Limit 131

4.8 Applications 133

4.8.1 Dynamic DNS 133
4.8.2 Schedule 135
4.8.3 UPnP 136
4.8.4 IGMP 138
4.8.5 Wake on LAN 139

4.9 VPN and Remote Access 141

4.9.1 IPSec Peer Identity 141
4.9.2 LAN to LAN 143
4.9.3 Connection Management 148

4.10 Certificate Management 149

4.10.1 Local Certificate 149
4.10.2 Trusted CA Certificate 151
4.10.3 Certificate Backup 152

4.11 VoIP 152

4.11.1 DialPlan 154
4.11.2 SIP Accounts 162
4.11.3 Phone Settings 165
4.11.4 Status 170

4.12 Wireless LAN 171

4.12.1 Basic Concepts 171
4.12.2 General Setup 174
4.11.3 Security 177
4.12.4 Access Control 179
4.12.5 WPS 180
4.12.6 WDS 182
4.12.6 AP Discovery 185
4.12.7 Station List 186

4.13 System Maintenance 187

4.13.1 System Status 187
4.13.2 TR-069 189
4.13.3 Administrator Password 190
4.13.4 Configuration Backup 190
4.13.5 Syslog/Mail Alert 192
4.13.6 Time and Date 194
4.13.7 Management 195
4.13.8 Reboot System 196
4.13.9 Firmware Upgrade 197

4.14 Diagnostics 198

4.14.1 Dial-out Trigger 198
4.14.2 Routing Table 199
4.14.3 ARP Cache Table 199
4.14.4 DHCP Table 200
4.14.5 NAT Sessions Table 201
4.14.6 Data Flow Monitor 202
4.14.7 Traffic Graph 203

4.14.8 Ping Diagnosis 204
4.14.9 Trace Route 205

Application and Examples 207

5.1 Request a certificate from a CA server on Windows CA Server 207
5.2 Request a CA Certificate and Set as Trusted on Windows CA Server 211
5.3 Calling Scenario for VoIP function 213
5.3.1 Calling via SIP Sever 213
5.3.2 Peer-to-Peer Calling 215
5.4 Upgrade Firmware for Your Router 216

Trouble Shooting 219

6.1 Checking the Hardware Status 219
6.2 Checking the Network Connection Settings on Your Computer 220
6.3 Pinging the Router from Your Computer 222
6.4 Check Online Status Page 223
6.5 Resetting the Router to Factory Default Settings 223
6.6 Technical Support 224

1 Preface

The DrayTek Vigor 2710 Series ADSL/ADSL2/ADSL2+ routers are designed to be the ideal ADSL-sharing and firewall devices for to the SoHo (Small Office / Home) user. They combine compatibility with all UK ADSL line types together with performance and features into an attractive, reliable and easy-to-use product, with the pedigree and thoughtful design DrayTek are renowned for. Wireless and VoIP equipped models further enhance the flexibility of the router and outgoing VPN makes it ideal as a teleworker router for your home VPN link to your main office.

Vigor 2710 series routers support SPI (Stateful Packet Inspection) firewall, which uses a new DrayTek object-based firewall to allow more setup flexibility than ever, enabling you to create combinations of users, rules and restrictions to suit multi-departmental organizations. The CSM (Content Security Management) feature allows more precise and efficient access control for URL/Web Content Filtering, IM (Instant Messenger) and P2P (Peer to Peer) applications.

Vigor2710 'n' models comply with 802.11n Draft-n standards. They support WEP/WPA/WPA2 encryption, MAC Address Control, Wireless LAN Isolation as well as wireless distribution system (WDS). Wireless Rate Control function can adjust the data rate of each wireless station (client).

The Vigor 2710 Series 'V' models build on the established DrayTek VoIP pedigree by adding even more new features. Twin analogue phone ports and an FXO analogue line port provide full PSTN and VoIP integration on the same phones, via both the Internet and your regular analogue line. The two phones can be used independently and simultaneously for both incoming and outgoing calls.

In addition, Vigor2710 series supports USB interface for connecting USB printer to share printer or USB storage device for sharing files. Vigor2710 series also provide two-level administration to control the manageability of the router based on administrative rights.

1.1 Web Configuration Buttons Explanation

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

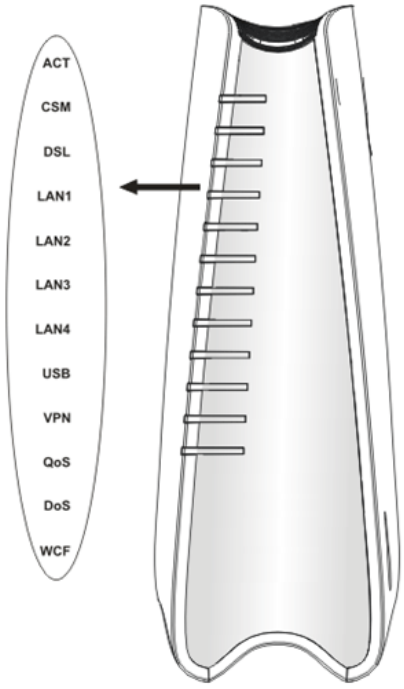
OK	Save and apply current settings.
Cancel	Cancel current settings and recover to the previous saved settings.
Clear	Clear all the selections and parameters settings, including selection from drop-down list. All the values must be reset with factory default settings.
Add	Add new settings for specified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

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

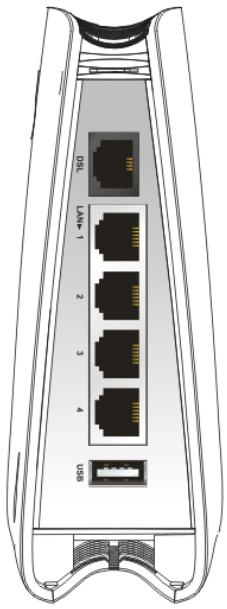
1.2 LED Indicators and Connectors

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

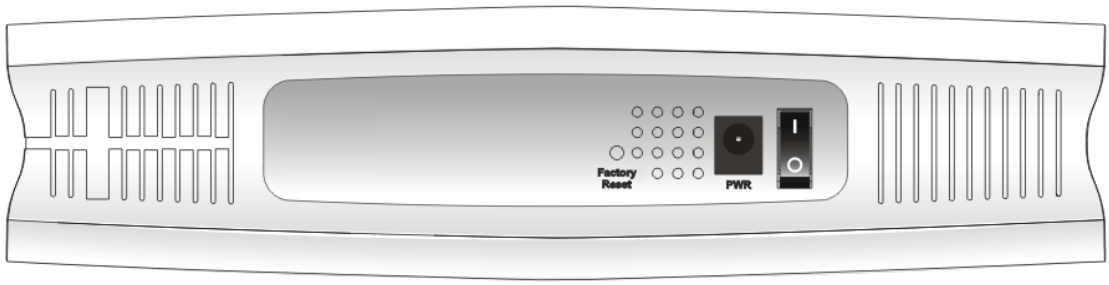
1.2.1 For Vigor2710



LED	Status	Explanation
ACT (Activity)	Blinking	The router is powered on and running normally.
	Off	The router is powered off.
CSM	On	The profile(s) of CSM (Content Security Management) for IM/P2P, URL/Web Content Filter application can be enabled from **Firewall >>General Setup**. (Such profile must be established under **CSM** menu).
DSL	On	The router is ready to access Internet through DSL link.
	Blinking	Slowly: The modem is ready. Quickly: The connection is training.
LAN 1/2/3/4	On	The port is connected.
	Off	The port is disconnected.
	Blinking	The data is transmitting.
USB	On	A USB device is connected and active.
	Blinking	The data is transmitting.
VPN	On	The VPN tunnel is active.
QoS	On	The QoS function is active.
DoS	On	The DoS/DDoS function is active.
	Blinking	It will blink while detecting an attack.
WCF	On	The profile(s) of CSM (Content Security Management) for Web Content Filter application can be enabled from **Firewall >>General Setup**. (Such profile must be established under **CSM** menu)

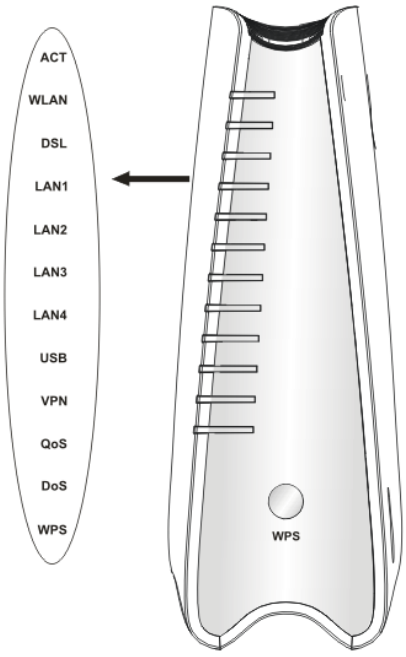


Interface	Description
DSL	Connecter for accessing the Internet through ADSL2/2+.
LAN (1-4)	Connecters for local networked devices.
USB	Connecter for USB storage device (Pen Driver/Mobile HD) or printer.

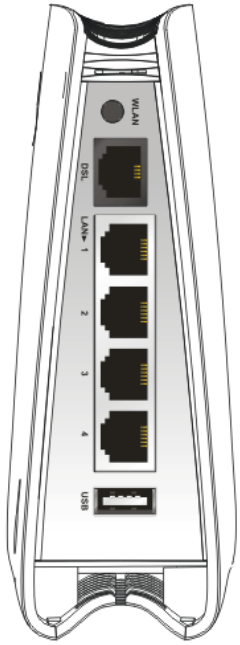


Interface	Description
Factory Reset	Restore the default settings. Usage: Turn on the router (ACT LED is blinking). Press the hole and keep for more than 5 seconds. When you see the ACT LED begins to blink rapidly than usual, release the button. Then the router will restart with the factory default configuration.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

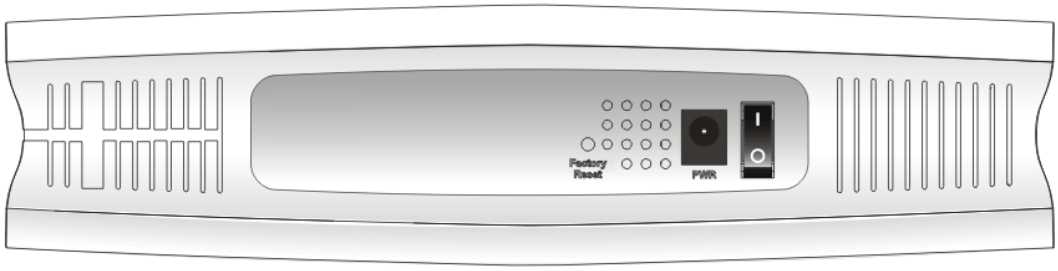
1.2.2 For Vigor2710n



LED	Status	Explanation
ACT (Activity)	Blinking	The router is powered on and running normally.
	Off	The router is powered off.
WLAN	On	Wireless access point is ready.
	Blinking	It will blink while wireless traffic goes through.
DSL	On	The router is ready to access Internet through DSL link.
	Blinking	Slowly: The modem is ready. Quickly: The connection is training.
LAN 1/2/3/4	On	The port is connected.
	Off	The port is disconnected.
	Blinking	The data is transmitting.
USB	On	A USB device is connected and active.
	Blinking	The data is transmitting.
VPN	On	The VPN tunnel is active.
QoS	On	The QoS function is active.
DoS	On	The DoS/DDoS function is active.
	Blinking	It will blink while detecting an attack.
WPS	On	The WPS is on.
	Off	The WPS is off.
	Blinking	Waiting for wireless client sending requests for connection about two minutes.
WPS Button	On	Press this button for 2 seconds to wait for client device making network connection through WPS. When the LED lights up, the WPS will be on.
	Off	The WPS is off.
	Blinking	Waiting for wireless client sending requests for connection about two minutes.

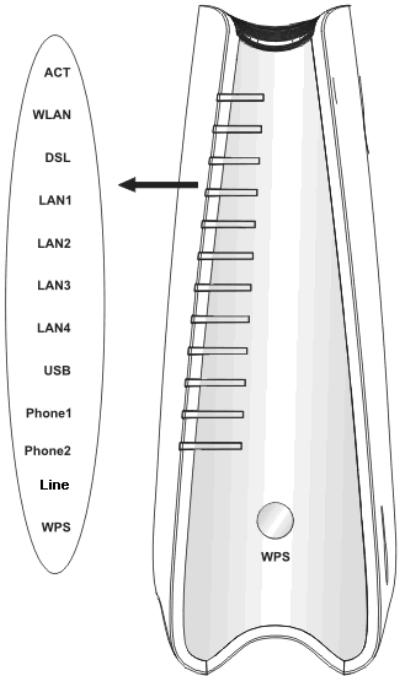


Interface	Description
WLAN	Press the button once to enable (WLAN LED on) or disable (WLAN LED off) wireless connection.
DSL	Connecter for accessing the Internet through ADSL2/2+.
LAN (1-4)	Connecters for local networked devices.
USB	Connecter for USB storage (Pen Driver Mobile/HD) or printer.

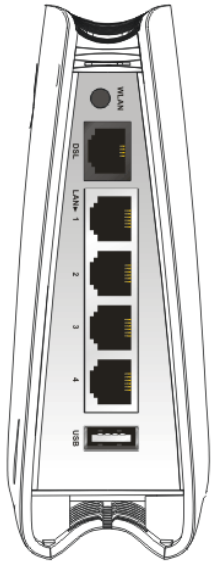


Interface	Description
Factory Reset	Restore the default settings. Usage: Turn on the router (ACT LED is blinking). Press the hole and keep for more than 5 seconds. When you see the ACT LED begins to blink rapidly than usual, release the button. Then the router will restart with the factory default configuration.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

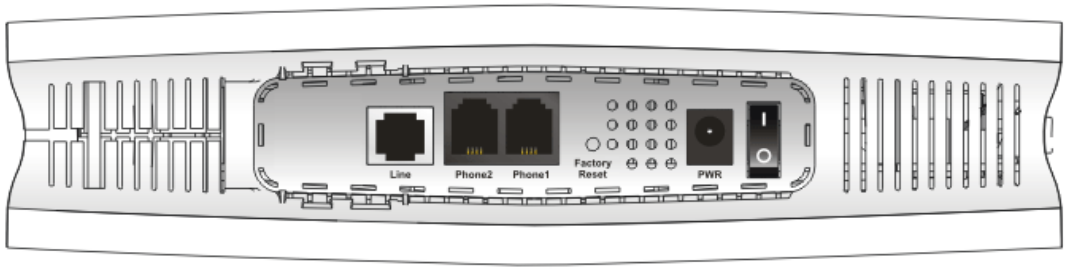
1.2.3 For Vigor2710Vn



LED	Status	Explanation
ACT (Activity)	Blinking	The router is powered on and running normally.
	Off	The router is powered off.
WLAN	On	Wireless access point is ready.
	Blinking	It will blink while wireless traffic goes through.
DSL	On	The router is ready to access Internet through DSL link.
	Blinking	Slowly: The modem is ready. Quickly: The connection is training.
LAN 1/2/3/4	On	The port is connected.
	Off	The port is disconnected.
	Blinking	The data is transmitting.
USB	On	A USB device is connected and active.
	Blinking	The data is transmitting.
Phone1/ Phone2	On	The phone connected to this port is off-hook.
	Off	The phone connected to this port is on-hook.
	Blinking	A phone call comes.
Line	On	A PSTN phone call comes (in and out). However, when the phone call is disconnected, the LED will be off about six seconds later.
	Off	There is no PSTN phone call.
WPS	On	The WPS is on.
	Off	The WPS is off.
	Blinking	Waiting for wireless client sending requests for connection about two minutes.
WPS Button	On	Press this button for 2 seconds to wait for client device making network connection through WPS. When the LED lights up, the WPS will be on.
	Off	The WPS is off.
	Blinking	Waiting for wireless client sending requests for connection about two minutes.



Interface	Description
WLAN	Press the button once to enable (WLAN LED on) or disable (WLAN LED off) wireless connection.
DSL	Connecter for accessing the Internet through ADSL2/2+.
LAN (1-4)	Connecters for local networked devices.
USB	Connecter for USB storage (Pen Driver Mobile/HD) or printer.

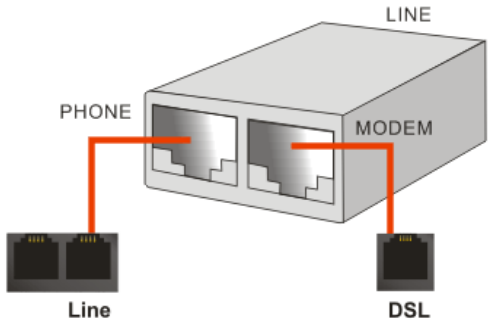


Interface	Description
Line	Connector of analog phone for PSTN life line.
Phone2/Phone1	Connecter of analog phone for VoIP communication.
Factory Reset	Restore the default settings. Usage: Turn on the router (ACT LED is blinking). Press the hole and keep for more than 5 seconds. When you see the ACT LED begins to blink rapidly than usual, release the button. Then the router will restart with the factory default configuration.
PWR	Connecter for a power adapter.
ON/OFF	Power Switch.

1.3 Hardware Installation

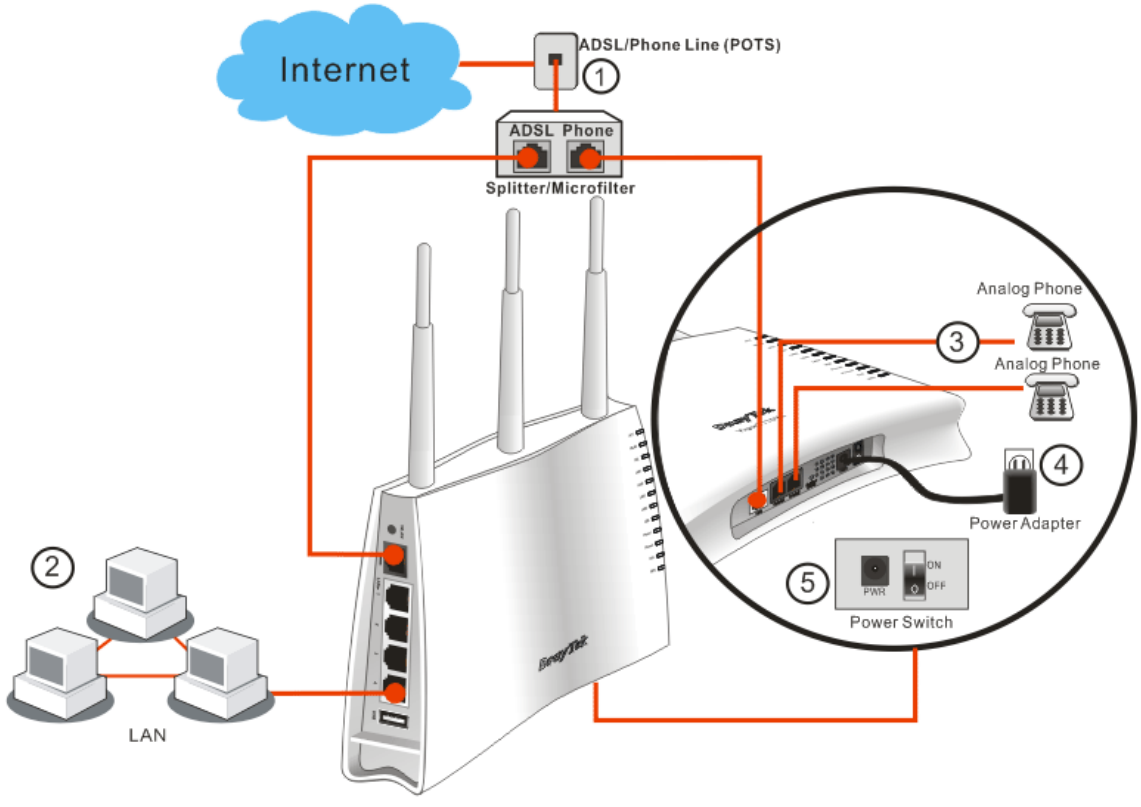
Before starting to configure the router, you have to connect your devices correctly.

1. Connect the ADSL interface to the external ADSL splitter with an ADSL line cable for all models. For Vigor2710Vn, also connect Line interface to external ADSL splitter.



2. Connect one end of an Ethernet cable (RJ-45) to one of the **LAN** ports of the router and the other end of the cable (RJ-45) into the Ethernet port on your computer.
3. Connect the telephone sets with phone lines (for using VoIP function). For the model without phone ports, skip this step.
4. Connect one end of the power adapter to the router's power port on the rear panel, and the other side into a wall outlet.
5. Power on the device by pressing down the power switch on the rear panel.
6. The system starts to initiate. After completing the system test, the **ACT** LED will light up and start blinking.

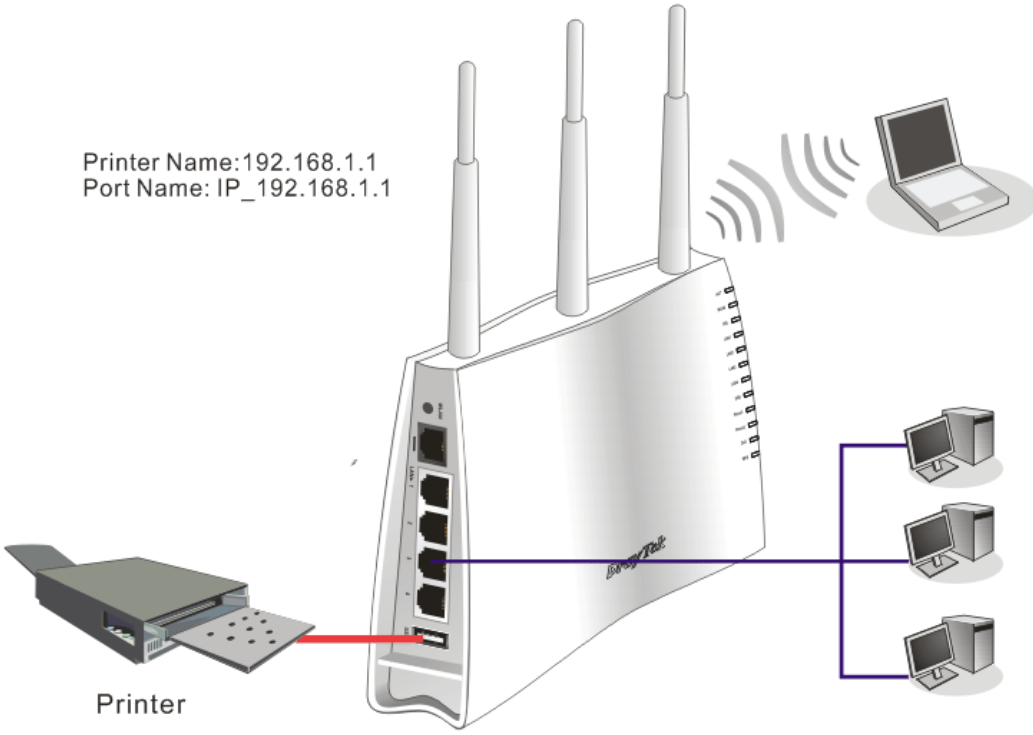
(For the detailed information of LED status, please refer to section 1.2.)



Caution:
1. Each of the Phone ports can be connected to an analog phone only. Do not connect the phone ports to the land line jack. Such connection might damage your router.
2. When the power is shutdown, VoIP phone will be disconnected. However, a phone set connected to Phone 2 port can be used as the traditional telephone for the line will be guided to land line jack via the router (loop through).

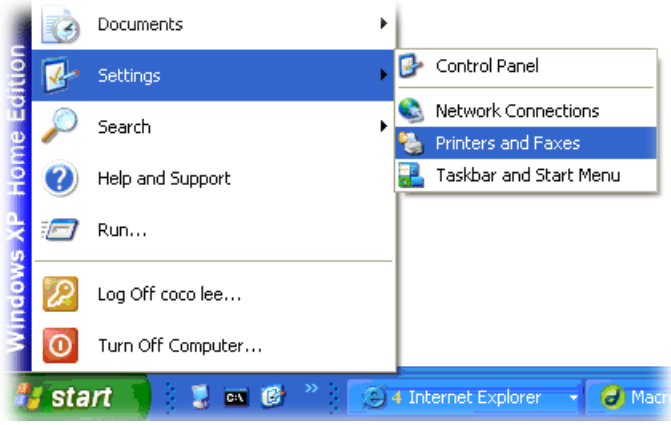
1.4 Printer Installation

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

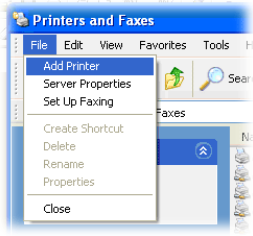


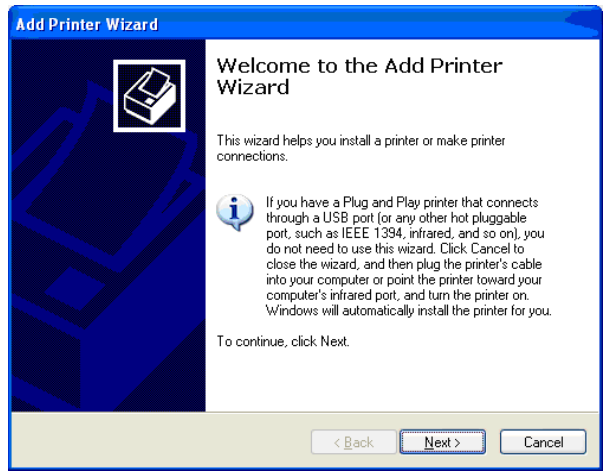
Before using it, please follow the steps below to configure settings for connected computers (or wireless clients).

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

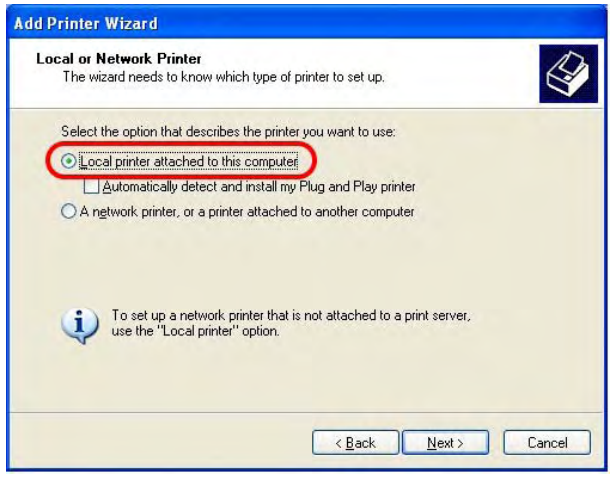


3. Open **File->Add a New Computer**. A welcome dialog will appear. Please click **Next**.

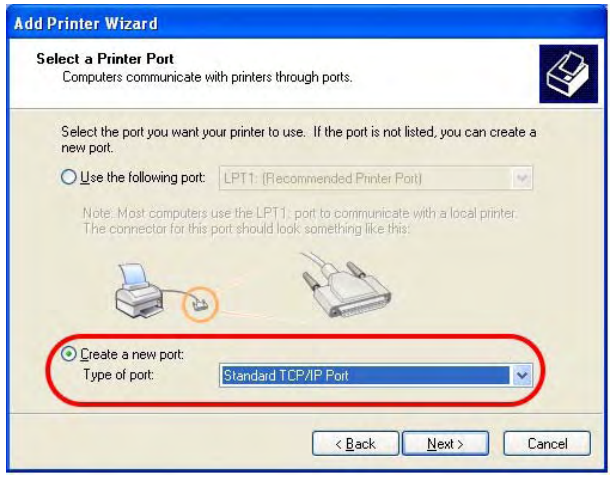




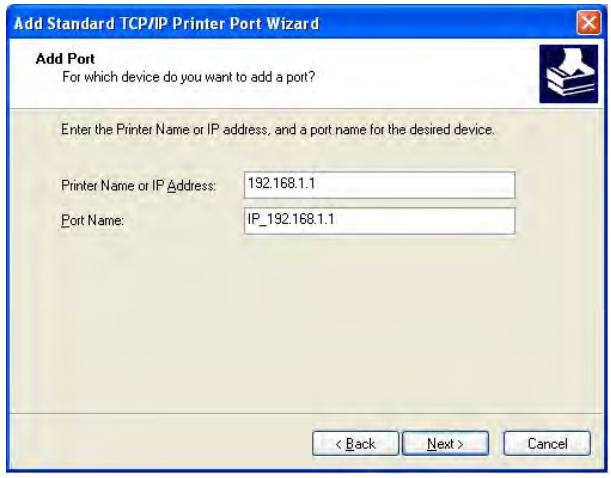
4. Click Local printer attached to this computer and click Next.



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

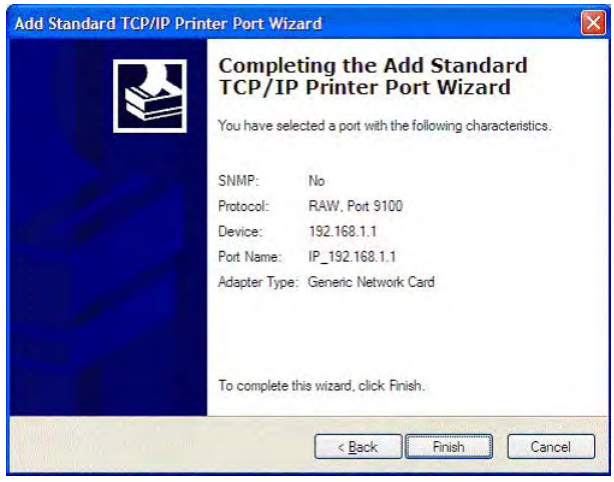


6. In the following dialog, type **192.168.1.1** (router's LAN IP) in the field of **Printer Name or IP Address** and type **IP_192.168.1.1** as the port name. Then, click **Next**.

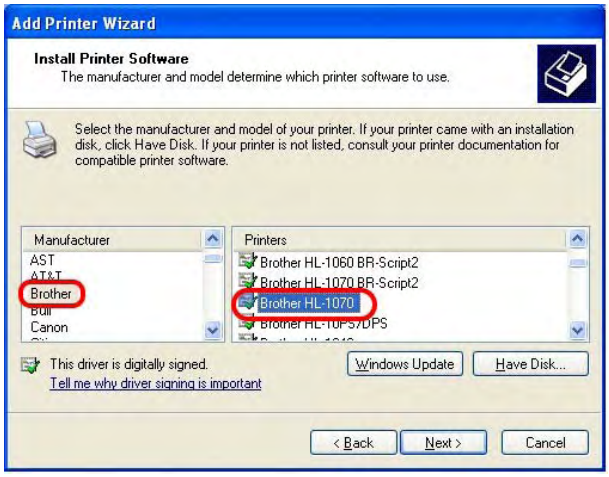


7. Click Standard and choose Generic Network Card.

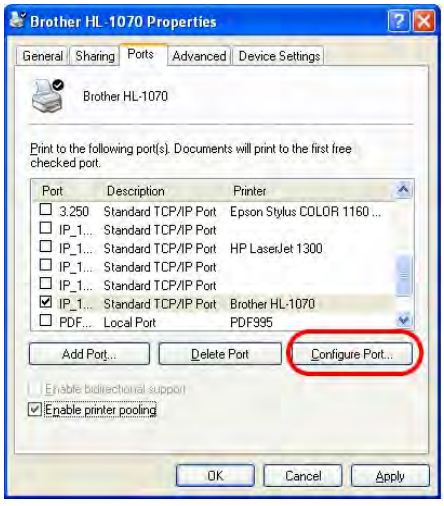
8. Then, in the following dialog, click **Finish**.



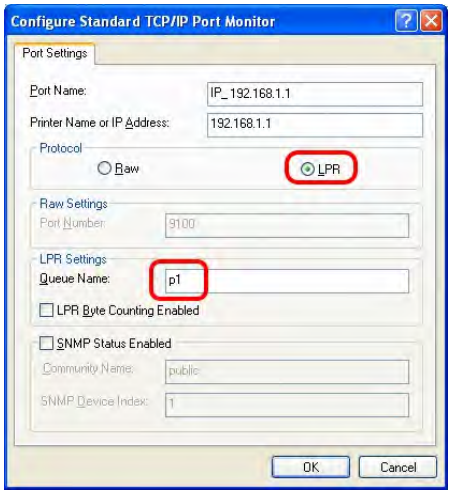
9. Now, your system will ask you to choose right name of the printer that you installed onto the router. Such step can make correct driver loaded onto your PC. When you finish the selection, click **Next**.



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

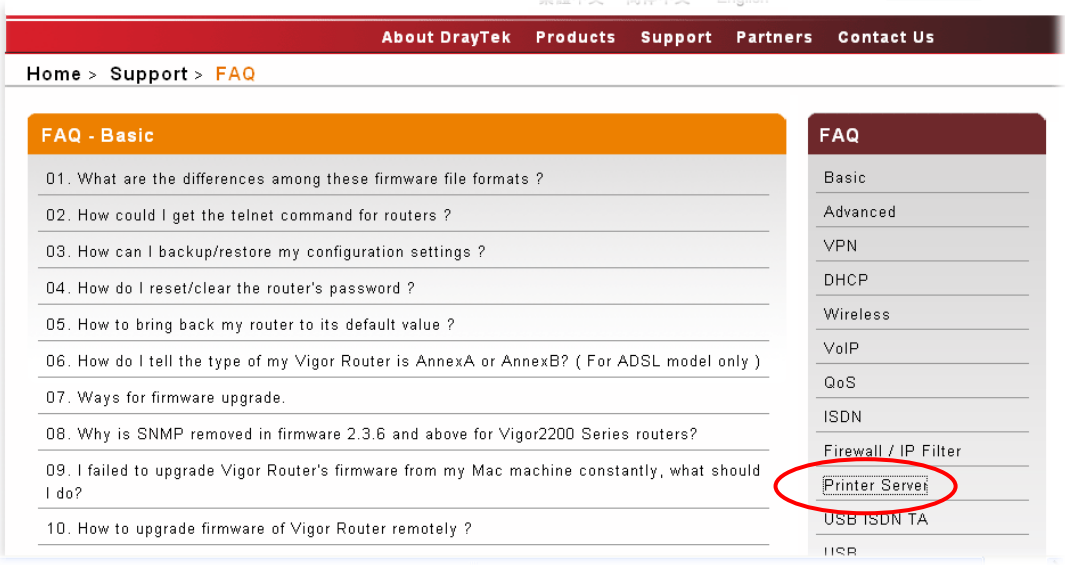


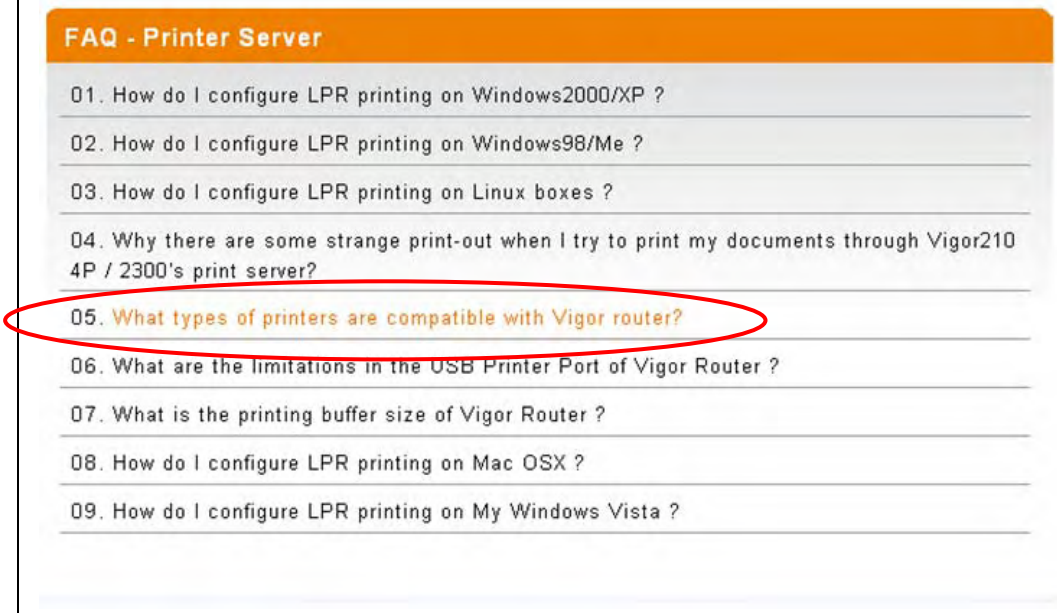
11. Select "**LPR**" on Protocol, type **p1** (number 1) as Queue Name. Then click **OK**. Next please refer to the red rectangle for choosing the correct protocol and UPR name.



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

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





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

This page is left blank.

2 Configuring Basic Settings

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

2.1 Two-Level Management

This chapter explains how to setup a password for an administrator/user and how to adjust basic/advanced settings for accessing Internet successfully.

For user mode operation, do not type any word on the window and click **Login** for the simple web pages for configuration. Yet, for admin mode operation, please type "admin/admin" on Username/Password and click **Login** for full configuration.

2.2 Accessing Web Page

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

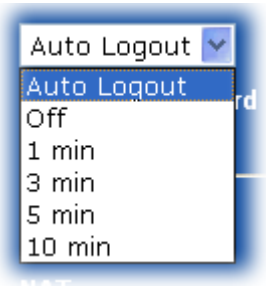
> **Notice:** You may either simply set up your computer to get IP dynamically from the router or set up the IP address of the computer to be the same subnet as **the default IP address of Vigor router 192.168.1.1**. For the detailed information, please refer to the later section - Trouble Shooting of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

2. Open a web browser on your PC and type **http://192.168.1.1.** The following window will be open to ask for username and password.

3. For user's operation, do not type any word on the window and click **Login** for the simple web pages for configuration. Yet, for administrator's operation, please type "admin/admin" on Username/Password and click **Login** for full configuration.

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

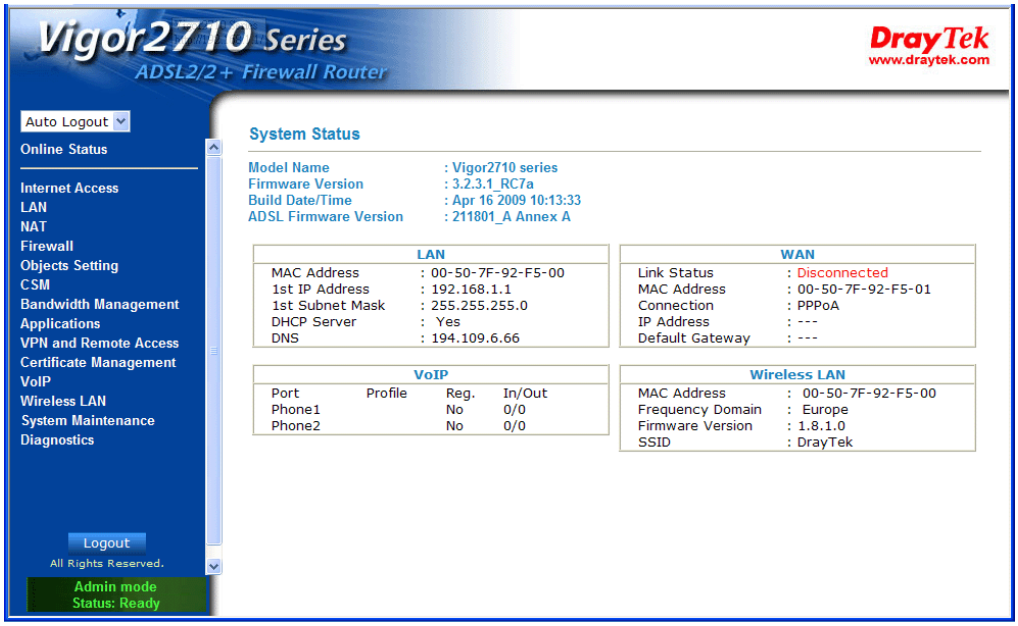
4. The web page can be logged out according to the chosen condition. The default setting is **Auto Logout**, which means the web configuration system will logout after 5 minutes without any operation. Change the setting for your necessity.



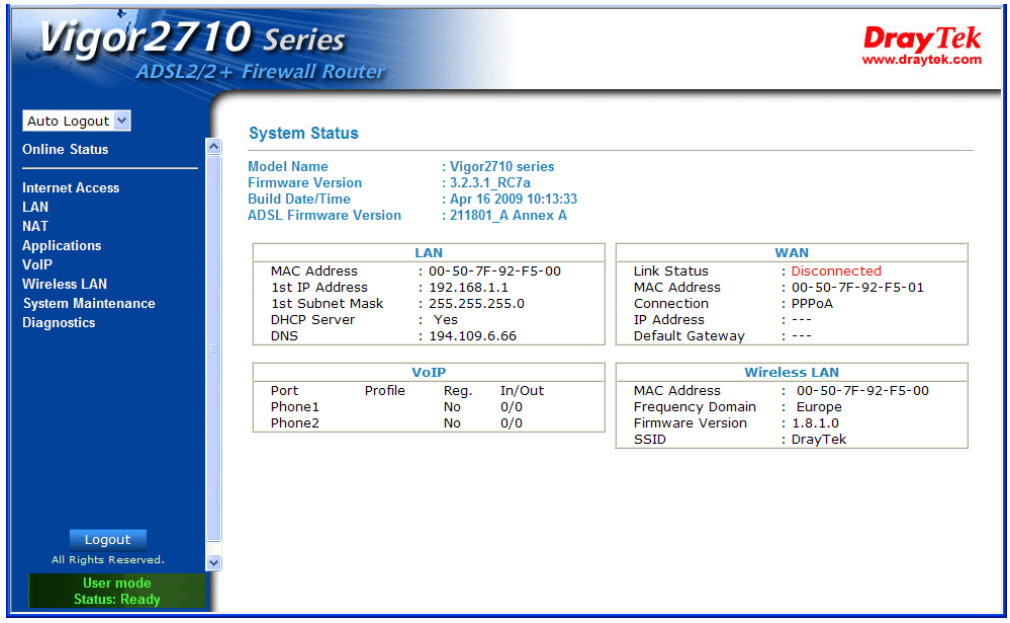
2.3 Changing Password

No matter user mode operation or admin mode operation, please change the password for the original security of the router.

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



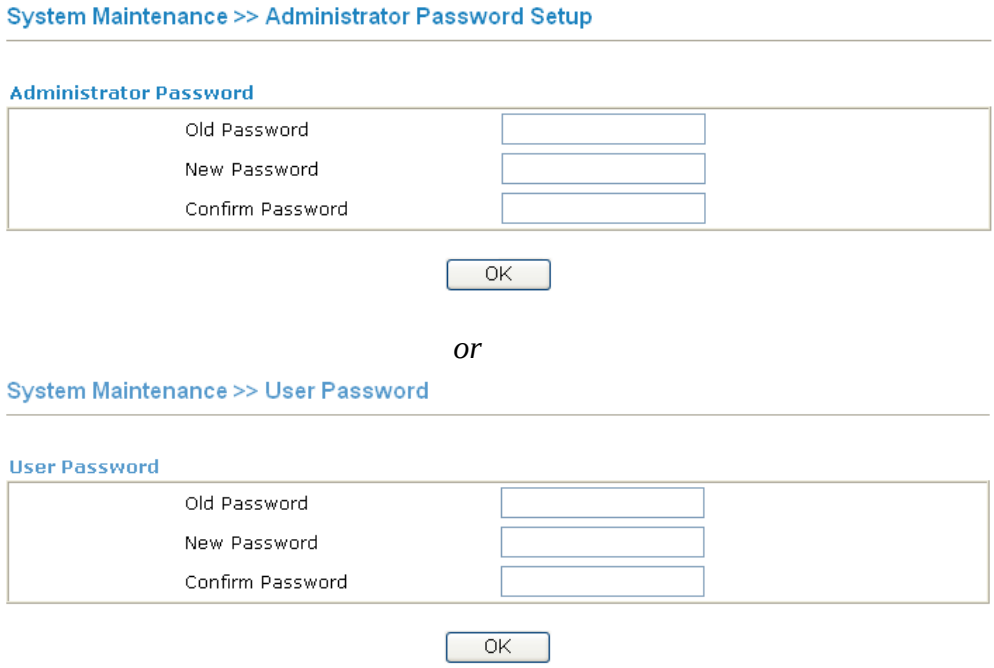
Main screen for admin mode operation (full configuration)



Main screen for user mode operation (simple configuration)

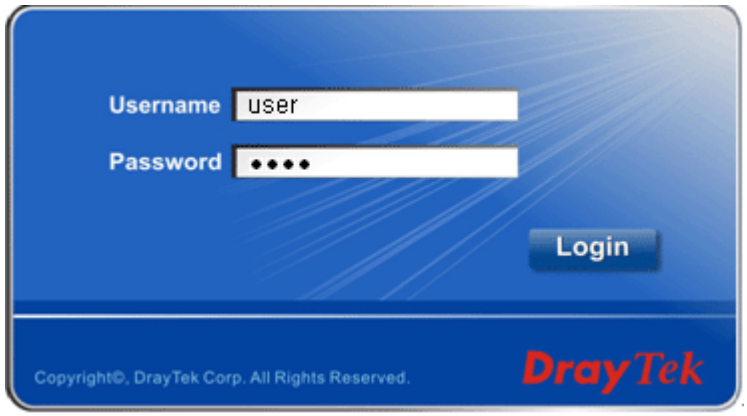
Note: The home page will change slightly in accordance with the type of the router you have.

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



5. Enter the login password (the default is blank) on the field of **Old Password**. Type **New Password**. Then click **OK** to continue.

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



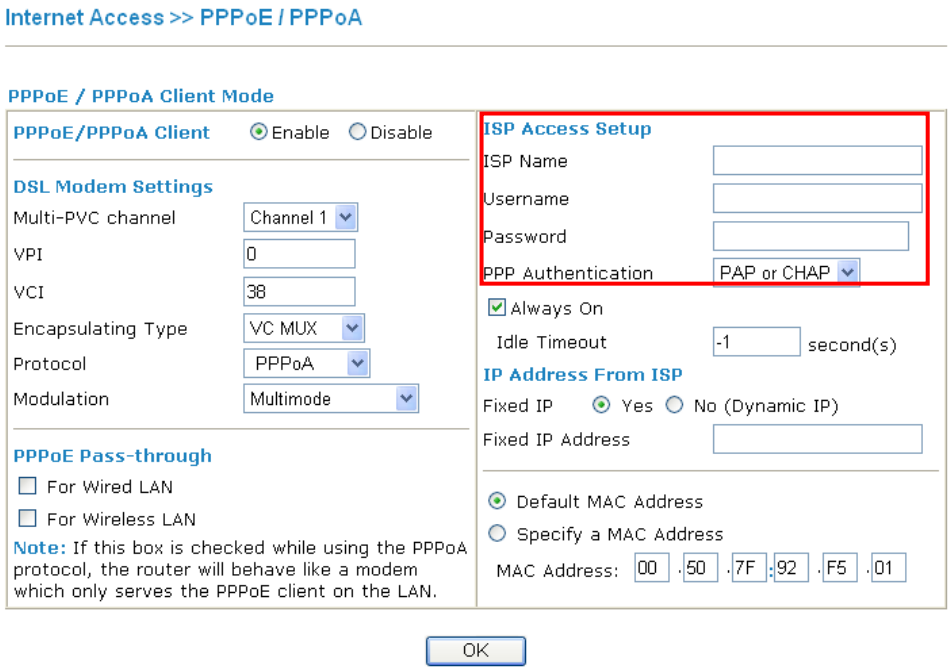
2.4 Configuring Router for Internet Connectivity

Open **Internet Access** page and then check whether the ISP settings are set correctly. Click PPPoE/PPPoA/MPoA/Multip-PVCs link to review the settings that you configured previously.

Note: The web page for **Internet Access** will change according to the mode (user/admin) operation you choose.

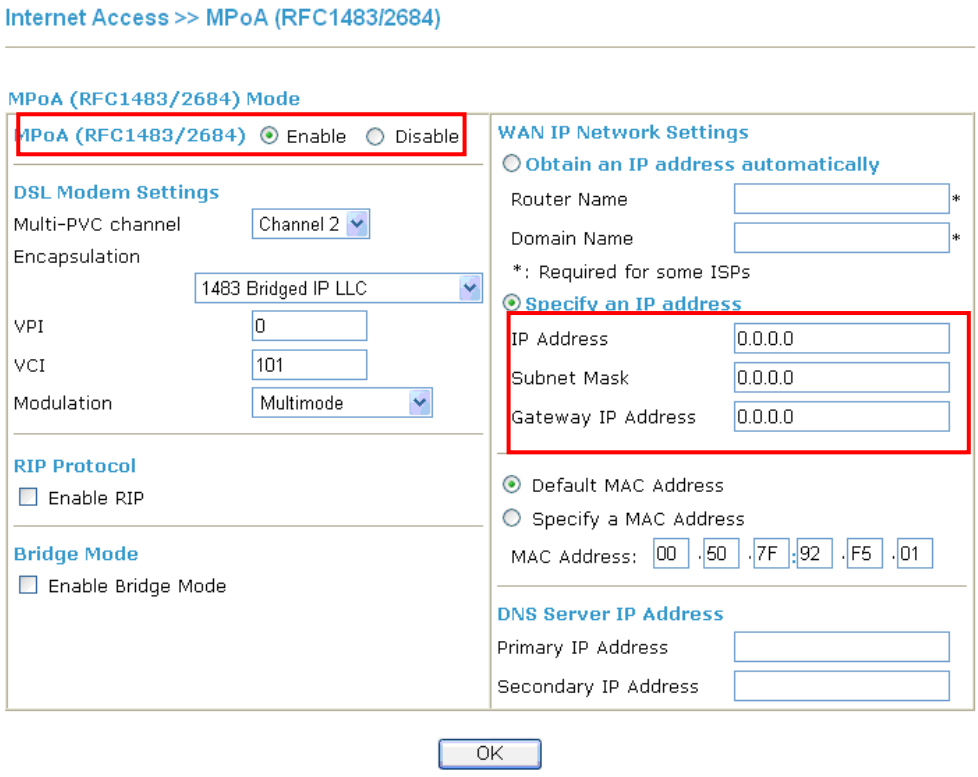
For PPPoE/PPPoA Users

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 is selected.



2. Check if **DSL Modem Settings** is set appropriately.
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**.

2.5 Online Status

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

Online status for PPPoE

Online Status

System Status — System Uptime: 0:1:58

Primary	Secondary

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

IP Address	TX Packets	RX Packets
192.168.1.5	404	391

WAN 1 Status — >> Drop PPPoE

Enable	Line	Name	Mode	Up Time	
Yes	ADSL		PPPoE	0:01:29	
IP	**GW IP**	**TX Packets**	**TX Rate(Bps)**	**RX Packets**	**RX Rate(Bps)**
61.230.203.119	61.230.192.254	38	15	39	40

ADSL Information (ADSL Firmware Version: 211801_A)

ATM Statistics	TX Blocks	RX Blocks	Corrected Blocks	Uncorrected Blocks
	63	353	6	1

ADSL Status	Mode	State	Up Speed	Down Speed	SNR Margin	Loop Att.
	G.DMT	SHOWTIME	256000	2048000	23	31

Online status for Static IP

Online Status

System Status — System Uptime: 0:1:16

Primary	Secondary

LAN Status — Primary DNS: 194.109.6.66 — Secondary DNS: 168.95.1.1

IP Address	TX Packets	RX Packets
192.168.1.5	585	500

WAN 1 Status

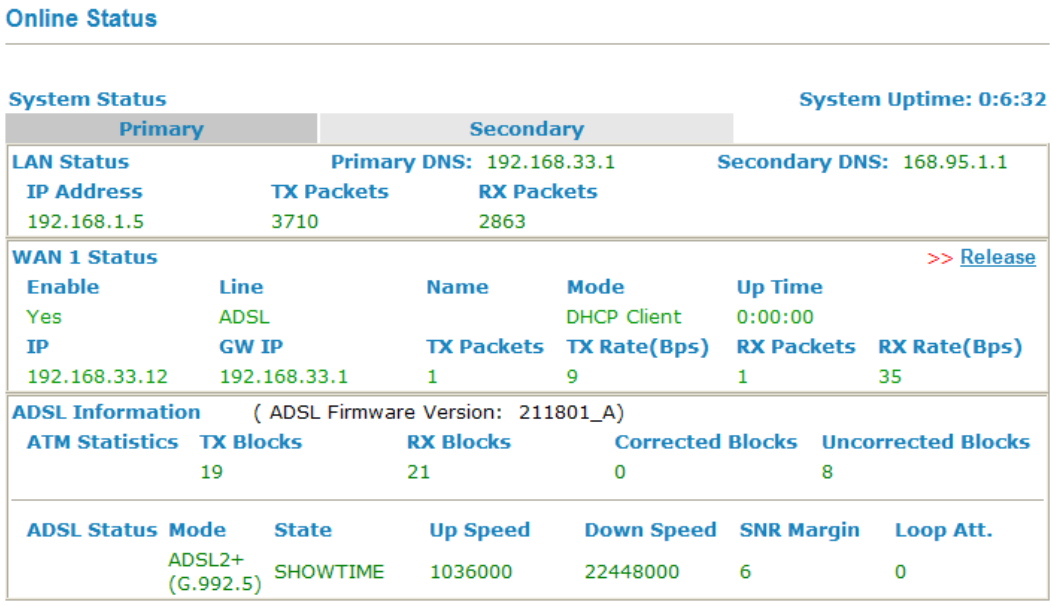
Enable	Line	Name	Mode	Up Time	
Yes	ADSL		Static IP	0:00:28	
IP	**GW IP**	**TX Packets**	**TX Rate(Bps)**	**RX Packets**	**RX Rate(Bps)**
192.168.33.12	192.168.33.1	2	4	1	9

ADSL Information (ADSL Firmware Version: 211801_A)

ATM Statistics	TX Blocks	RX Blocks	Corrected Blocks	Uncorrected Blocks
	6	9	0	18

ADSL Status	Mode	State	Up Speed	Down Speed	SNR Margin	Loop Att.
	ADSL2+ (G.992.5)	SHOWTIME	1026000	22215000	6	0

Online status for DHCP



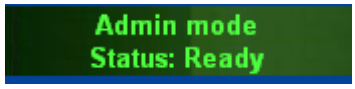
Detailed explanation is shown below:

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

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

2.6 Saving Configuration

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



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

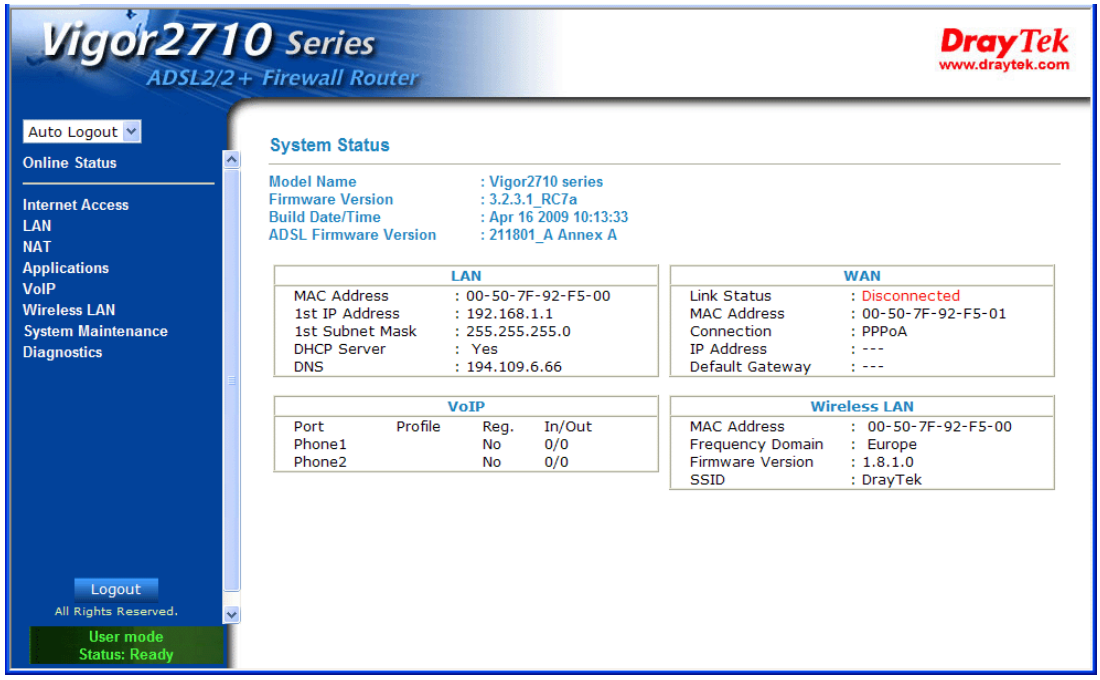
Settings Saved means your settings are saved once you click **Finish** or **OK** button.

3 User Mode Operation

This chapter will guide users to execute simple configuration through user mode operation. As for other examples of application, please refer to chapter 5.

1. Open a web browser on your PC and type **http://192.168.1.1.** The window will ask for typing username and password.
2. **Do not** type any word (both username and password are Null for user operation) on the window and click **Login** on the window.

Now, the **Main Screen** will appear. Be aware that "User mode" will be displayed on the bottom left side.



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 the host PCs can share a common Internet connection.

Get Your Public IP Address from ISP

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

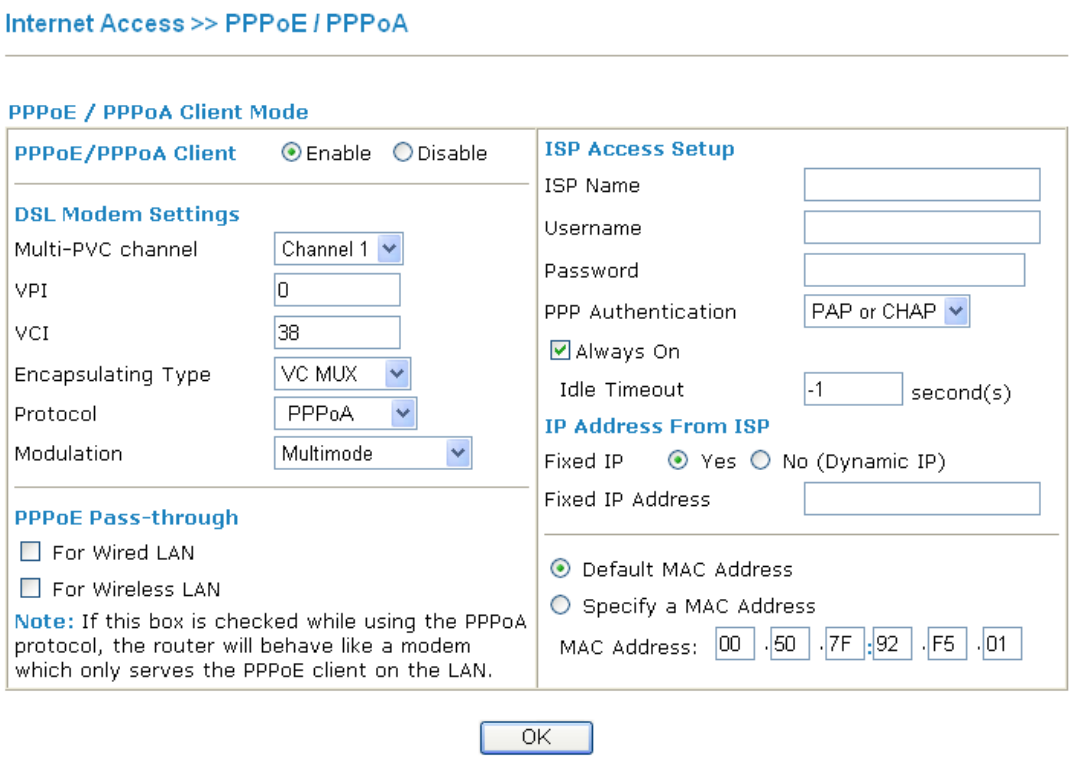
When a router begins to connect to your ISP, a serial of discovery process will occur to ask for a connection. Then a session will be created. Your user ID and password is authenticated via **PAP** or **CHAP** with **RADIUS** authentication system. And your IP address, DNS server, and other related information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

Below shows the menu items for Internet Access.

3.1.2 PPPoE/PPPoA

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

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.



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

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

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. When PPPoA protocol is selected, the PPPoE package transmitted by PC will be transformed into PPPoA package and sent to WAN server. Thus, the PC can access Internet through such direction.
For Wired LAN – If you check this box, PCs on the same network can use another set of PPPoE session (different with the Host PC) to access into Internet.
For Wireless LAN – If you check this box, PCs on the same wireless network can use another set of PPPoE session (different with the Host PC) to access into Internet.

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

Username – Type in the username provided by ISP in this field.
Password – Type in the password provided by ISP in this field.
PPP Authentication – Select **PAP only** or **PAP or CHAP** for PPP.
Idle Timeout – Set the timeout for breaking down the Internet after passing through the time without any action. This setting is active only when the **Active on demand** option for Active Mode is selected in **WAN>> General Setup** page.

IP Address From ISP

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

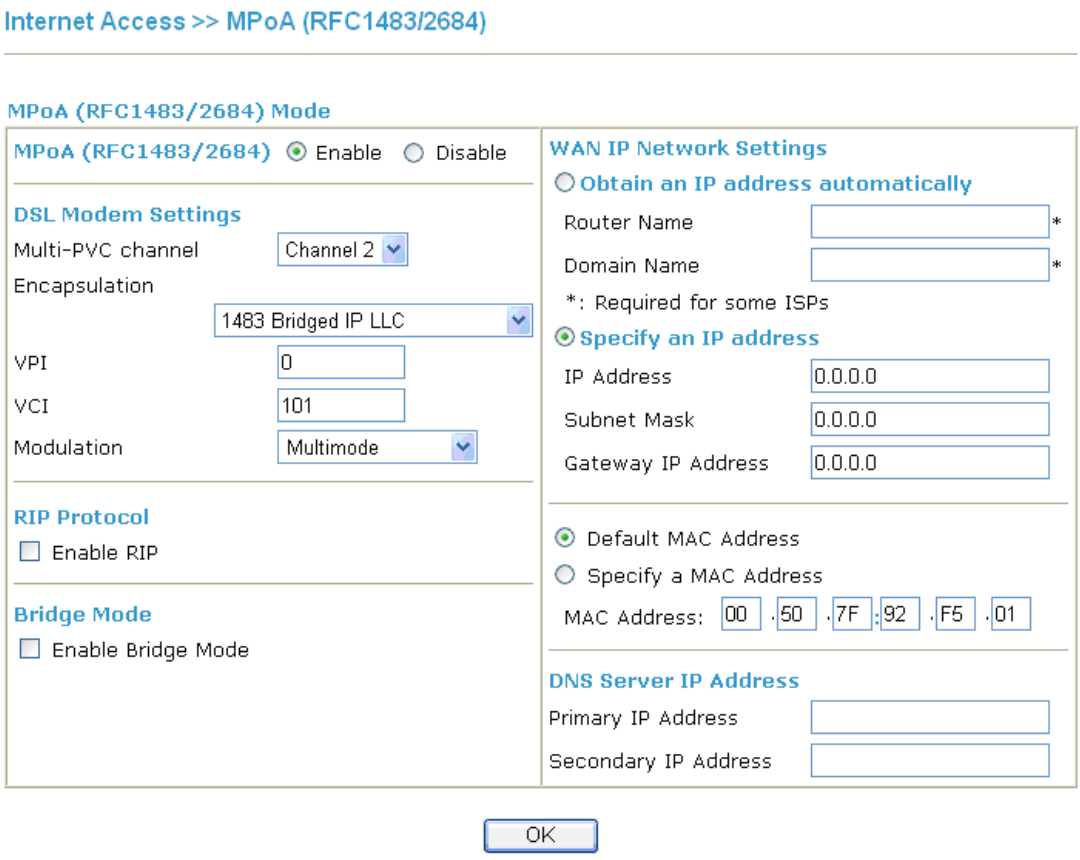
Fixed IP – Click **Yes** to use this function and type in a fixed IP address in the box of **Fixed IP Address**.
Default MAC Address – You can use **Default MAC Address** or specify another MAC address by typing on the boxes of MAC Address for the router.
Specify a MAC Address – Type the MAC address for the router manually.

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

3.1.3 MPoA

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

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



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.
Specify an IP address – Click this radio button to specify some data.
IP Address – Type in the private IP address.

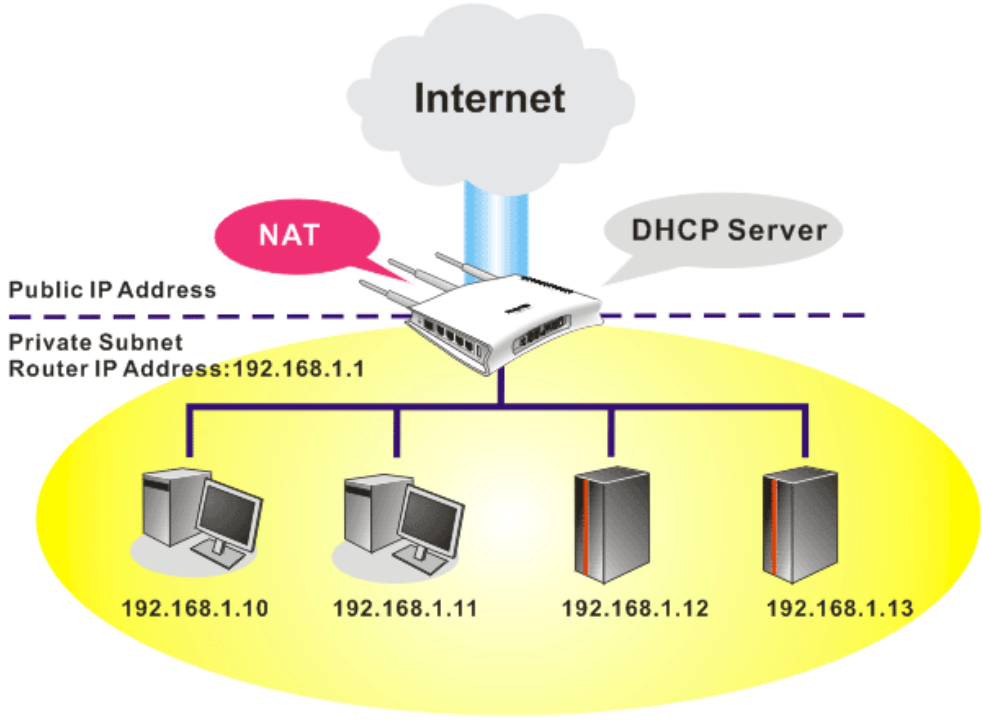
	Subnet Mask – Type in the subnet mask. **Gateway IP Address** – Type in gateway IP address. **Default MAC Address** Type in MAC address for the router. You can use **Default MAC Address** or specify another MAC address for your necessity. **MAC Address** – Type in the MAC address for the router manually.
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.

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

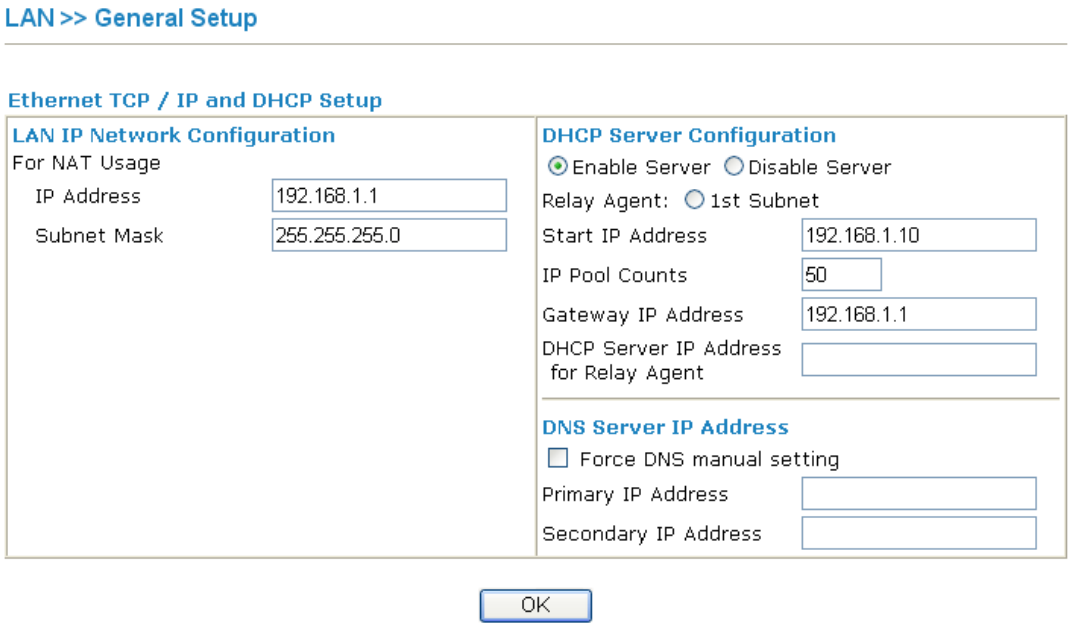
The most generic function of Vigor router is NAT. It creates a private subnet of your own. As mentioned previously, the router will talk to other public hosts on the Internet by using public IP address and talking to local hosts by using its private IP address. What NAT does is to translate the packets 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.



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**.



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

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

DHCP Server Configuration — DHCP stands for Dynamic Host Configuration Protocol. The router by factory default acts a DHCP server for your network so it automatically dispatch related IP settings to any local user configured as a DHCP client. It is highly recommended that you leave the router enabled as a DHCP server if you do not have a DHCP server for your network.

If you want to use another DHCP server in the network other than the Vigor Router's, you can let Relay Agent help you to redirect the DHCP request to the specified location.
Enable Server - Let the router assign IP address to every host in the LAN.
Disable Server – Let you manually assign IP address to every host in the LAN.
Relay Agent – (1st subnet) Specify the subnet that DHCP server is located the relay agent should redirect the DHCP request to.
Start IP Address - Enter a value of the IP address pool for the DHCP server to start with when issuing IP addresses. If the 1st IP address of your router is 192.168.1.1, the starting IP address must be 192.168.1.2 or greater, but smaller than 192.168.1.254.
IP Pool Counts - Enter the maximum number of PCs that you want the DHCP server to assign IP addresses to. The default is 50 and the maximum is 253.
Gateway IP Address - Enter a value of the gateway IP address for the DHCP server. The value is usually as same as the 1st IP address

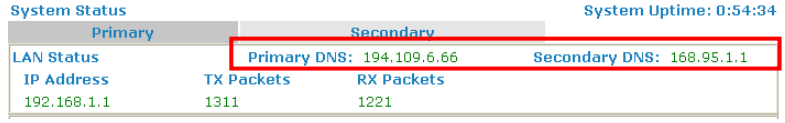
of the router, which means the router is the default gateway.
DHCP Server IP Address for Relay Agent - Set the IP address of the DHCP server you are going to use so the Relay Agent can help to forward the DHCP request to the DHCP server.

DNS Server Configuration

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

Force DNS manual setting - Force Vigor router to use DNS servers in this page instead of DNS servers given by the Internet Access server (PPPoE, PPTP, L2TP or DHCP server).
Primary IP Address -You must specify a DNS server IP address here because your ISP should provide you with usually more than one DNS Server. If your ISP does not provide it, the router will automatically apply default DNS Server IP address: 194.109.6.66 to this field.
Secondary IP Address - You can specify secondary DNS server IP address here because your ISP often provides you more than one DNS Server. If your ISP does not provide it, the router will automatically apply default secondary DNS Server IP address: 194.98.0.1 to this field.

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



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.

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:

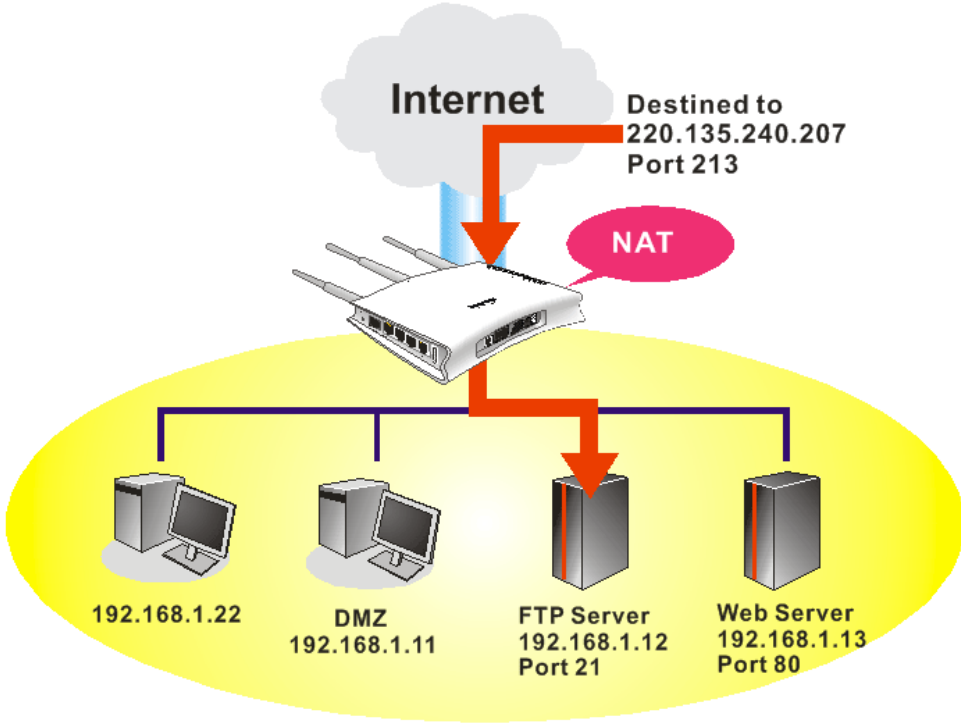
- **Save cost on applying public IP address and apply efficient usage of IP address.** NAT allows the internal IP addresses of local hosts to be translated into one public IP address, thus you can have only one IP address on behalf of the entire internal hosts.
- **Enhance security of the internal network 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.

Below shows the menu items for NAT.

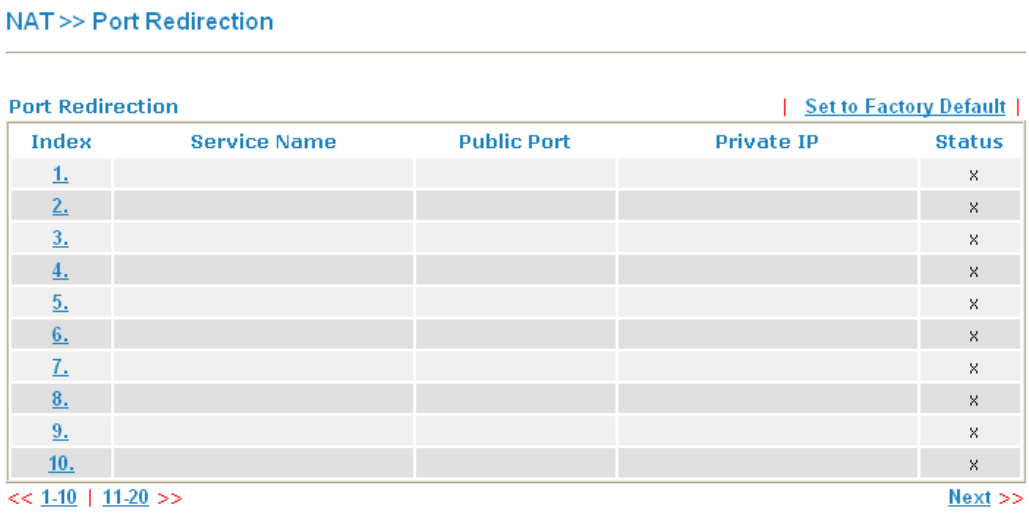
3.3.1 Port Redirection

Port Redirection is usually set up for server related service inside the local network (LAN), such as web servers, FTP servers, E-mail servers etc. Most of the case, you need a public IP address for each server and this public IP address/domain name are recognized by all users. Since the server is actually located inside the LAN, the network well protected by NAT of the router, and identified by its private IP address/port, the goal of Port Redirection function is to forward all access request with public IP address from external users to the mapping private IP address/port of the server.

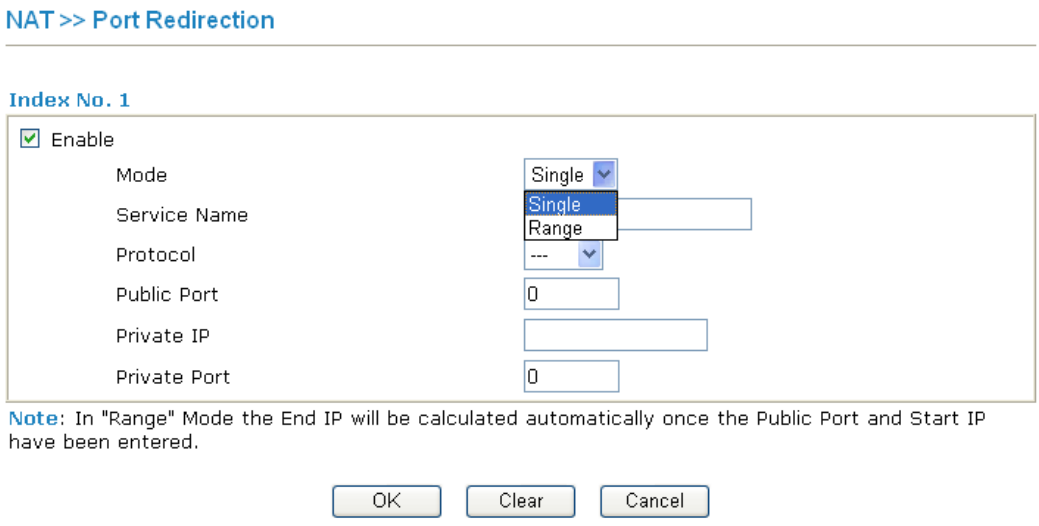


The port redirection can only apply to incoming traffic.

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



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



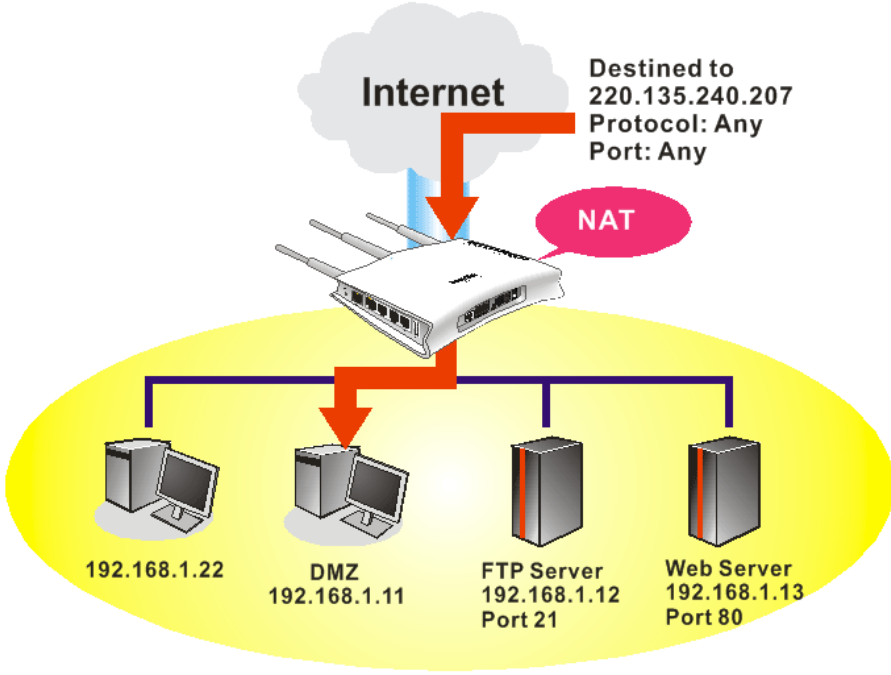
Enable	Check this box to enable such port redirection setting.
Mode	Two options (Single and Range) are provided here for you to choose. To set a range for the specific service, select **Range**. In Range mode, if the public port (start port and end port) and the starting IP of private IP had been entered,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

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

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

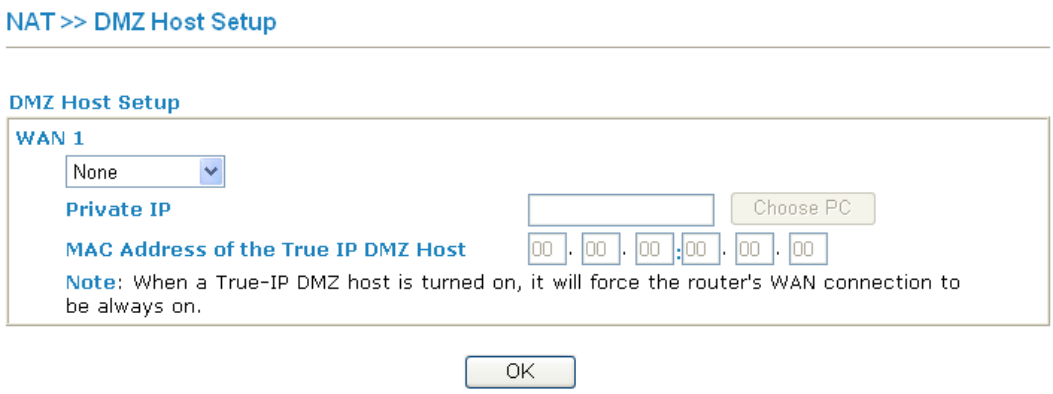
3.3.2 DMZ Host

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



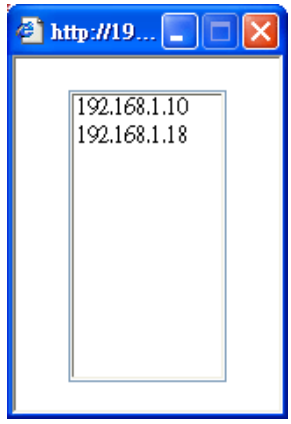
The inherent security properties of NAT are somewhat bypassed if you set up DMZ host. We suggest you to add additional filter rules or a secondary firewall.

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



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.



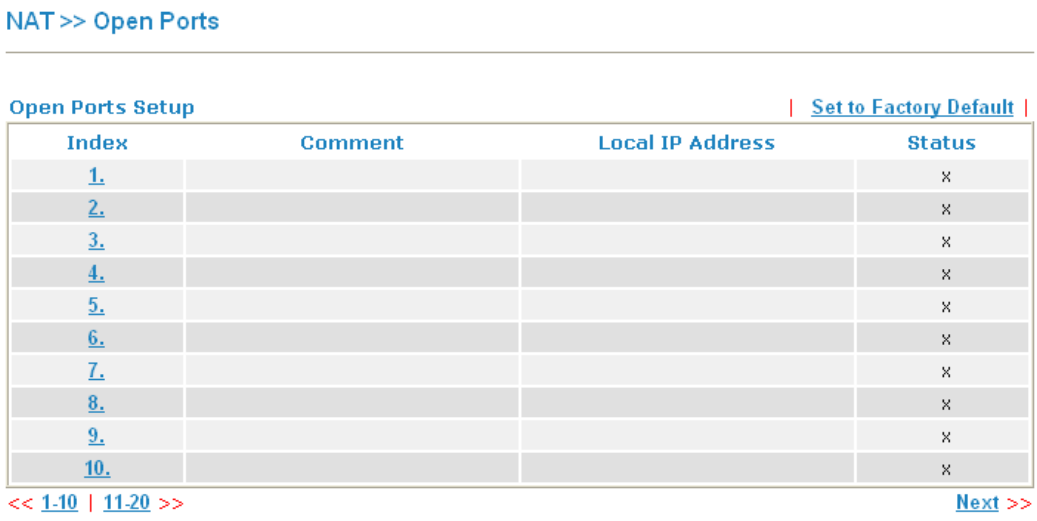
After you have selected one private IP from the above dialog, click **OK** to save the setting.

3.3.3 Open Ports

Open Ports allows you to open a range of ports for the traffic of special applications.

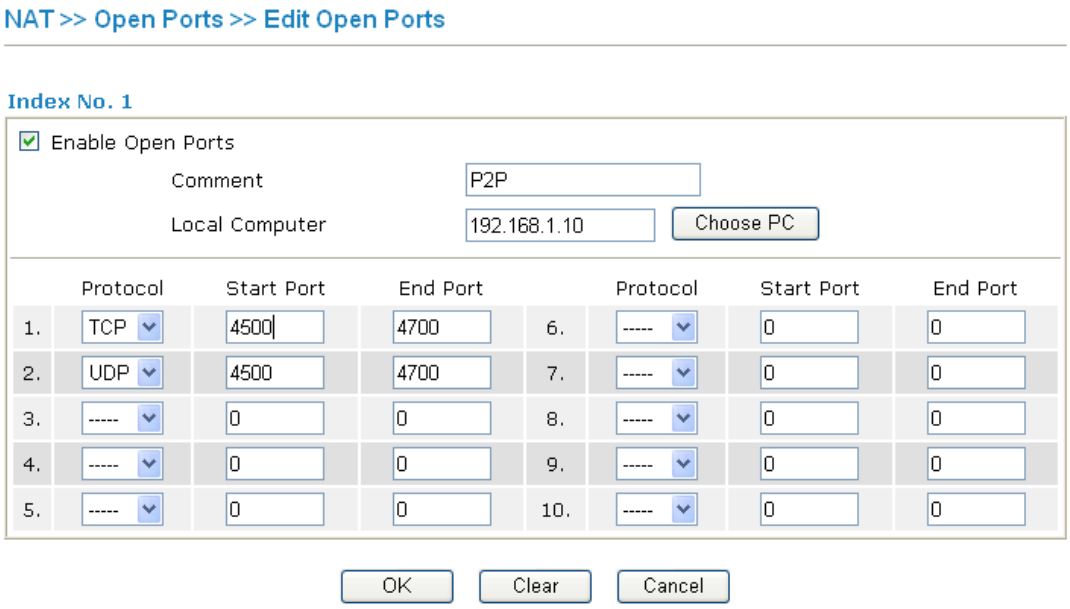
Common application of Open Ports includes P2P application (e.g., BT, KaZaA, Gnutella, WinMX, eMule and others), Internet Camera etc. Ensure that you keep the application involved up-to-date to avoid falling victim to any security exploits.

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.
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.



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.

3.4 Applications

Below shows the menu items for Applications.

3.4.1 Dynamic DNS

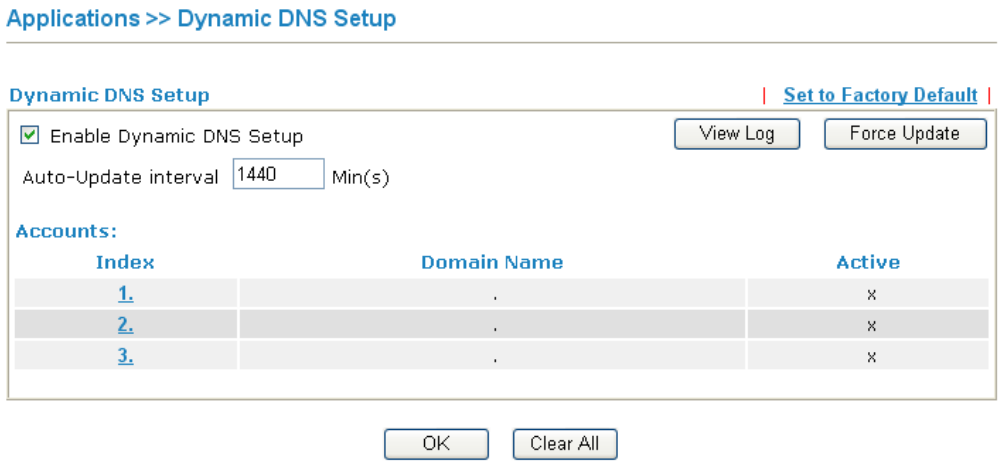
The ISP often provides you with a dynamic IP address when you connect to the Internet via your ISP. It means that the public IP address assigned to your router changes each time you access the Internet. The Dynamic DNS feature lets you assign a domain name to a dynamic WAN IP address. It allows the router 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.

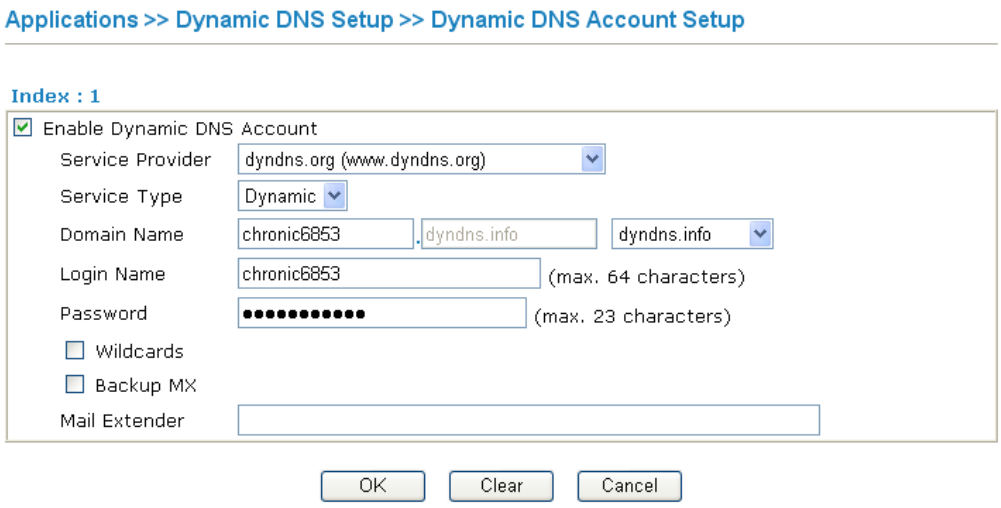
Enable the Function and Add a Dynamic DNS Account

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**.



Set to Factory Default	Clear all profiles and recover to factory settings.
Enable Dynamic DNS Setup	Check this box to enable DDNS function.
Auto-Update interval	Execute auto-update with the interval set here.
Index	Click the number below Index to access into the setting page of DDNS setup to set account(s).
Domain Name	Display the domain name that you set on the setting page of DDNS setup.
Active	Display if this account is active or inactive.
View Log	Display DDNS log status.
Force Update	Force the router updates its information to DDNS server.

3. Select Index number 1 to add an account for the router. Check **Enable Dynamic DNS Account**, and choose correct Service Provider: dyndns.org, type the registered hostname: *hostname* and domain name suffix: dyndns.org in the **Domain Name** block.



Enable Dynamic DNS Account	Check this box to enable the current account. If you did check the box, you will see a check mark appeared on the Active column of the previous web page in step 2).
WAN Interface	Select the WAN interface order to apply settings here.
Service Provider	Select the service provider for the DDNS account.
Service Type	Select a service type (Dynamic, Custom or Static). If you choose Custom, you can modify the domain that is chosen in the Domain Name field.
Domain Name	Type in one domain name that you applied previously. Use the drop down list to choose the desired domain.
Login Name	Type in the login name that you set for applying domain.
Password	Type in the password that you set for applying domain.

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

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

Disable the Function and Clear all Dynamic DNS Accounts

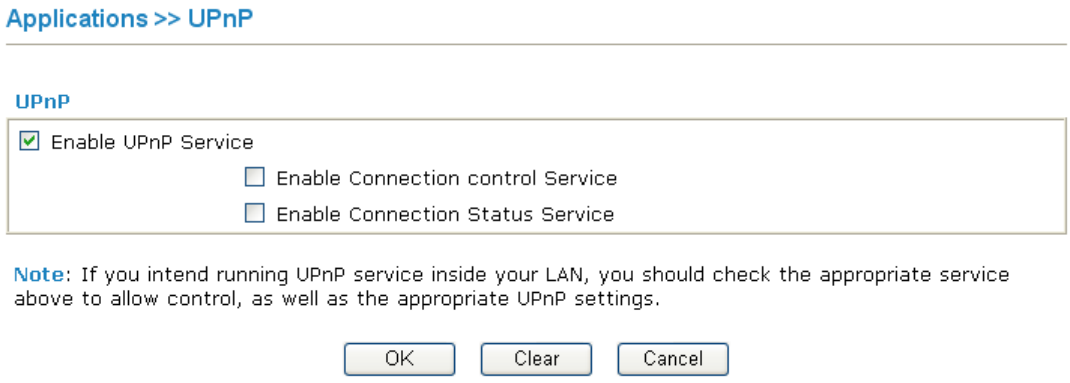
In the DDNS setup menu, uncheck **Enable Dynamic DNS Setup**, and push **Clear All** button to disable the function and clear all accounts from the router.

Delete a Dynamic DNS Account

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

3.4.2 UPnP

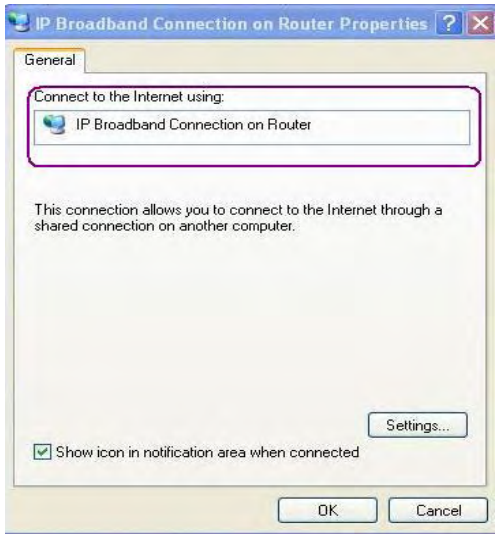
The **UPnP** (Universal Plug and Play) protocol is supported to bring to network connected devices the ease of installation and configuration which is already available for directly connected PC peripherals with the existing Windows 'Plug and Play' system. For NAT routers, the major feature of UPnP on 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 provide the associated support for MSN Messenger to allow full use of the voice, video and messaging features.

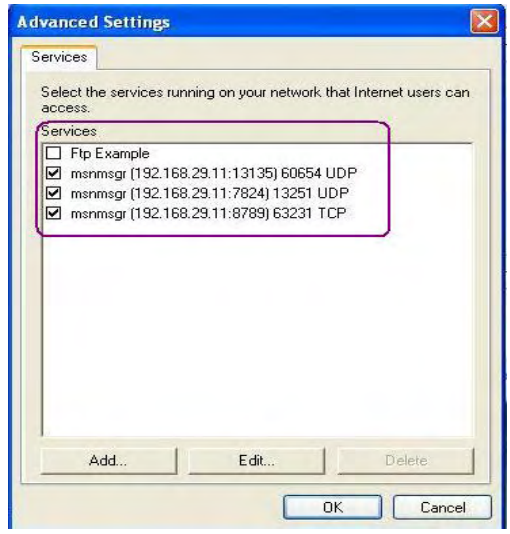


Enable UPNP Service Accordingly, you can enable either the **Connection Control Service** or **Connection Status Service**.

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 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/ISDN network.

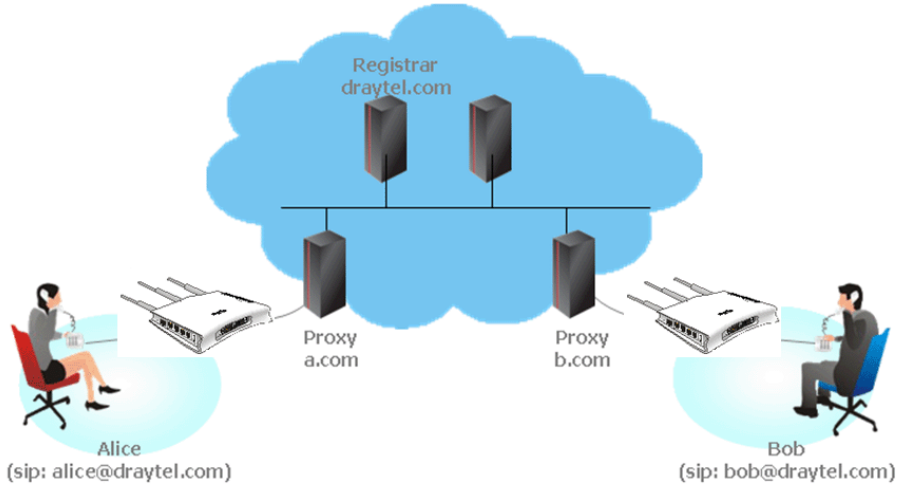
After a call is setup, the voice streams transmit via RTP (Real-Time Transport Protocol). Different codecs (methods to compress and encode the voice) can be embedded into RTP packets. Vigor V models provide various codecs, including G.711 A/μ-law, G.723, G.726 and G.729 A & B. Each codec uses a different 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:



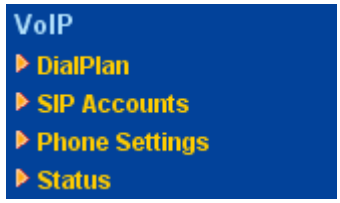
  The major benefit of this mode is that you don't have to memorize your friend's IP address, which might change very frequently if it's dynamic. Instead of that, you will only have to using **dial plan** or directly dial your friend's **account name** if you are with the same SIP Registrar.

- **Peer-to-Peer**

  Before calling, you have to know your friend's IP Address. The Vigor VoIP Routers will build connection between each other.

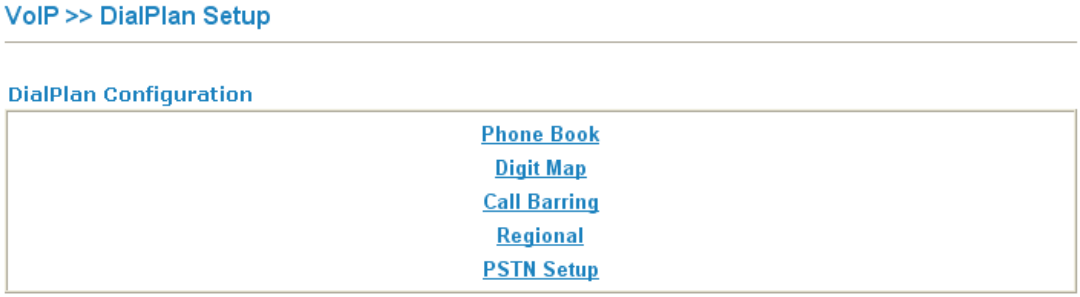
  Our Vigor V models firstly apply efficient codecs designed to make the best use of available bandwidth, but Vigor V models also equip with automatic QoS assurance.

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.



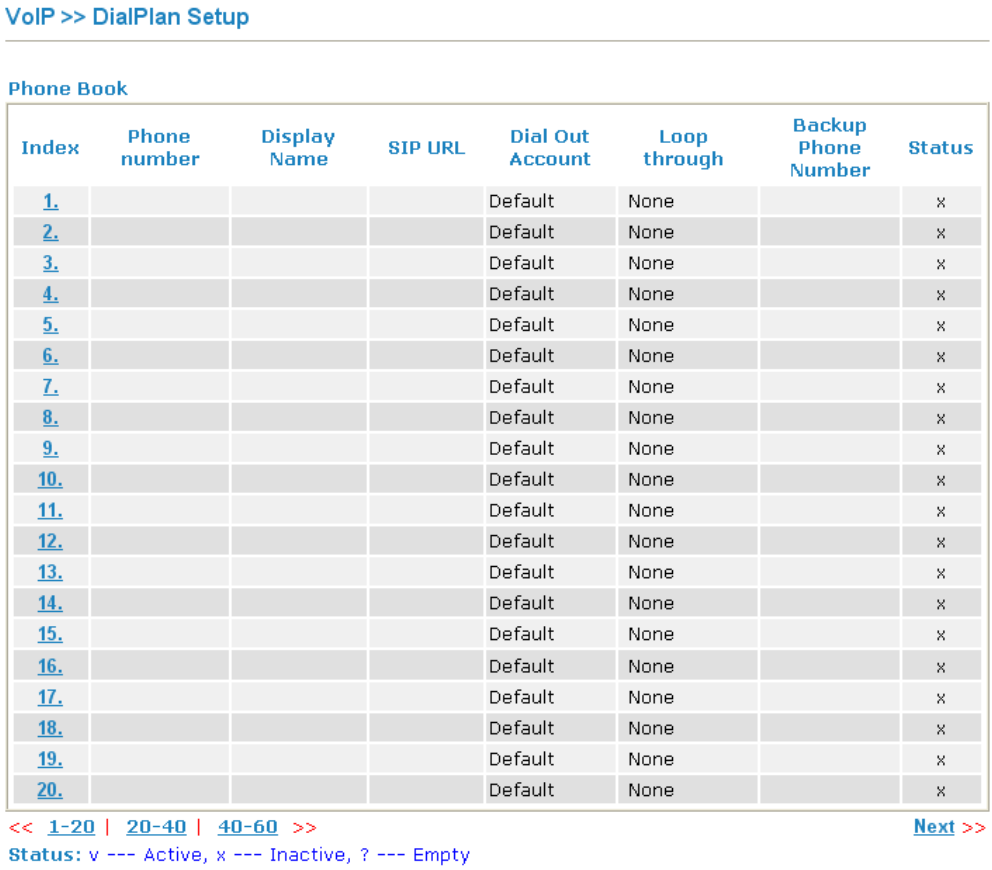
3.5.1 DialPlan

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.

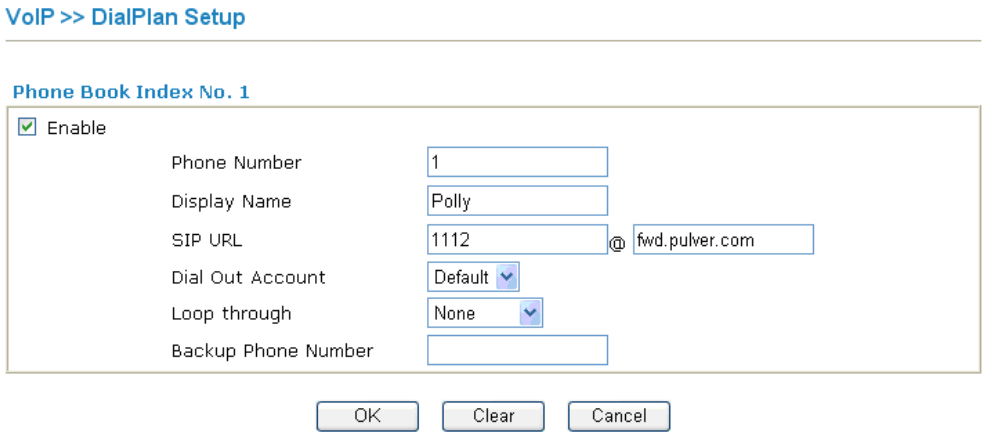


Phone Book

In this section, you can set your VoIP contacts in the “phonebook”. It can help you to make calls quickly and easily by using “speed-dial” **Phone Number**. There are total 60 index entries in the phonebook for you to store all your friends and family members’ SIP addresses. **Loop through** and **Backup Phone Number** will be displayed if you are using Vigor 2710Vn for setting the phone book.



Click any index number to display the dial plan setup page.

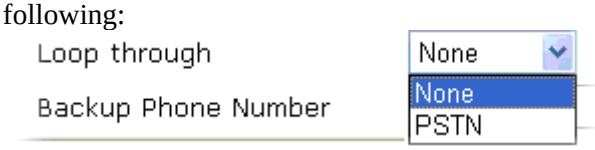


Enable	Click this to enable this entry.
Phone Number	The speed-dial number of this index. This can be any number you choose, using digits **0-9** and ***** .
Display Name	The Caller-ID that you want to be displayed on your friend's screen. This let your friend can easily know who's calling without memorizing lots of SIP URL Address.
SIP URL	Enter your friend's SIP Address.
Dial Out Account	Choose one of the SIP accounts for this profile to dial out. It is useful for both sides (caller and callee) that registered to different SIP Registrar servers. If caller and callee do not use

the same SIP server, sometimes, the VoIP phone call connection may not succeed. By using the specified dial out account, the successful connection can be assured.

Loop through

For the model of Vigor 2710Vn, the selection should be as the following:

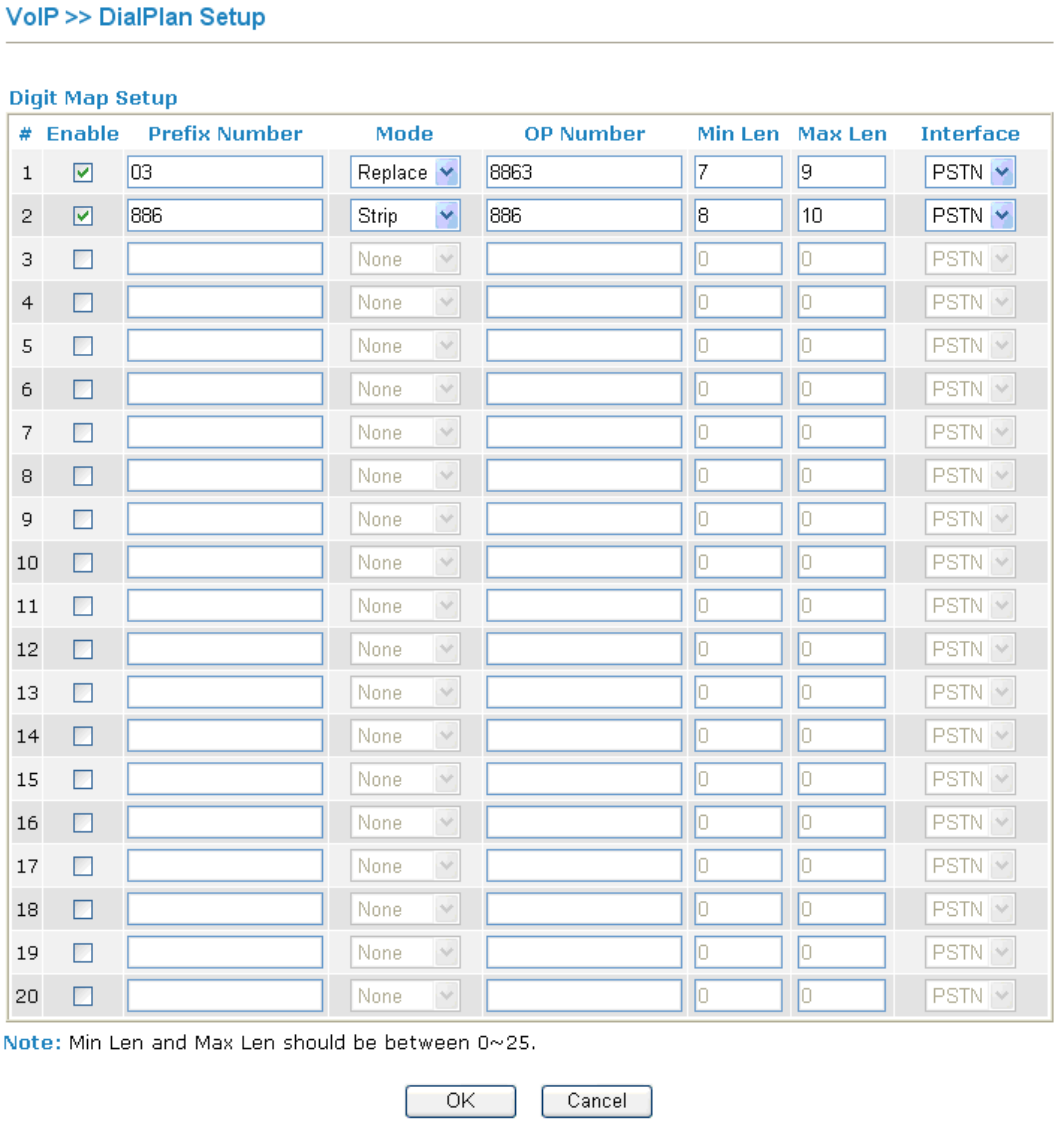


Backup Phone Number

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 prefix number of 03 will be replaced by 8863. For example: dial number of “031111111” will be changed to “88631111111” and sent to SIP server.

Mode

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.

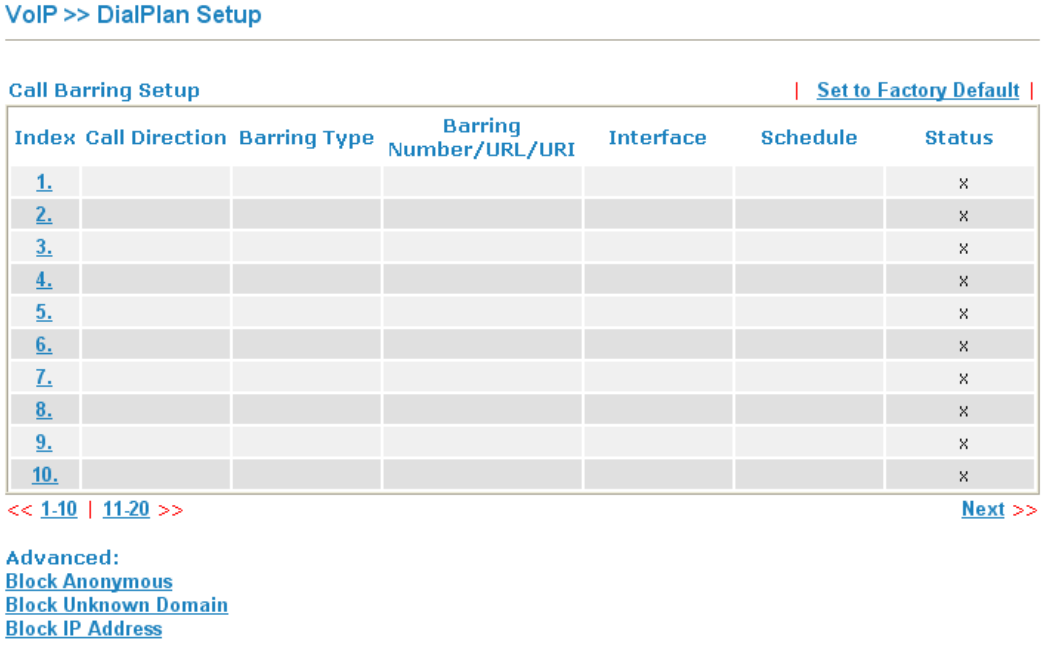
Min Len Set the minimal length of the dial number for applying the prefix number settings. Take the above picture (Prefix Table Setup web page) as an example, if the dial number is between 7 and 9, that number can apply the prefix number settings here.

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

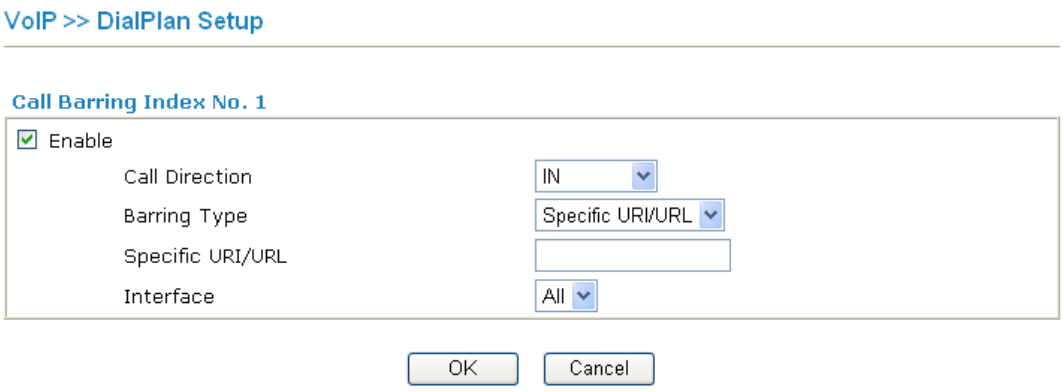
Interface Choose the one that you want to enable the prefix number settings from the saved SIP accounts. Please set up one SIP account first to make this interface available.

Call Barring

Call barring is used to block phone calls coming from the one that is not welcomed.

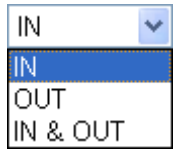


Click any index number to display the dial plan setup page.

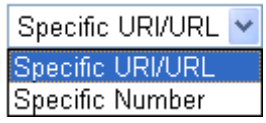


Enable Click this to enable this entry.

Call Direction Determine the direction for the phone call, IN – incoming call, OUT-outgoing call, IN & OUT – both incoming and outgoing calls.



Barring Type Determine the type of the VoIP phone call, URI/URL or number.

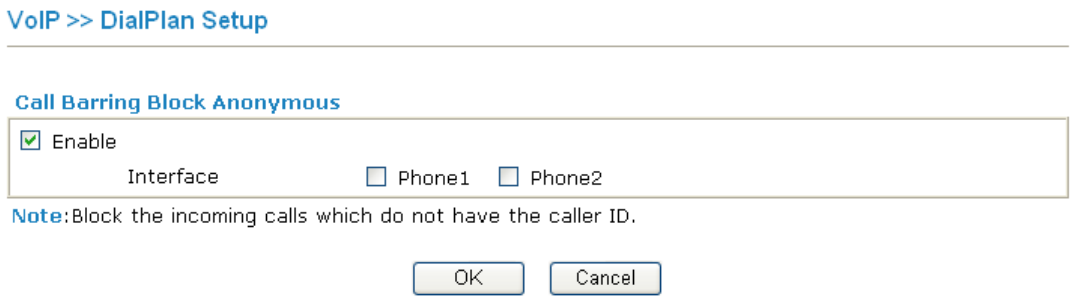


Specific URI/URL or Specific Number This field will be changed based on the type you selected for barring Type.

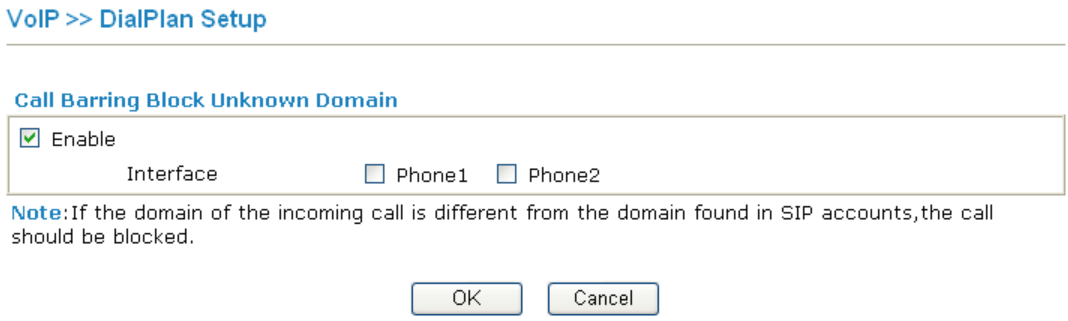
Interface **All** means all the phone calls will be blocked with such mechanism.

Additionally, you can set advanced settings for call barring such as **Block Anonymous**, **Block Unknown Domain** or **Block IP Address**. Simply click the relational links to open the web page.

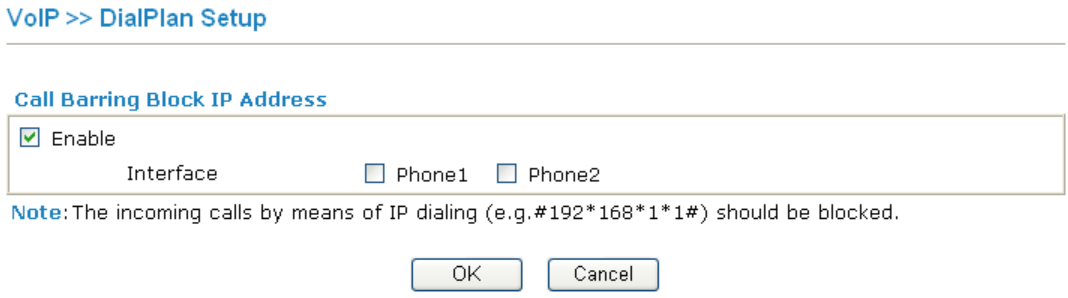
For **Block Anonymous –** this function can block the incoming calls without caller ID on the interface (Phone port) specified in the following window. Such control also can be done based on preconfigured schedules.



For **Block Unknown Domain –** this function can block incoming calls (through Phone port) from unrecognized domain that is not specified in SIP accounts. Such control also can be done based on preconfigured schedules.

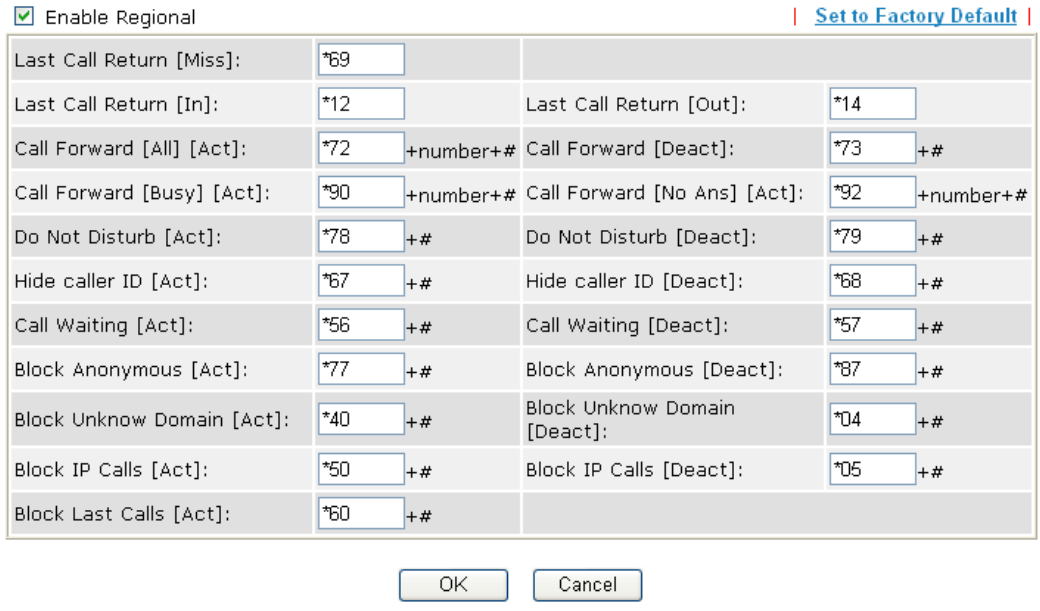


For **Block IP Address –** this function can block incoming calls (through Phone port) coming from IP address. Such control also can be done based on preconfigured schedules.



Regional

This page allows you to process incoming or outgoing phone calls by regional. Default values (common used in most areas) will be shown on this web page. You ***can change*** the number based on the region that the router is placed.

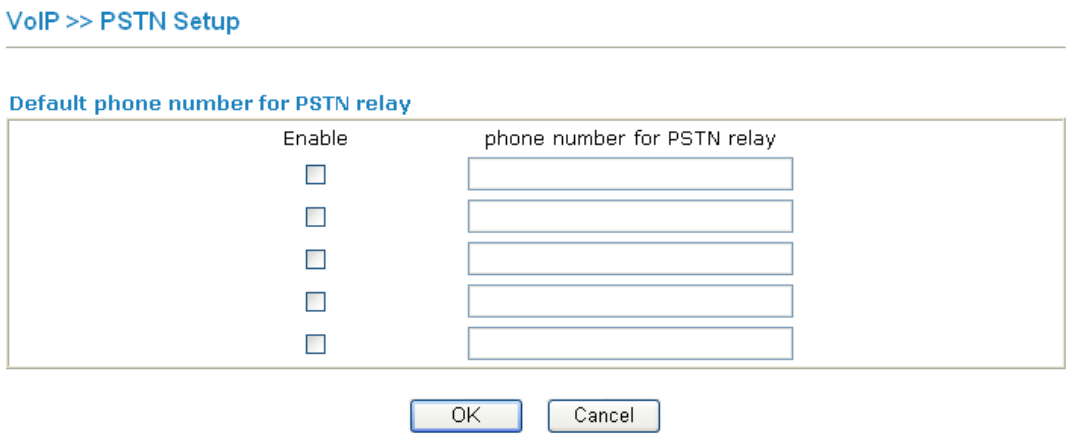


Last Call Return [Miss]	Sometimes, people might miss some phone calls. Please dial number typed in this field to know where the last phone call comes from and call back to that one.
Last Call Return [In]	You have finished an incoming phone call, however you want to call back again for some reason. Please dial number typed in this field to call back to that one.
Last Call Return [Out]	Dial the number typed in this field to call the previous outgoing phone call again.
Call Forward [All][Act]	Dial the number typed in this field to forward all the incoming calls to the specified place.
Call Forward [Deact]	Dial the number typed in this field to release the call forward function.
Call Forward [Busy][Act]	Dial the number typed in this field to forward all the incoming calls to the specified place while the phone is busy.
Call Forward [No Ans][Act]	Dial the number typed in this field to forward all the incoming calls to the specified place while there is no answer of the connected phone.
Do Not Disturb [Act]	Dial the number typed in this field to invoke the function of DND.
Do Not Distrub [Deact]	Dial the number typed in this field to release the DND function.
Hide caller ID [Act]	Dial the number typed in this field to make your phone number (ID) not displayed on the display panel of remote end.
Hide caller ID [Deact]	Dial the number typed in this field to release this function.
Call Waiting [Act]	Dial the number typed in this field to make all the incoming calls waiting for your answer.
Call Waiting [Deact]	Dial the number typed in this field to release this function.
Block Anonymous[Act]	Dial the number typed in this field to block all the incoming calls with unknown ID.
Block Anonymous[Deact]	Dial the number typed in this field to release this function.
Block Unknown Domain [Act]	Dial the number typed in this field to block all the incoming calls from unknown domain.
Block Unknown Domain [Deact]	Dial the number typed in this field to release this function.
Block IP Calls [Act]	Dial the number typed in this filed to block all the incoming calls from IP address.
Block IP Calls [Deact]	Dial the number typed in this field to release this function.

Block Last Calls [Act] Dial the number typed in this field to block the last incoming phone call.

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**.

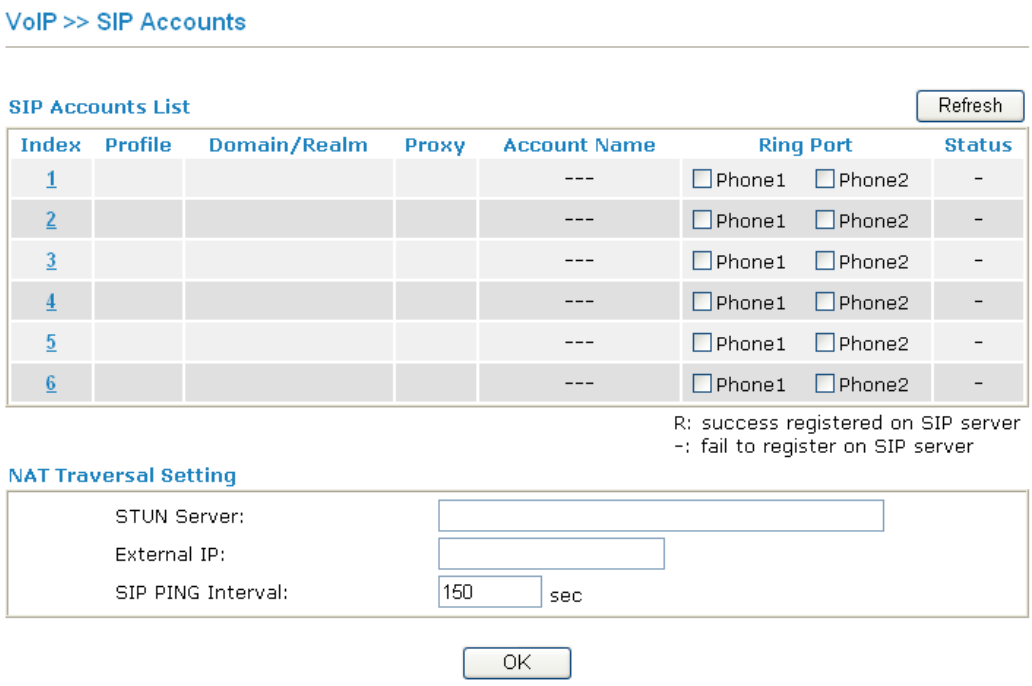


Then, check the **Enable** box to make the PSTN number available for dial whenever you need.

3.5.2 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. Set Phone1 or Phone 2 as the default ring port for the SIP account.
STUN Server	Type in the IP address or domain of the STUN server.
External IP	Type in the gateway IP address.
SIP PING interval	The default value is 150 (sec). 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.

VoIP >> SIP Accounts

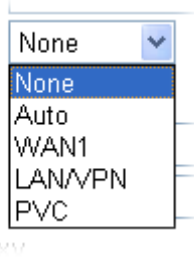
SIP Account Index No. 1

Profile Name		(11 char max.)
Register via	None	Call without Registration
SIP Port	5060	
Domain/Realm		(63 char max.)
Proxy		(63 char max.)
Act as outbound proxy		
Display Name		(23 char max.)
Account Number/Name	---	(63 char max.)
Authentication ID		(63 char max.)
Password		(63 char max.)
Expiry Time	1 hour	3600 sec
NAT Traversal Support	None	
Ring Port	Phone 1 Phone 2	
Ring Pattern	1	

OK Cancel

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 **Call without registration**. Choosing **Auto** is recommended.



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.

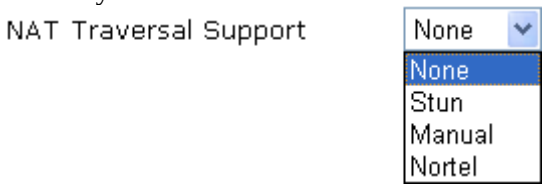
Account Number/Name Enter your account name of SIP Address, e.g. every text before @.

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.



None – Disable this function.
Stun – Choose this option if there is Stun server provided for your router.
Manual – Choose this option if you want to specify an external IP address as the NAT transversal support.
Nortel – If the soft-switch that you use supports Nortel solution, you can choose this option.

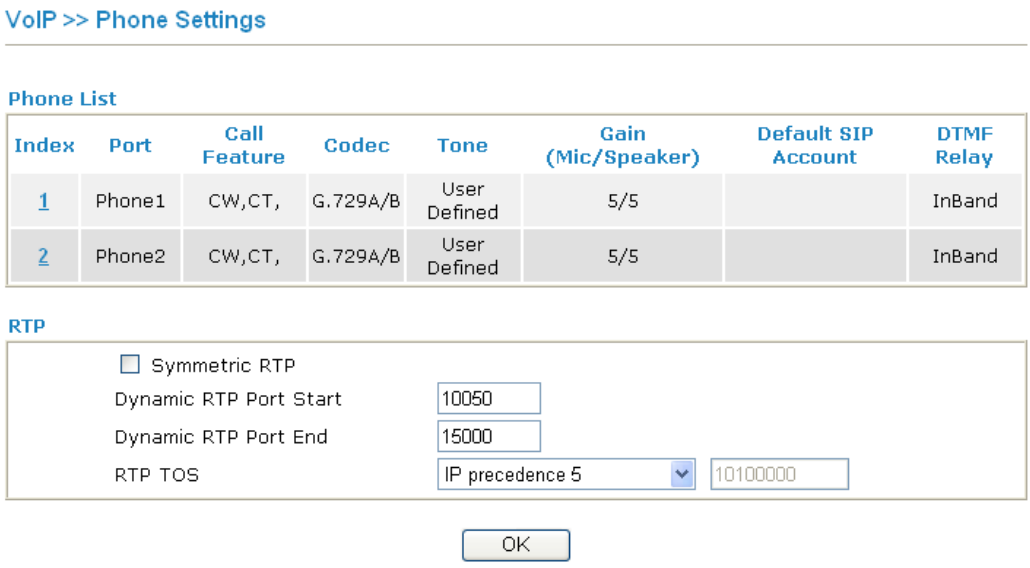
Ring Port — Set Phone1 or Phone2 as the default ring port for this SIP account.

Ring Pattern — Choose a ring tone type for the VoIP phone call.

3.5.3 Phone Settings

This page allows user to set phone settings for Phone 1 and Phone 2 respectively. However, it changes slightly according to different model you have.

For Vigor2710V/Vigor2710Vn models, you will see the following page:



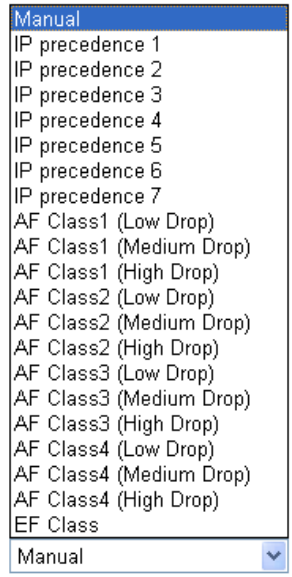
Phone List

Port –there are two phone ports provided here for you to configure.
Phone1/Phone2 allows you to set general settings for PSTN phones.
Call Feature – A brief description for call feature will be shown in this field for your reference.
Codec – The default Codec setting for each port will be shown in this field for your reference. You can click the number below the Index field to change it for each phone port.
Tone - Display the tone settings that configured in the advanced settings page of Phone Index.
Gain - Display the volume gain settings for Mic/Speaker that configured in the advanced settings page of Phone Index.
Default SIP Account – You can click the number below the Index field to choose SIP account for each phone port.
DTMF Relay – Display DTMF mode that configured in the advanced settings page of Phone Index.

RTP

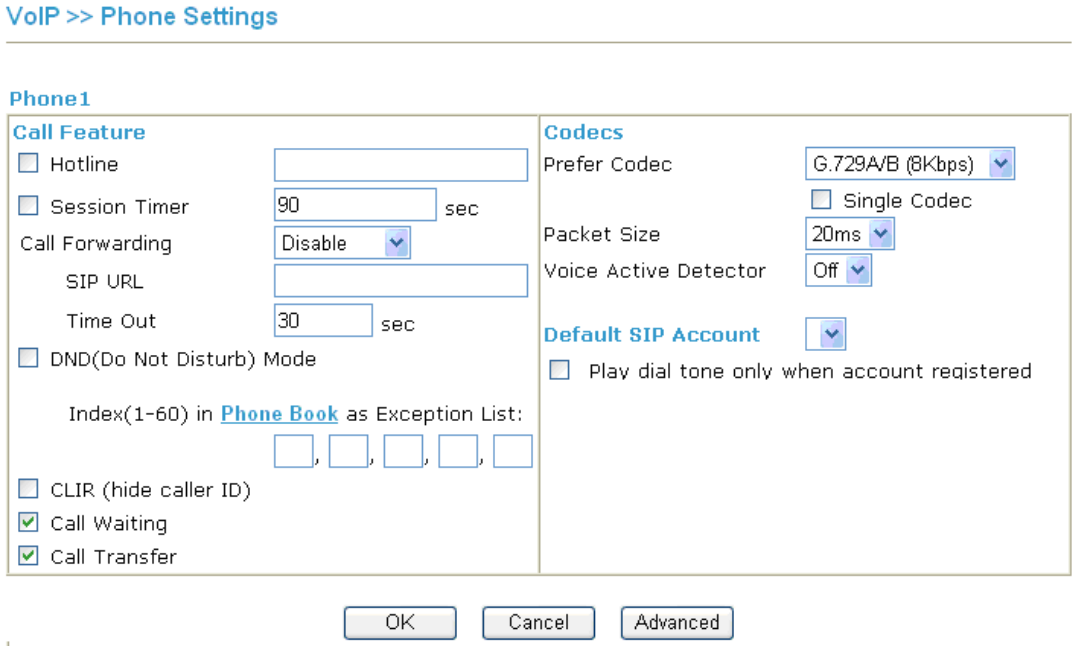
Symmetric RTP – Check this box to invoke the function. To make the data transmission going through on both ends of local router and remote router not misleading due to IP lost (for example, sending data from the public IP of remote router to the private IP of local router), you can check this box to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



Detailed Settings for Phone Port

Click the number link for Phone port, you can access into the following page for configuring Phone settings.

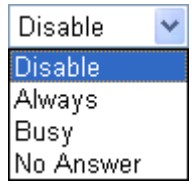


Hotline — Check the box to enable it. Type in the SIP URL in the field for dialing automatically when you pick up the phone set.

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.

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.

Index (1-60) in Phone Book - Enter the index of phone book profiles. Refer to section **DialPlan>>Phone Book** for detailed configuration.

CLIR (hide caller ID)

Check this box to hide the caller ID on the display panel of the phone set.

Call Waiting

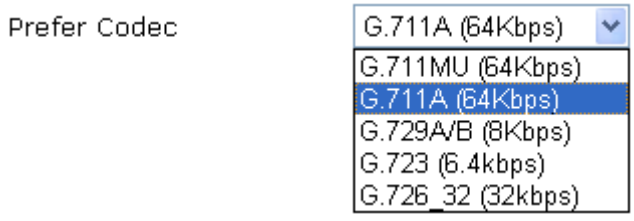
Check this box to invoke this function. A notice sound will appear to tell the user new phone call is waiting for your response. Click hook flash to pick up the waiting phone call.

Call Transfer

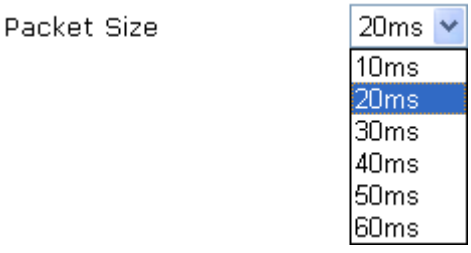
Check this box to invoke this function. Click hook flash to initiate another phone call. When the phone call connection succeeds, hang up the phone. The other two sides can communicate, then.

Prefer Codec

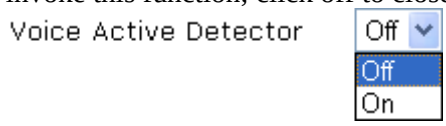
Select one of five codecs as the default for your VoIP calls. The codec used for each call will be negotiated with the peer party before each session, and so may not be your default choice. The default codec is G.729A/B; it occupies little bandwidth while maintaining good voice quality.
If your upstream 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.

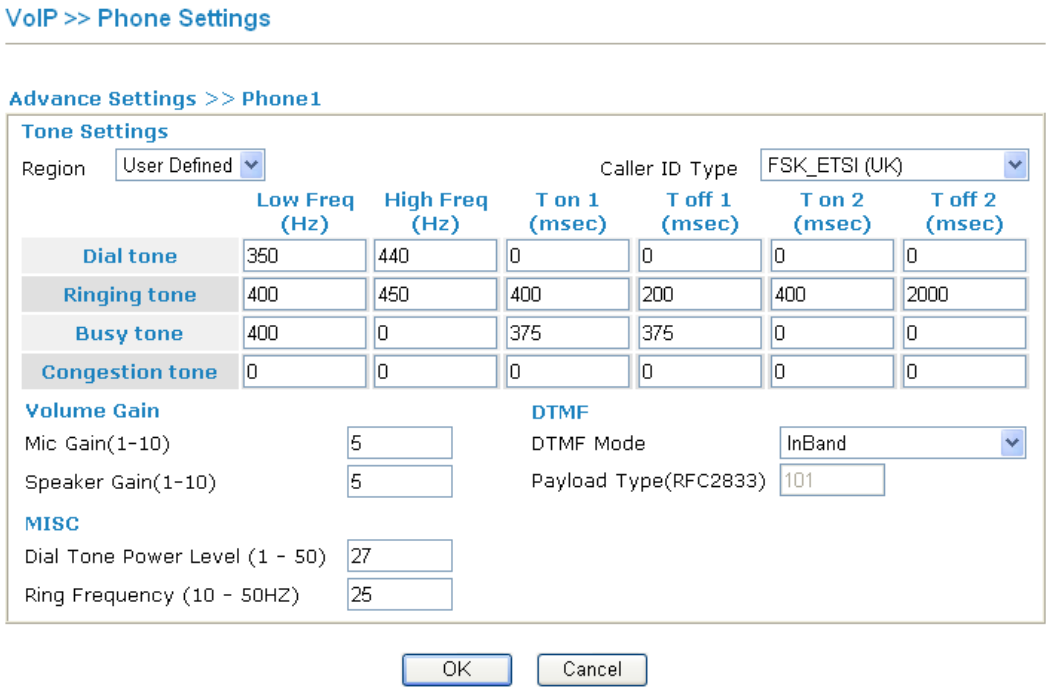


Default SIP Account

You can set SIP accounts (up to six groups) on SIP Account page. Use the drop down list to choose one of the profile names for the accounts as the default one for this phone setting.

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

In addition, you can press the **Advanced** button to configure tone settings, volume gain, MISC and DTMF mode. **Advanced** setting is provided for fitting the telecommunication custom for the local area of the router installed. Wrong tone settings might cause inconvenience for users. To set the sound pattern of the phone set, simply choose a proper region to let the system find out the preset tone settings and caller ID type automatically. Or you can adjust tone settings manually if you choose User Defined. TOn1, TOff1, TOn2 and TOff2 mean the cadence of the tone pattern. TOn1 and TOn2 represent sound-on; TOff1 and TOff2 represent the sound-off.



Region

Select the proper region which you are located. The common settings of **Caller ID Type**, **Dial tone**, **Ringing tone**, **Busy tone** and **Congestion tone** will be shown automatically on the page. If you cannot find out a suitable one, please choose **User Defined** and fill out the corresponding values for dial tone, ringing tone, busy tone, congestion tone by yourself for

VoIP phone.

Also, you can specify each field for your necessity. It is recommended for you to use the default settings for VoIP communication.

Volume Gain

Mic Gain (1-10)/Speaker Gain (1-10) - Adjust the volume of microphone and speaker by entering number from 1- 10. The larger of the number, the louder the volume is.

MISC

Dial Tone Power Level - This setting is used to adjust the loudness of the dial tone. The smaller the number is, the louder the dial tone is. It is recommended for you to use the default setting.

Ring Frequency - This setting is used to drive the frequency of the ring tone. It is recommended for you to use the default setting.

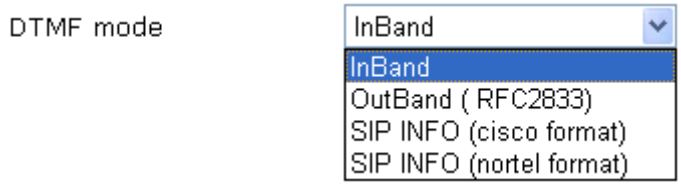
DTMF

DTMF Mode – There are four DTMF modes for you to choose.

***InBand* -** Choose this one then the Vigor will send the DTMF tone as audio directly when you press the keypad on the phone

***OutBand* -** Choose this one then the Vigor will capture the keypad number you pressed and transform it to digital form then send to the other side; the receiver will generate the tone according to the digital form it receive. This function is very useful when the network traffic congestion occurs and it still can remain the accuracy of DTMF tone.

***SIP INFO*-** Choose this one then the Vigor will capture the DTMF tone and transfer it into SIP form. Then it will be sent to the remote end with SIP message.

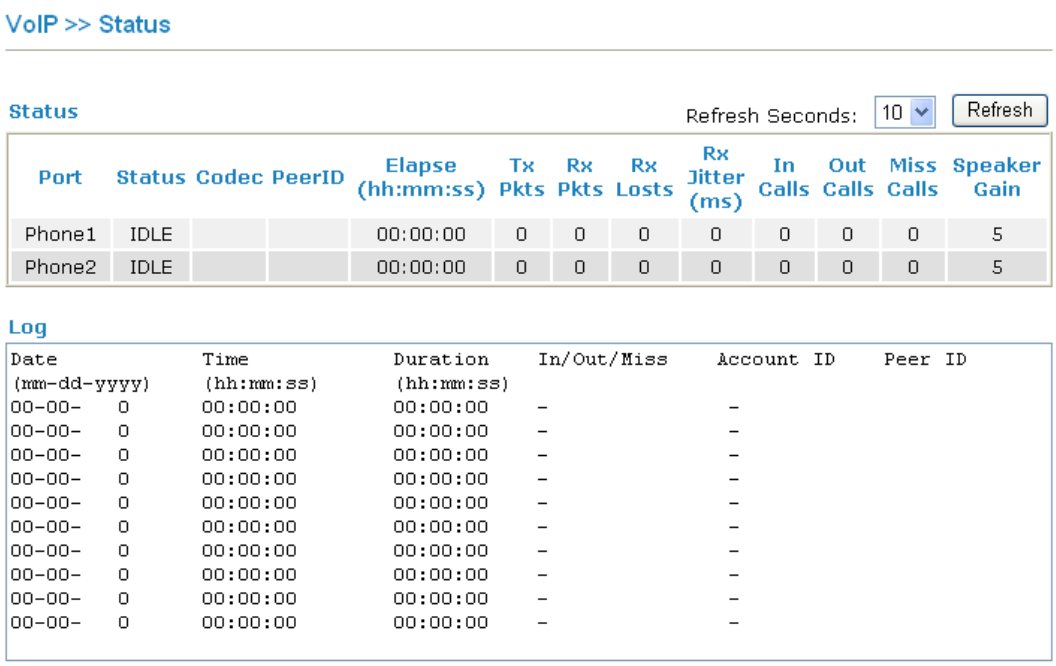


Payload Type (rfc2833) - Choose a number from 96 to 127,

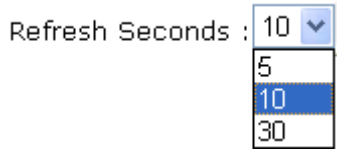
the default value was 101. This setting is available for the OutBand (RFC2833) mode.

3.5.4 Status

From this page, you can find codec, connection and other important call status for each port.



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 Phone1 and Phone2.

Status It shows the VoIP connection status.
IDLE - Indicates that the VoIP function is idle.
HANG_UP - Indicates that the connection is not established (busy tone).
CONNECTING - Indicates that the user is calling out.
WAIT_ANS - Indicates that a connection is launched and waiting for remote user's answer.
ALERTING - Indicates that a call is coming.
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).

Elapse The format is represented as hours:minutes: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	Accumulation for the times of in call.
Out Calls	Accumulation for the times of out call.
Miss Calls	Accumulation for the times of missing call.
Speaker Gain	The volume of present call.
Log	Display logs of VoIP calls.

3.6 Wireless LAN

This function is used for “n/Vn” models.

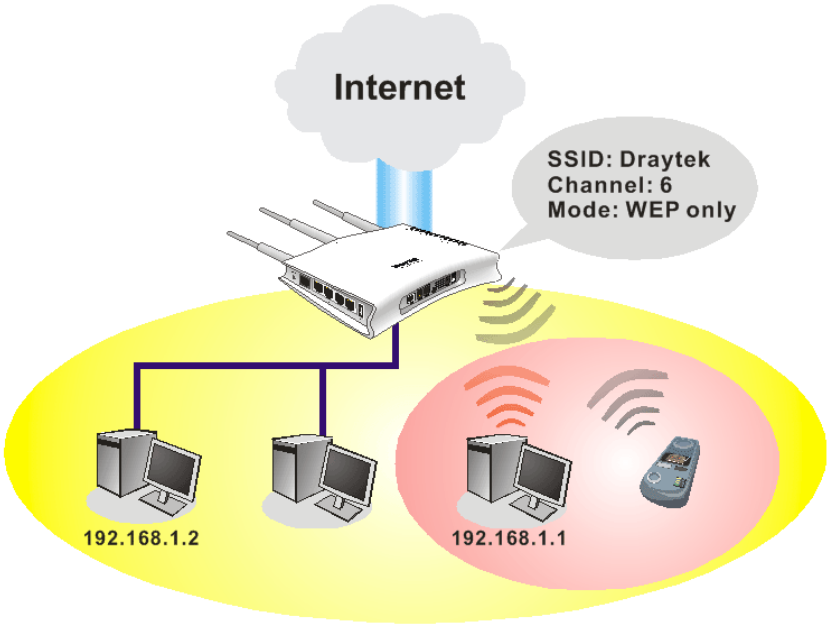
3.6.1 Basic Concepts

Over recent years, the market for wireless communications has enjoyed tremendous growth. Wireless technology now reaches or is capable of reaching virtually every location on the surface of the earth. Hundreds of millions of people exchange information every day via wireless communication products. The Vigor “n” 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 802.11n protocol. To boost its performance further, the Vigor Router is also loaded with advanced wireless technology to lift up data rate up to 300 Mbps*. Hence, you can finally smoothly enjoy stream music and video.

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

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



Security Overview

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

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

WEP (Wired Equivalent Privacy) is a legacy method to encrypt each frame transmitted via radio using either a 64-bit or 128-bit key. Usually access point will preset a set of four keys and it will communicate with each station using only one out of the four keys.

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

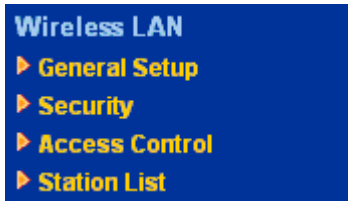
In WPA-Personal, a pre-defined key is used for encryption during data transmission. WPA applies Temporal Key Integrity Protocol (TKIP) for data encryption while WPA2 applies AES. The WPA-Enterprise combines not only encryption but also authentication.

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

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

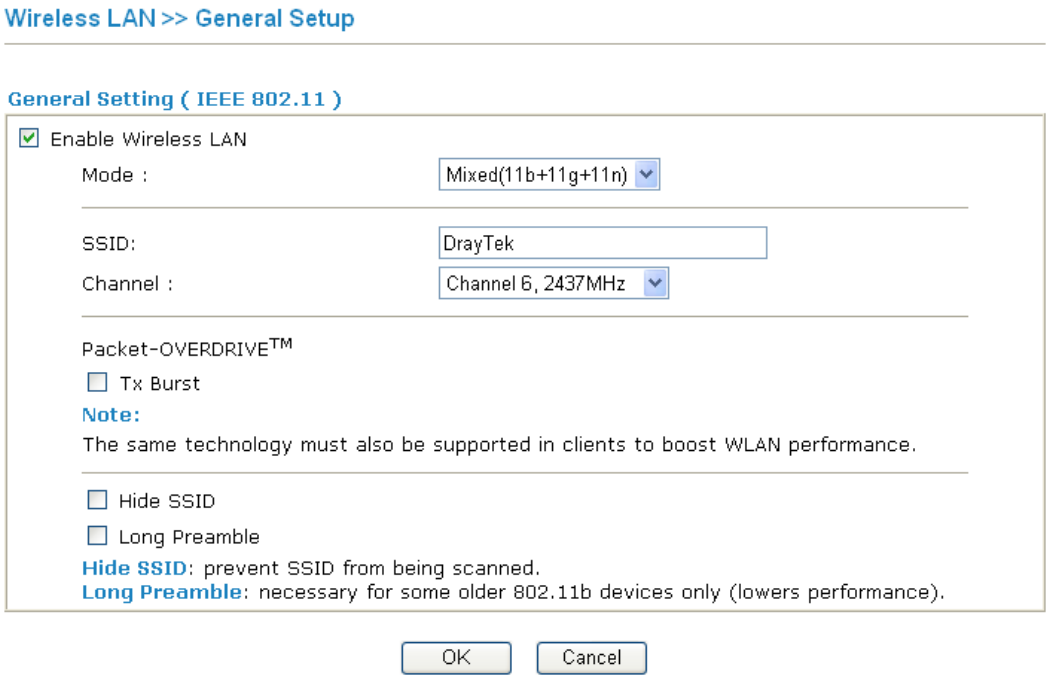
Manage Wireless Stations - Station List will display all the station in your wireless network and the status of their connection.

Below shows the menu items for Wireless LAN.



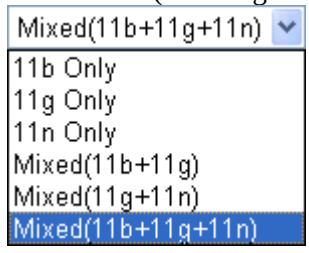
3.6.2 General Setup

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



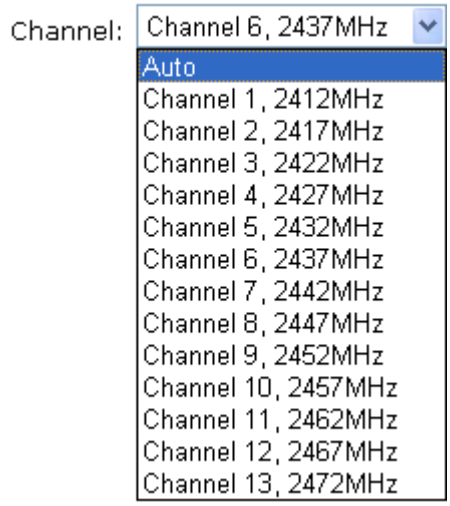
Enable Wireless LAN — Check the box to enable wireless function.

Mode — At present, the router can connect to Mixed (11b+11g), 11g Only, 11b Only, Mixed (11g+11n), 11n Only and Mixed (11b+11g+11n) stations simultaneously. Simply choose Mix (11b+11g+11n) mode.



SSID — Means the identification of the wireless LAN. SSID can be any text numbers or various special characters. The default SSID is "DrayTek". We suggest you to change it.

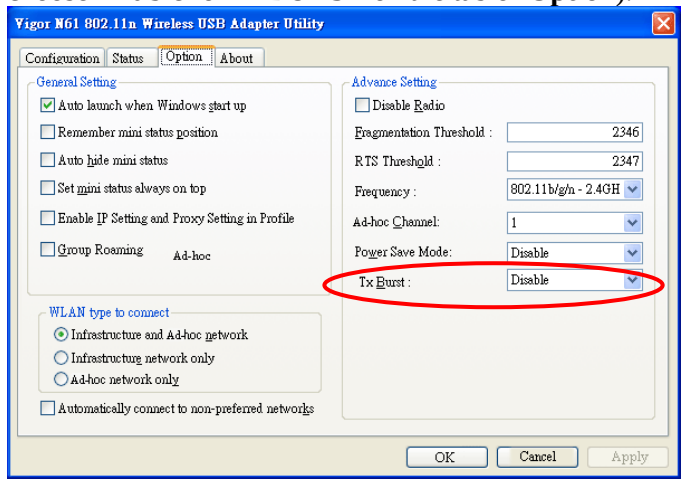
Channel — Means the channel of frequency of the wireless LAN. The default channel is 6. You may switch channel if the selected channel is under serious interference. If you have no idea of choosing the frequency, please select Auto to let system determine for you.



Packet-OVERDRIVE

This feature can enhance the performance in data transmission about 40%* more (by checking **Tx Burs**t). It is active only when both sides of Access Point and Station (in wireless client) invoke this function at the same time. That is, the wireless client must support this feature and invoke the function, too.

Note: Vigor N61 wireless adapter supports this function. Therefore, you can use and install it into your PC for matching with Packet-OVERDRIVE (refer to the following picture of Vigor N61 wireless utility window, choose **Enable** for **TxBURST** on the tab of **Option**).



Hide SSID

Check it to prevent from wireless sniffing and make it harder for unauthorized clients or STAs to join your wireless LAN. Depending on the wireless utility, the user may only see the information except SSID or just cannot see any thing about Vigor wireless router while site surveying. The system allows you to set four sets of SSID for different usage. In default, the first set of SSID will be enabled. You can hide it for your necessity.

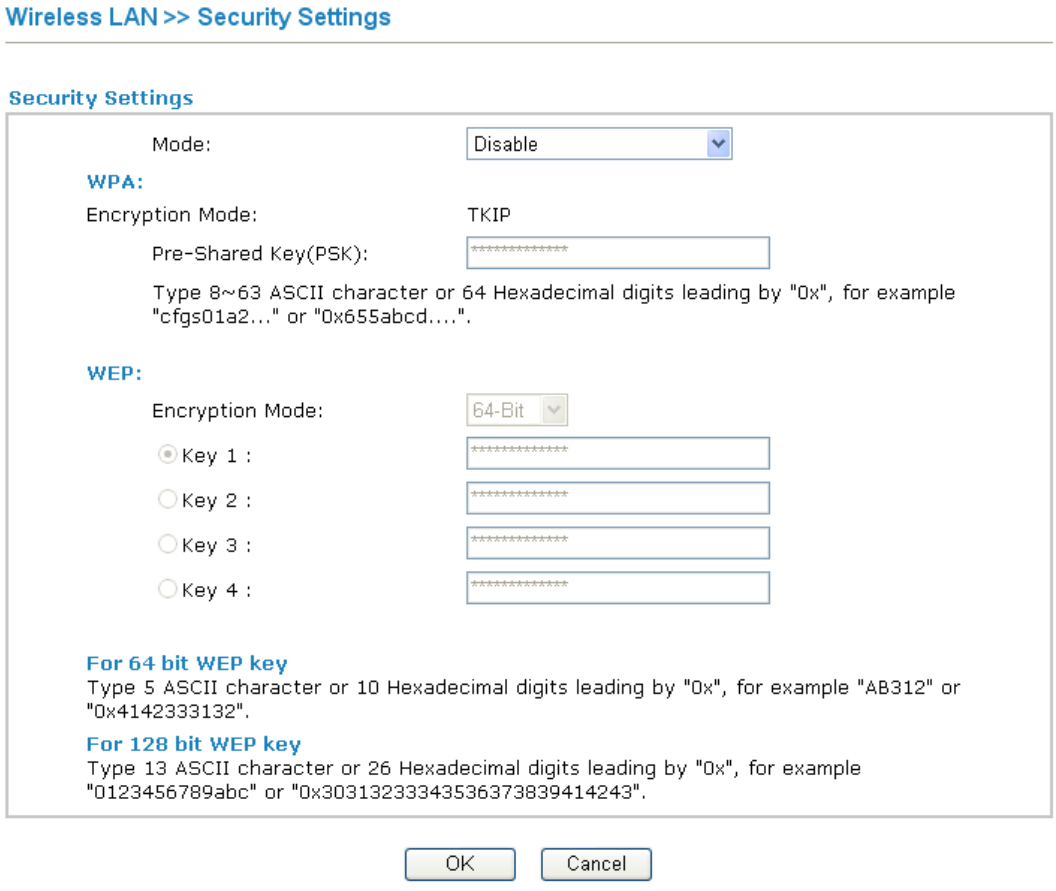
Long Preamble

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 devices only support long preamble. Check it to use **Long Preamble** if needed to communicate with this kind of devices.

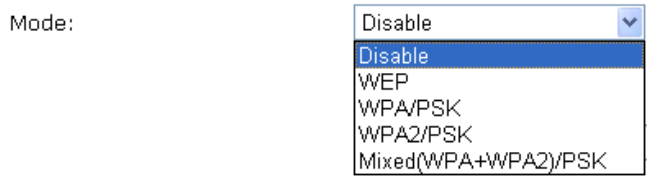
3.6.3 Security

By clicking the **Security Settings**, a new web page will appear so that you could configure the settings of WEP and WPA.



Mode

There are several modes provided for you to choose.



Disable - Turn off the encryption mechanism.
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.

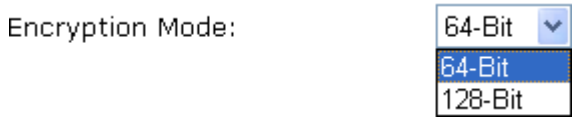
WPA

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...").
Type - Select from Mixed (WPA+WPA2) or WPA2 only.
Pre-Shared Key (PSK) - Either **8~63** ASCII characters, such as 012345678..(or 64 Hexadecimal digits leading by 0x, such as "0x321253abcde...").

WEP

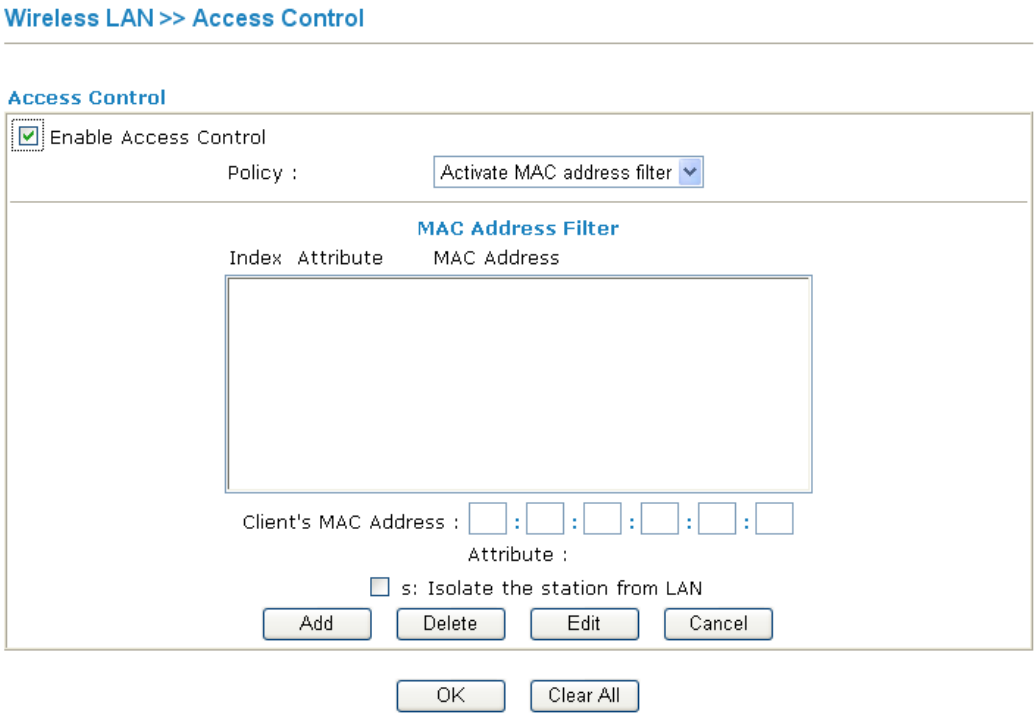
64-Bit - For 64 bits WEP key, either **5** ASCII characters, such as 12345 (or 10 hexadecimal digitals leading by 0x, such as 0x4142434445.)
128-Bit - For 128 bits WEP key, either **13** ASCII characters, such as ABCDEFGHIJKLM (or 26 hexadecimal digits leading by 0x, such as 0x41424344454647484 94A4B4C4D).



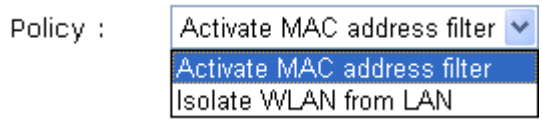
All wireless devices must support the same WEP encryption bit size and have the same key. **Four keys** can be entered here, but only one key can be selected at a time. The keys can be entered in ASCII or Hexadecimal. Check the key you wish to use.

3.6.4 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.

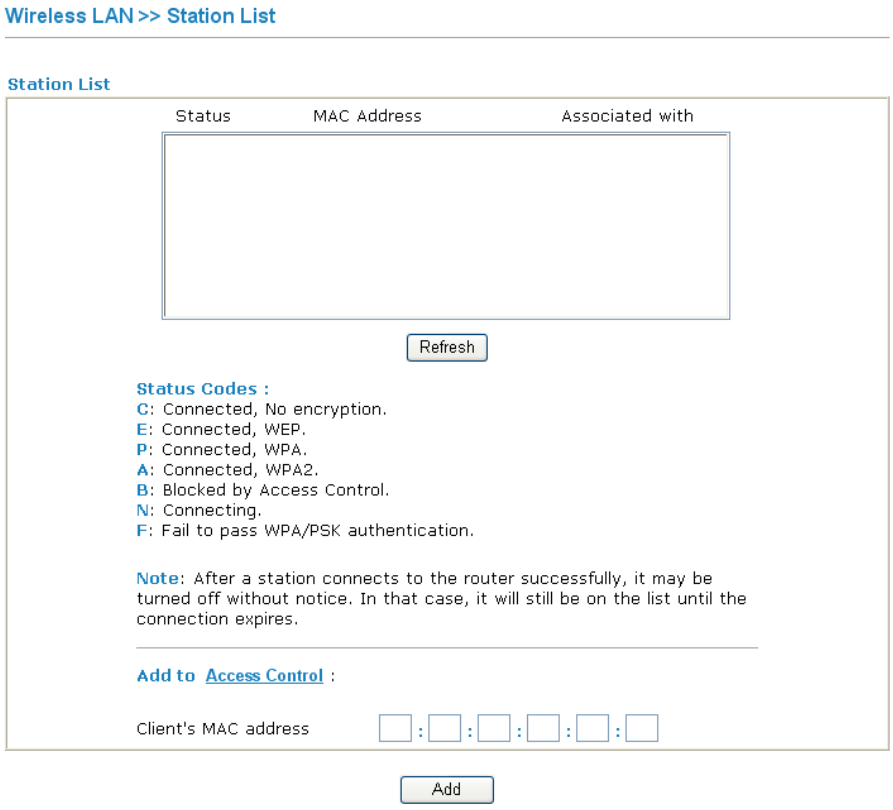


Enable Access Control Select to enable the MAC Address access control feature.

Policy	Select to enable any one of the following policy. Choose **Activate MAC address filter** to type in the MAC addresses for other clients in the network manually. Choose **Isolate WLAN from LAN** will separate all the WLAN stations from LAN based on the MAC Address list. 
MAC Address Filter	Display all MAC addresses that are edited before. Four buttons (Add, Remove, **Client's MAC Address** - Manually enter the MAC address of wireless client.
Attribute	**s -** select to isolate the wireless connection of the wireless client of the MAC address from LAN.
Add	Add a new MAC address into the list.
Delete	Delete the selected MAC address in the list.
Edit	Edit the selected MAC address in the list.
Cancel	Give up the access control set up.
OK	Click it to save the access control list.
Clear All	Clean all entries in the MAC address list.

3.6.5 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.

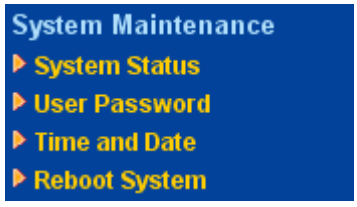


Refresh	Click this button to refresh the status of station list.
Add	Click this button to add current typed MAC address into **Access Contro**l.

3.7 System Maintenance

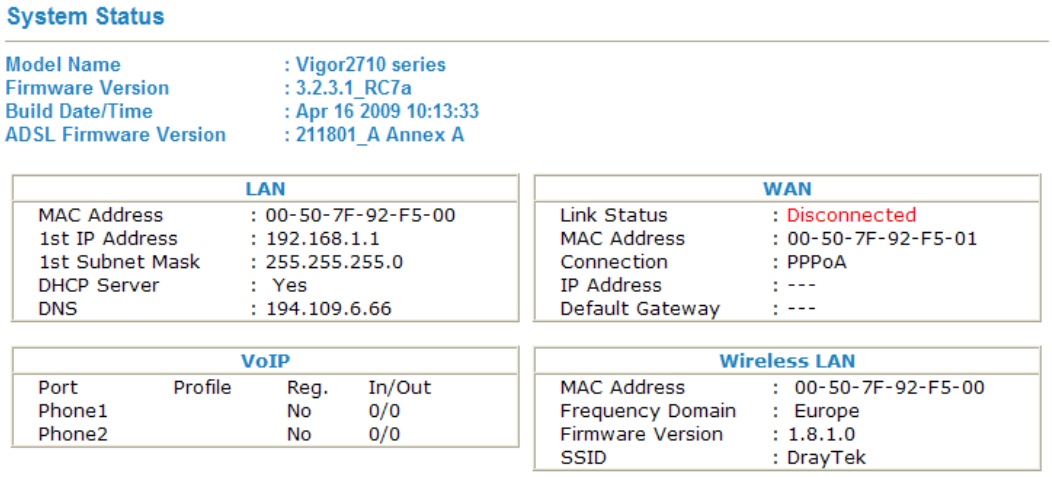
For the system setup, there are several items that you have to know the way of configuration: System Status, User Password, Time setup and Reboot System.

Below shows the menu items for System Maintenance.



3.7.1 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.

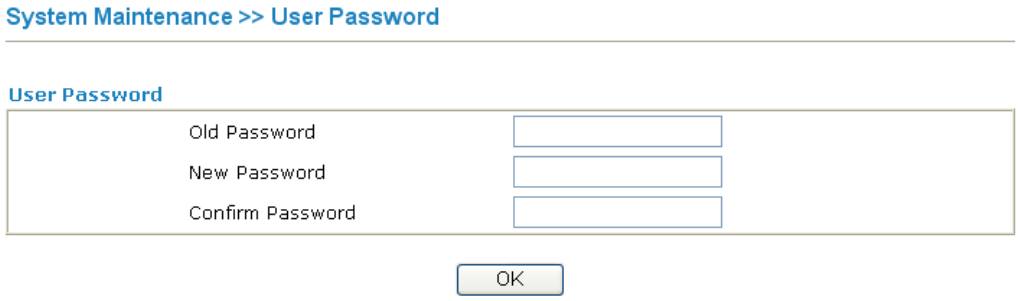


Model Name	Display the model name of the router.
Firmware Version	Display the firmware version of the router.
Build Date/Time	Display the date and time of the current firmware build.
ADSL Firmware Version	Display the ADSL firmware version.
LAN-------	
MAC Address	Display the MAC address of the LAN Interface.
1st IP Address	Display the IP address of the LAN interface.
1st Subnet Mask	Display the subnet mask address of the LAN interface.
DHCP Server	Display the current status of DHCP server of the LAN interface.
DNS	Display the assigned IP address of the primary DNS.
WAN-------	
Link Status	Display current connection status.
MAC Address	Display the MAC address of the WAN Interface.
Connection	Display the connection type.
IP Address	Display the IP address of the WAN interface.
Default Gateway	Display the assigned IP address of the default gateway.
VoIP-------	
Port	Indicate the VoIP phone port.
Profile	Display the profile name for SIP account.
In/Out	Display the number for incoming/outgoing phone call.
Wireless LAN-------	
MAC Address	Display the MAC address of the wireless LAN.
Frequency Domain	It can be Europe (13 usable channels), USA (11 usable channels) etc. The available channels supported by the wireless products in different countries are various.

Firmware Version	It indicates information about equipped WLAN miniPCi card. This also helps to provide availability of some features that are bound with some WLAN miniPCi.
SSID	Display the SSID of the router.

3.7.2 User Password

This page allows you to set new password for user operation.

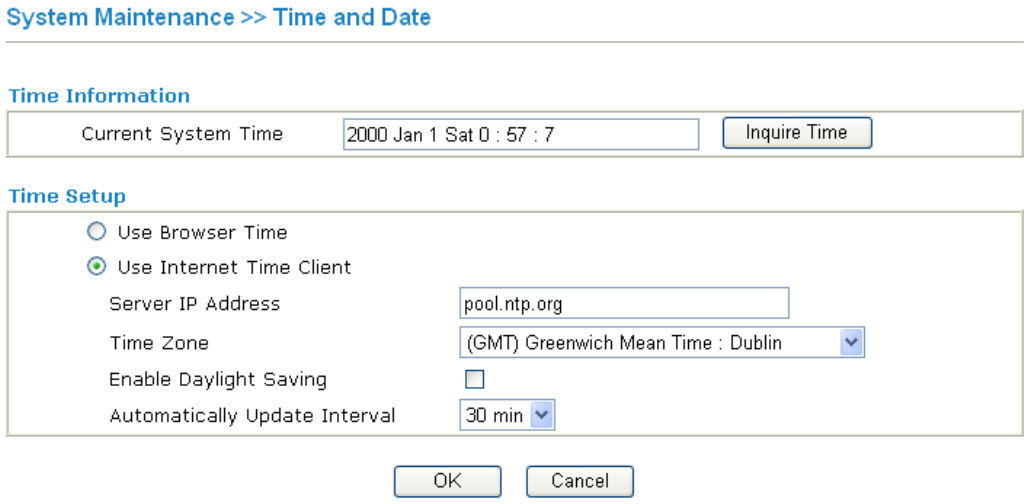


Old Password	Type in the old password. The factory default setting for password is blank.
New Password	Type in new password in this filed.
Confirm Password	Type in the new password again.

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

3.7.3 Time and Date

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



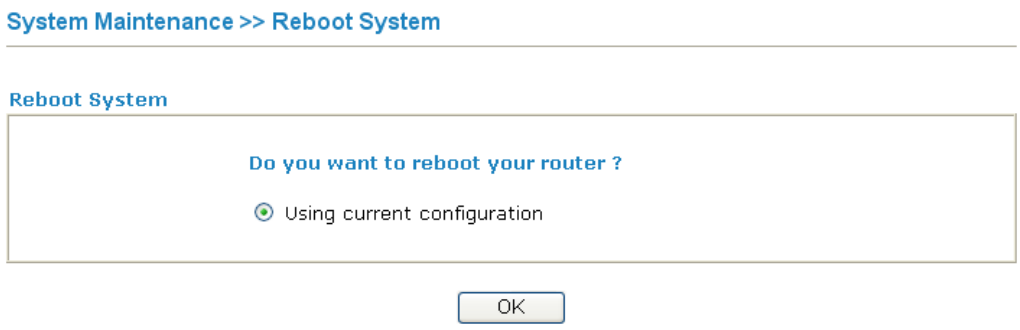
Current System Time	Click **Inquire Time** to get the current time.
Use Browser Time	Select this option to use the browser time from the remote administrator PC host as router's system time.
Use Internet Time	Select to inquire time information from Time Server on the Internet using assigned protocol.
Server IP Address	Type the IP address of the time server.

Time Zone	Select the time zone where the router is located.
Enable Daylight Saving	Check the box to activate daylight saving function. Such feature is useful for some areas.
Automatically Update Interval	Select a time interval for updating from the NTP server.

Click **OK** to save these settings.

3.7.4 Reboot System

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



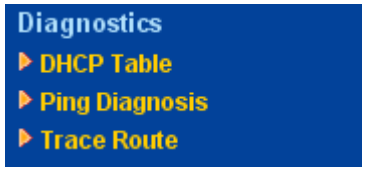
Click **OK**. The router will take 5 seconds to reboot the system.

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

3.8 Diagnostics

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

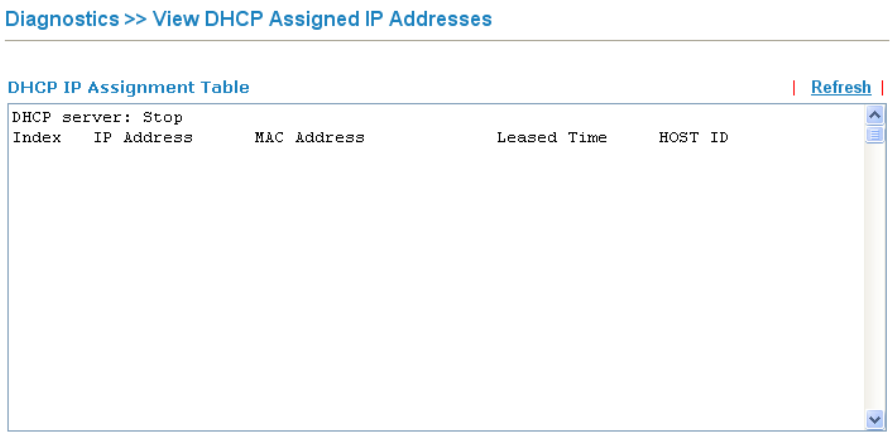
Below shows the menu items for Diagnostics.



3.8.1 DHCP Table

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

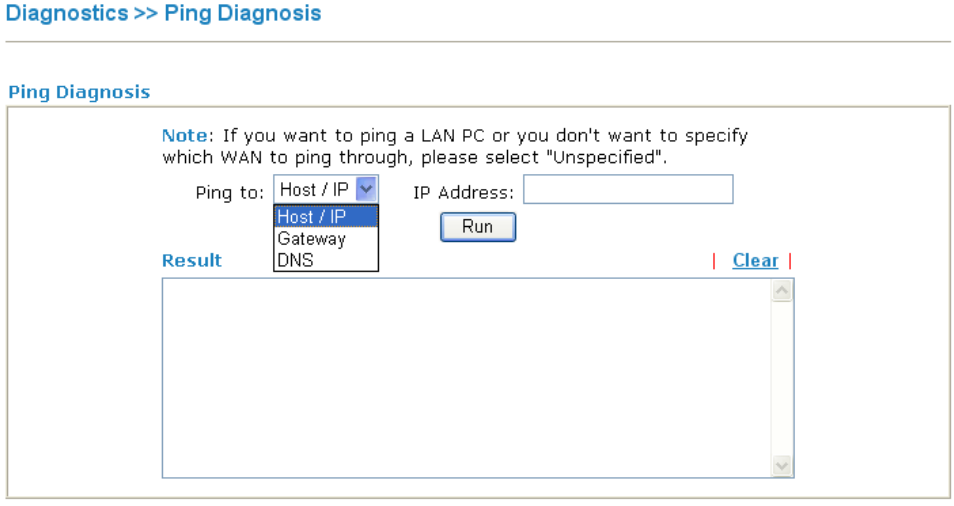
Click **Diagnostics** and click **DHCP Table** to open the web page.



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.

3.8.2 Ping Diagnosis

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

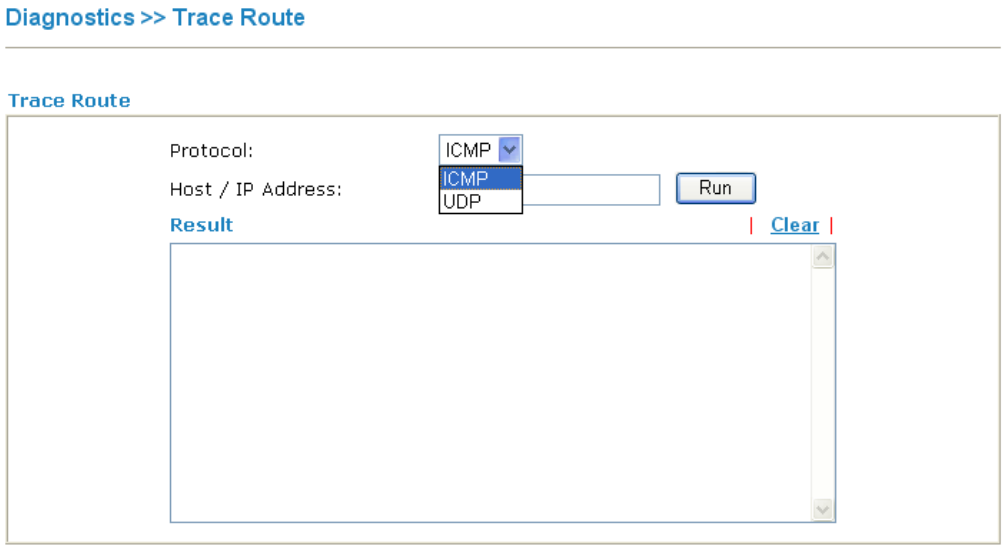


Ping to	Use the drop down list to choose the destination that you want to ping.

IP Address	Type in the IP address of the Host/IP that you want to ping.
Run	Click this button to start the ping work. The result will be displayed on the screen.
Clear	Click this link to remove the result on the window.

3.8.3 Trace Route

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



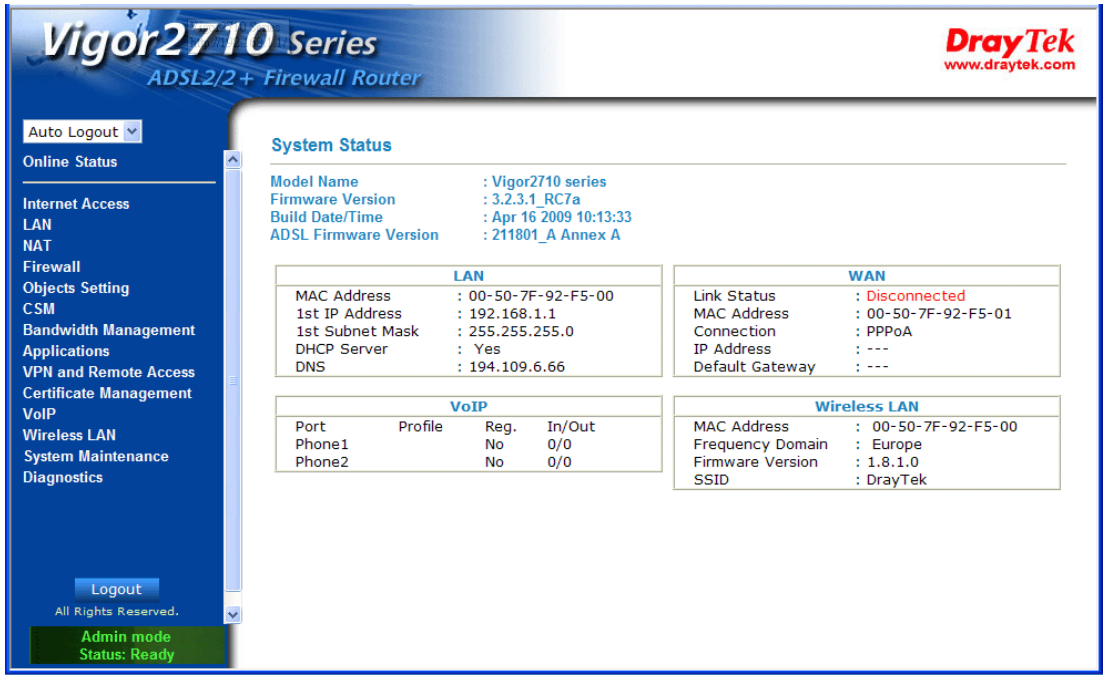
Protocol	Use the drop down list to choose the interface that you want to ping through.
Host/IP Address	It indicates the IP address of the host.
Run	Click this button to start route tracing work.
Clear	Click this link to remove the result on the window.

4 Admin Mode Operation

This chapter will guide users to execute advanced (full) configuration through admin mode operation. As for other examples of application, please refer to chapter 5.

1. Open a web browser on your PC and type **http://192.168.1.1.** The window will ask for typing username and password.
2. Please type “admin/admin” on Username/Password for administration operation.

Now, the **Main Screen** will appear. Be aware that “Admin mode” will be displayed on the bottom left side.



4.1 Internet Access

4.1.1 Basics of Internet Protocol (IP) Network

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

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

What are Public IP Address and Private IP Address

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

Get Your Public IP Address from ISP

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

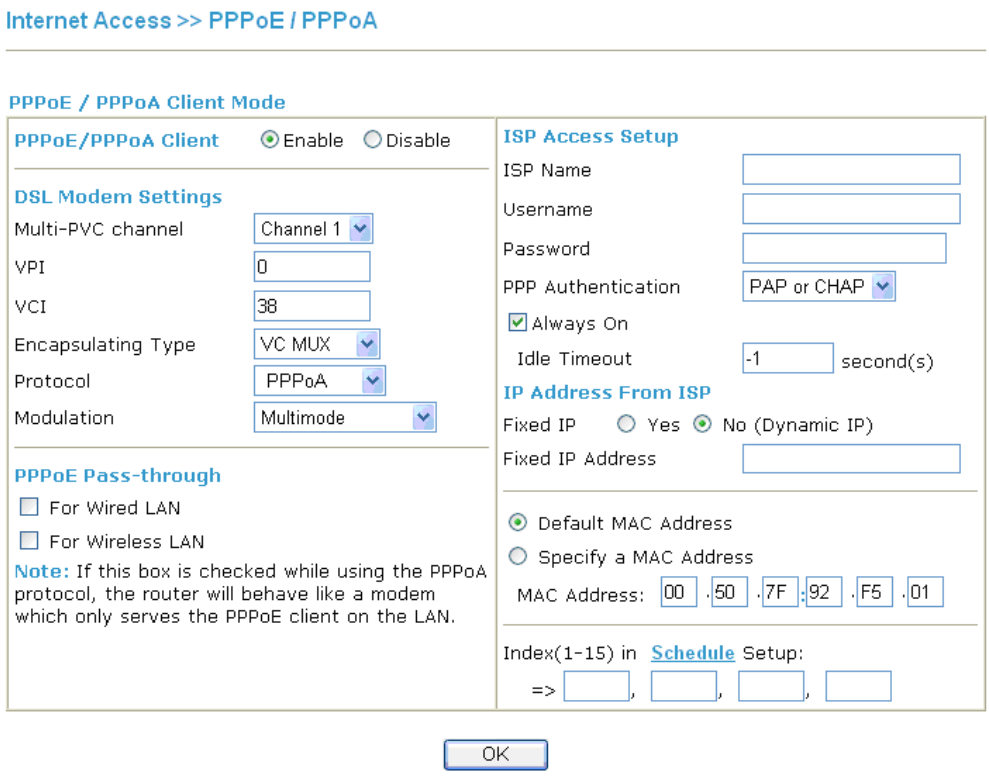
When a router begins to connect to your ISP, a serial of discovery process will occur to ask for a connection. Then a session will be created. Your user ID and password is authenticated via **PAP** or **CHAP** with **RADIUS** authentication system. And your IP address, DNS server, and other related information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

Below shows the menu items for Internet Access.

4.1.2 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.



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

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

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. When PPPoA protocol is selected, the PPPoE package transmitted by PC will be transformed into PPPoA package and sent to WAN server. Thus, the PC can access Internet through such direction.
For Wired LAN – If you check this box, PCs on the same network can use another set of PPPoE session (different with the Host PC) to access into Internet.
For Wireless LAN – If you check this box, PCs on the same wireless network can use another set of PPPoE session (different with the Host PC) to access into Internet.

ISP Access Setup Enter your allocated username, password and authentication parameters according to the information provided by your ISP. If you want to connect to Internet all the time, you can check **Always On**.
Username – Type in the username provided by ISP in this field.

Password – Type in the password provided by ISP in this field.
PPP Authentication – Select **PAP only** or **PAP or CHAP** for PPP.
Idle Timeout – Set the timeout for breaking down the Internet after passing through the time without any action. This setting is active only when the **Active on demand** option for Active Mode is selected in **WAN>> General Setup** page.

IP Address From ISP

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

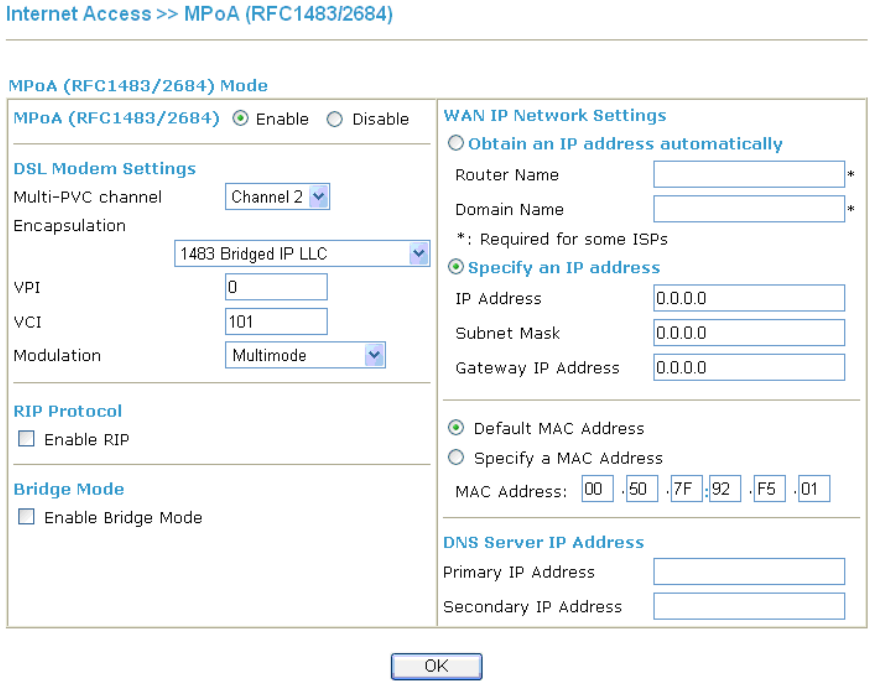
Fixed IP – Click **Yes** to use this function and type in a fixed IP address in the box of **Fixed IP Address**.
Default MAC Address – You can use **Default MAC Address** or specify another MAC address by typing on the boxes of MAC Address for the router.
Specify a MAC Address – Type the MAC address for the router manually.
Index (1-15) in Schedule Setup - You can type in four sets of time schedule for your request. All the schedules can be set previously in **Applications – Schedule** web page and you can use the number that you have set in that web page.

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

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



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. **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.

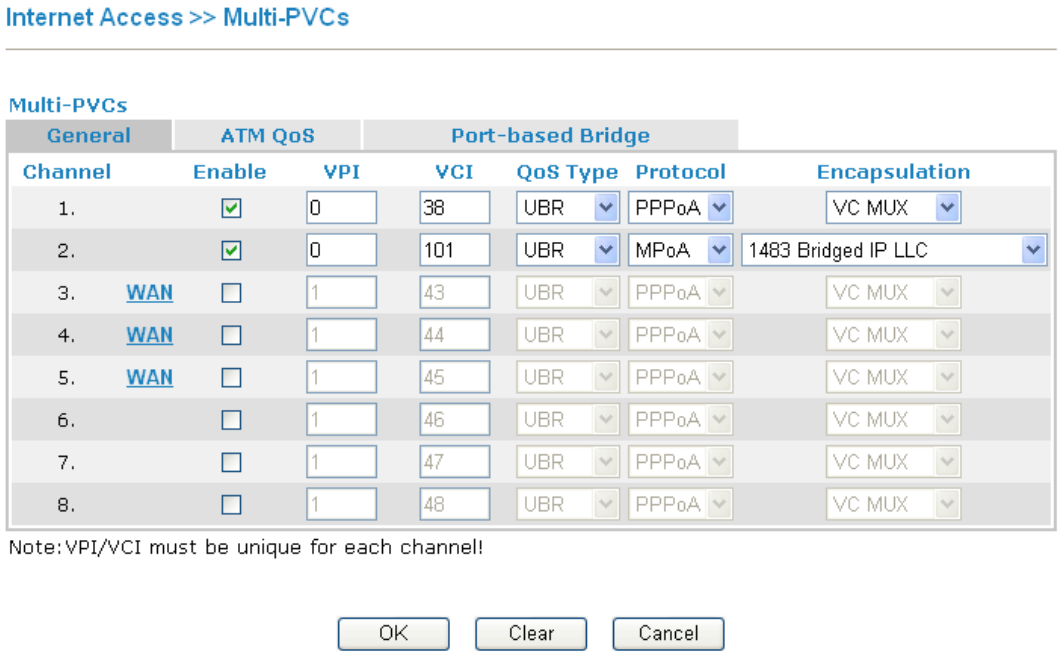
After finishing all the settings here, please click **OK** to activate them.

4.1.4 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.

General

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

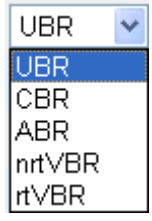


Enable Check this box to enable that channel. The channels that you enabled here will be shown in the **Multi-PVC channel** drop down list on the web page of **Internet Access**. Though you can enable eight channels in this page, yet only one channel can be chosen on the web page of **Internet Access**.

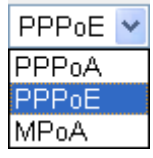
VPI Type in the value provided by your ISP.

VCI Type in the value provided by your ISP.

QoS Type Select a proper QoS type for the channel.

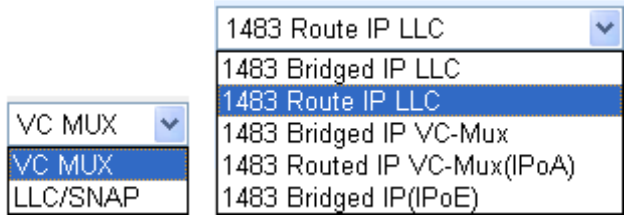


Protocol Select a proper protocol for this channel.

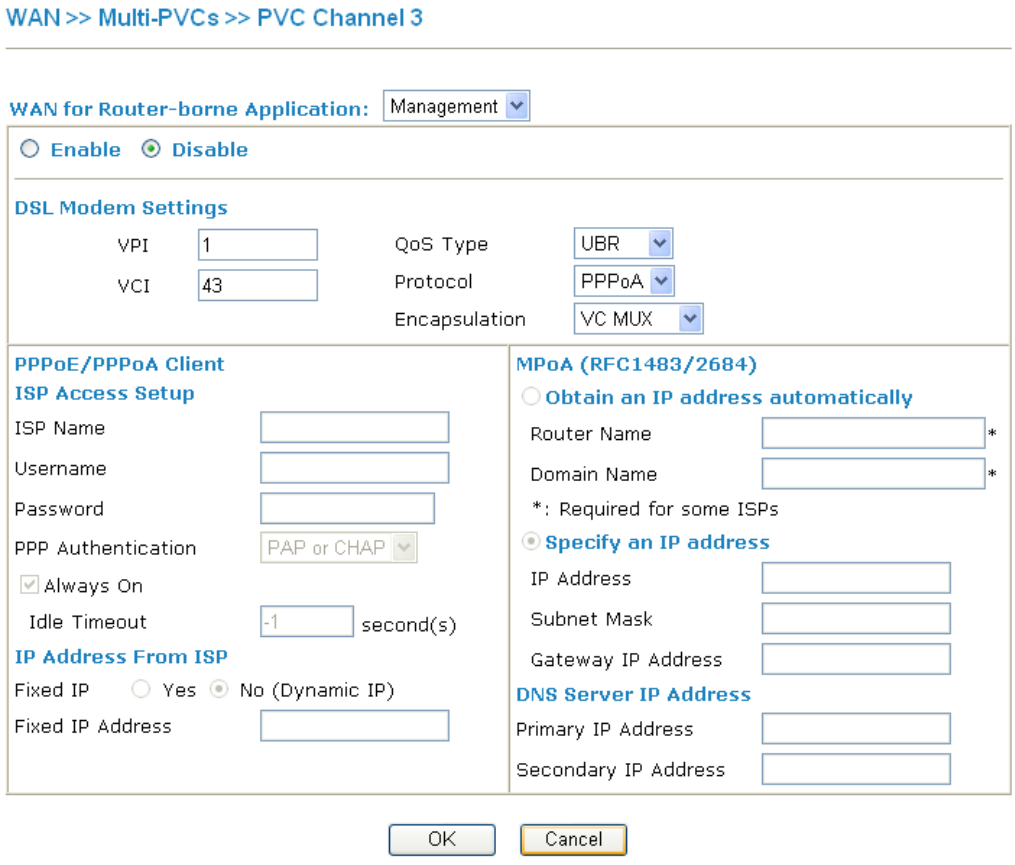


Encapsulation

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



WAN link for Channel 3, 4, 5 are provided for router-borne application such as TR069 and VoIP. The settings must be applied and obtained from your ISP. For your special request, please contact with your ISP and then click WAN link of Channel 3, 4 or 5 to configure your router.



WAN for Router-borne Application

Choose the router service for channel 3, 4 or 5.

Management - It can be specified for general management (Web configuration/telnet/TR069). If you choose Management, the configuration for this PVC will be effective for Web configuration/telnet/TR069.
VoIP - It can be specified for VoIP only. If you choose VoIP, the configuration for this PVC will be effective for VoIP data transmitting and receiving.

Enable/Disable

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

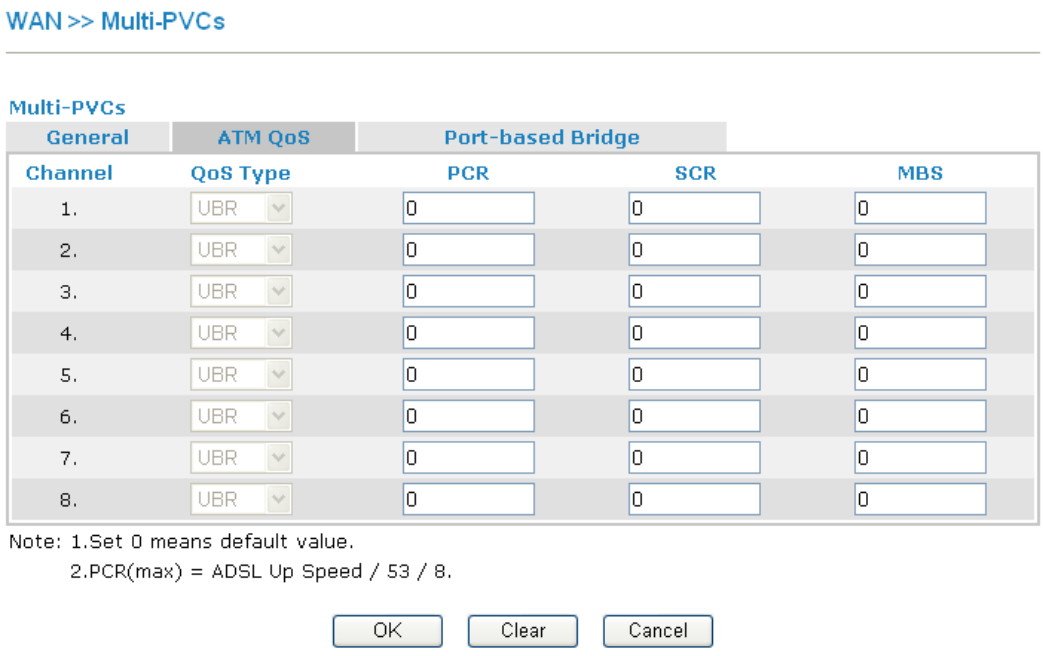
DSL Modem Settings

Set up the DSL parameters required by your ISP. These are vital for building DSL connection to your ISP.
VPI - Type in the value provided by ISP.

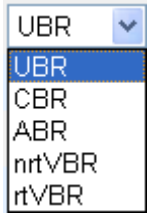
	VCI - Type in the value provided by ISP. **QoS Type** -Select a proper QoS type for the channel. **Protocol** - Select a proper protocol for this channel. There are three options, PPPoE, PPPoA and MPoA for you to select. The following settings will be changed according to the protocol selected here. **Encapsulating Type** - Drop down the list to choose the type provided by ISP.
ISP Access Setup	Enter your allocated username, password and authentication parameters according to the information provided by your ISP. If you want to connect to Internet all the time, you can check **Always On**. **Username** – Type in the username provided by ISP in this field. **Password** – Type in the password provided by ISP in this field. **PPP Authentication** – Select **PAP only** or **PAP or CHAP** for PPP. **Idle Timeout** – Set the timeout for breaking down the Internet after passing through the time without any action. This setting is active only when the **Always On** option is note selected.
IP Address from ISP	**Fixed IP** - Click **Yes** to use this function and type in a fixed IP address in the box of **Fixed IP Address**. **Fixed IP Address** -Type a fixed IP address.
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.
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.
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.

ATM QoS

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



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



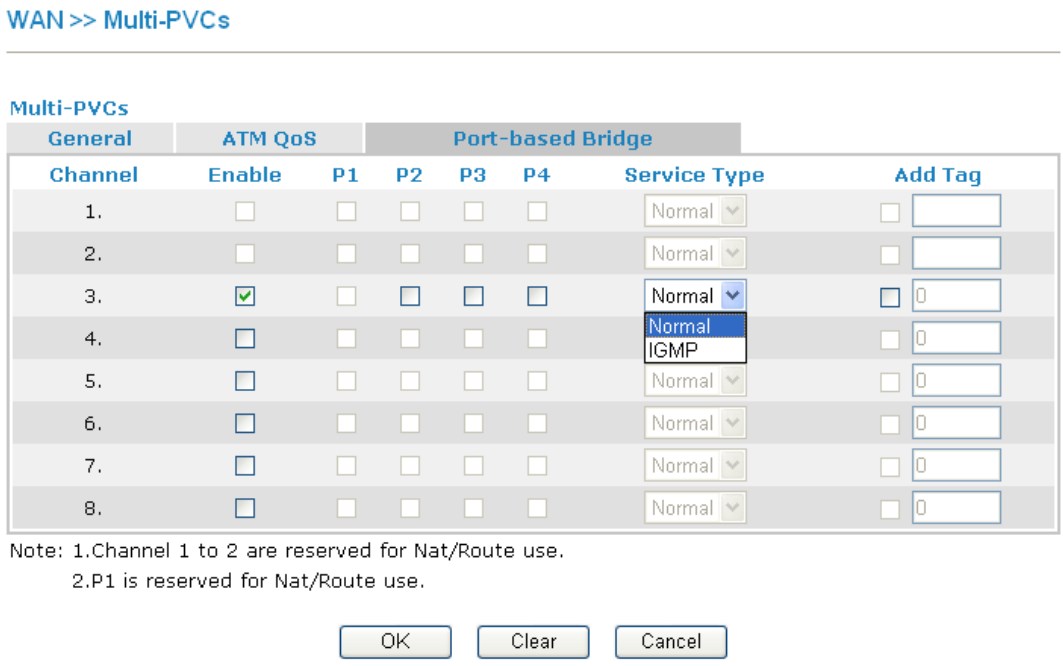
PCR It represents Peak Cell Rate. The default setting is “0”.

SCR It represents Sustainable Cell Rate. The value of SCR must be smaller than PCR.

MBS It represents Maximum Burst Size. The range of the value is 10 to 50.

Port-based Bridge

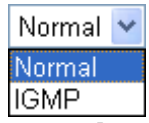
General page lets you set the first PVC. As to set the second PVC line, please click the **Port-based Bridge** tab to open Bridge configuration page.



Enable — Check this box to enable that channel. Only channel 3 to 8 can be set in this page, for channel 1 to 2 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 3 to 8.

Service Type — Normally, service type is used for the service of video stream (e.g., IPTV). It can divide the packets from remote control and from video stream into different PVC. In general, the protocol used by remote control is IGMP.



Normal – It means that the PVC can accept all packets except IGMP.
IGMP – It means that the PVC can accept packets of IGMP only.

Add Tag — To identify the usage of PVC, check this box to invoke this setting. And type the number for VLAN ID (number).

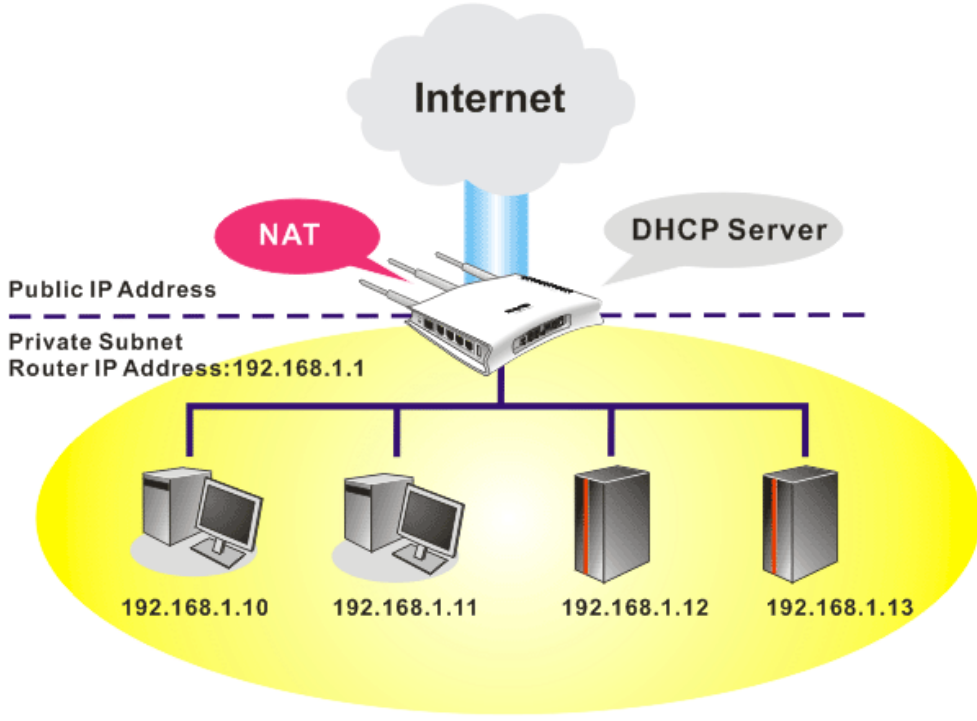
Click **Clear** to remove all the configurations in this page if you do not satisfy it. When you finish the configuration, please click **OK** to save and exit this page. Or click Cancel to abort the configuration and exit this page.

4.2 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.

4.2.1 Basics of LAN

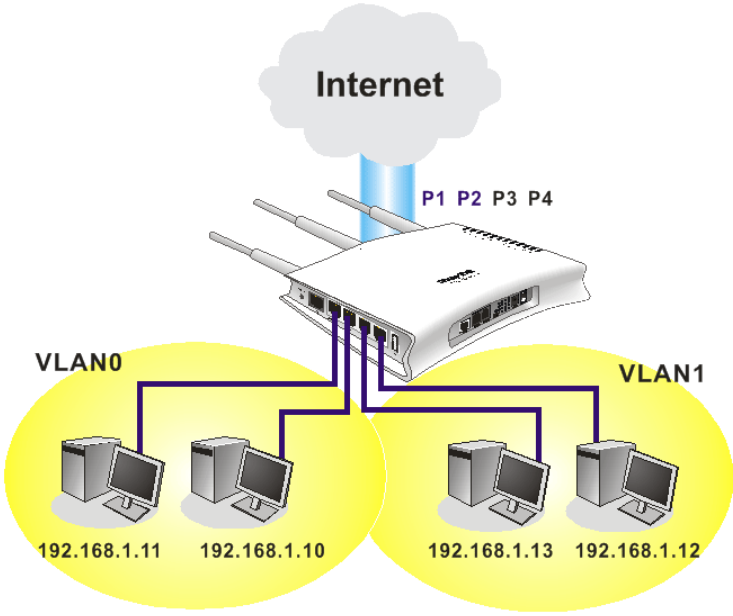
The most generic function of Vigor router is NAT. It creates a private subnet of your own. As mentioned previously, the router will talk to other public hosts on the Internet by using public IP address and talking to local hosts by using its private IP address. What NAT does is to translate the packets 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 are Virtual LANs

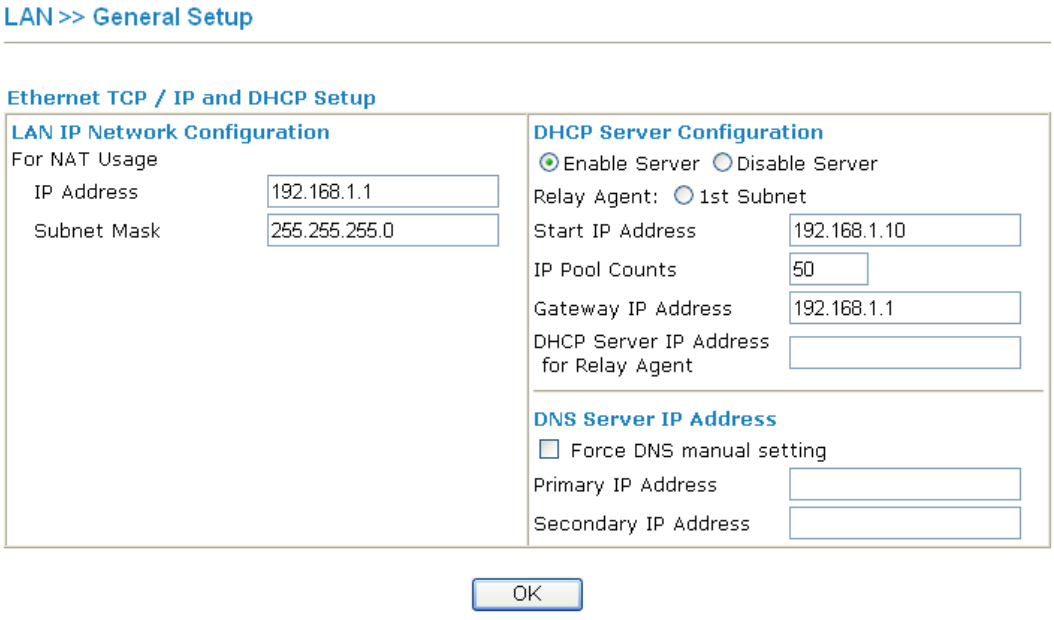
You can group local hosts by physical ports and create up to 4 virtual LANs. To manage the communication between different groups, please set up rules in Virtual LAN (VLAN) function and the rate of each.



4.2.2 General Setup

This page provides you the general settings for LAN.

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



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)
DHCP Server Configuration	DHCP stands for Dynamic Host Configuration Protocol. The router by factory default acts a DHCP server for your network so it automatically dispatch related IP settings to any local user configured as a DHCP client. It is highly recommended that you leave the router enabled as a DHCP server if you do not have a DHCP server for your network.

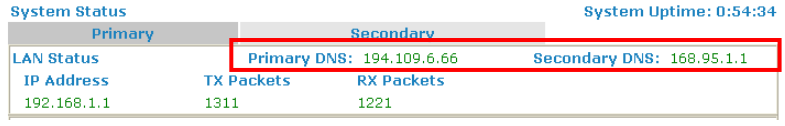
If you want to use another DHCP server in the network other than the Vigor Router's, you can let Relay Agent help you to redirect the DHCP request to the specified location.
Enable Server - Let the router assign IP address to every host in the LAN.
Disable Server – Let you manually assign IP address to every host in the LAN.
Relay Agent – Specify the subnet that DHCP server is located the relay agent should redirect the DHCP request to.
Start IP Address - Enter a value of the IP address pool for the DHCP server to start with when issuing IP addresses. If the 1st IP address of your router is 192.168.1.1, the starting IP address must be 192.168.1.2 or greater, but smaller than 192.168.1.254.
IP Pool Counts - Enter the maximum number of PCs that you want the DHCP server to assign IP addresses to. The default is 50 and the maximum is 253.
Gateway IP Address - Enter a value of the gateway IP address for the DHCP server. The value is usually as same as the 1st IP address of the router, which means the router is the default gateway.
DHCP Server IP Address for Relay Agent - Set the IP address of the DHCP server you are going to use so the Relay Agent can help to forward the DHCP request to the DHCP server.

DNS Server Configuration

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

Force DNS manual setting - Force Vigor router to use DNS servers in this page instead of DNS servers given by the Internet Access server (PPPoE, PPTP, L2TP or DHCP server).
Primary IP Address -You must specify a DNS server IP address here because your ISP should provide you with usually more than one DNS Server. If your ISP does not provide it, the router will automatically apply default DNS Server IP address: 194.109.6.66 to this field.
Secondary IP Address - You can specify secondary DNS server IP address here because your ISP often provides you more than one DNS Server. If your ISP does not provide it, the router will automatically apply default secondary DNS Server IP address: 194.98.0.1 to this field.

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

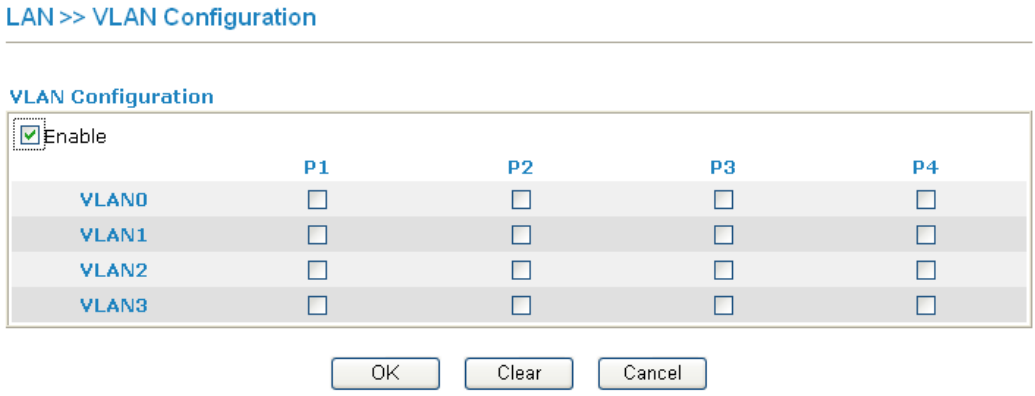


If both the Primary IP and Secondary IP Address fields are left empty, the router will assign its own IP address to local users as a DNS proxy server and maintain a DNS cache.

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.

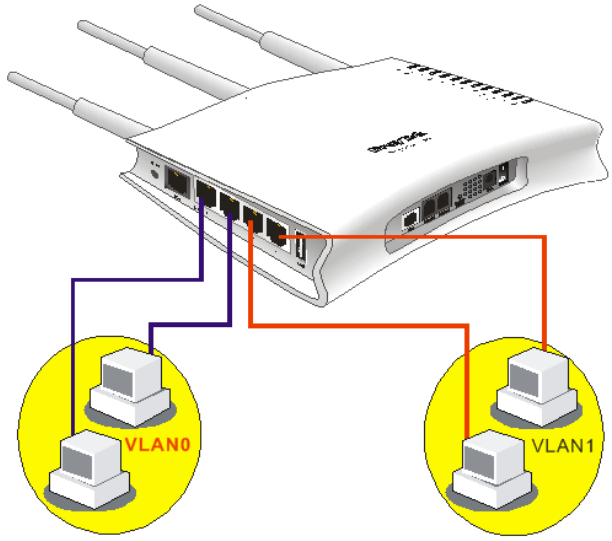
4.2.3 VLAN

Virtual LAN function provides you a very convenient way to manage hosts by grouping them based on the physical port. Go to **LAN** page and select **VLAN**. The following page will appear. Click **Enable** to invoke VLAN function.

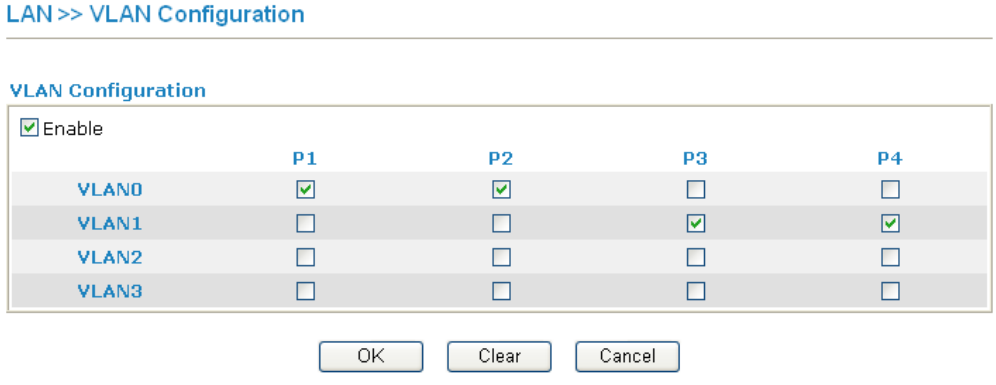


To add or remove a VLAN, please refer to the following example.

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.

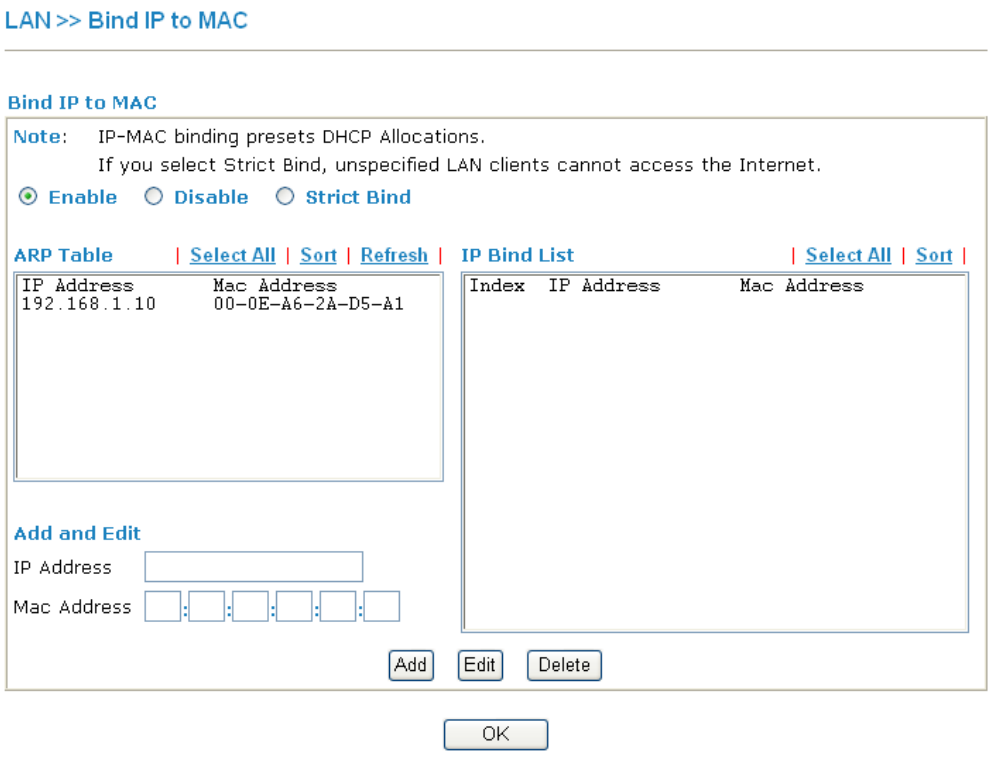


To remove VLAN, uncheck the needed box and click **OK** to save the results.

4.2.4 Bind IP to MAC

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

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



Enable	Click this radio button to invoke this function. However, IP/MAC which is not listed in IP Bind List also can connect to Internet.
Disable	Click this radio button to disable this function. All the settings on this page will be invalid.
Strict Bind	Click this radio button to block the connection of the IP/MAC which is not listed in IP Bind List.
ARP Table	This table is the LAN ARP table of this router. The information for IP and MAC will be displayed in this field. Each pair of IP and MAC address listed in ARP table can be selected and added to IP Bind List by clicking **Add** below.
Add and Edit	**IP Address** – Type the IP address that will be used for the specified MAC address. **Mac Address** – Type the MAC address that is used to bind with the assigned IP address.
Refresh	It is used to refresh the ARP table. When there is one new PC added to the LAN, you can click this link to obtain the newly ARP table information.
IP Bind List	It displays a list for the IP bind to MAC information.
Add	It allows you to add the one you choose from the ARP table or the IP/MAC address typed in **Add and Edit** to the table of **IP Bind List**.

Edit	It allows you to edit and modify the selected IP address and MAC address that you create before.
Remove	You can remove any item listed in **IP Bind List**. Simply click and select the one, and click **Remove**. The selected item will be removed from the **IP Bind List**.

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

4.3 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:

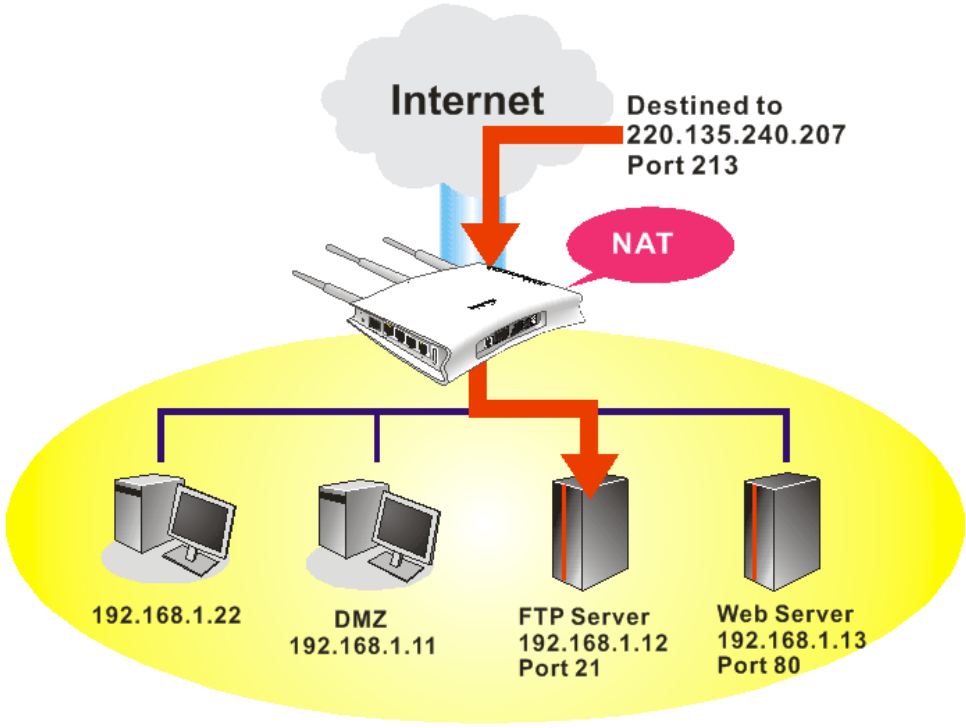
- **Save cost on applying public IP address and apply efficient usage of IP address.** NAT allows the internal IP addresses of local hosts to be translated into one public IP address, thus you can have only one IP address on behalf of the entire internal hosts.
- **Enhance security of the internal network 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.

Below shows the menu items for NAT.

4.3.1 Port Redirection

Port Redirection is usually set up for server related service inside the local network (LAN), such as web servers, FTP servers, E-mail servers etc. Most of the case, you need a public IP address for each server and this public IP address/domain name are recognized by all users. Since the server is actually located inside the LAN, the network well protected by NAT of the router, and identified by its private IP address/port, the goal of Port Redirection function is to forward all access request with public IP address from external users to the mapping private IP address/port of the server.



The port redirection can only apply to incoming traffic.

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

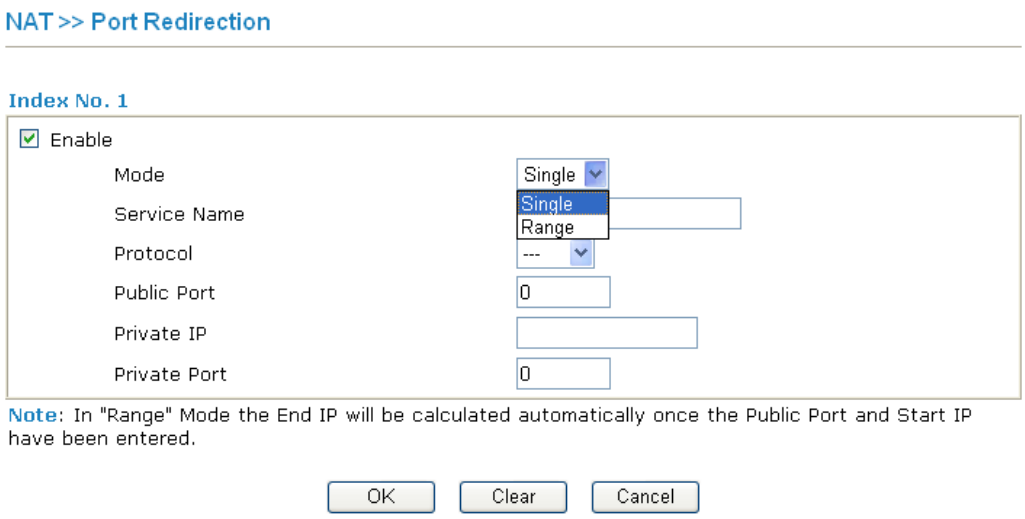
NAT >> Port Redirection

Port Redirection | Set to Factory Default |

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

<< 1-10 | 11-20 >> Next >>

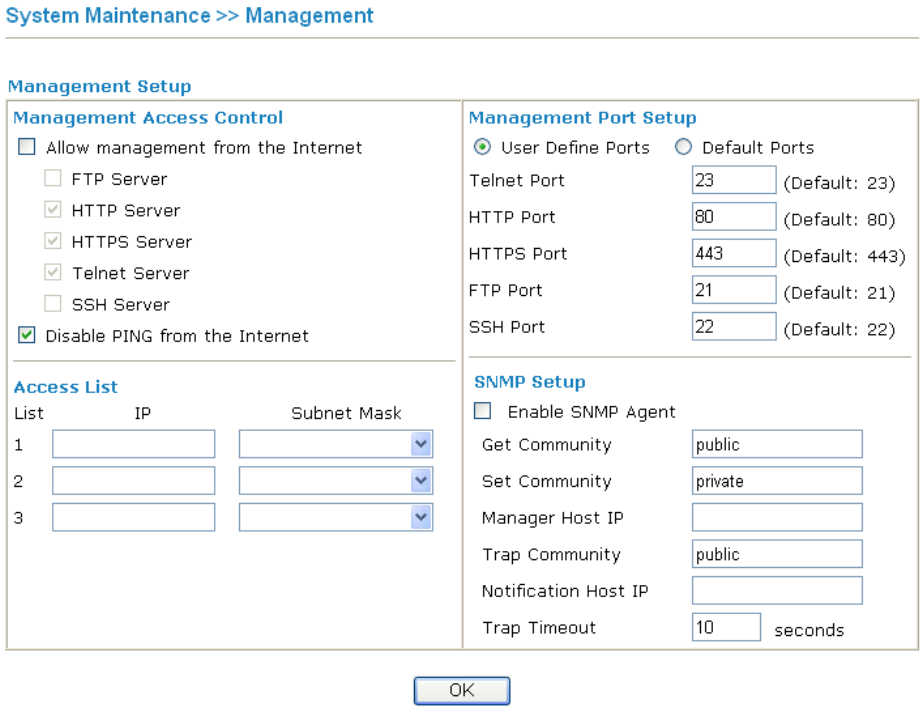
Press any number under Index to access into next page for configuring port redirection.



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

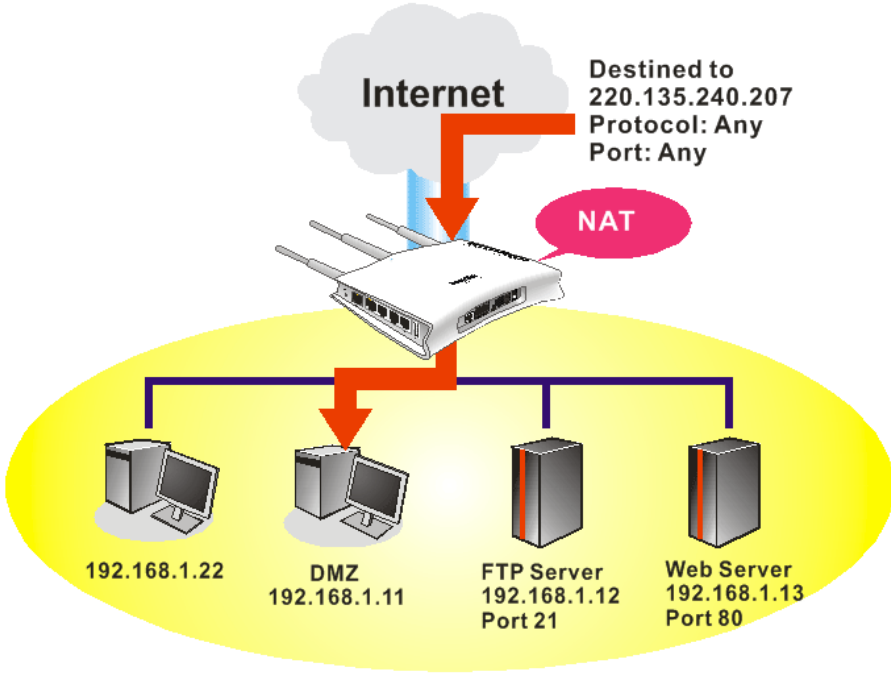
Note that the router has its own built-in services (servers) such as Telnet, HTTP and FTP etc. Since the common port numbers of these services (servers) are all the same, you may need to reset the router in order to avoid confliction.

For example, the built-in web configurator in the router is with default port 80, which may conflict with the web server in the local network, http://192.168.1.13:80. Therefore, you need to **change the router's http port to any one other than the default port 80** to avoid conflict, such as 8080. This can be set in the **System Maintenance >>Management Setup**. You then will access the admin screen of by suffixing the IP address with 8080, e.g., http://192.168.1.1:8080 instead of port 80.



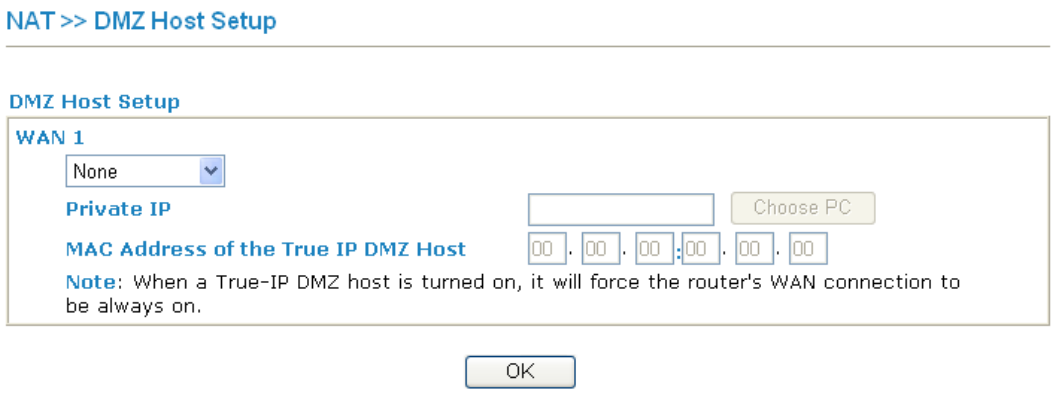
4.3.2 DMZ Host

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



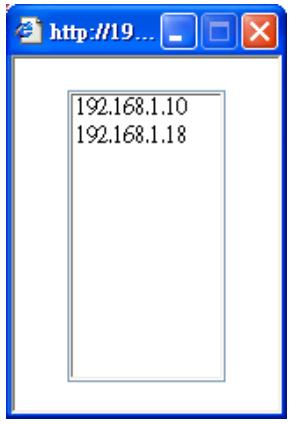
The inherent security properties of NAT are somewhat bypassed if you set up DMZ host. We suggest you to add additional filter rules or a secondary firewall.

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



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.



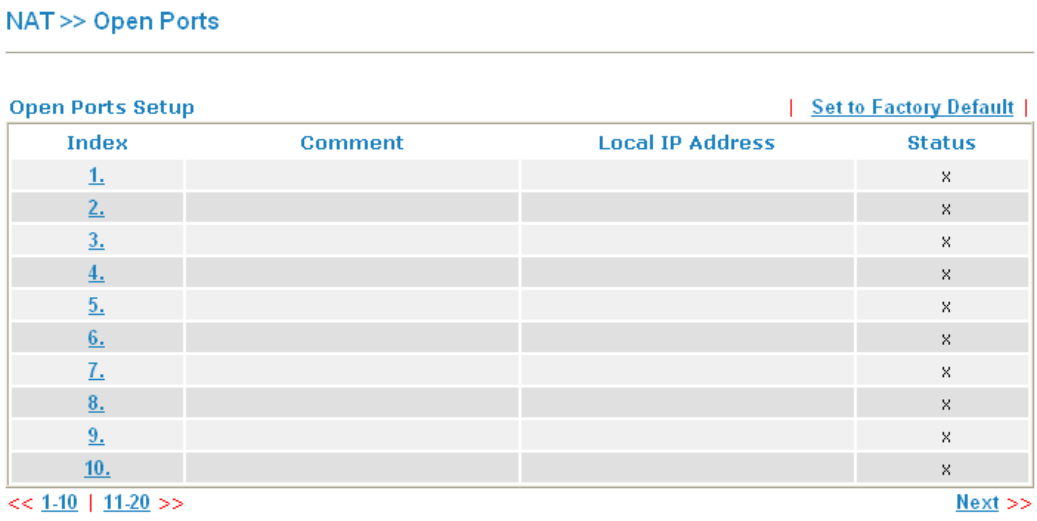
When you have selected one private IP from the above dialog, click **OK** to save the setting.

4.3.3 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.

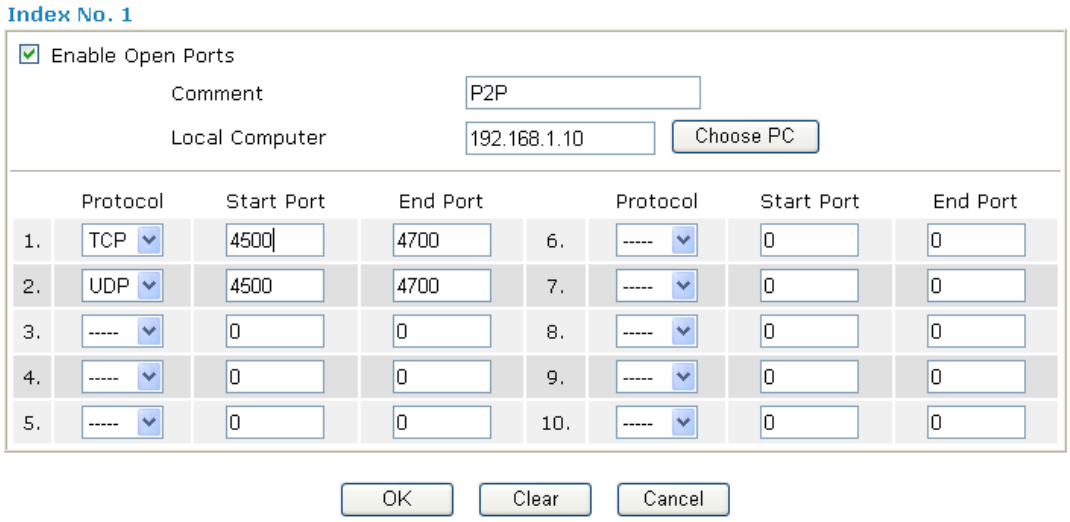
Click **Open Ports** to open the following page:



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.
Local IP Address	Display the private IP address of the local host offering the service.
Status	Display the state for the corresponding entry. X or V is to represent the **Inactive** or **Active** state.

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

NAT >> Open Ports >> Edit Open Ports



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.

4.4 Firewall

4.4.1 Basics for Firewall

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

Firewall Facilities

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

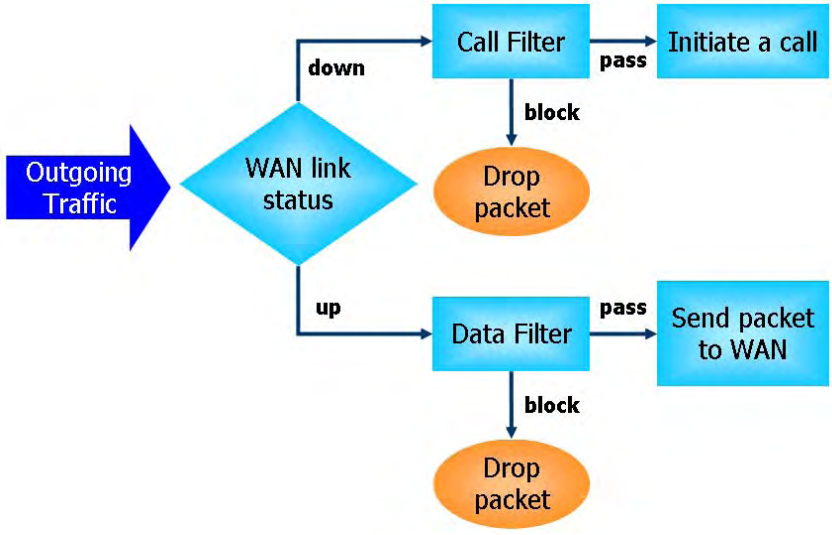
- User-configurable IP filter (Call Filter/ Data Filter).
- Stateful Packet Inspection (SPI): tracks packets and denies unsolicited incoming data
- Selectable Denial of Service (DoS) /Distributed DoS (DDoS) attacks protection

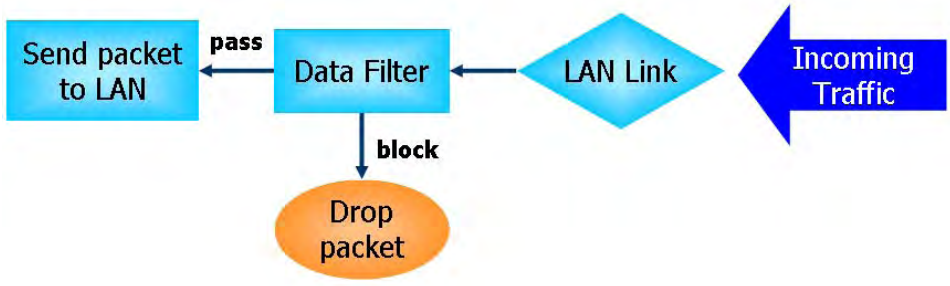
IP Filters

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

- **Call Filter -** When there is no existing Internet connection, **Call Filter** is applied to all traffic, all of which should be outgoing. It will check packets according to the filter rules. If legal, the packet will pass. Then the router shall **"initiate a call"** to build the Internet connection and send the packet to Internet.
- **Data Filter** - When there is an existing Internet connection, **Data Filter** is applied to incoming and outgoing traffic. It will check packets according to the filter rules. If legal, the packet will pass the router.

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





Stateful Packet Inspection (SPI)

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

Denial of Service (DoS) Defense

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

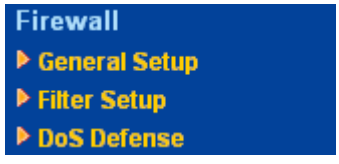
The **DoS Defense** function enables the Vigor router to inspect every incoming packet based on the attack signature database. Any malicious packet that might duplicate itself to paralyze the host in the secure LAN will be strictly blocked and a Syslog message will be sent as warning, if you set up Syslog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

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

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

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

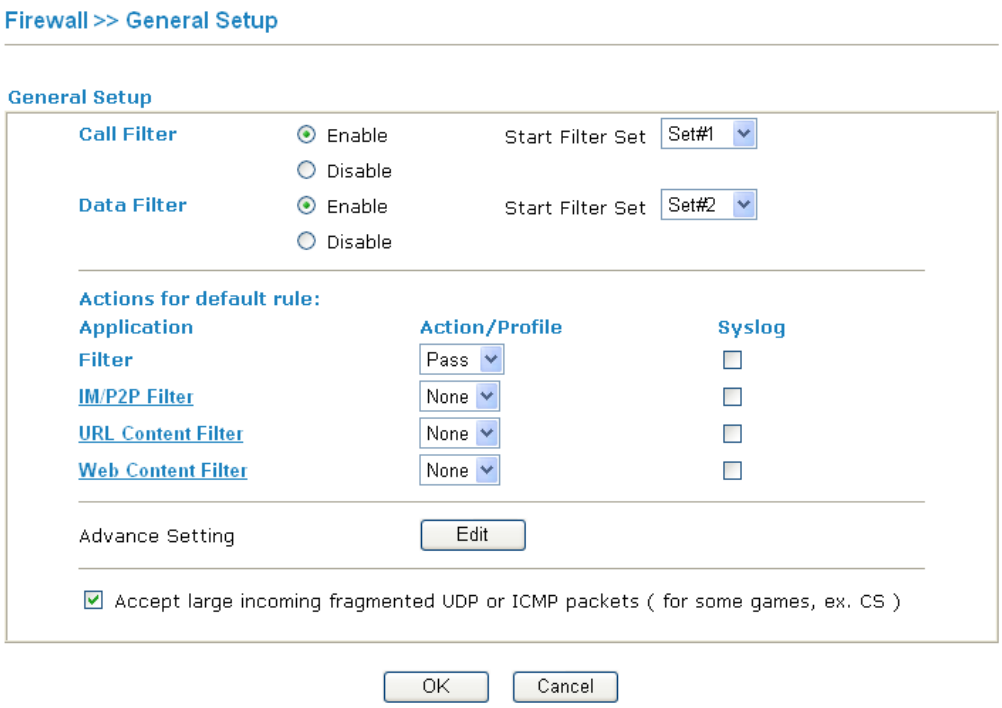
Below shows the menu items for Firewall.



4.4.2 General Setup

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

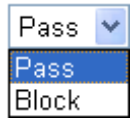
Click **Firewall** and click **General Setup** to open the general setup page.



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

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

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



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

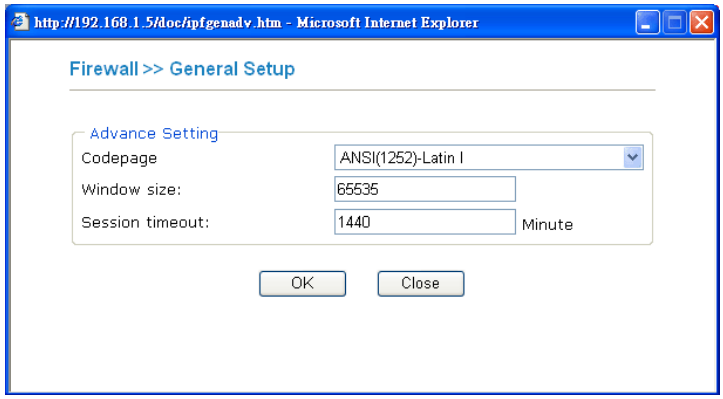
URL Content Filter — Select one of the **URL Content Filter** profile settings (created in **CSM>> URL Content Filter**) for applying with this router. Please set at least one profile for choosing in **CSM>> URL Content Filter** web page first. For troubleshooting needs, you can specify to record information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

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

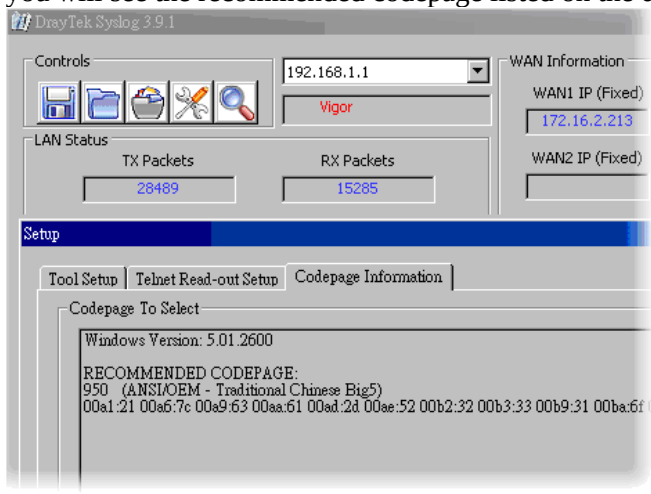
Web Content Filter Select one of the **Web Content Filter** profile settings (created in **CSM>> Web Content Filter**) for applying with this router. Please set at least one profile for anti-virus in **CSM>> Web Content Filter** web page first. For troubleshooting needs, you can specify to record information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

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

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



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



Window size – It determines the size of TCP protocol (0~65535). The more the value is, the better the performance will

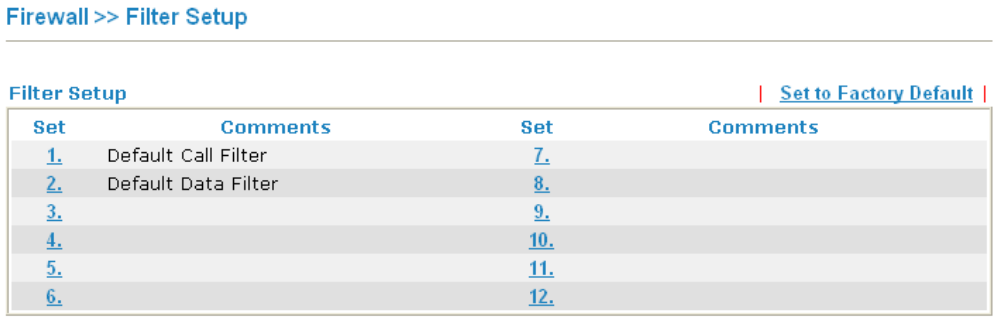
be. However, if the network is not stable, small value will be proper.

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

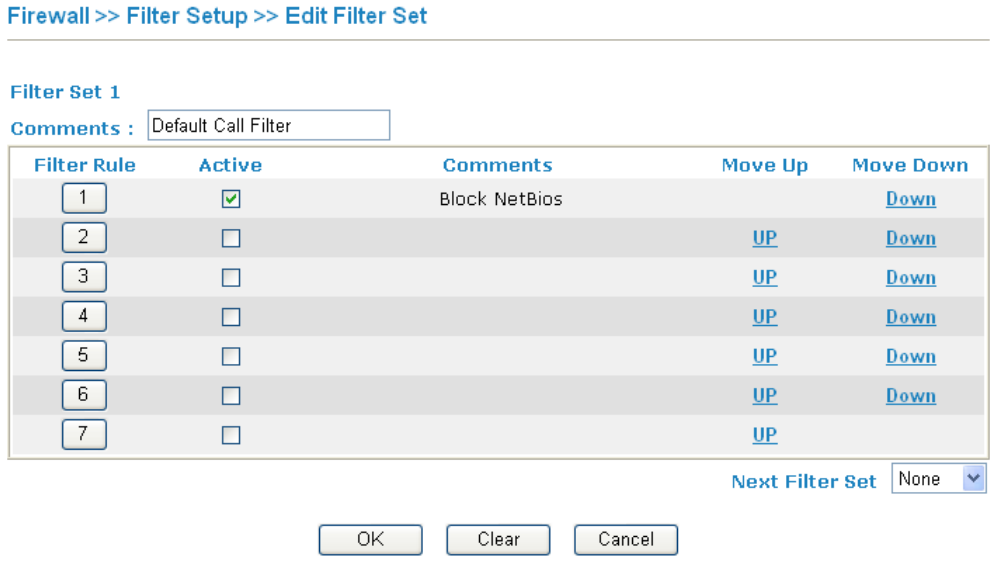
Some on-line games (for example: Half Life) will use lots of fragmented UDP packets to transfer game data. Instinctively as a secure firewall, Vigor router will reject these fragmented packets to prevent attack unless you enable "**Accept large incoming fragmented UDP or ICMP Packets**". By checking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

4.4.3 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.

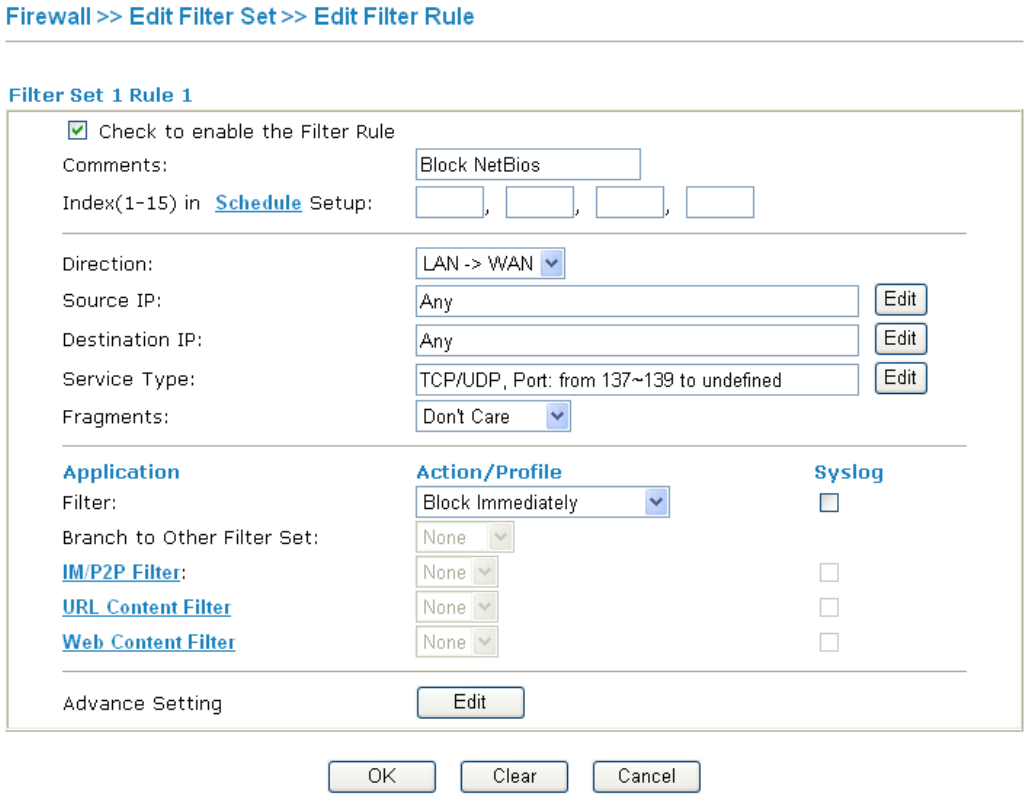


Filter Rule Click a button numbered (1 ~ 7) to edit the filter rule. Click the button will open Edit Filter Rule web page. For the detailed information, refer to the following page.

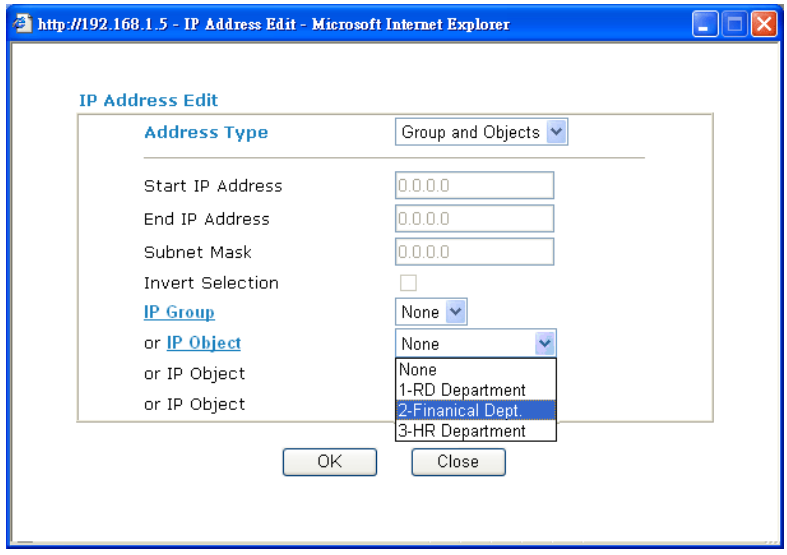
Active Enable or disable the filter rule.

Comment	Enter filter set comments/description. Maximum length is 23–character long.
Move Up/Down	Use **Up** or **Down** link to move the order of the filter rules.
Next Filter Set	Set the link to the next filter set to be executed after the current filter run. Do not make a loop with many filter sets.

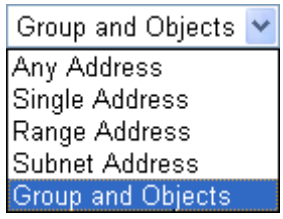
To edit **Filter Rule**, click the **Filter Rule** index button to enter the **Filter Rule** setup page.



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



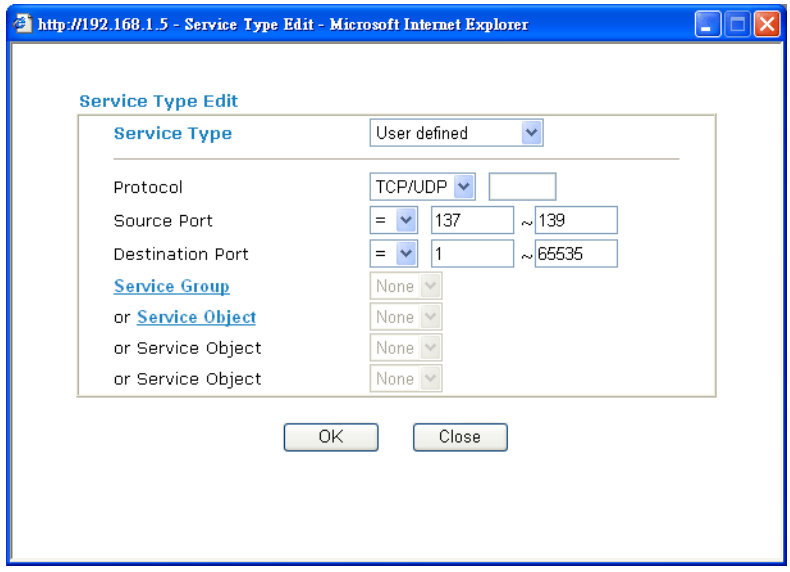
To set the IP address manually, please choose **Any Address/Single Address/Range Address/Subnet Address** as the Address Type and type them in this dialog. In addition, if you want to use the IP range from defined groups or objects, please choose **Group and Objects** as the Address Type.



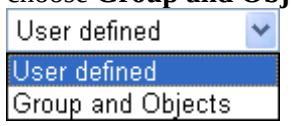
From the **IP Group** drop down list, choose the one that you want to apply. Or use the **IP Object** drop down list to choose the object that you want.

Service Type

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



To set the service type manually, please choose **User defined** as

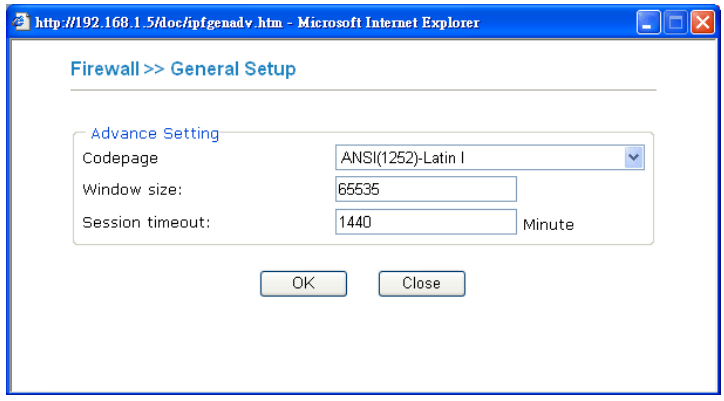
	the Service Type and type them in this dialog. In addition, if you want to use the service type from defined groups or objects, please choose **Group and Objects** as the Service Type.  **Protocol -** Specify the protocol(s) which this filter rule will apply to. **Source/Destination Port -** ***(=)*** – when the first and last value are the same, it indicates one port; when the first and last values are different, it indicates a range for the port and available for this service type. ***(!=)*** – when the first and last value are the same, it indicates all the ports except the port defined here; when the first and last values are different, it indicates that all the ports except the range defined here are available for this service type. ***(>)*** – the port number greater than this value is available. ***(<)*** – the port number less than this value is available for this profile. **Service Group/Object** - Use the drop down list to choose the one that you want.
Fragments	Specify the action for fragmented packets. And it is used for **Data Filter** only. ***Don't care*** -No action will be taken towards fragmented packets. ***Unfragmented*** -Apply the rule to unfragmented packets. ***Fragmented*** - Apply the rule to fragmented packets. ***Too Short*** - Apply the rule only to packets that are too short to contain a complete header.
Filter	Specifies the action to be taken when packets match the rule. **Block Immediately** - Packets matching the rule will be dropped immediately. **Pass Immediately** - Packets matching the rule will be passed immediately. **Block If No Further Match** - A packet matching the rule, and that does not match further rules, will be dropped. **Pass If No Further Match** - A packet matching the rule, and that does not match further rules, will be passed through.
Branch to other Filter Set	If the packet matches the filter rule, the next filter rule will branch to the specified filter set. Select next filter rule to branch from the drop-down menu. Be aware that the router will apply the specified filter rule for ever and will not return to previous filter rule any more.
IM/P2P Filter	Select a CSM profile for global IM/P2P application blocking. All the hosts in LAN must follow the standard configured in the CSM profile selected here. For detailed information, refer to the section of CSM profile setup. For troubleshooting needs, you can specify to record information for IM/P2P by checking the Log box. It will be sent to Syslog server. Please refer to section 3.12.5 **Syslog/Mail Alert** for more detailed information.
URL Content Filter	Select one of the **URL Content Filter** profile settings (created in **CSM>> URL Content Filter**) for applying with this router. Please set at least one profile for choosing in **CSM>> URL Content**

Filter web page first. For troubleshooting needs, you can specify to record information for **URL Content Filter** by checking the Log box. It will be sent to Syslog server. Please refer to section 3.12.5 **Syslog/Mail Alert** for more detailed information.

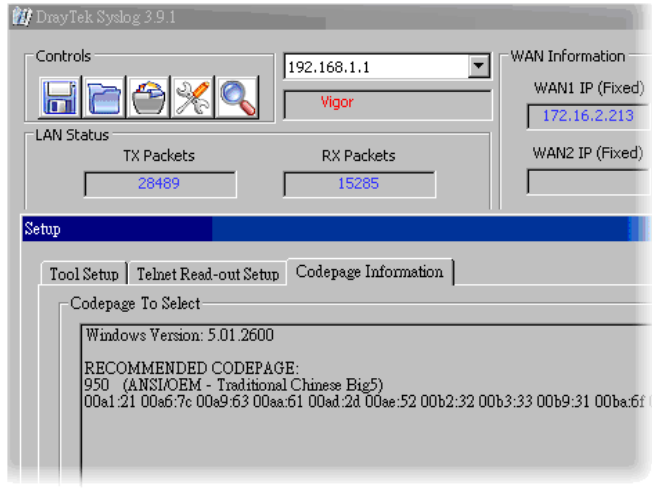
Web Content Filter Select one of the **Web Content Filter** profile settings (created in **CSM>> Web Content Filter**) for applying with this router. Please set at least one profile for anti-virus in **CSM>> Web Content Filter** web page first. For troubleshooting needs, you can specify to record information for **Web Content Filter** by checking the Log box. It will be sent to Syslog server. Please refer to section 3.12.5 **Syslog/Mail Alert** for more detailed information.

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

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



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

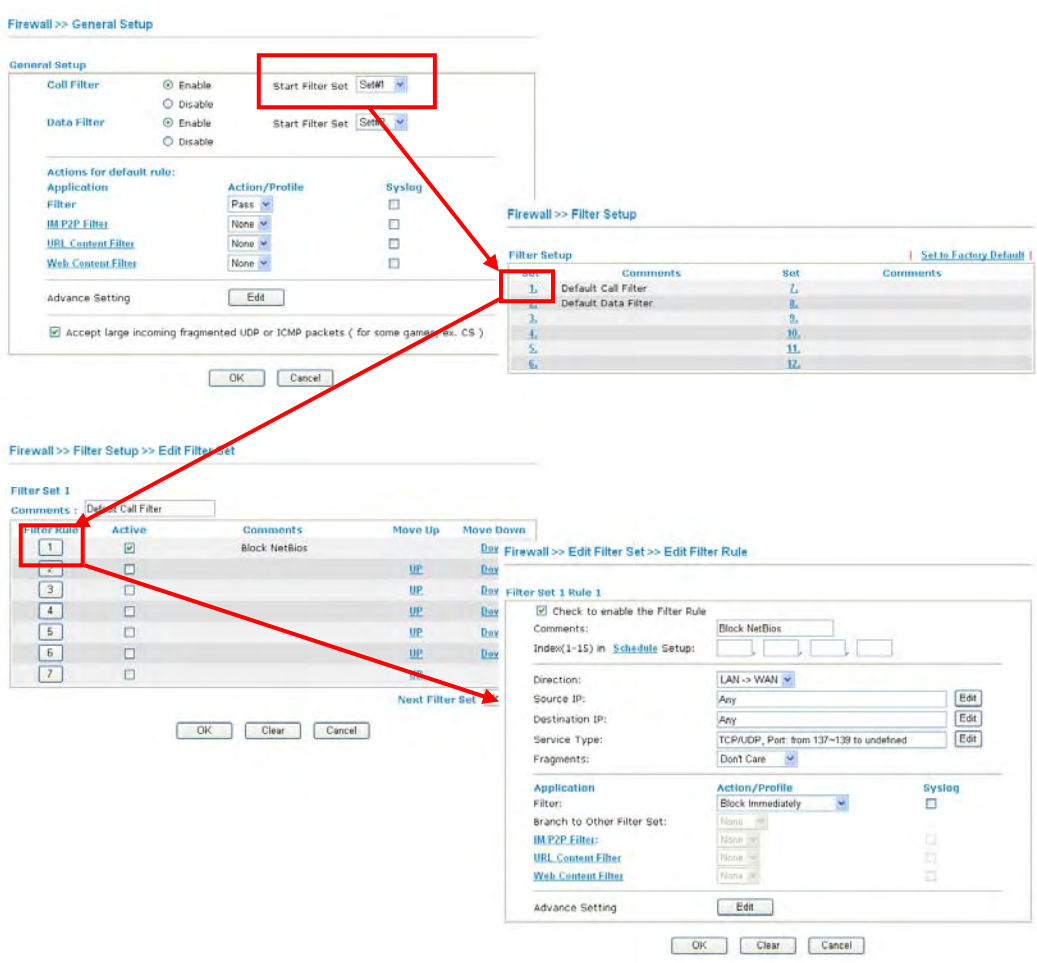


Window size – It determines the size of TCP protocol (0~65535). The more the value is, the better the performance will be. However, if the network is not stable, small value will be proper.

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

Example

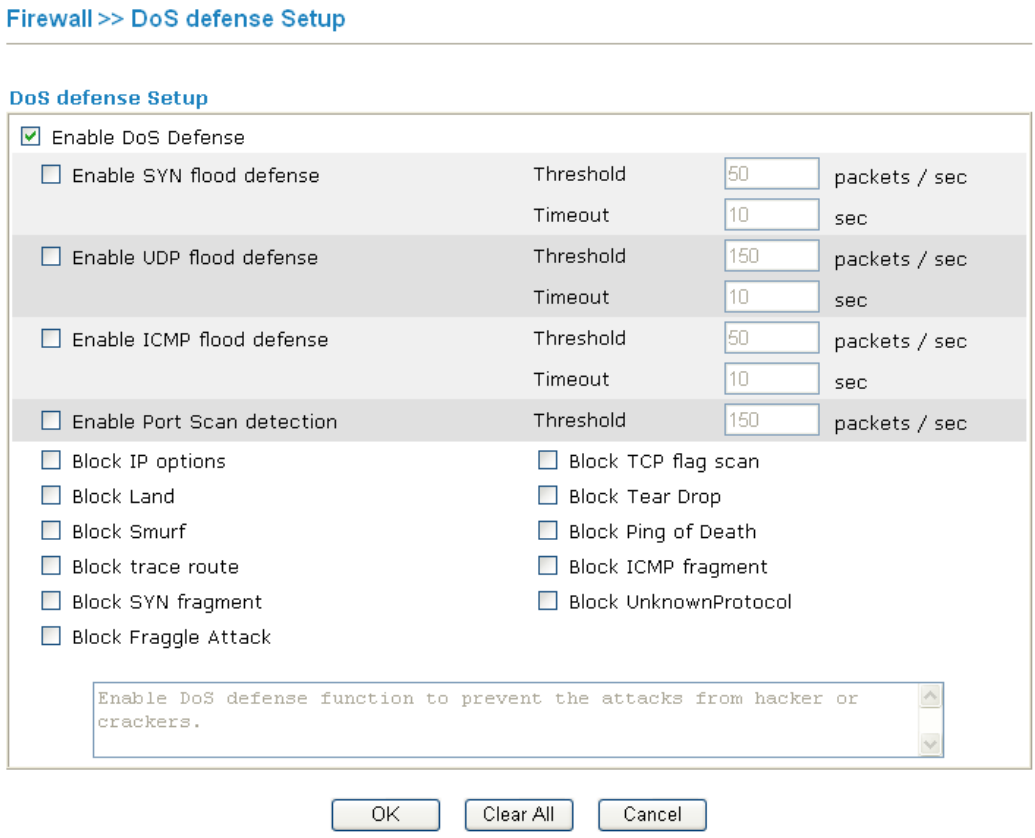
As stated before, all the traffic will be separated and arbitrated using on of two IP filters: call filter or data filter. You may preset 12 call filters and data filters in **Filter Setup** and even link them in a serial manner. Each filter set is composed by 7 filter rules, which can be further defined.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



4.4.4 DoS Defense

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

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



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

detection	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.

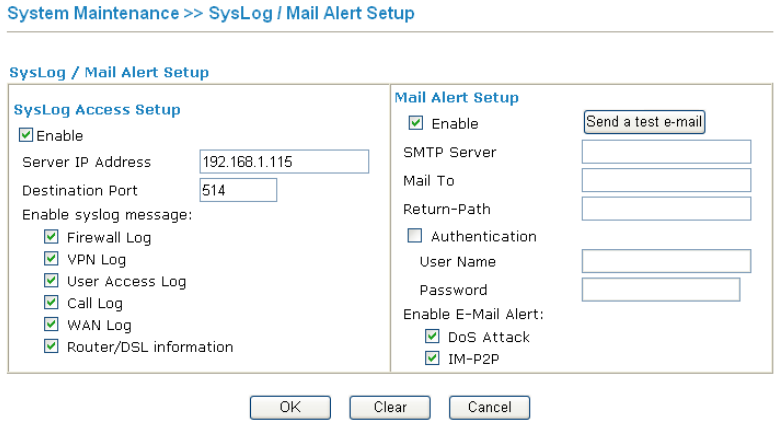
Block Unknown Protocol

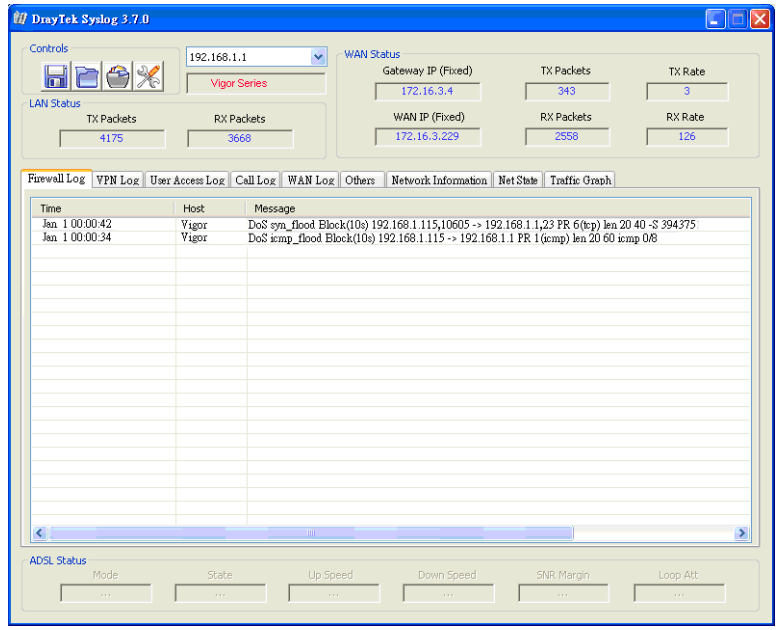
Check the box to activate the Block Unknown Protocol function. Individual IP packet has a protocol field in the datagram header to indicate the protocol type running over the upper layer. However, the protocol types greater than 100 are reserved and undefined at this time. Therefore, the router should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

Warning Messages

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

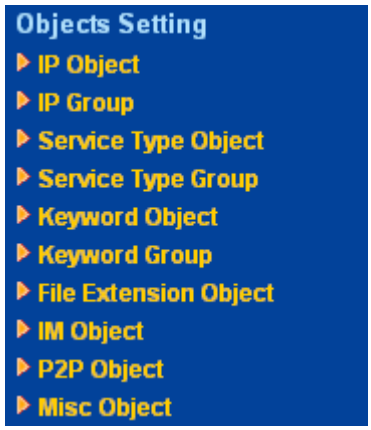
All the warning messages related to **DoS Defense** will be sent to user and user can review it through Syslog daemon. Look for the keyword **DoS** in the message, followed by a name to indicate what kind of attacks is detected.





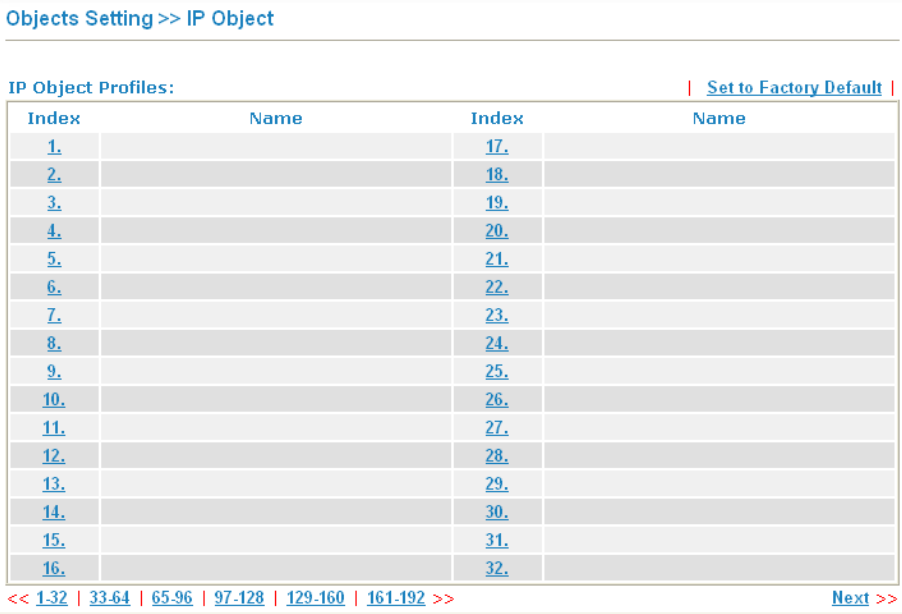
4.5 Objects Settings

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



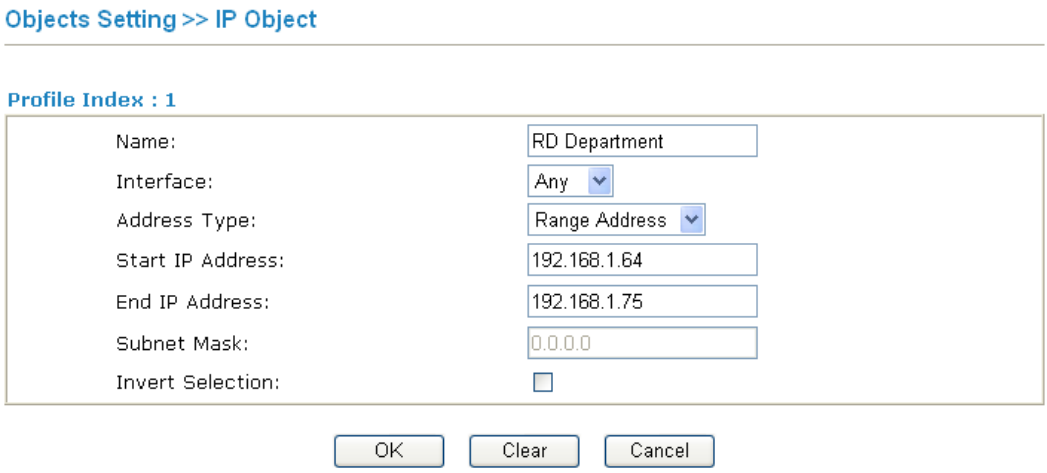
4.5.1 IP Object

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



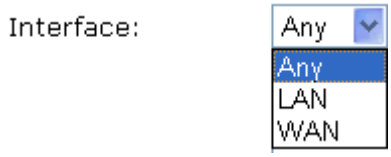
Set to Factory Default Clear all profiles.

Click the number under Index column for settings in detail.



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

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



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

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

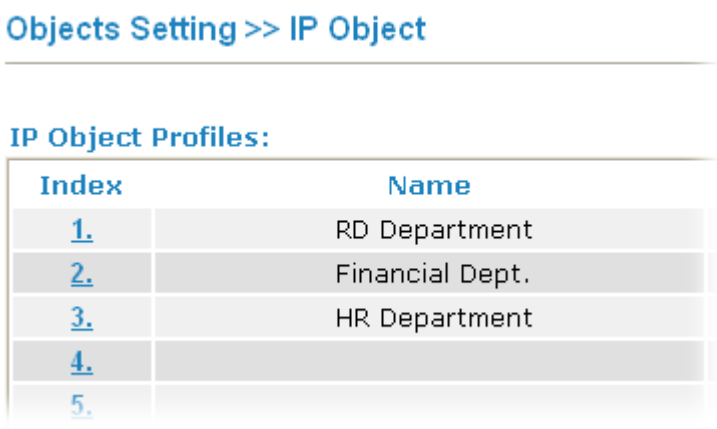
Start IP Address Type the start IP address for Single Address type.

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

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

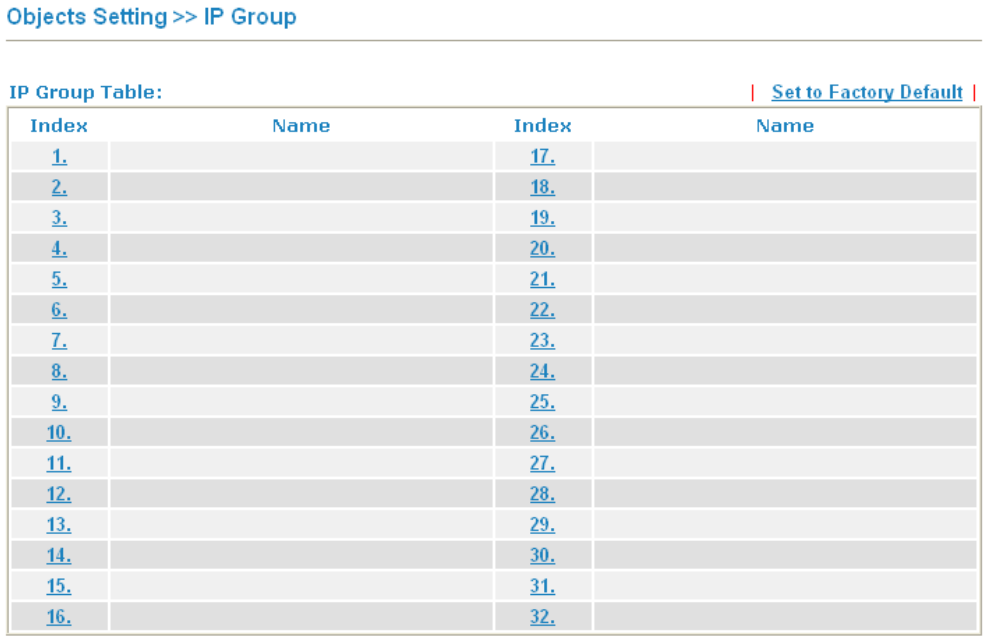
Invert Selection If it is checked, all the IP addresses except the ones listed above will be applied later while it is chosen.

Below is an example of IP objects settings.



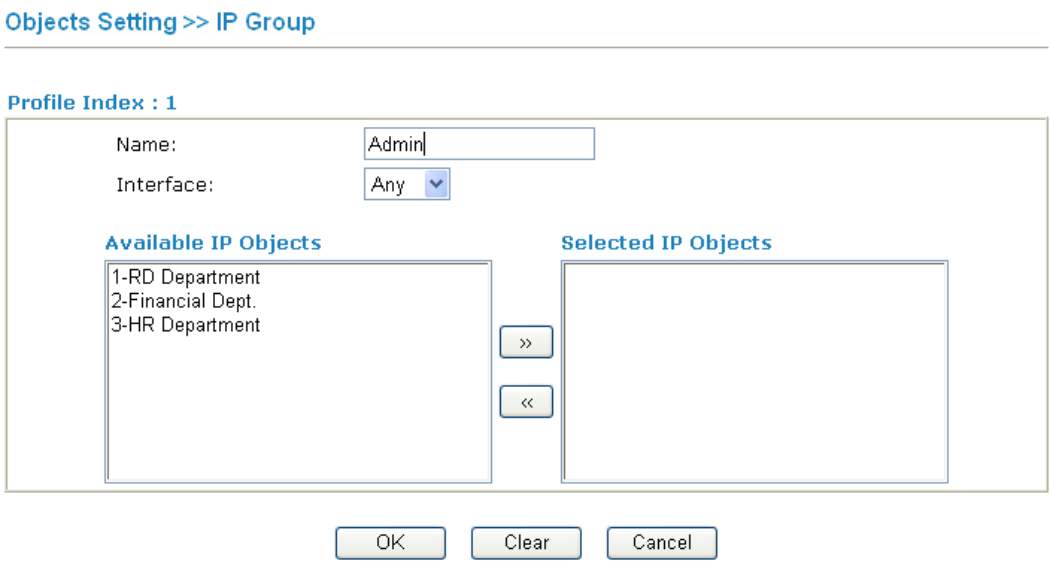
4.5.2 IP Group

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



Set to Factory Default Clear all profiles.

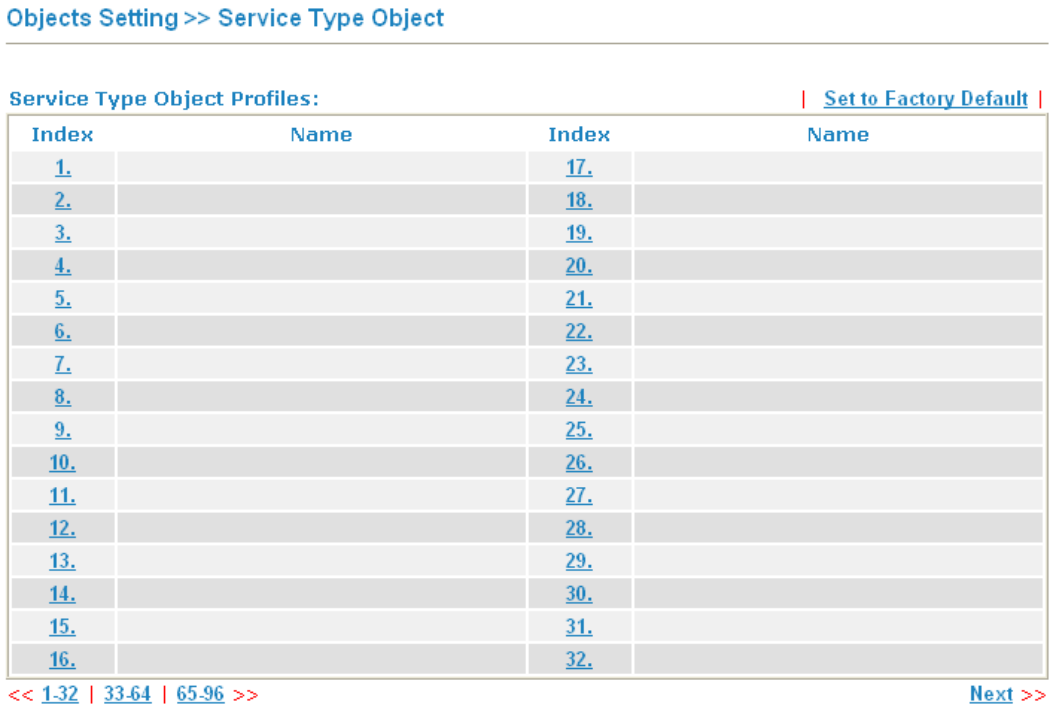
Click the number under Index column for settings in detail.



Name	Type a name for this profile. Maximum 15 characters are allowed.
Interface	Choose WAN, LAN or Any to display all the available IP objects with the specified interface.
Available IP Objects	All the available IP objects with the specified interface chosen above will be shown in this box.
Selected IP Objects	Click >> button to add the selected IP objects in this box.

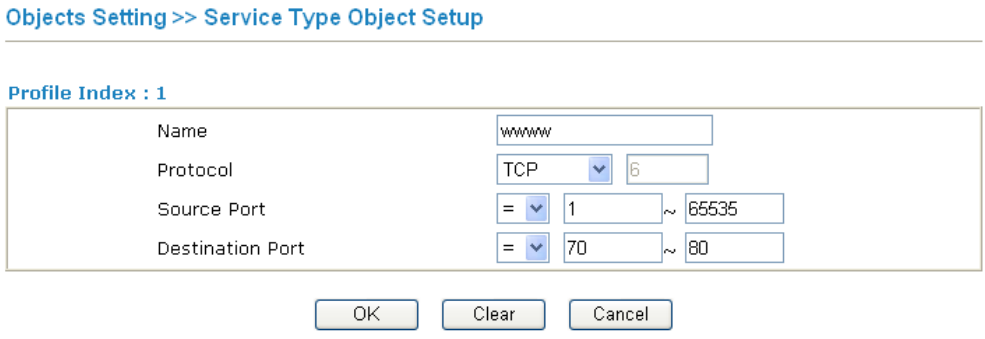
4.5.3 Service Type Object

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



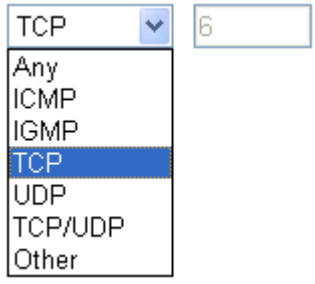
Set to Factory Default Clear all profiles.

Click the number under Index column for settings in detail.



Name Type a name for this profile.

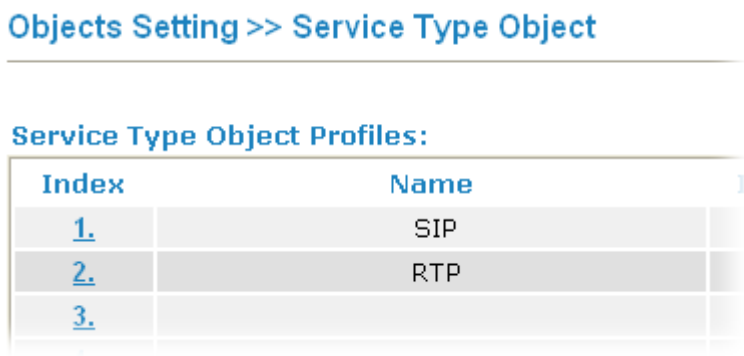
Protocol Specify the protocol(s) which this profile will apply to.



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

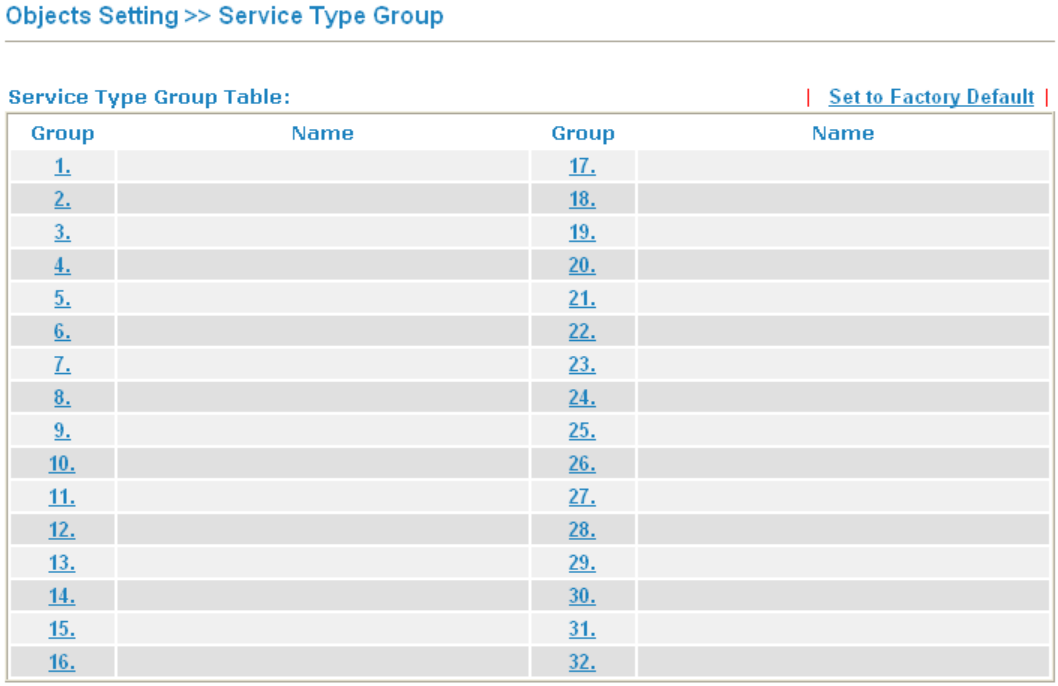
(=) – when the first and last value are the same, it indicates one port; when the first and last values are different, it indicates a range for the port and available for this profile.
(!=) – when the first and last value are the same, it indicates all the ports except the port defined here; when the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

Below is an example of service type objects settings.



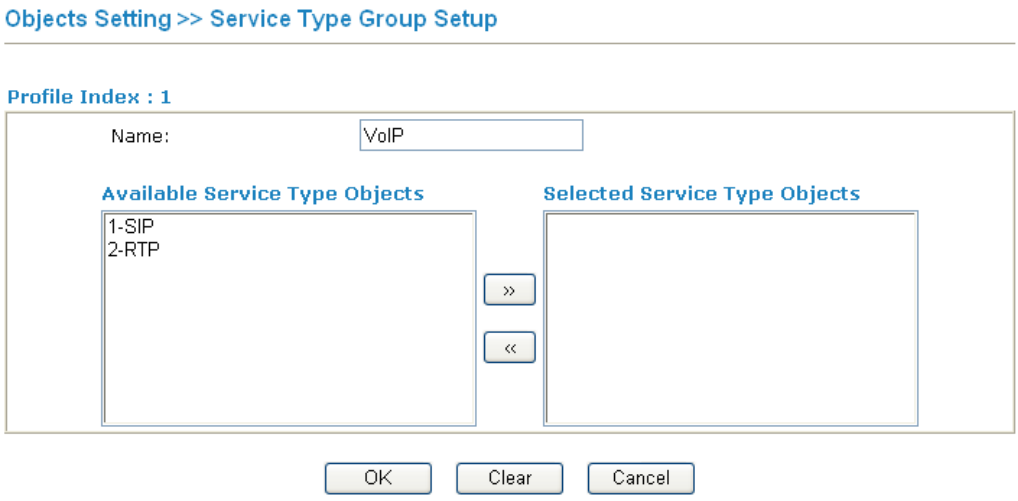
4.5.4 Service Type Group

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



Set to Factory Default Clear all profiles.

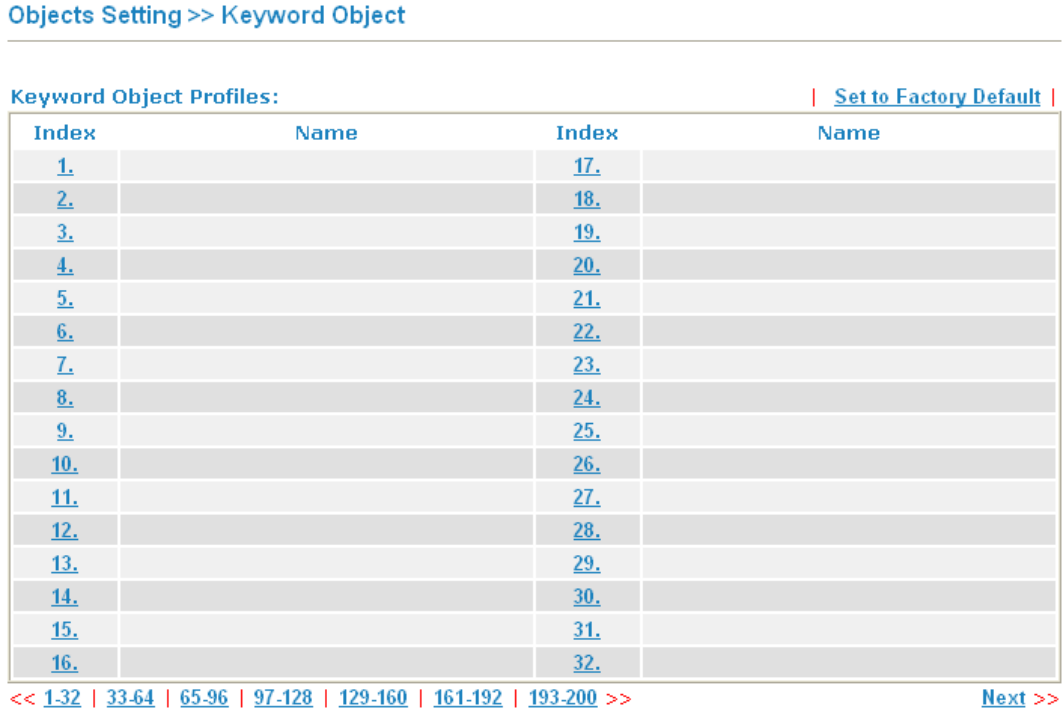
Click the number under Index column for settings in detail.



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

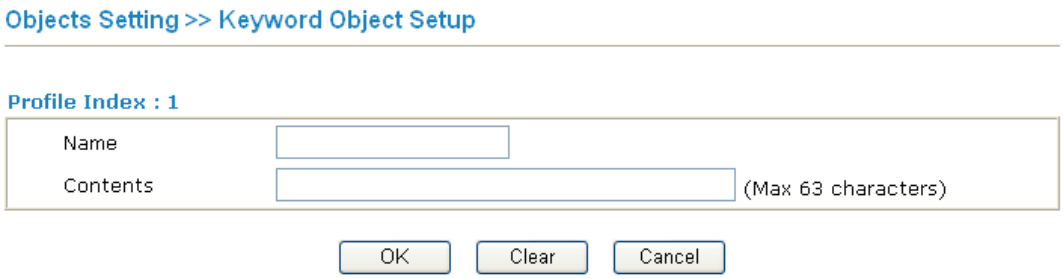
4.5.5 Keyword Object

You can set 200 keyword object profiles for choosing as black /white list in **CSM >>URL Web Content Filter Profile.**



Set to Factory Default	Clear all profiles.

Click the number under Index column for setting in detail.

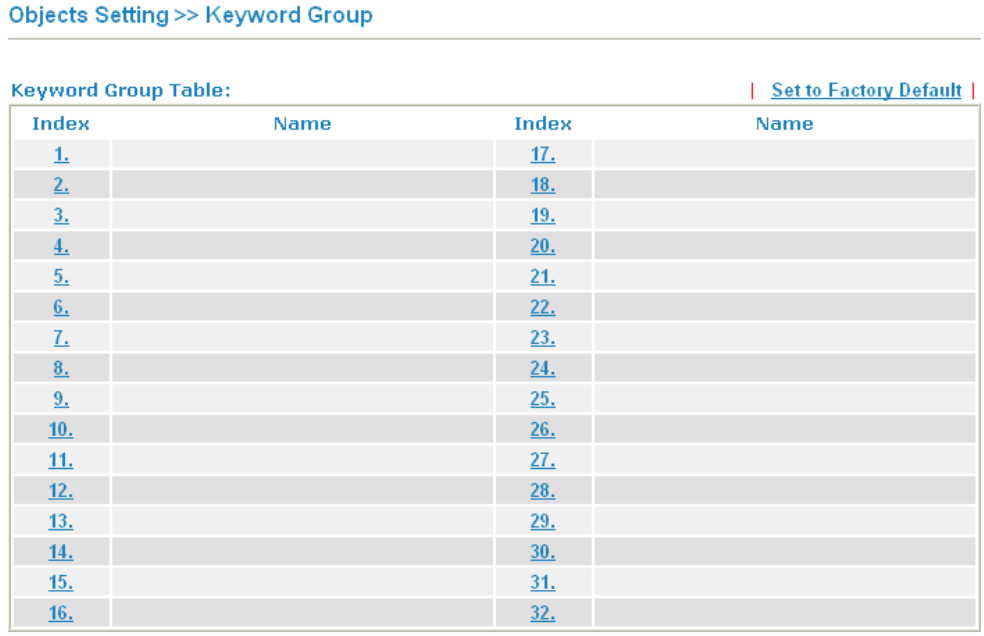


Name Type a name for this profile, e.g., game.

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

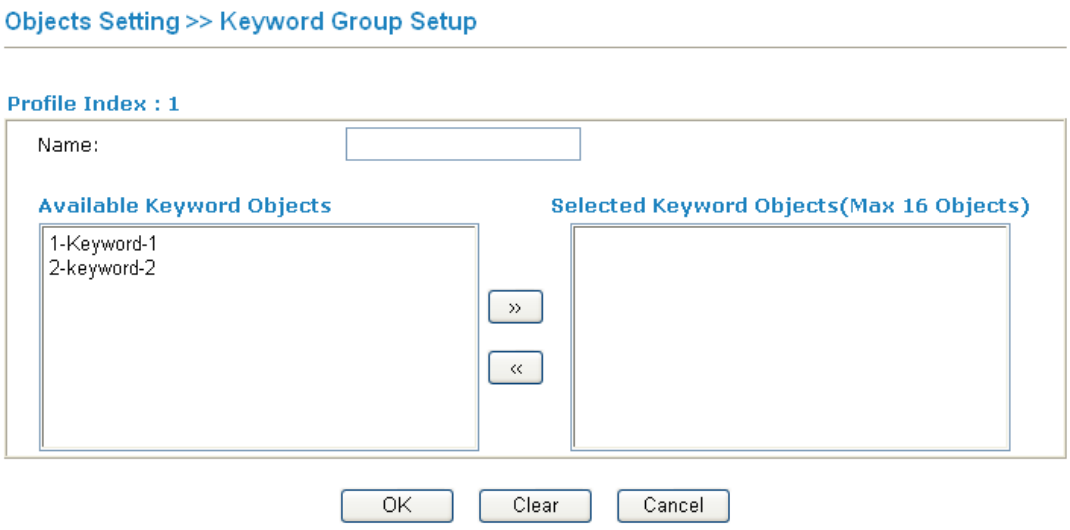
4.5.6 Keyword Group

This page allows you to bind several keyword objects into one group. The keyword groups set here will be chosen as black /white list in **CSM >>URL Web Content Filter Profile**.



Set to Factory Default Clear all profiles.

Click the number under Index column for setting in detail.



Name Type a name for this group.

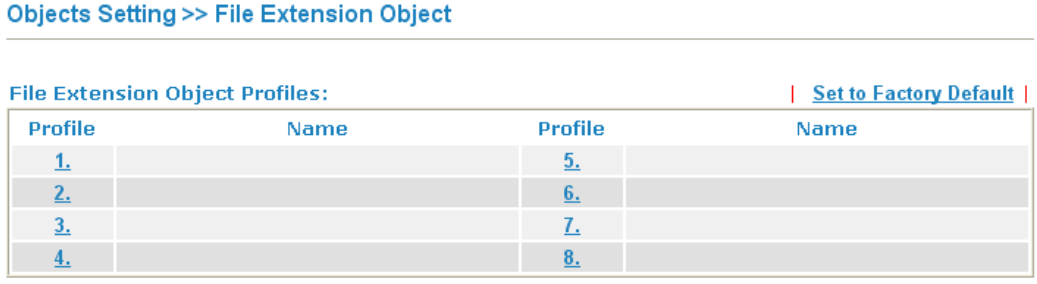
Available Keyword Objects You can gather keyword objects from Keyword Object page within one keyword group. All the available Keyword objects that you have created will be shown in this box.

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

4.5.7 File Extension Object

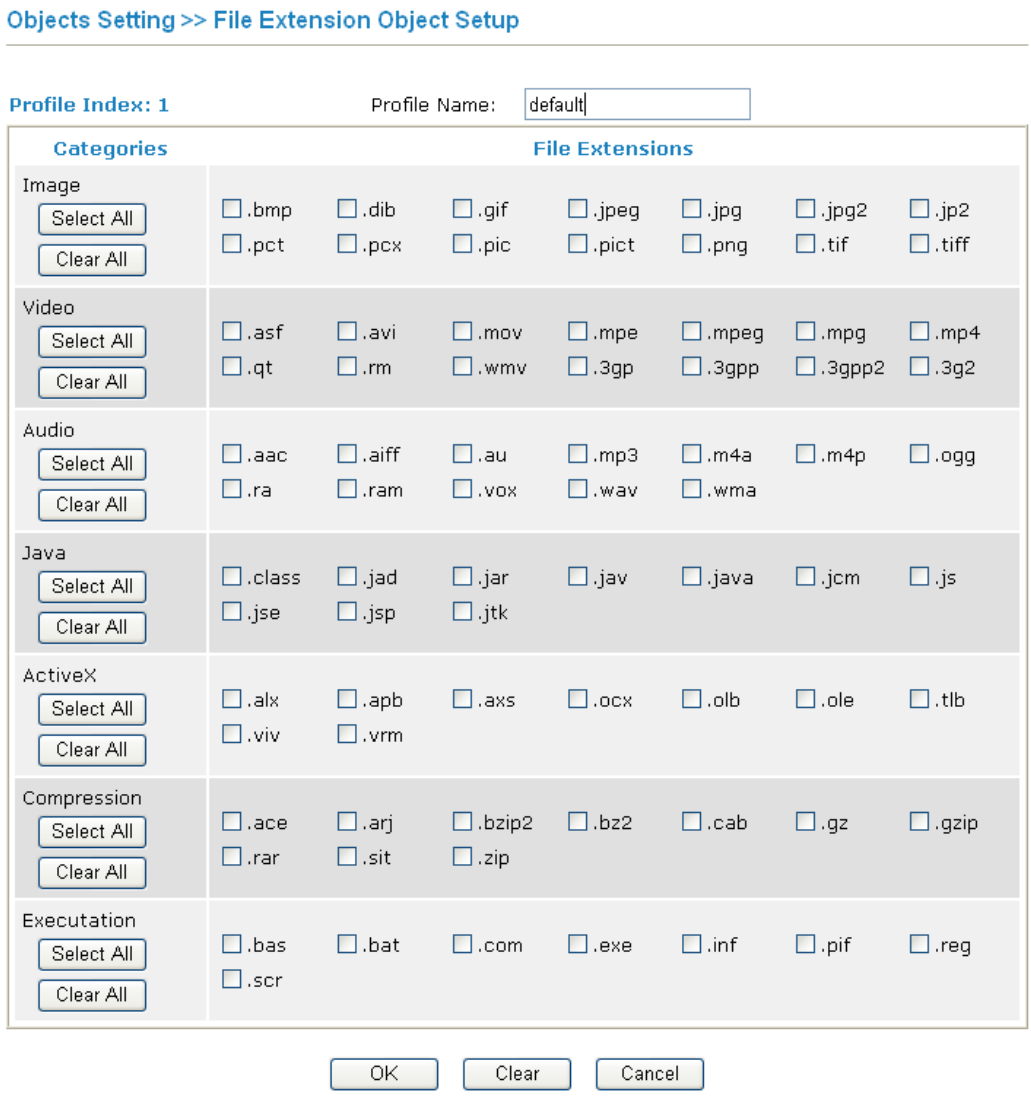
This page allows you to set eight profiles which will be applied in **CSM>>URL Content Filter**. All the files with the extension names specified in these profiles will be processed according to the chosen action.

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



Set to Factory Default Clear all profiles.

Click the number under Profile column for configuration in details.

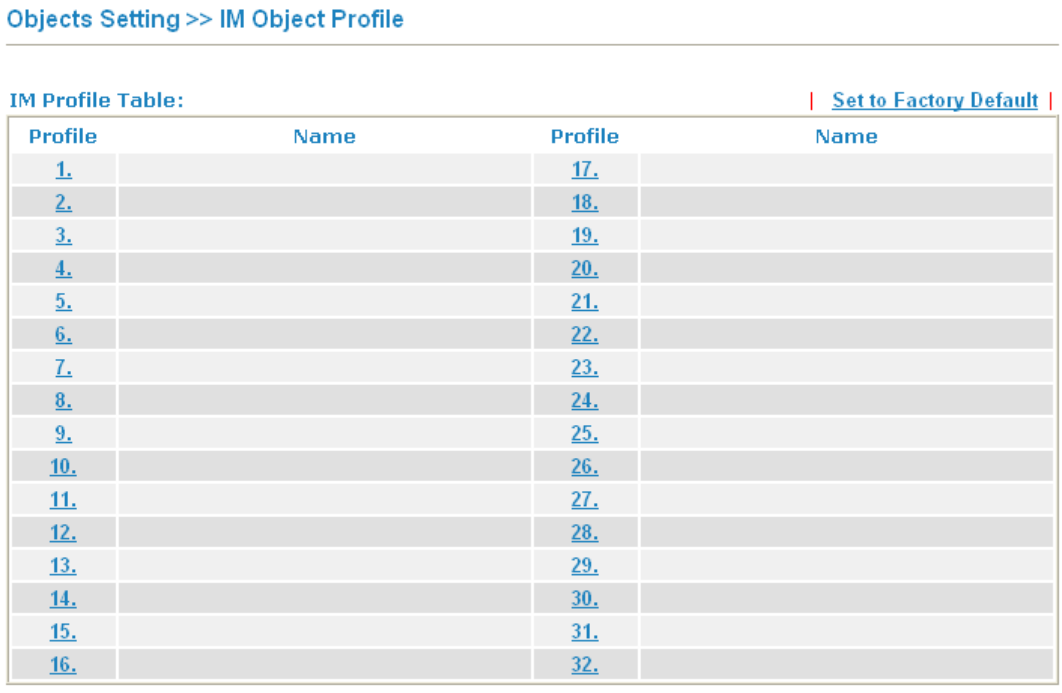


Profile Name Type a name for this profile.

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

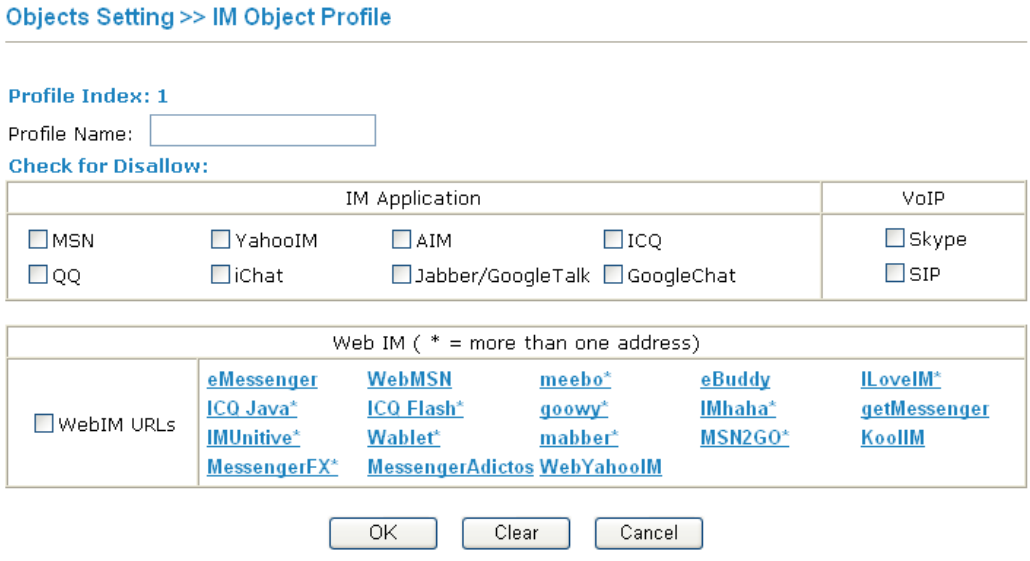
4.5.8 IM Object

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



Set to Factory Default Clear all profiles.

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

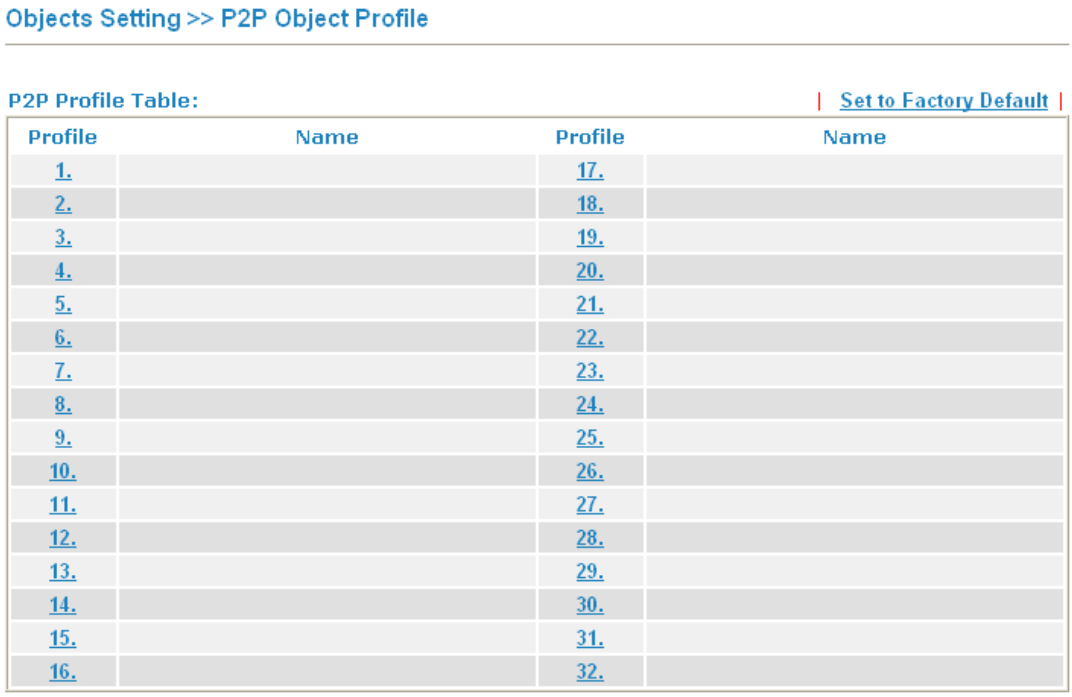


Profile Name Type a name for this profile.

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

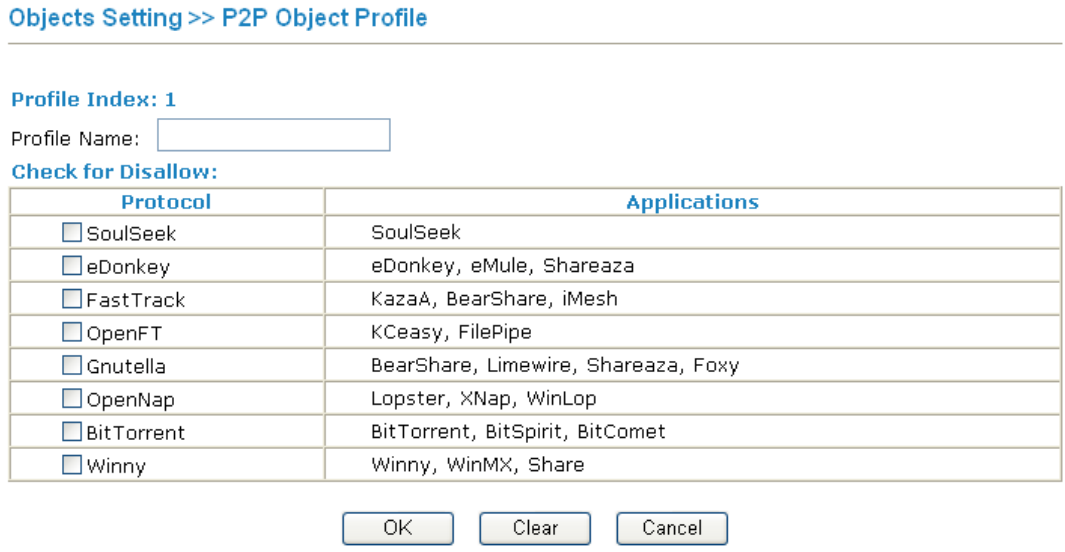
4.5.9 P2P Object

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



Set to Factory Default Clear all profiles.

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

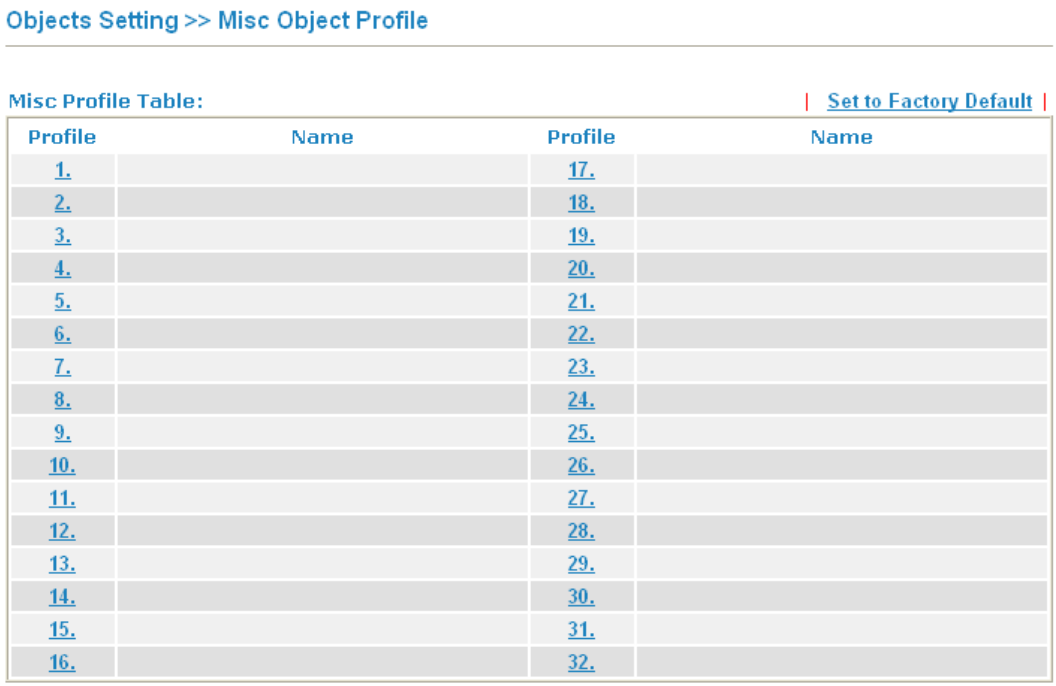


Profile Name Type a name for this profile.

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

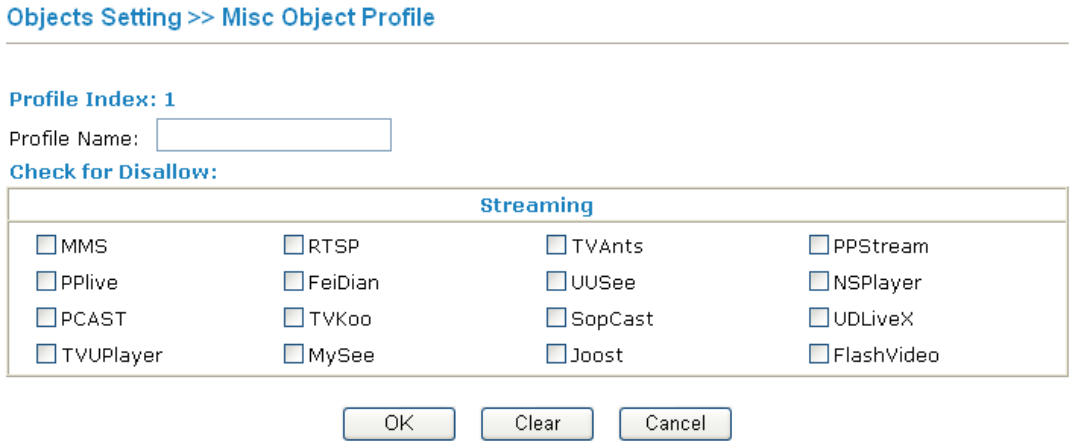
4.5.10 Misc Object

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



Set to Factory Default Clear all profiles.

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



Profile Name Type a name for this profile.

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

4.6 CSM Profile

Content Security Management (CSM)

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

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 CSM functionality.

IM/P2P Filter

As the popularity of all kinds of instant messenger application arises, communication cannot become much easier. Nevertheless, while some industry may leverage this as a great tool to connect with their customers, some industry may take reserve attitude in order to reduce employee 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 CSM functionality.

URL Content Filter

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

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

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

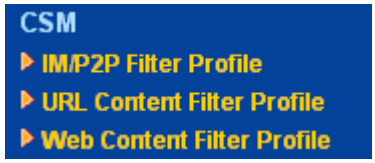
Web Content Filter

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

Once you have activated your Web Filtering service in Vigor router and chosen the categories of website you wish to restrict, each URL address requested (e.g.www.bbc.co.uk) will be

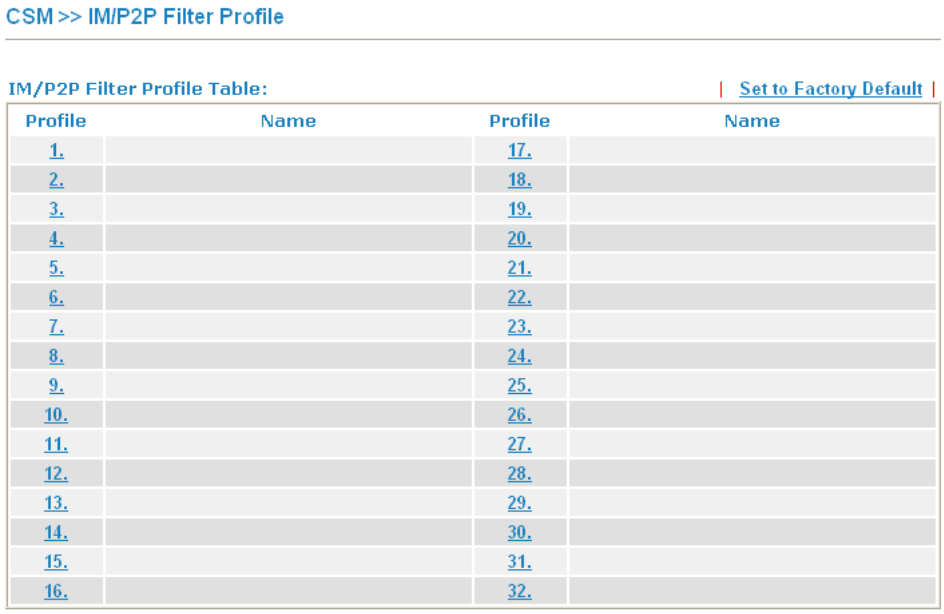
checked against our server database. This database is updated as frequent as daily by a global team of Internet researchers. The server will look up the URL and return a category to your router. Your Vigor router will then decide whether to allow access to this site according to the categories you have selected. Please note that this action will not introduce any delay in your Web surfing because each of multiple load balanced database servers can handle millions of requests for categorization.

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



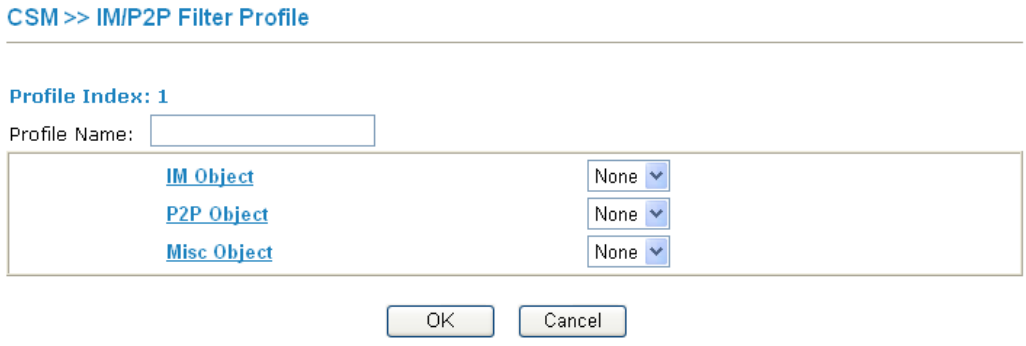
4.6.1 IM/P2P Filter Profile

You can define policy profiles for different policy of IM (Instant Messenger)/P2P (Peer to Peer) application. CSM profile can be used in Filter Setup page.



Set to Factory Default Clear all profiles.

Click the number under Index column for settings in detail.



Profile Name Type a name for the CSM profile.

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

4.6.2 URL Content Filter Profile

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

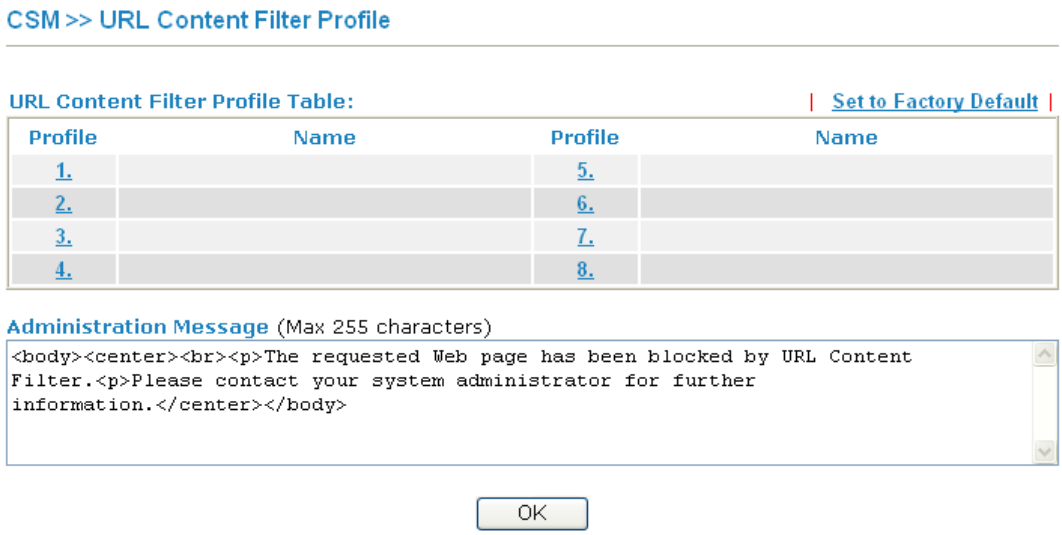
Once a user type in or click on an URL with objectionable keywords, URL keyword blocking facility will decline the HTTP request to that web page thus can limit user's access to the website. You may imagine **URL Content Filter** as a well-trained convenience-store clerk who won't sell adult magazines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

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

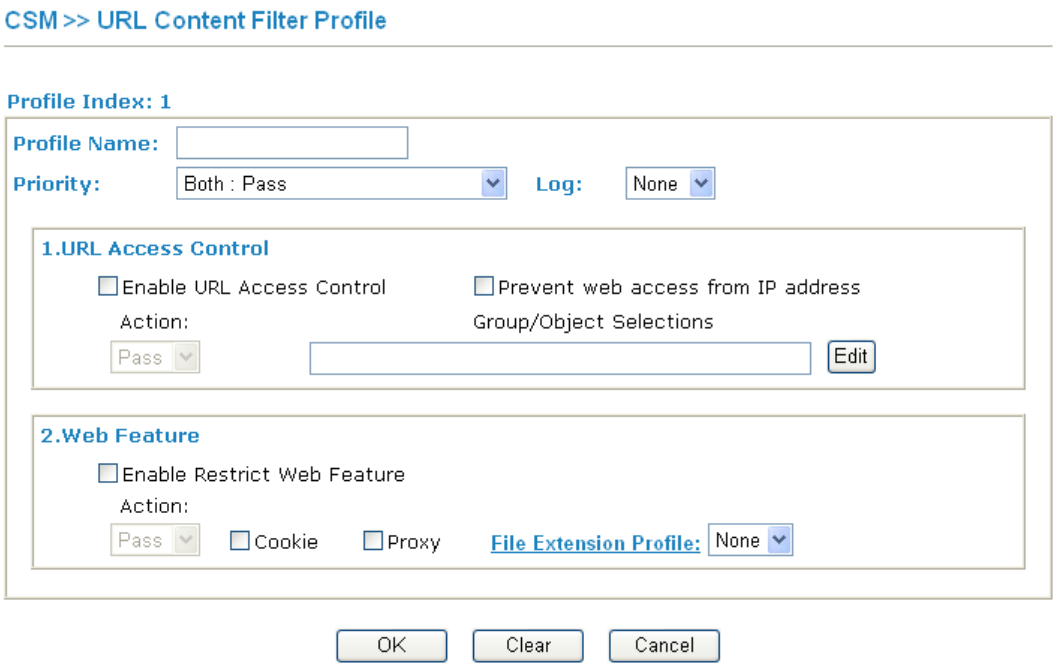
For example, if you add key words such as "sex", Vigor router will limit web access to web sites or web pages such as "www.sex.com", "www.backdoor.net/images/sex/p_386.html". Or you may simply specify the full or partial URL such as "www.sex.com" or "sex.com".

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

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

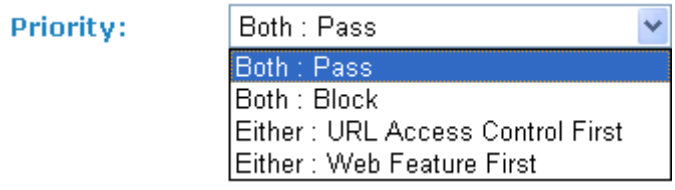


You can set eight profiles as URL content filter. Simply click the index number under Profile to open the following web page.



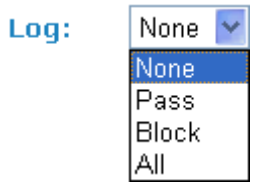
Profile Name Type the name for such profile.

Priority It determines the action that this router will apply.
Both: Pass – The router will let all the packages that match with the conditions specified in URL Access Control and Web Feature below passing through. When you choose this setting, both configuration set in this page for URL Access Control and Web Feature will be inactive.
Both:Block –The router will block all the packages that match with the conditions specified in URL Access Control and Web Feature below. When you choose this setting, both configuration set in this page for URL Access Control and Web Feature will be inactive.
Either: URL Access Control First – When all the packages matching with the conditions specified in URL Access Control and Web Feature below, such function can determine the priority for the actions executed. For this one, the router will process the packages with the conditions set below for URL first, then Web feature second.
Either: Web Feature First –When all the packages matching with the conditions specified in URL Access Control and Web Feature below, such function can determine the priority for the actions executed. For this one, the router will process the packages with the conditions set below for web feature first, then URL second.



Log **None** – There is no log file will be recorded for this profile.
Pass – Only the log about Pass will be recorded in Syslog.
Block – Only the log about Block will be recorded in Syslog.

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



URL Access Control

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

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

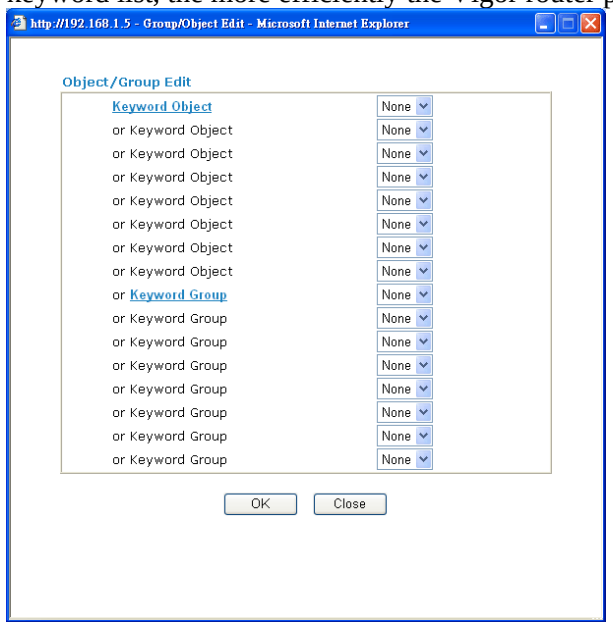
Action – This setting is available only when **Either : URL Access Control First** or **Either : Web Feature First** is selected. ***Pass*** - Allow accessing into the corresponding webpage with the keywords listed on the box below.

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

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

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

keyword list, the more efficiently the Vigor router perform.



Web Feature

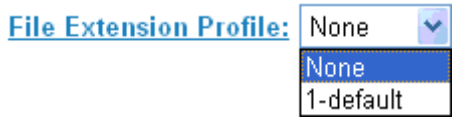
Enable Restrict Web Feature - Check this box to make the keyword being blocked or passed.

Action - This setting is available only when **Either : URL Access Control First** or **Either : Web Feature Firs** is selected. **Pass** allows accessing into the corresponding webpage with the keywords listed on the box below.
***Pass* -** Allow accessing into the corresponding webpage with the keywords listed on the box below.
***Block* -** Restrict accessing into the corresponding webpage with the keywords listed on the box below.
If the web pages do not match with the specified feature set here, it will be processed with reverse action.

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

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

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

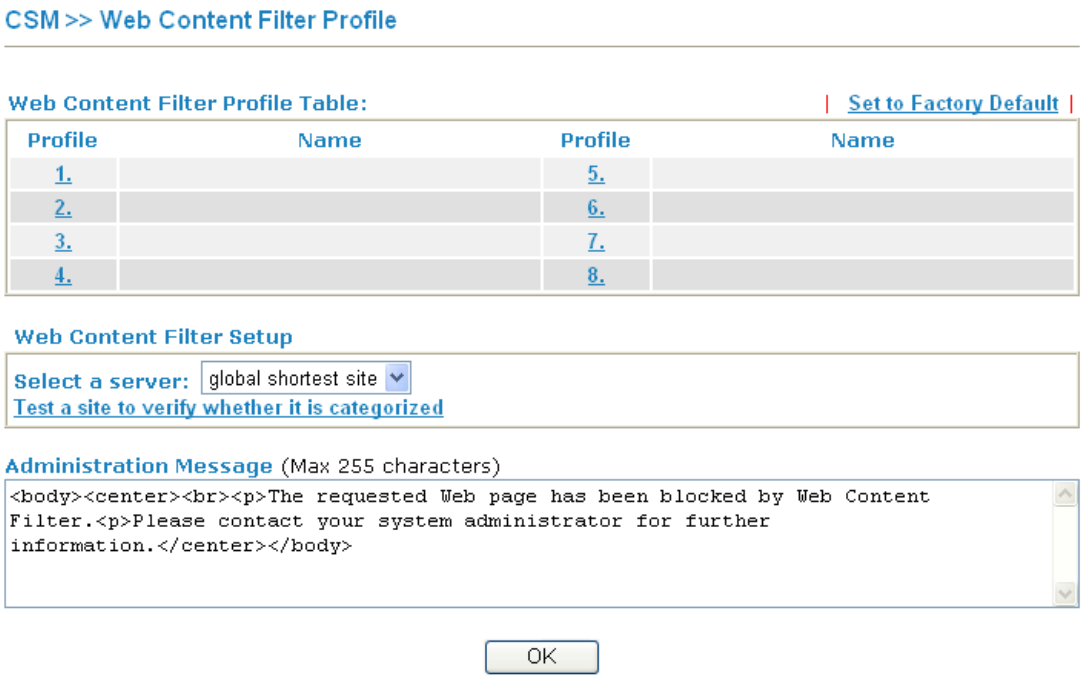


4.6.3 Web Content Filter Profile

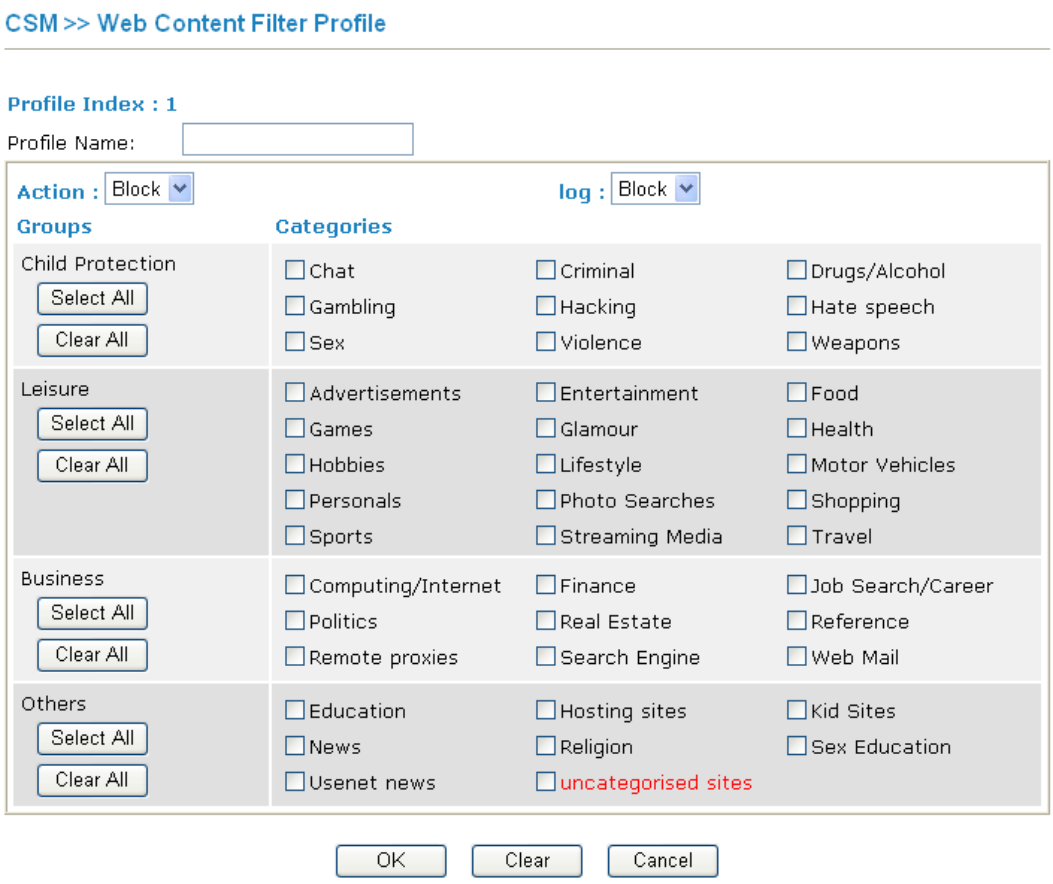
We all know that the content on the Internet just like other types of media may be inappropriate sometimes. As a responsible parent or employer, you should protect those in your trust against the hazards. With Web filtering service of the Vigor router, you can protect your business from common primary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

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

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



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

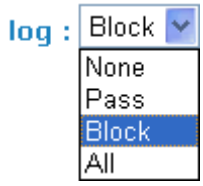


Action

Pass - allow accessing into the corresponding webpage with the categories listed on the box below.
Block - restrict accessing into the corresponding webpage with the categories listed on the box below.
If the web pages do not match with the specified feature set here, it will be processed with reverse action.

Log

None – There is no log file will be recorded for this profile.
Pass – Only the log about Pass will be recorded in Syslog.
Block – Only the log about Block will be recorded in Syslog.
All – All the actions (Pass and Block) will be recorded in Syslog.



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

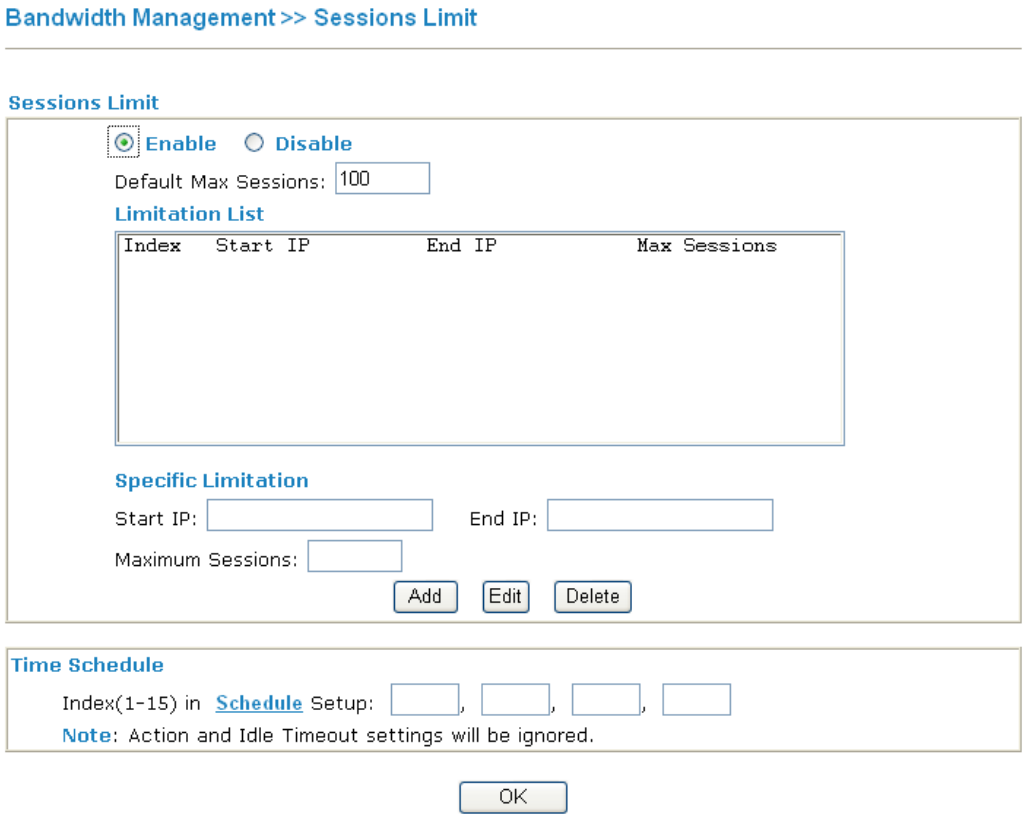
4.7 Bandwidth Management

Below shows the menu items for Bandwidth Management.

4.7.1 Sessions Limit

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

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



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

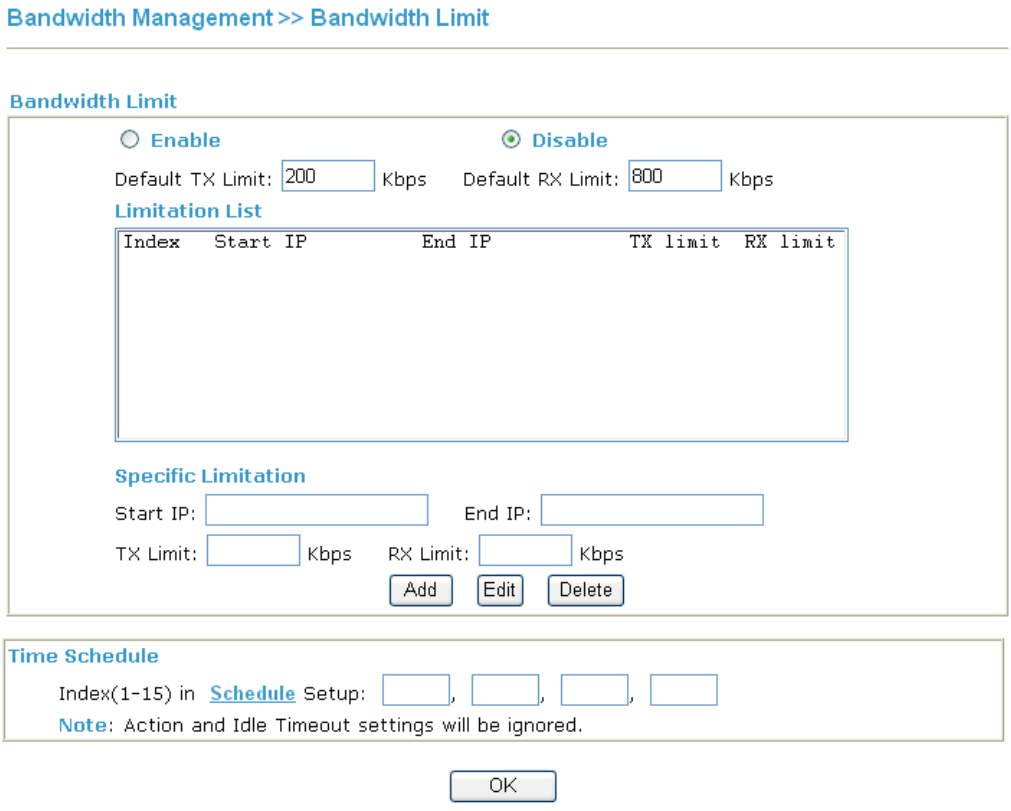
Enable	Click this button to activate the function of limit session.
Disable	Click this button to close the function of limit session.
Default session limit	Defines the default session number used for each computer in LAN.
Limitation List	Displays a list of specific limitations that you set on this web page.
Start IP	Defines the start IP address for limit session.
End IP	Defines the end IP address for limit session.

Maximum Sessions	Defines the available session number for each host in the specific range of IP addresses. If you do not set the session number in this field, the system will use the default session limit for the specific limitation you set for each index.
Add	Adds the specific session limitation onto the list above.
Edit	Allows you to edit the settings for the selected limitation.
Remove	Remove the selected settings existing on the limitation list.
Index (1-15) in Schedule Setup	You can type in four sets of time schedule for your request. All the schedules can be set previously in **Application – Schedule** web page and you can use the number that you have set in that web page.

4.7.2 Bandwidth Limit

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

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



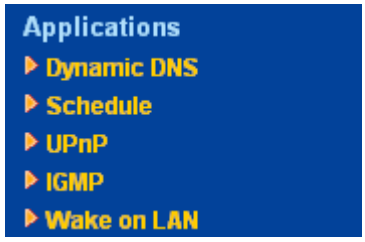
To activate the function of limit bandwidth, simply click **Enable** and set the default upstream and downstream limit.

Enable	Click this button to activate the function of limit bandwidth.
Disable	Click this button to close the function of limit bandwidth.
Default TX limit	Define the default speed of the upstream for each computer in LAN.
Default RX limit	Define the default speed of the downstream for each computer in LAN.

Limitation List	Display a list of specific limitations that you set on this web page.
Start IP	Define the start IP address for limit bandwidth.
End IP	Define the end IP address for limit bandwidth.
TX limit	Define the limitation for the speed of the upstream. If you do not set the limit in this field, the system will use the default speed for the specific limitation you set for each index.
RX limit	Define the limitation for the speed of the downstream. If you do not set the limit in this field, the system will use the default speed for the specific limitation you set for each index.
Add	Add the specific speed limitation onto the list above.
Edit	Allows you to edit the settings for the selected limitation.
Delete	Remove the selected settings existing on the limitation list.
Index (1-15) in Schedule Setup	You can type in four sets of time schedule for your request. All the schedules can be set previously in **Application – Schedule** web page and you can use the number that you have set in that web page.

4.8 Applications

Below shows the menu items for Applications.



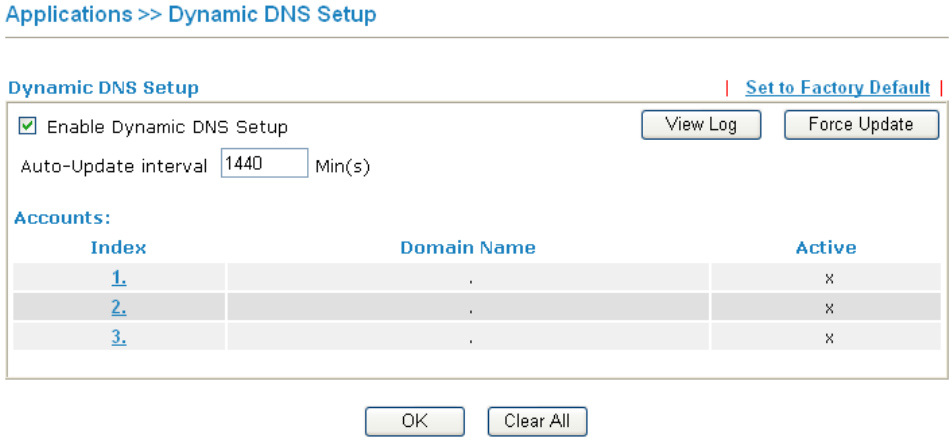
4.8.1 Dynamic DNS

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

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

Enable the Function and Add a Dynamic DNS Account

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



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

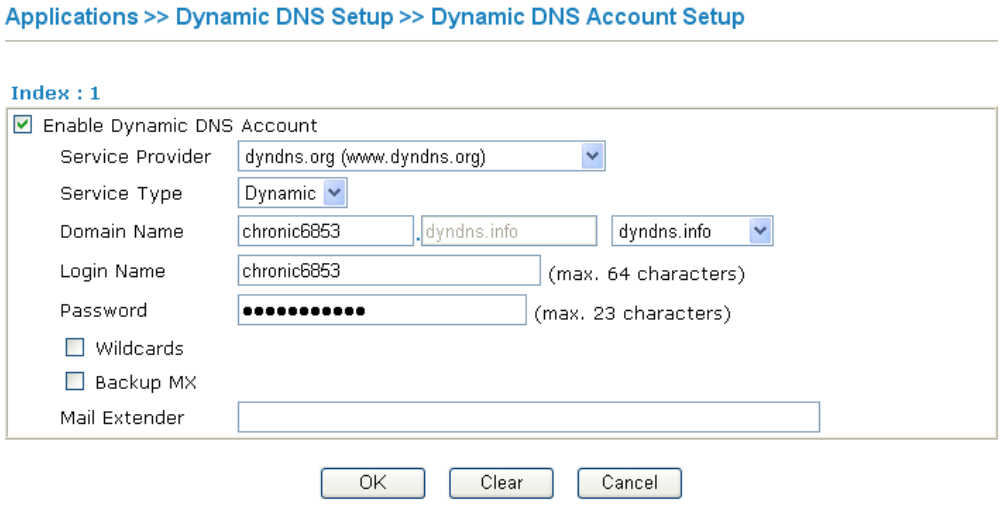
Auto-Update interval Execute auto-update with the interval set here.

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

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

Domain Name	Display the domain name that you set on the setting page of DDNS setup.
Active	Display if this account is active or inactive.
View Log	Display DDNS log status.
Force Update	Force the router updates its information to DDNS server.

7. 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.



Enable Dynamic DNS Account	Check this box to enable the current account. If you did check the box, you will see a check mark appeared on the Active column of the previous web page in step 2).
WAN Interface	Select the WAN interface order to apply settings here.
Service Provider	Select the service provider for the DDNS account.
Service Type	Select a service type (Dynamic, Custom or Static). If you choose Custom, you can modify the domain that is chosen in the Domain Name field.
Domain Name	Type in one domain name that you applied previously. Use the drop down list to choose the desired domain.
Login Name	Type in the login name that you set for applying domain.
Password	Type in the password that you set for applying domain.

8. 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.

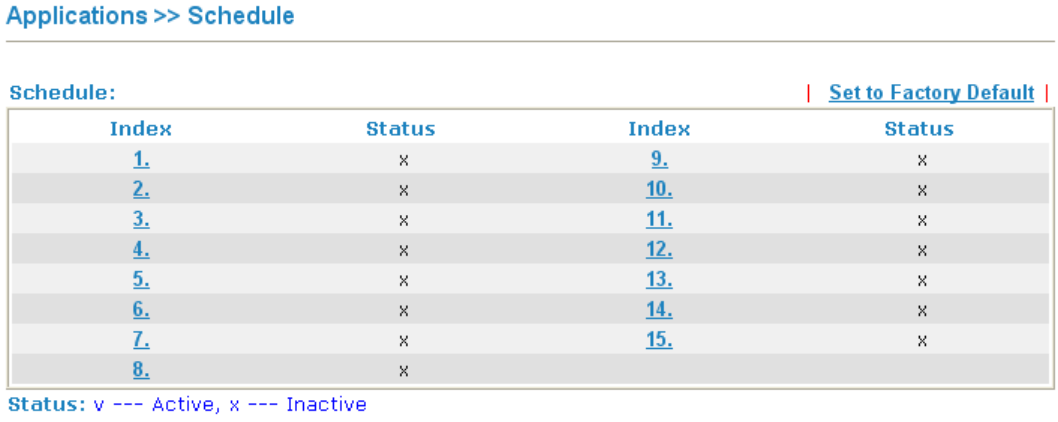
Delete a Dynamic DNS Account

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

4.8.2 Schedule

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

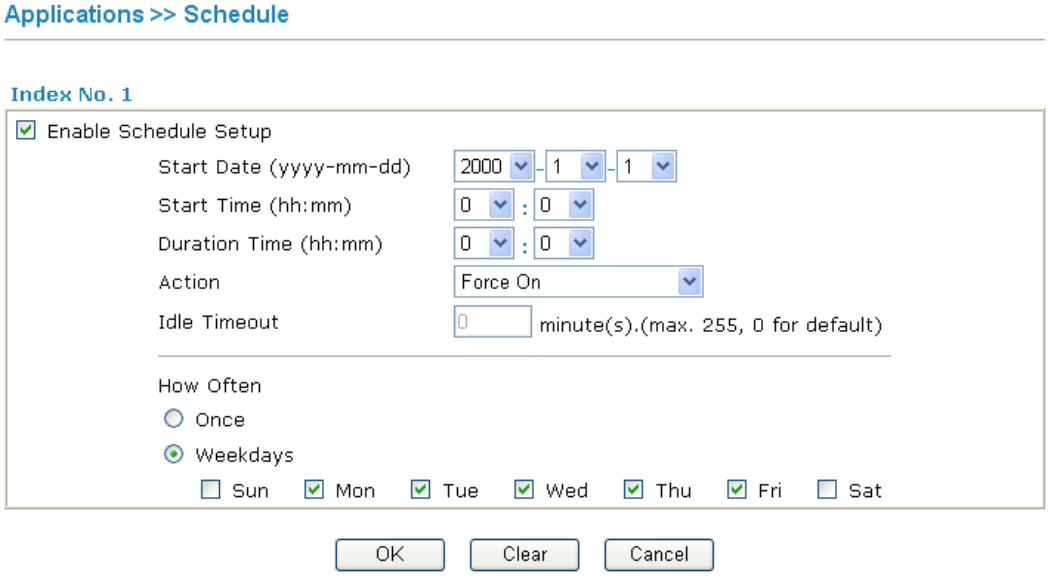
You have to set your time before set schedule. In **System Maintenance>> Time and Date** menu, press **Inquire Time** button to set the Vigor router's clock to current time of your PC. The clock will reset once if you power down or reset the router. There is another way to set up time. You can inquiry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



Set to Factory Default	Clear all profiles and recover to factory settings.
Index	Click the number below Index to access into the setting page of schedule.
Status	Display if this schedule setting is active or inactive.

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

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



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

Example

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

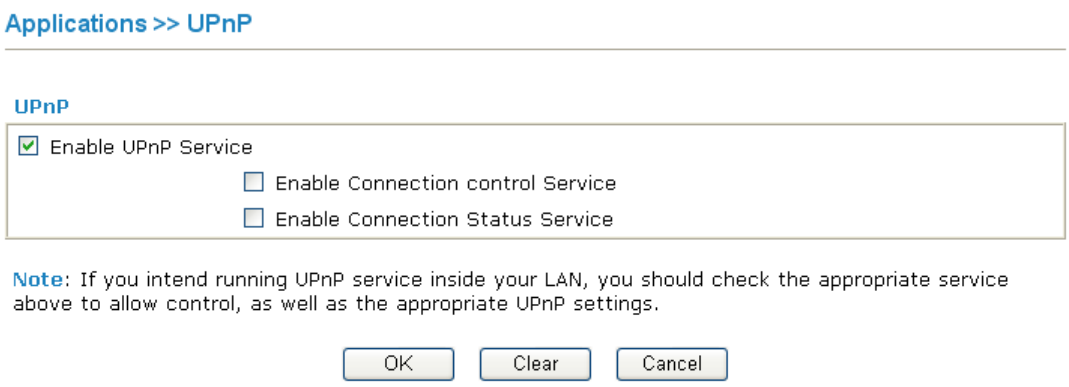
Office Hour:				
(Force On)				
Mon - Sun	**9:00 am**	**to**	**6:00 pm**	

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

4.8.3 UPnP

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

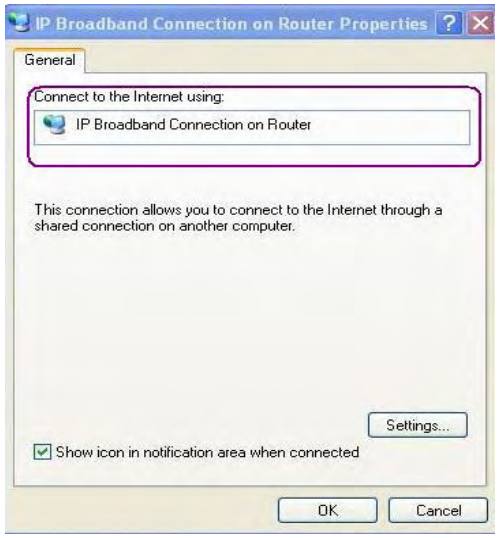
UPnP is available on Windows XP and the router provide the associated support for MSN Messenger to allow full use of the voice, video and messaging features.

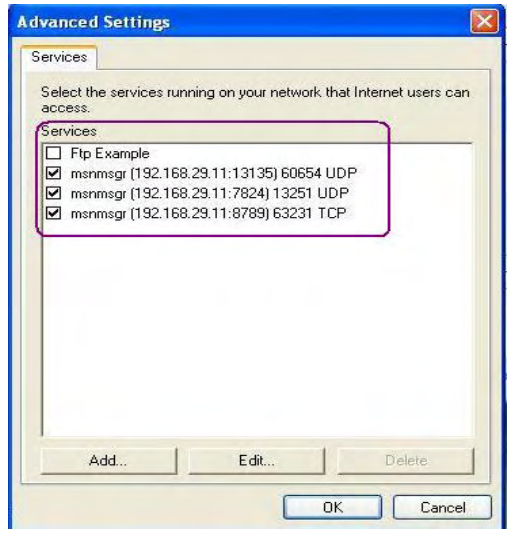


Enable UPNP Service Accordingly, you can enable either the **Connection Control Service** or **Connection Status Service**.

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

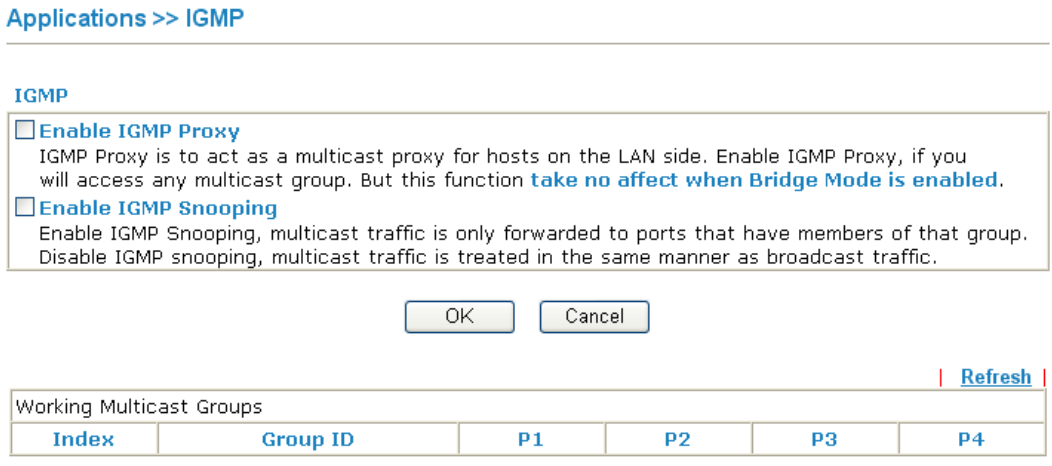
Activating the UPnP function on your network may incur some security threats. You should consider carefully these risks before activating the UPnP function.

- 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.

4.8.4 IGMP

IGMP is the abbreviation of *Internet Group Management Protocol*. It is a communication protocol which is mainly used for managing the membership of Internet Protocol multicast groups.



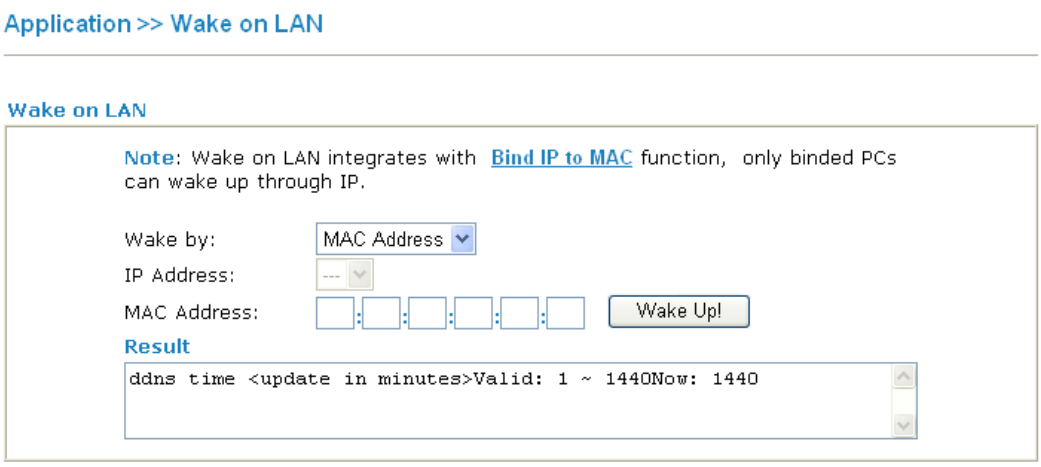
Enable IGMP Proxy	Check this box to enable this function. The application of multicast will be executed through WAN port.
Enable IGMP Snooping	Check this box to enable this function. Multicast traffic will be forwarded to ports that have members of that group. Disabling IGMP snooping will make multicast traffic treated in the same manner as broadcast traffic.
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, all the multicast groups will be listed and all the LAN ports (P1 to P4) are available for use.

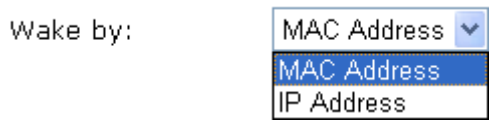
4.8.5 Wake on LAN

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

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

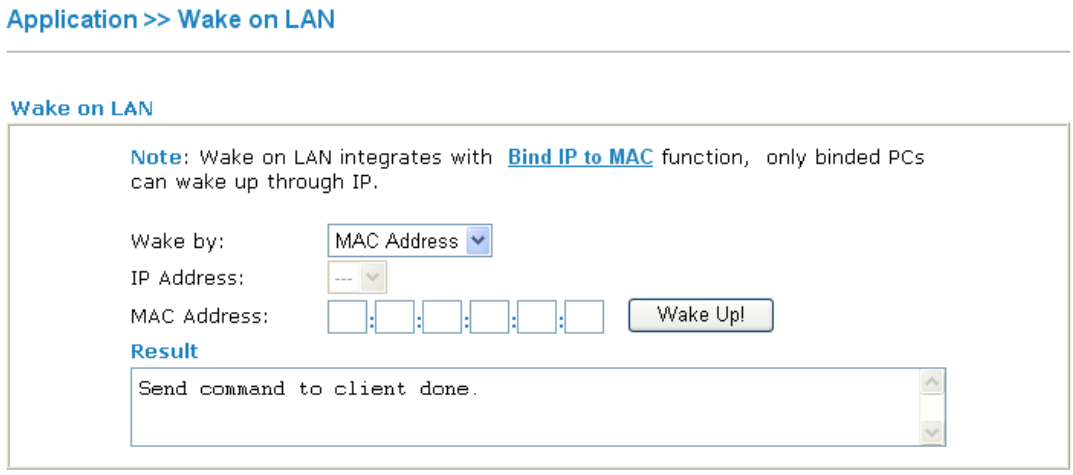


Wake by	Two types provide for you to wake up the binded IP. If you choose Wake by MAC Address, you have to type the correct MAC address of the host in MAC Address boxes. If you choose Wake by IP Address, you have to choose the correct IP address.



IP Address	The IP addresses that have been configured in **Firewall>>Bind IP to MAC** will be shown in this drop down list. Choose the IP address from the drop down list that you want to wake up.
MAC Address	Type any one of the MAC address of the binded PCs.

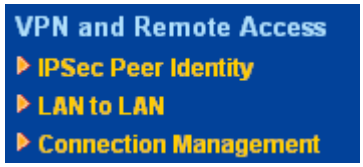
Wake Up Click this button to wake up the selected IP. See the following figure. The result will be shown on the box.



4.9 VPN and Remote Access

A Virtual Private Network (VPN) is the extension of a private network that encompasses links across shared or public networks like the Internet. In short, by VPN technology, you can send data between two computers across a shared or public network in a manner that emulates the properties of a point-to-point private link.

Below shows the menu items for VPN.



4.9.1 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.

VPN and Remote Access >> IPSec Peer Identity

X509 Peer ID Accounts: | Set to Factory Default |

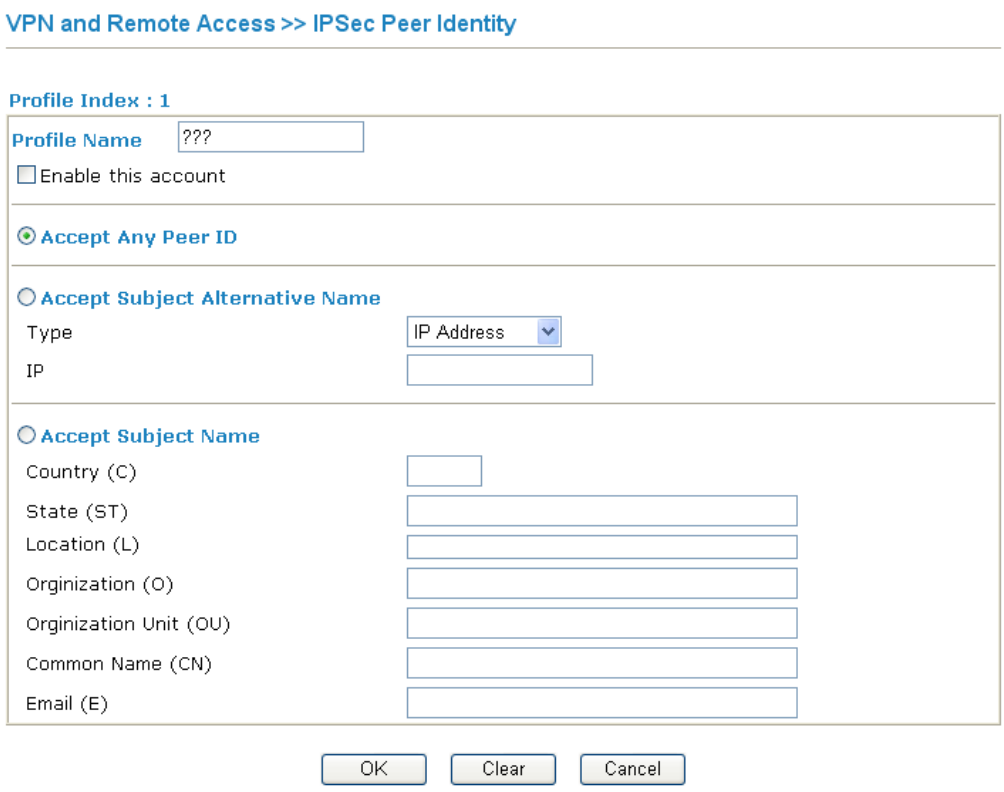
Index	Name	Status	Index	Name	Status
1.	???	X	17.	???	X
2.	???	X	18.	???	X
3.	???	X	19.	???	X
4.	???	X	20.	???	X
5.	???	X	21.	???	X
6.	???	X	22.	???	X
7.	???	X	23.	???	X
8.	???	X	24.	???	X
9.	???	X	25.	???	X
10.	???	X	26.	???	X
11.	???	X	27.	???	X
12.	???	X	28.	???	X
13.	???	X	29.	???	X
14.	???	X	30.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

Set to Factory Default Click it to clear all indexes.

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

Name Display the profile name of that index.

Click each index to edit one peer digital certificate. There are three security levels of digital signature authentication: Fill each necessary field to authenticate the remote peer. The following explanation will guide you to fill all the necessary fields.

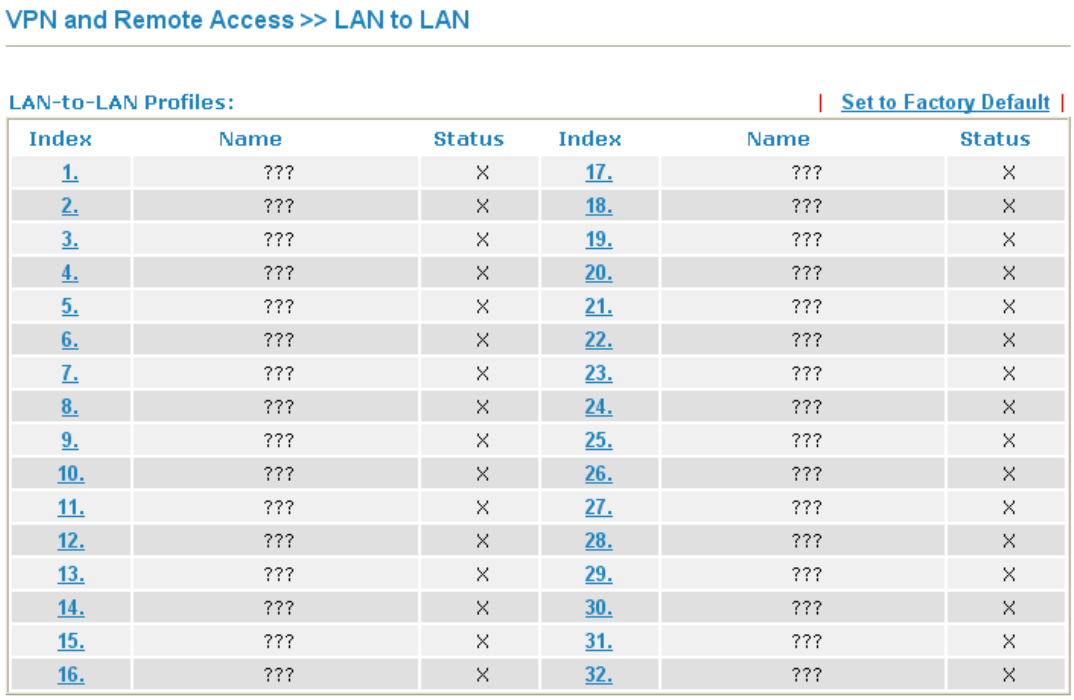


Profile Name	Type in a name in this file.
Accept Any Peer ID	Click to accept any peer regardless of its identity.
Accept Subject Alternative Name	Click to check one specific field of digital signature to accept the peer with matching value. The field can be **IP Address, Domain,** or **E-mail Address**. The box under the Type will appear according to the type you select and ask you to fill in corresponding setting.
Accept Subject Name	Click to check the specific fields of digital signature to accept the peer with matching value. The field includes **Country (C), State (ST), Location (L), Organization (O), Organization Unit (OU), Common Name (CN),** and **Email (E)**.

4.9.2 LAN to LAN

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

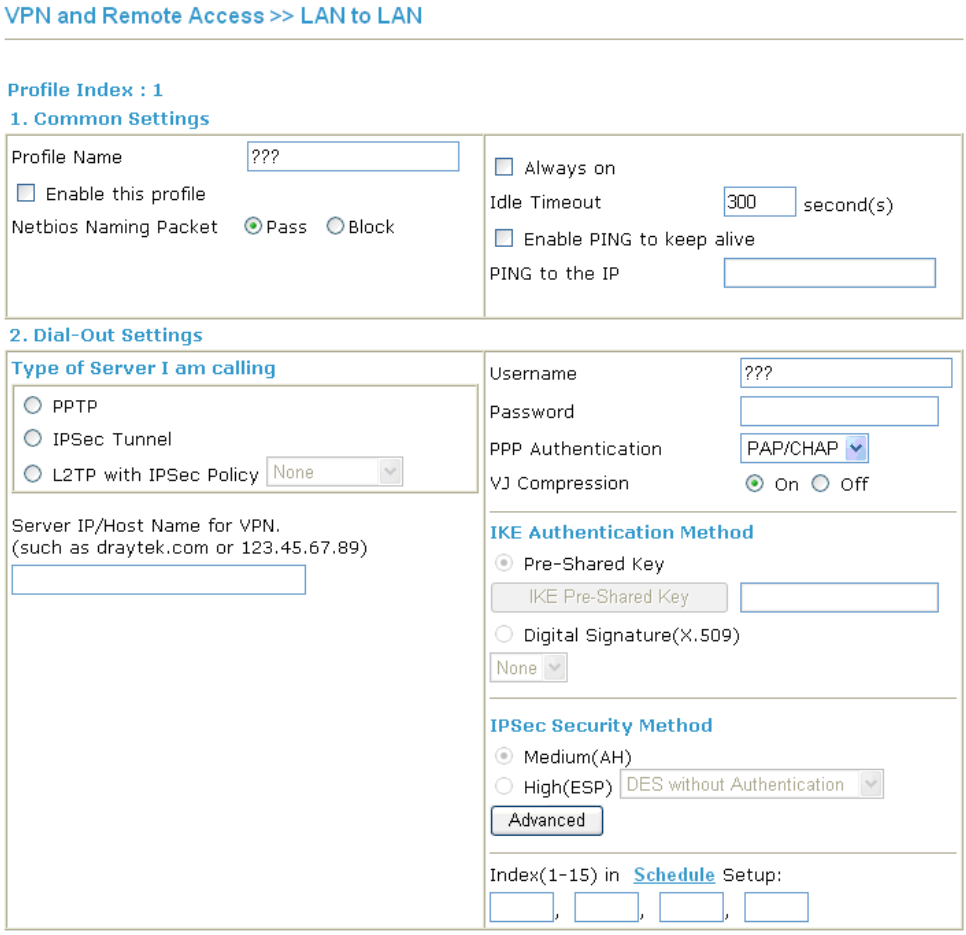
The router supports 2 dialout VPN tunnels and provides up to **32** profiles simultaneously. The following figure shows the summary table.



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 3 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.



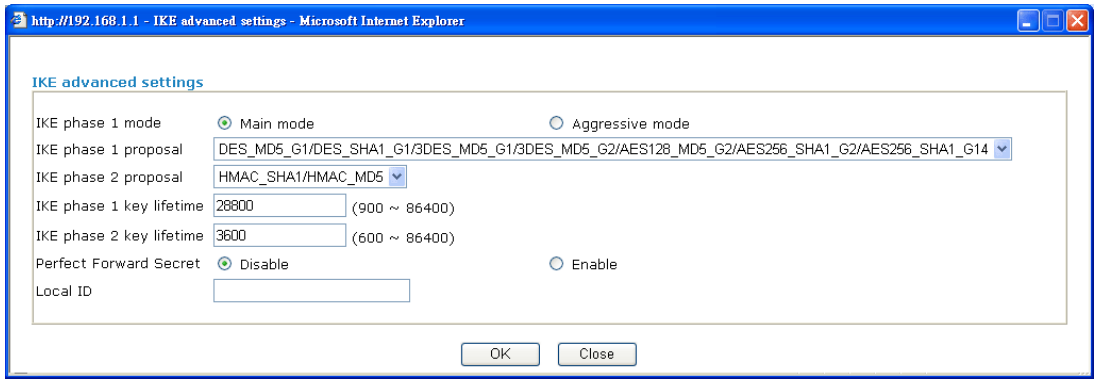
Profile Name	Specify a name for the profile of the LAN-to-LAN connection.
Enable this profile	Check here to activate this profile.
Netbios Naming Packet	**Pass** – click it to have an inquiry for data transmission between the hosts located on both sides of VPN Tunnel while connecting. **Block** – When there is conflict occurred between the hosts on both sides of VPN Tunnel in connecting, such function can block data transmission of Netbios Naming Packet inside the tunnel.
Always On or Idle Timeout	**Always On**-Check to enable router always keep VPN connection. **Idle Timeout:** The default value is 300 seconds. If the connection has been idled over the value, the router will drop the connection.
Enable PING to keep alive	This function is to help the router to determine the status of IPSec VPN connection, especially useful in the case of abnormal VPN IPSec tunnel disruption. For details, please refer to the note below. Check to enable the transmission of PING packets to a specified IP address.
PING to the IP	Enter the IP address of the remote host that located at the other-end of the VPN tunnel.

	Enable PING to Keep Alive is used to handle abnormal IPSec VPN connection disruption. It will help to provide the state of a VPN connection for router's judgment of redial. Normally, if any one of VPN peers wants to disconnect the connection, it should follow a serial of packet exchange procedure to inform each other. However, if the remote peer disconnect without notice, Vigor router will by no where to know this situation. To resolve this dilemma, by continuously sending PING packets to the remote host, the Vigor router can know the true existence of this VPN connection and react accordingly. This is independent of DPD (dead peer detection).
PPTP	Build a PPTP VPN connection to the server through the Internet. You should set the identity like User Name and Password below for the authentication of remote server.
IPSec Tunnel	Build an IPSec VPN connection to the server through Internet.
L2TP with …	Build a L2TP VPN connection through the Internet. You can select to use L2TP alone or with IPSec. Select from below: **None:** Do not apply the IPSec policy. Accordingly, the VPN connection employed the L2TP without IPSec policy can be viewed as one pure L2TP connection. **Nice to Have:** Apply the IPSec policy first, if it is applicable during negotiation. Otherwise, the dial-out VPN connection becomes one pure L2TP connection. **Must:** Specify the IPSec policy to be definitely applied on the L2TP connection.
User Name	This field is applicable when you select 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.
PPP Authentication	This field is applicable when you select PPTP or L2TP with or without IPSec policy above. PAP/CHAP is the most common selection due to wild compatibility.
VJ compression	This field is applicable when you select PPTP or L2TP with or without IPSec policy above. VJ Compression is used for TCP/IP protocol header compression. Normally set to **Yes** to improve bandwidth utilization.
IKE Authentication Method	This group of fields is applicable for IPSec Tunnels and L2TP with IPSec Policy. **Pre-Shared Key** - Input 1-63 characters as pre-shared key. **Digital Signature (X.509)** - Select one predefined Profiles set in the **VPN and Remote Access >>IPSec Peer Identity**.
IPSec Security Method	This group of fields is a must for IPSec Tunnels and L2TP with IPSec Policy.
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.

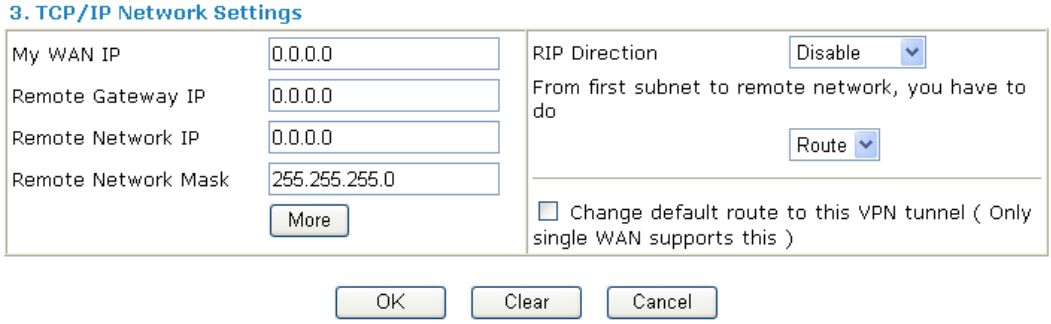
Advanced

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.



My WAN IP
This field is only applicable when you select PPTP or L2TP with or without IPSec policy above. The default value is 0.0.0.0, which means the Vigor router will get a PPP IP address from the remote router during the IPCP negotiation phase. If the PPP IP address is fixed by remote side, specify the fixed IP address here. Do not change the default value if you do not select PPTP or L2TP.

Remote Gateway IP
This field is only applicable when you select PPTP or L2TP with or without IPSec policy above. The default value is 0.0.0.0, which means the Vigor router will get a remote Gateway PPP IP address from the remote router during the IPCP negotiation phase. If the PPP IP address is fixed by remote side, specify the fixed IP address here. Do not change the default value if you do not select PPTP or L2TP.

Remote Network IP/ Remote Network Mask
Add a static route to direct all traffic destined to this Remote Network IP Address/Remote Network Mask through the VPN connection. For IPSec, this is the destination clients IDs of phase 2 quick mode.

More
Add a static route to direct all traffic destined to more Remote Network IP Addresses/ Remote Network Mask through the VPN connection. This is usually used when you find there are several subnets behind the remote VPN router.

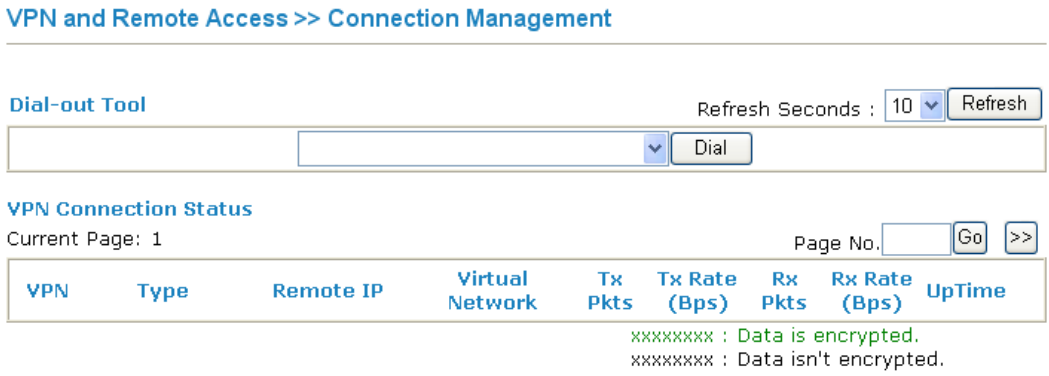
RIP Direction
The option specifies the direction of RIP (Routing Information Protocol) packets. You can enable/disable one of direction here. Herein, we provide four options: TX/RX Both, TX Only, RX Only, and Disable.

From first subnet to remote network, you have to do
If the remote network only allows you to dial in with single IP, please choose **NAT**, otherwise choose **Route**.

Change default route to this VPN tunnel
Check this box to change the default route with this VPN tunnel.

4.9.3 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.

4.10 Certificate Management

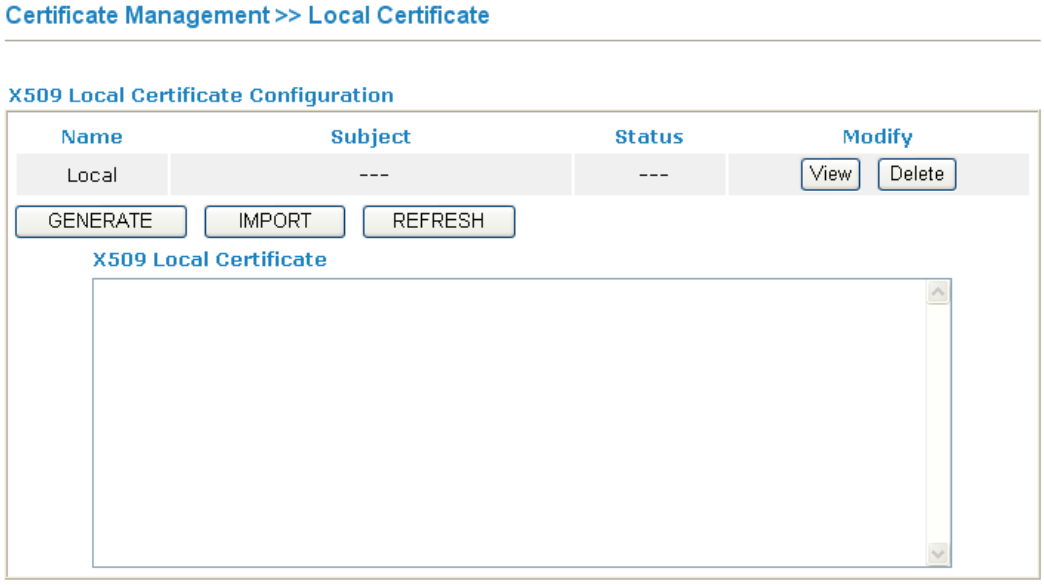
A digital certificate works as an electronic ID, which is issued by a certification authority (CA). It contains information such as your name, a serial number, expiration dates etc., and the digital signature of the certificate-issuing authority so that a recipient can verify that the certificate is real. Here Vigor router support digital certificates conforming to standard X.509.

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

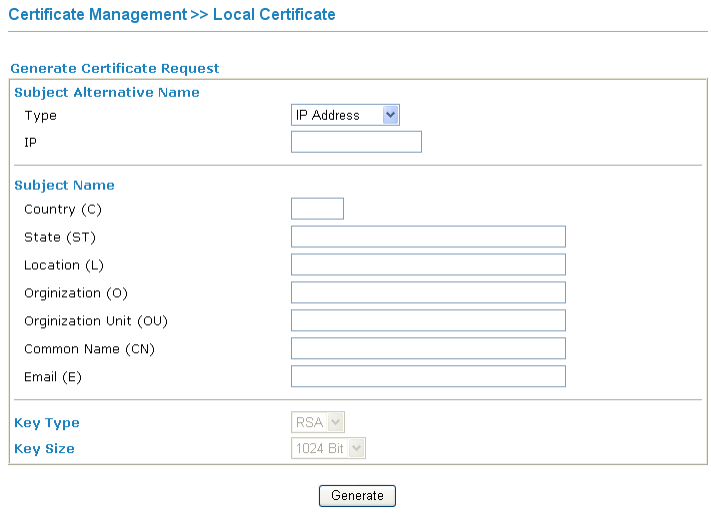
Here you can manage generate and manage the local digital certificates, and set trusted CA certificates. Remember to adjust the time of Vigor router before using the certificate so that you can get the correct valid period of certificate.

Below shows the menu items for Certificate Management.

4.10.1 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.

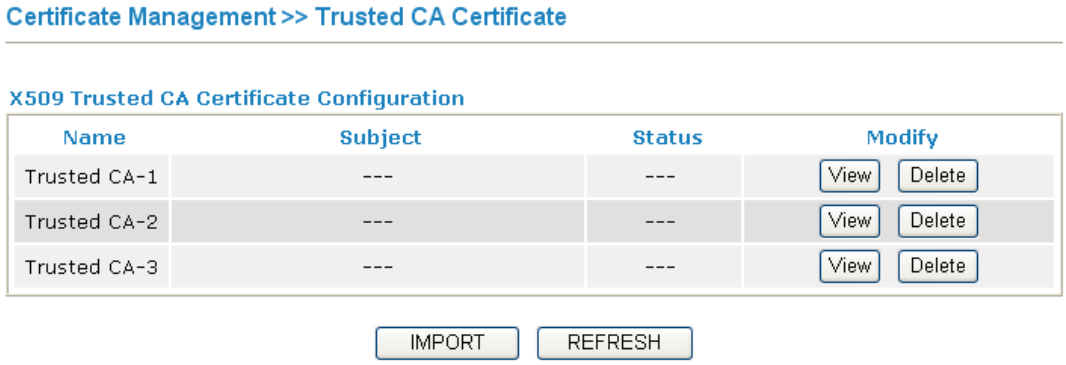
Refresh Click this button to refresh the information listed below.

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

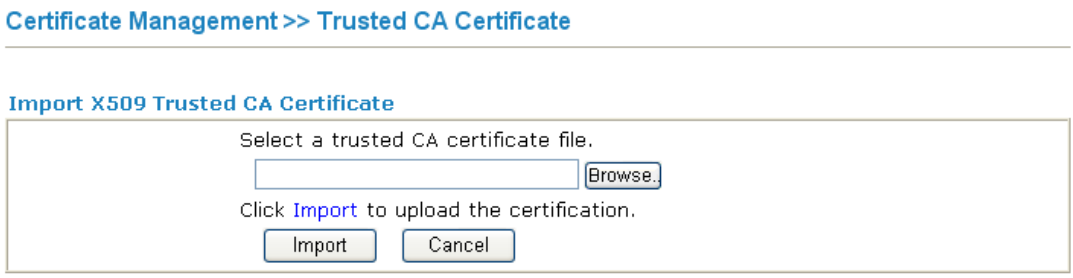
After clicking **Generate**, the generated information will be displayed on the window below:

4.10.2 Trusted CA Certificate

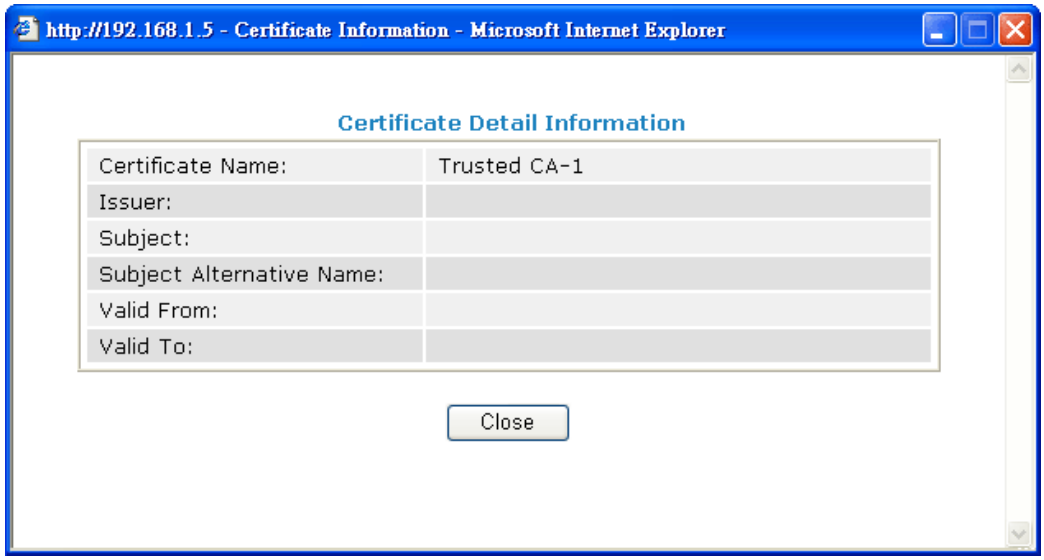
Trusted CA certificate lists three sets of trusted CA certificate.



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.



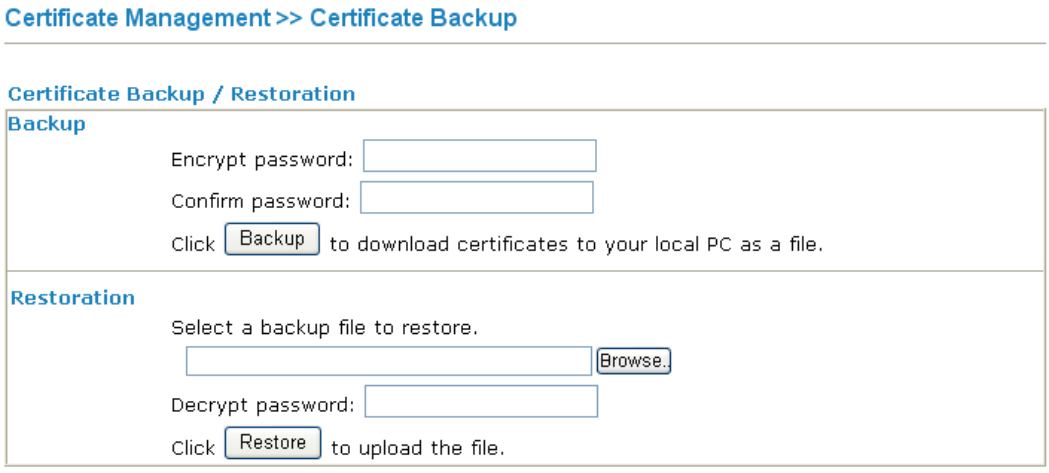
For viewing each trusted CA certificate, click **View** to open the certificate detail information window. If you want to delete a CA certificate, choose the one and click **Delete** to remove all the certificate information.



4.10.3 Certificate Backup

Local certificate and Trusted CA certificate for this router can be saved within one file. Please click **Backup** on the following screen to save them. If you want to set encryption password for these certificates, please type characters in both fields of **Encrypt password** and **Retype password**.

Also, you can use **Restore** to retrieve these two settings to the router whenever you want.



4.11 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/ISDN network.

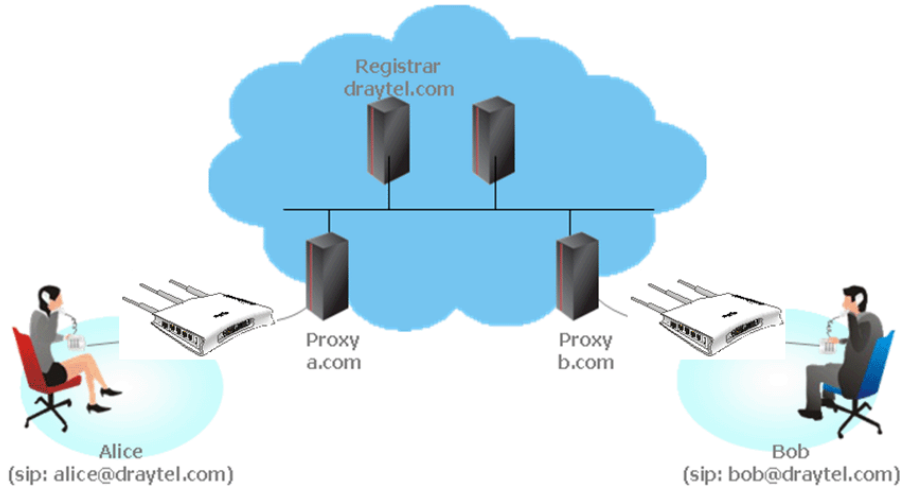
After a call is setup, the voice streams transmit via RTP (Real-Time Transport Protocol). Different codecs (methods to compress and encode the voice) can be embedded into RTP packets. Vigor V models provide various codecs, including G.711 A/μ-law, G.723, G.726 and G.729 A & B. Each codec uses a different 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:

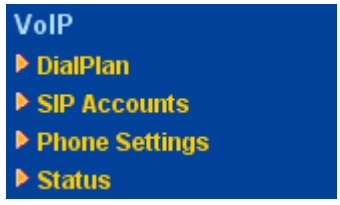


The major benefit of this mode is that you don't have to memorize your friend's IP address, which might change very frequently if it's dynamic. Instead of that, you will only have to using **dial plan** or directly dial your friend's **account name** if you are with the same SIP Registrar. Please refer to the **section 4.5.1.**

- **Peer-to-Peer**

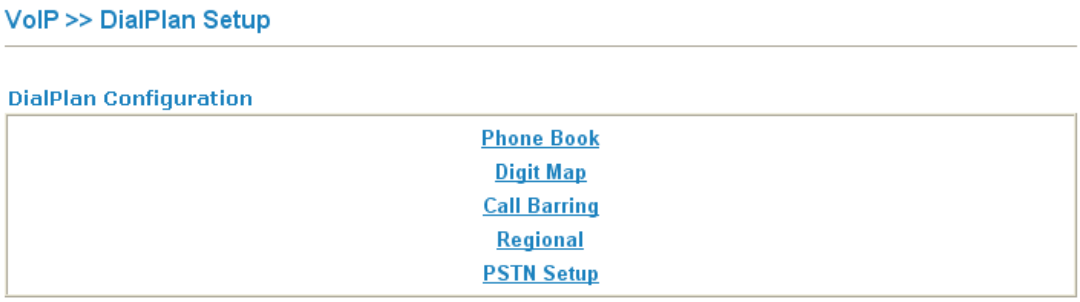
Before calling, you have to know your friend's IP Address. The Vigor VoIP Routers will build connection between each other. Please refer to the **section 4.5.2.**

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.



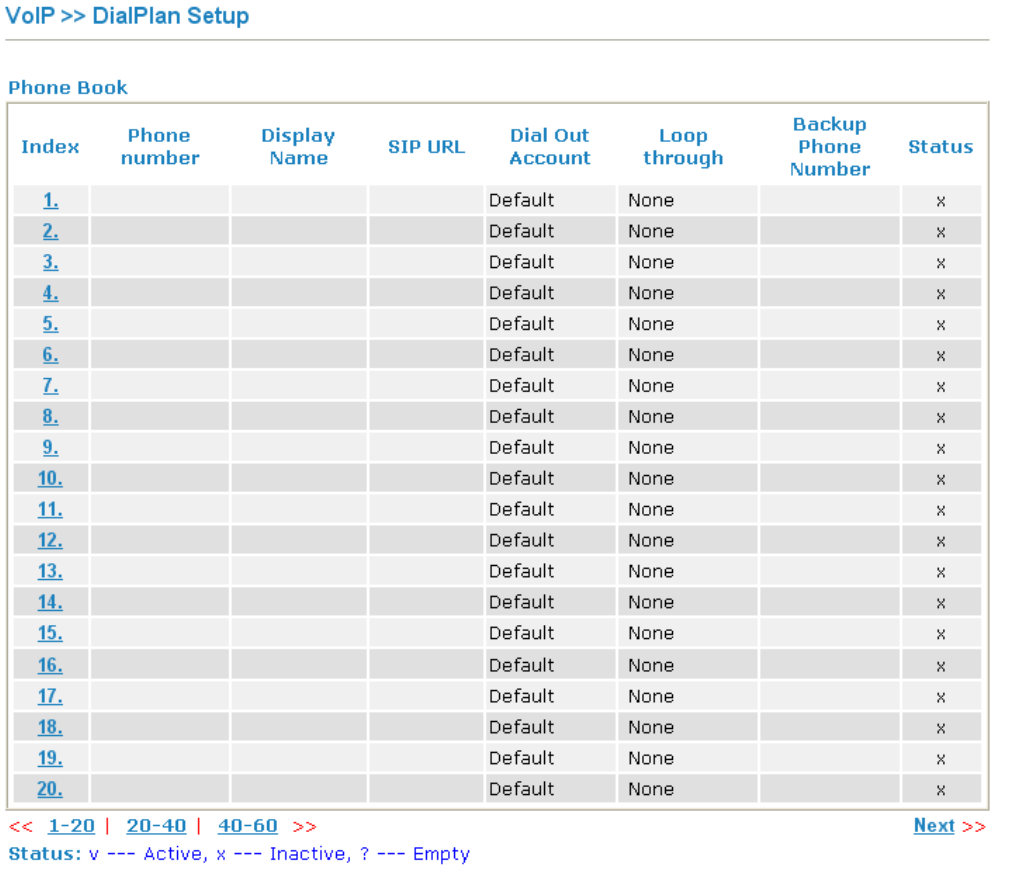
4.11.1 DialPlan

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.

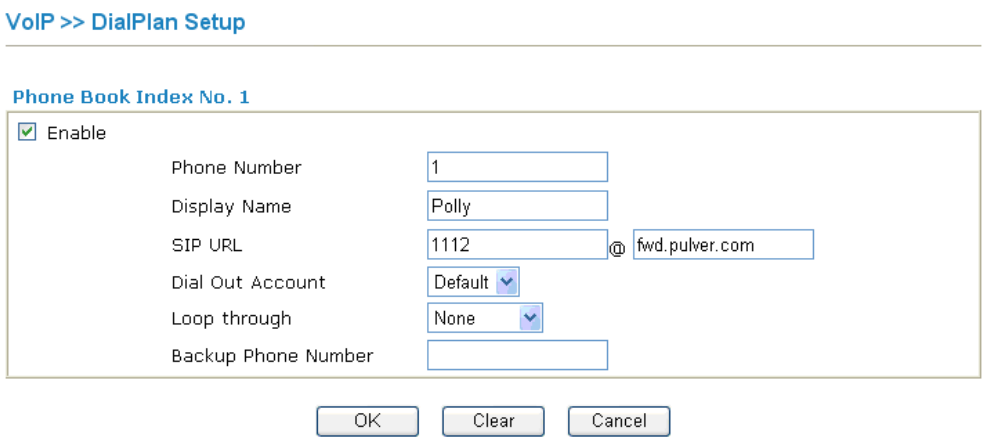


Phone Book

In this section, you can set your VoIP contacts in the "phonebook". It can help you to make calls quickly and easily by using "speed-dial" **Phone Number**. There are total 60 index entries in the phonebook for you to store all your friends and family members' SIP addresses. **Loop through** and **Backup Phone Number** will be displayed if you are using Vigor 2710Vn for setting the phone book.



Click any index number to display the dial plan setup page.



Enable Click this to enable this entry.

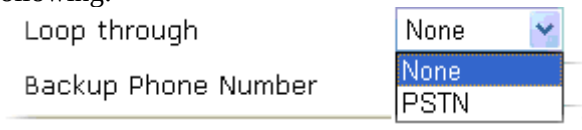
Phone Number The speed-dial number of this index. This can be any number you choose, using digits **0**-**9** and ***** .

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.

Dial Out Account Choose one of the SIP accounts for this profile to dial out. It is useful for both sides (caller and callee) that registered to different SIP Registrar servers. If caller and callee do not use the same SIP server, sometimes, the VoIP phone call connection may not succeed. By using the specified dial out account, the successful connection can be assured.

Loop through For the model of Vigor 2710Vn, 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.

VoIP >> DialPlan Setup

Digit Map Setup

#	Enable	Prefix Number	Mode	OP Number	Min Len	Max Len	Interface
1	☑	03	Replace	8863	7	9	PSTN
2	☑	886	Strip	886	8	10	PSTN
3	☐		None		0	0	PSTN
4	☐		None		0	0	PSTN
5	☐		None		0	0	PSTN
6	☐		None		0	0	PSTN
7	☐		None		0	0	PSTN
8	☐		None		0	0	PSTN
9	☐		None		0	0	PSTN
10	☐		None		0	0	PSTN
11	☐		None		0	0	PSTN
12	☐		None		0	0	PSTN
13	☐		None		0	0	PSTN
14	☐		None		0	0	PSTN
15	☐		None		0	0	PSTN
16	☐		None		0	0	PSTN
17	☐		None		0	0	PSTN
18	☐		None		0	0	PSTN
19	☐		None		0	0	PSTN
20	☐		None		0	0	PSTN

Note: Min Len and Max Len should be between 0~25.

OK Cancel

Enable Check this box to invoke this setting.

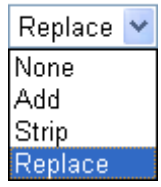
Prefix Number The phone number set here is used to add, strip, or replace the OP number.

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 prefix number of 03 will be replaced by 8863. For example: dial number of “031111111” will be changed to “88631111111” and sent to SIP server.

Mode



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.

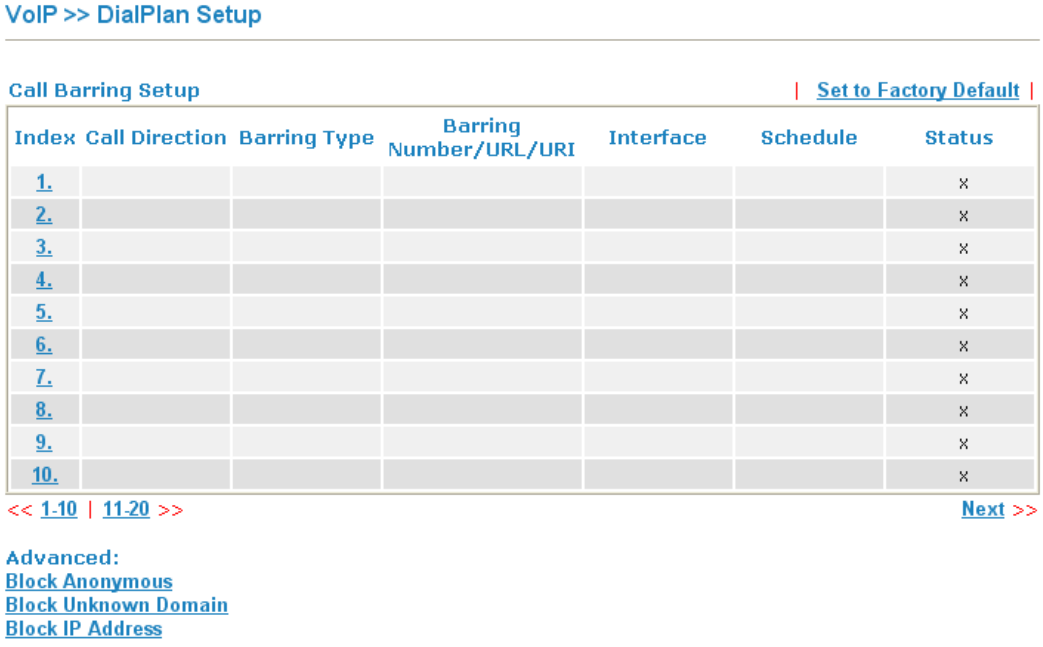
Min Len Set the minimal length of the dial number for applying the prefix number settings. Take the above picture (Prefix Table Setup web page) as an example, if the dial number is between 7 and 9, that number can apply the prefix number settings here.

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

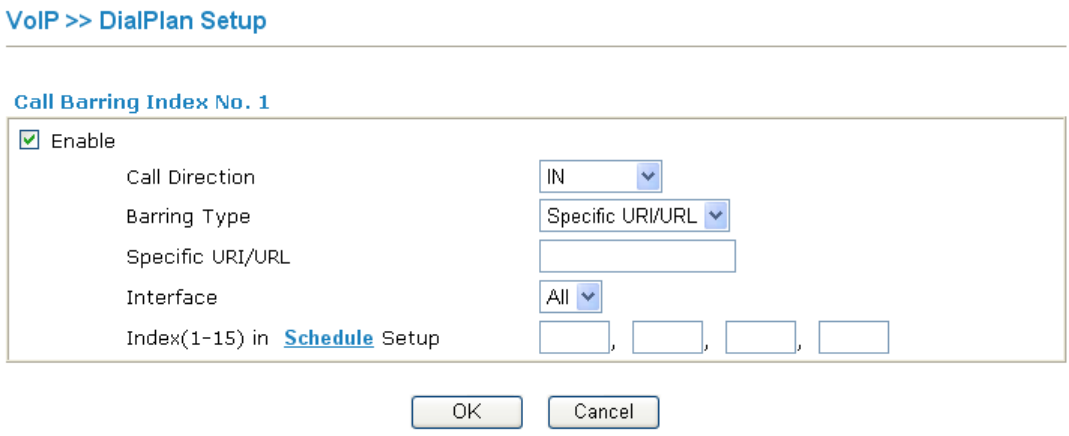
Interface Choose the one that you want to enable the prefix number settings from the saved SIP accounts. Please set up one SIP account first to make this interface available.

Call Barring

Call barring is used to block phone calls coming from the one that is not welcomed.

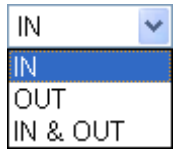


Click any index number to display the dial plan setup page.

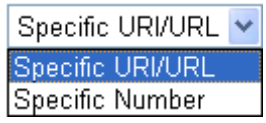


Enable — Click this to enable this entry.

Call Direction — Determine the direction for the phone call, IN – incoming call, OUT-outgoing call, IN & OUT – both incoming and outgoing calls.



Barring Type — Determine the type of the VoIP phone call, URI/URL or number.



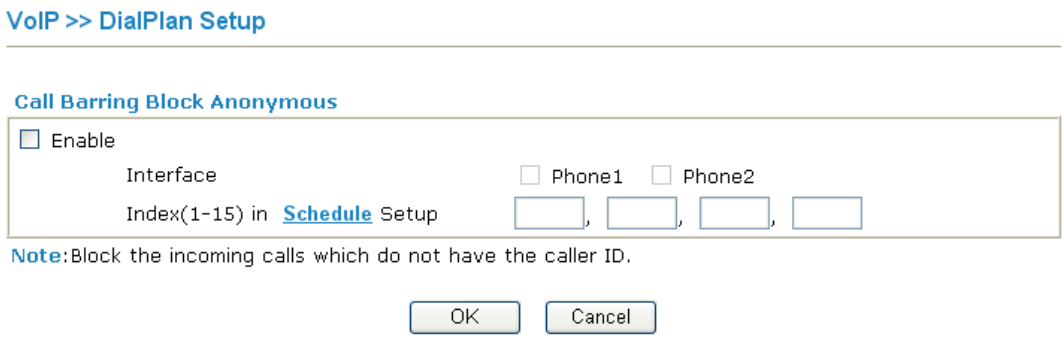
Specific URI/URL or Specific Number — This field will be changed based on the type you selected for barring Type.

Interface — **All** means all the phone calls will be blocked with such mechanism.

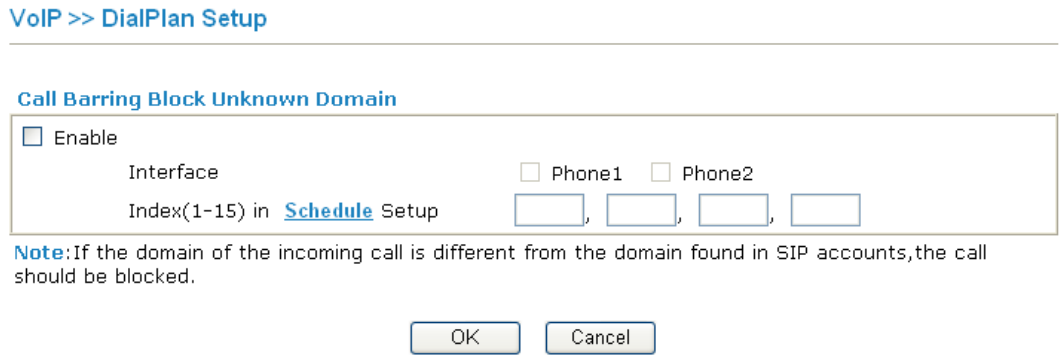
Index (1-15) in Schedule — Enter the index of schedule profiles to control the call barring according to the preconfigured schedules. Refer to section **Application>> Schedule** for detailed configuration.

Additionally, you can set advanced settings for call barring such as **Block Anonymous**, **Block Unknown Domain** or **Block IP Address**. Simply click the relational links to open the web page.

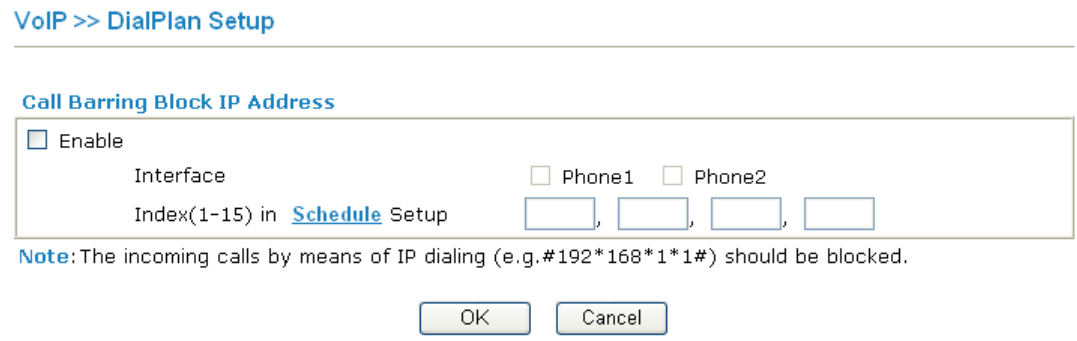
For **Block Anonymous –** this function can block the incoming calls without caller ID on the interface (Phone port) specified in the following window. Such control also can be done based on preconfigured schedules.



For **Block Unknown Domain –** this function can block incoming calls (through Phone port) from unrecognized domain that is not specified in SIP accounts. Such control also can be done based on preconfigured schedules.

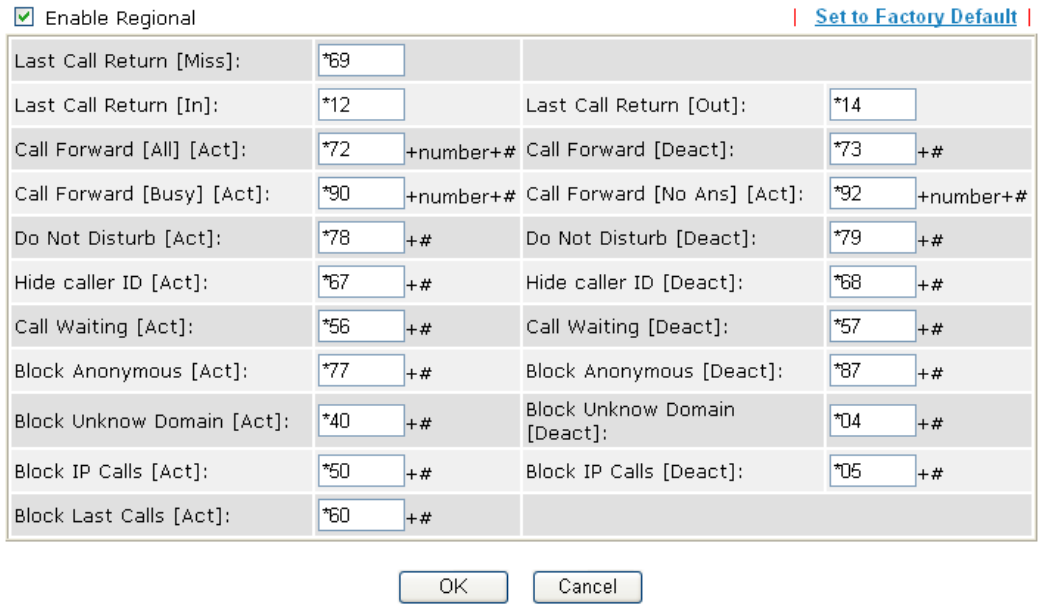


For **Block IP Address –** this function can block incoming calls (through Phone port) coming from IP address. Such control also can be done based on preconfigured schedules.



Regional

This page allows you to process incoming or outgoing phone calls by regional. Default values (common used in most areas) will be shown on this web page. You ***can change*** the number based on the region that the router is placed.



Last Call Return [Miss] Sometimes, people might miss some phone calls. Please dial number typed in this field to know where the last phone call comes from and call back to that one.

Last Call Return [In] You have finished an incoming phone call, however you want to call back again for some reason. Please dial number typed in this field to call back to that one.

Last Call Return [Out] Dial the number typed in this field to call the previous outgoing phone call again.

Call Forward [All][Act] Dial the number typed in this field to forward all the incoming calls to the specified place.

Call Forward [Deact] Dial the number typed in this field to release the call forward function.

Call Forward [Busy][Act] Dial the number typed in this field to forward all the incoming calls to the specified place while the phone is busy.

Call Forward [No Ans][Act] Dial the number typed in this field to forward all the incoming calls to the specified place while there is no answer of the connected phone.

Do Not Disturb [Act] Dial the number typed in this field to invoke the function of DND.

Do Not Distrub [Deact] Dial the number typed in this field to release the DND function.

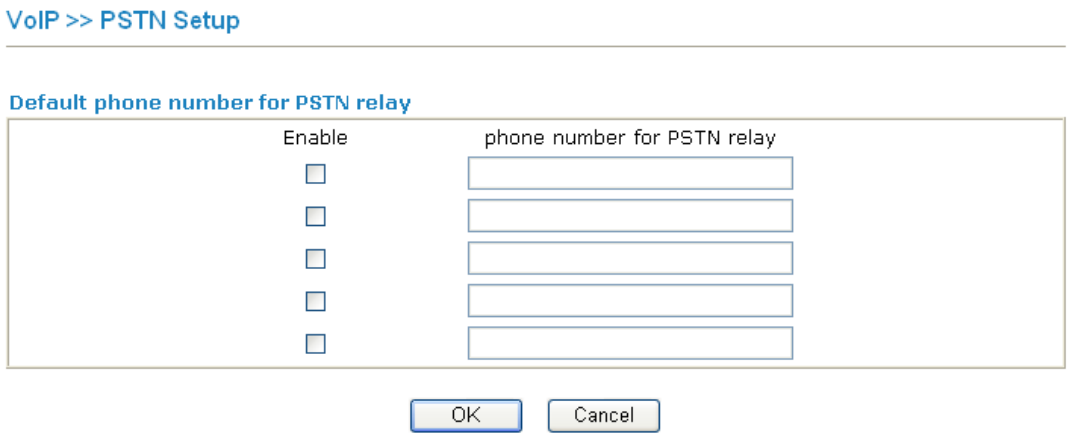
Hide caller ID [Act] Dial the number typed in this field to make your phone number (ID) not displayed on the display panel of remote end.

Hide caller ID [Deact] Dial the number typed in this field to release this function.

Call Waiting [Act]	Dial the number typed in this field to make all the incoming calls waiting for your answer.
Call Waiting [Deact]	Dial the number typed in this field to release this function.
Block Anonymous[Act]	Dial the number typed in this field to block all the incoming calls with unknown ID.
Block Anonymous[Deact]	Dial the number typed in this field to release this function.
Block Unknown Domain [Act]	Dial the number typed in this field to block all the incoming calls from unknown domain.
Block Unknown Domain [Deact]	Dial the number typed in this field to release this function.
Block IP Calls [Act]	Dial the number typed in this filed to block all the incoming calls from IP address.
Block IP Calls [Deact]	Dial the number typed in this field to release this function.
Block Last Calls [Act]	Dial the number typed in this field to block the last incoming phone call.

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**.

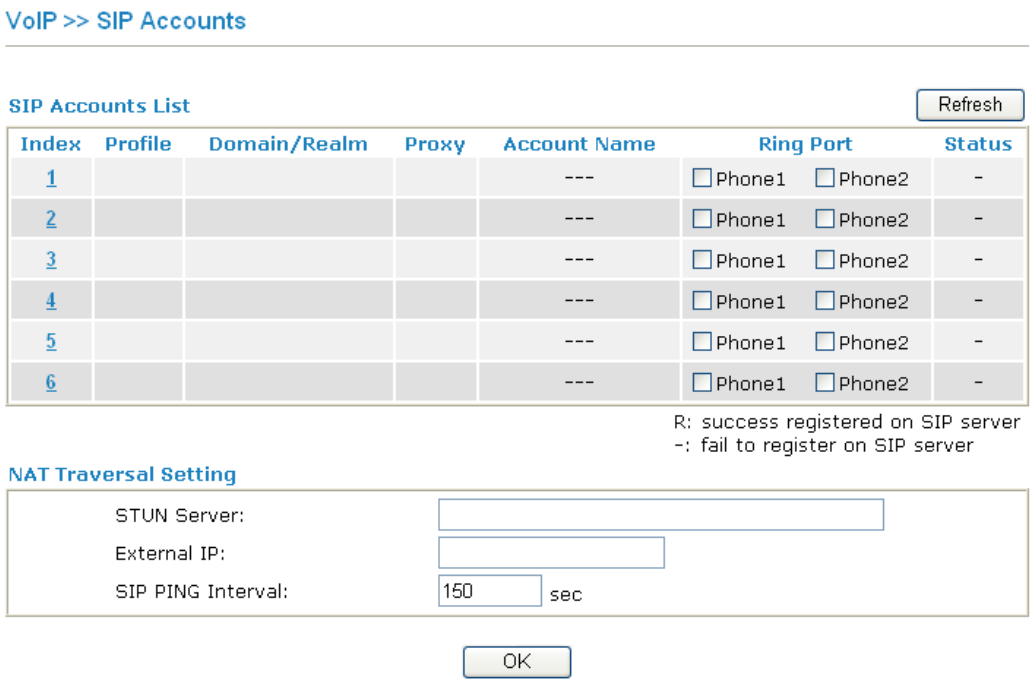


Then, check the **Enable** box to make the PSTN number available for dial whenever you need.

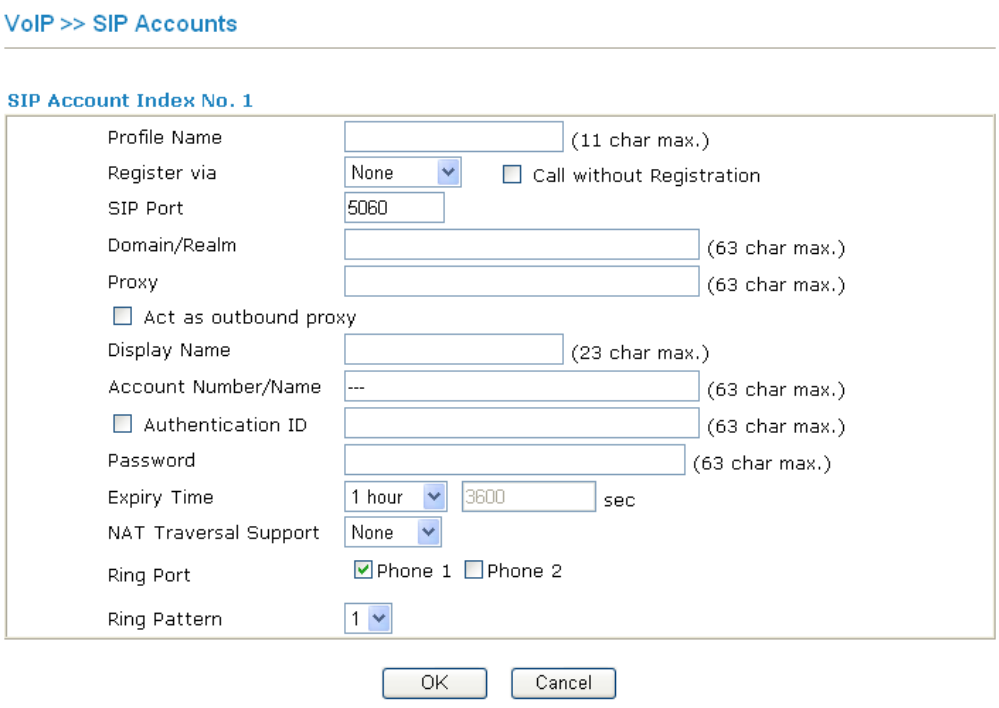
4.11.2 SIP Accounts

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.



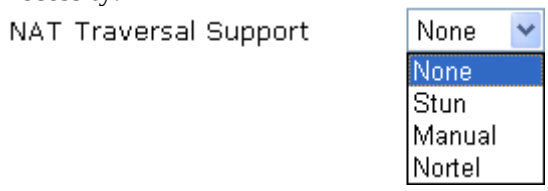
Index	Click this link to access into next page for setting SIP account.
Profile	Display the profile name of the account.
Domain/Realm	Display the domain name or IP address of the SIP registrar server.
Proxy	Display the domain name or IP address of the SIP proxy server.
Account Name	Display the account name of SIP address before @.
Ring Port	Specify which port will ring when receiving a phone call. Set Phone1 or Phone 2 as the default ring port for the SIP account.
STUN Server	Type in the IP address or domain of the STUN server.
External IP	Type in the gateway IP address.
SIP PING interval	The default value is 150 (sec). 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 **Call without Registration**. 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.

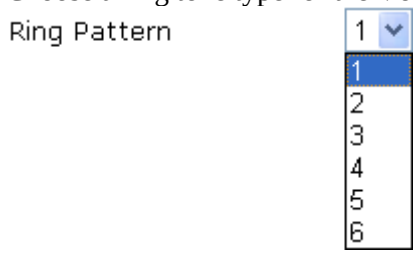
NAT Traversal Support If the router (e.g.**,** broadband router) you use connects to internet by other device, you have to set this function for your necessity.



None – Disable this function.
Stun – Choose this option if there is Stun server provided for your router.
Manual – Choose this option if you want to specify an external IP address as the NAT transversal support.
Nortel – If the soft-switch that you use supports Nortel solution, you can choose this option.

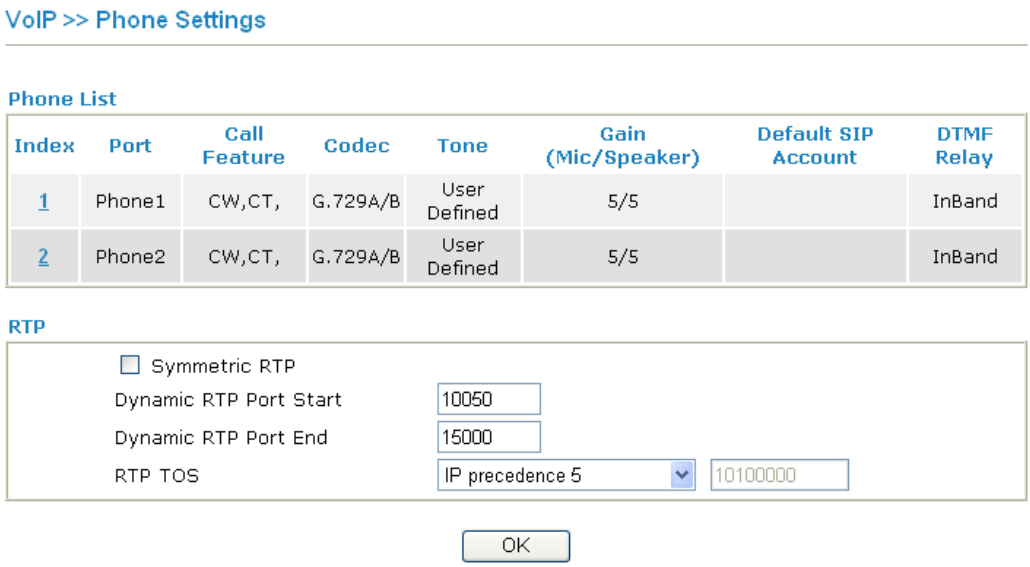
Ring Port Set Phone1 or Phone2 as the default ring port for this SIP account.

Ring Pattern Choose a ring tone type for the VoIP phone call.



4.11.3 Phone Settings

This page allows user to set phone settings for Phone 1 and Phone 2 respectively. However, it changes slightly according to different model you have.



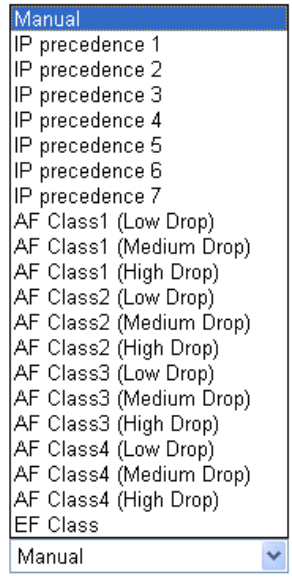
Phone List

Port –there are two phone ports provided here for you to configure.
Phone1/Phone2 allows you to set general settings for PSTN phones.
Call Feature – A brief description for call feature will be shown in this field for your reference.
Codec – The default Codec setting for each port will be shown in this field for your reference. You can click the number below the Index field to change it for each phone port.
Tone - Display the tone settings that configured in the advanced settings page of Phone Index.
Gain - Display the volume gain settings for Mic/Speaker that configured in the advanced settings page of Phone Index.
Default SIP Account – "draytel_1" is the default SIP account. You can click the number below the Index field to change SIP account for each phone port.
DTMF Relay – Display DTMF mode that configured in the advanced settings page of Phone Index.

RTP

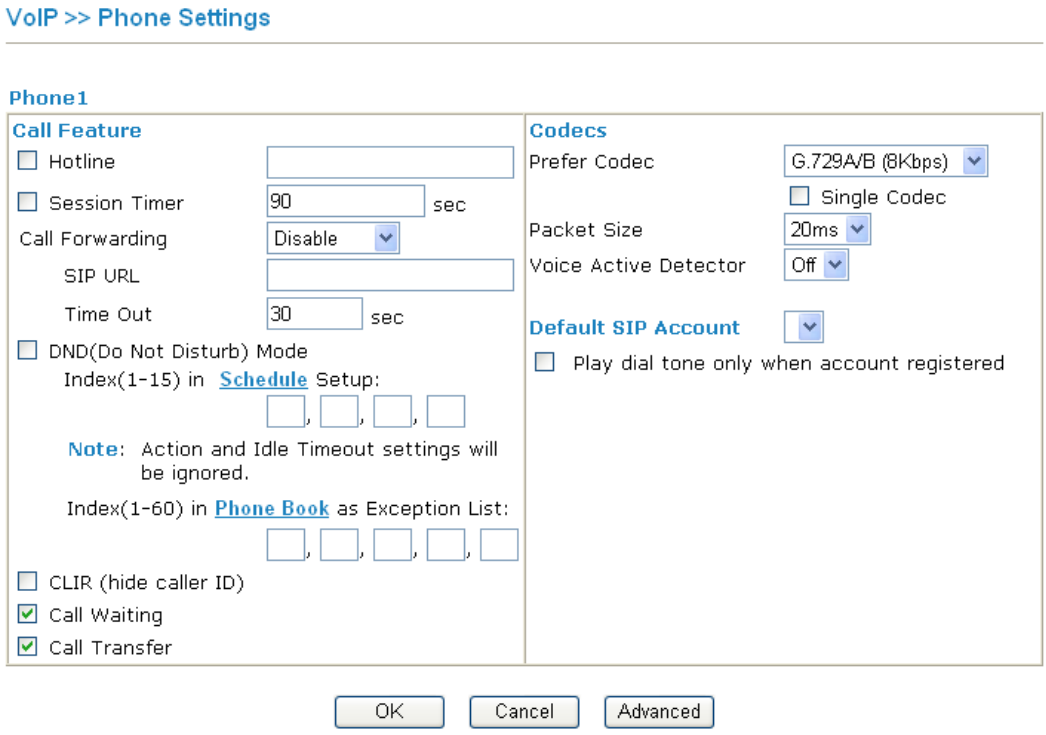
Symmetric RTP – Check this box to invoke the function. To make the data transmission going through on both ends of local router and remote router not misleading due to IP lost (for example, sending data from the public IP of remote router to the private IP of local router), you can check this box to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



Detailed Settings for Phone Port

Click the number link for Phone port, you can access into the following page for configuring Phone settings.

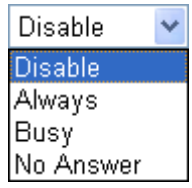


Hotline Check the box to enable it. Type in the SIP URL in the field for dialing automatically when you pick up the phone set.

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.

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.

Index (1-15) in Schedule - Enter the index of schedule profiles to control the DND mode according to the preconfigured schedules. Refer to section **Application>>Schedule** for detailed configuration.
Index (1-60) in Phone Book - Enter the index of phone book profiles. Refer to section **DialPlan>> Phone Book** for detailed configuration.

CLIR (hide caller ID)

Check this box to hide the caller ID on the display panel of the phone set.

Call Waiting

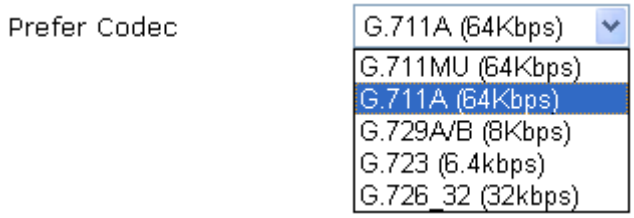
Check this box to invoke this function. A notice sound will appear to tell the user new phone call is waiting for your response. Click hook flash to pick up the waiting phone call.

Call Transfer

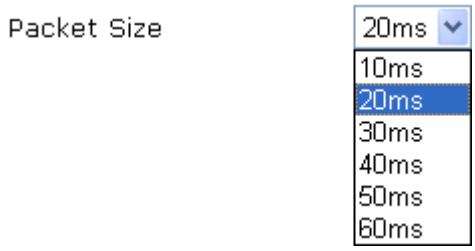
Check this box to invoke this function. Click hook flash to initiate another phone call. When the phone call connection succeeds, hang up the phone. The other two sides can communicate, then.

Prefer Codec

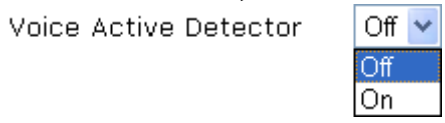
Select one of five codecs as the default for your VoIP calls. The codec used for each call will be negotiated with the peer party before each session, and so may not be your default choice. The default codec is G.729A/B; it occupies little bandwidth while maintaining good voice quality.
If your upstream 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.

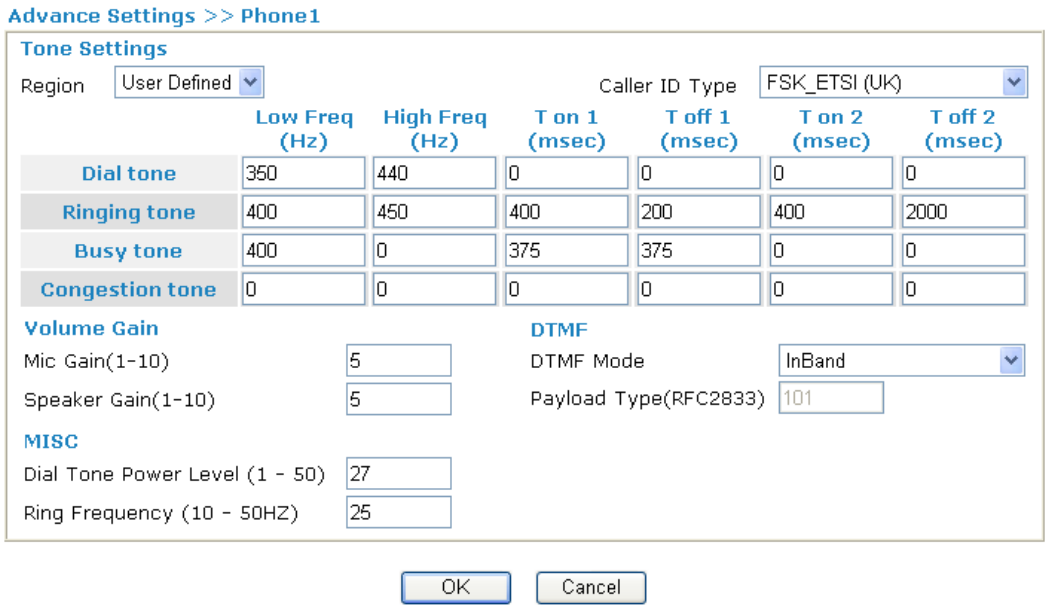


Default SIP Account

You can set SIP accounts (up to six groups) on SIP Account page. Use the drop down list to choose one of the profile names for the accounts as the default one for this phone setting.

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

In addition, you can press the **Advanced** button to configure tone settings, volume gain, MISC and DTMF mode. **Advanced** setting is provided for fitting the telecommunication custom for the local area of the router installed. Wrong tone settings might cause inconvenience for users. To set the sound pattern of the phone set, simply choose a proper region to let the system find out the preset tone settings and caller ID type automatically. Or you can adjust tone settings manually if you choose User Defined. TOn1, TOff1, TOn2 and TOff2 mean the cadence of the tone pattern. TOn1 and TOn2 represent sound-on; TOff1 and TOff2 represent the sound-off.



Region

Select the proper region which you are located. The common settings of **Caller ID Type**, **Dial tone**, **Ringing tone**, **Busy tone** and **Congestion tone** will be shown automatically on the page. If you cannot find out a suitable one, please choose **User Defined** and fill out the corresponding values for dial tone, ringing tone, busy tone, congestion tone by yourself for VoIP phone.

Also, you can specify each field for your necessity. It is recommended for you to use the default settings for VoIP communication.

Volume Gain

Mic Gain (1-10)/Speaker Gain (1-10) - Adjust the volume of microphone and speaker by entering number from 1- 10. The larger of the number, the louder the volume is.

MISC

Dial Tone Power Level - This setting is used to adjust the loudness of the dial tone. The smaller the number is, the louder the dial tone is. It is recommended for you to use the default setting.

Ring Frequency - This setting is used to drive the frequency of the ring tone. It is recommended for you to use the default setting.

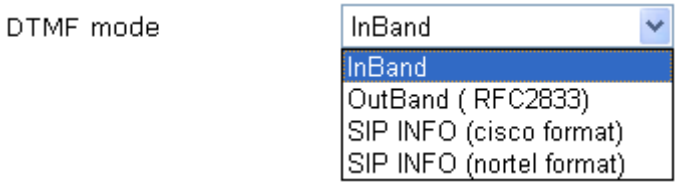
DTMF

DTMF Mode – There are four DTMF modes for you to choose.

InBand - Choose this one then the Vigor will send the DTMF tone as audio directly when you press the keypad on the phone

OutBand - Choose this one then the Vigor will capture the keypad number you pressed and transform it to digital form then send to the other side; the receiver will generate the tone according to the digital form it receive. This function is very useful when the network traffic congestion occurs and it still can remain the accuracy of DTMF tone.

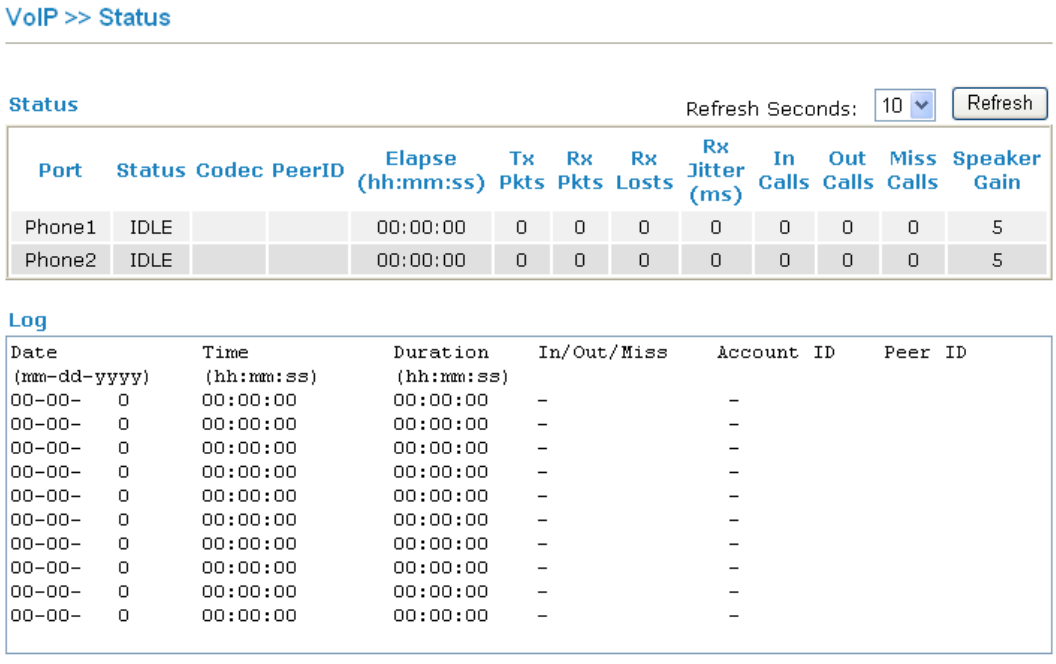
SIP INFO- Choose this one then the Vigor will capture the DTMF tone and transfer it into SIP form. Then it will be sent to the remote end with SIP message.

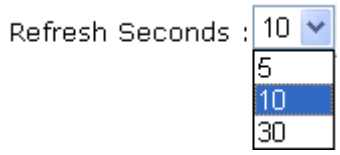


Payload Type (rfc2833) - Choose a number from 96 to 127, the default value was 101. This setting is available for the OutBand (RFC2833) mode.

4.11.4 Status

From this page, you can find codec, connection and other important call status for each port.



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 Phone1 and Phone2.
Status	It shows the VoIP connection status. **IDLE -** Indicates that the VoIP function is idle. **HANG_UP -** Indicates that the connection is not established (busy tone). **CONNECTING -** Indicates that the user is calling out. **WAIT_ANS -** Indicates that a connection is launched and waiting for remote user's answer. **ALERTING -** Indicates that a call is coming. **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).
Elapse	The format is represented as hours:minutes: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	Accumulation for the times of in call.
Out Calls	Accumulation for the times of out call.
Miss Calls	Accumulation for the times of missing call.
Speaker Gain	The volume of present call.
Log	Display logs of VoIP calls.

4.12 Wireless LAN

This function is used for "n" models only.

4.12.1 Basic Concepts

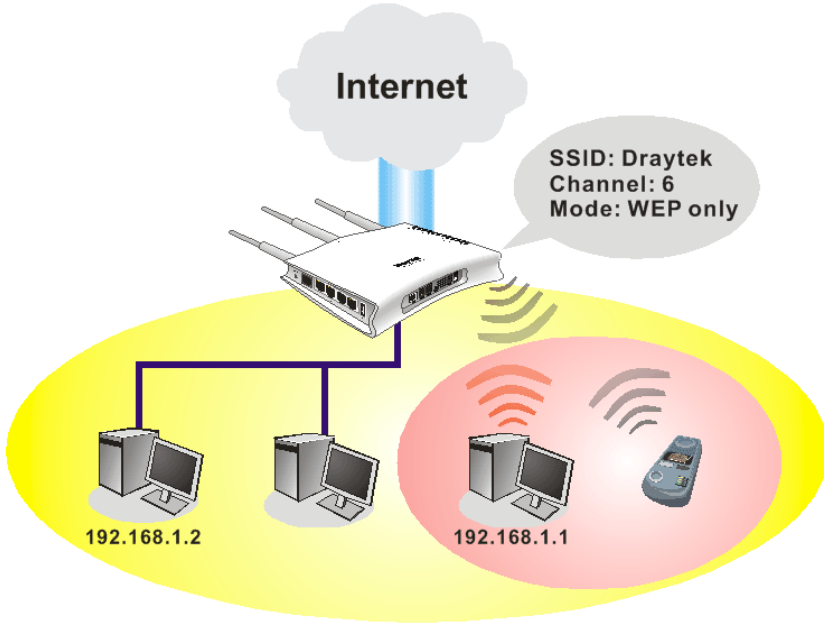
Over recent years, the market for wireless communications has enjoyed tremendous growth. Wireless technology now reaches or is capable of reaching virtually every location on the surface of the earth. Hundreds of millions of people exchange information every day via wireless communication products. The Vigor "n" 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 802.11n protocol. To boost its performance further, the Vigor Router is also loaded with advanced wireless technology to lift up data rate up to 300 Mbps*. Hence, you can finally smoothly enjoy stream music and video.

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

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



Security Overview

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

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

WEP (Wired Equivalent Privacy) is a legacy method to encrypt each frame transmitted via radio using either a 64-bit or 128-bit key. Usually access point will preset a set of four keys and it will communicate with each station using only one out of the four keys.

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

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

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

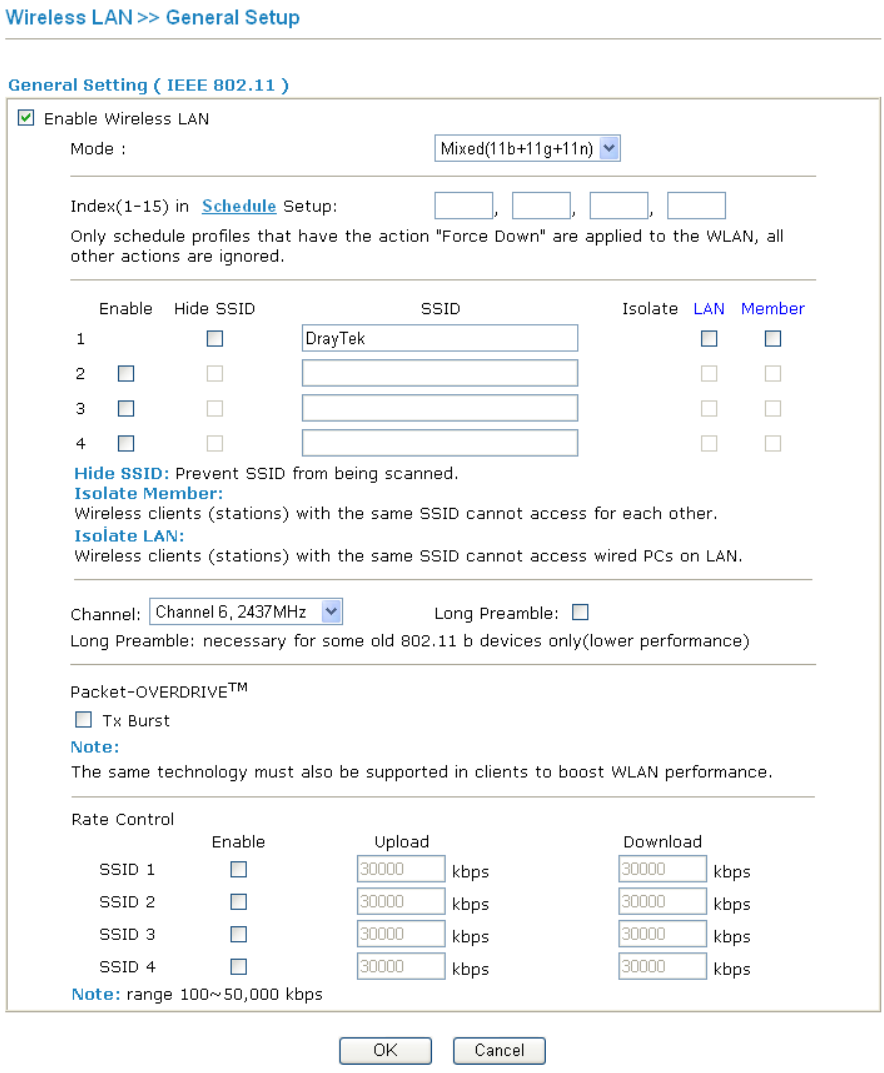
Separate the Wireless and the Wired LAN- WLAN Isolation enables you to isolate your wireless LAN from wired LAN for either quarantine or limit access reasons. To isolate means neither of the parties can access each other. To elaborate an example for business use, you may set up a wireless LAN for visitors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

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

Below shows the menu items for Wireless LAN.

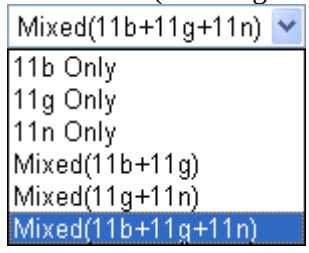
4.12.2 General Setup

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



Enable Wireless LAN Check the box to enable wireless function.

Mode At present, the router can connect to Mixed (11b+11g), 11g Only, 11b Only, Mixed (11g+11n), 11n Only and Mixed (11b+11g+11n) stations simultaneously. Simply choose Mix (11b+11g+11n) mode.



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.

Hide SSID

Check it to prevent from wireless sniffing and make it harder for unauthorized clients or STAs to join your wireless LAN. Depending on the wireless utility, the user may only see the information except SSID or just cannot see any thing about Vigor wireless router while site surveying. The system allows you to set four sets of SSID for different usage. In default, the first set of SSID will be enabled. You can hide it for your necessity.

SSID

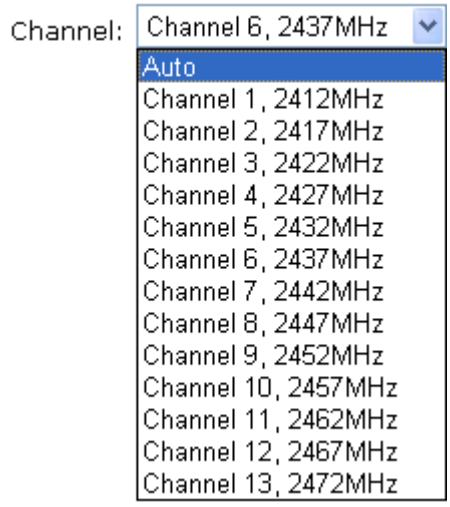
Means the identification of the wireless LAN. SSID can be any text numbers or various special characters. The default SSID is "Draytek. We suggest you to change it.

Isolate

LAN – Check this box to make the wireless clients (stations) with the same SSID cannot access wired PCs on LAN.
Member –Check this box to make the wireless clients (stations) with the same SSID not accessing for each other.

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. If you have no idea of choosing the frequency, please select Auto to let system determine for you.



Long Preamble

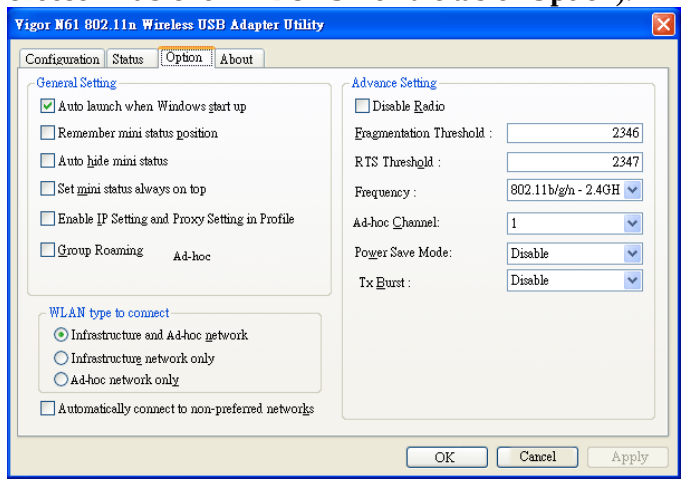
This option is to define the length of the sync field in an 802.11 packet. Most modern wireless network uses short preamble with 56 bit sync filed instead of long preamble with 128 bit sync field. However, some original 11b wireless network devices only support long preamble. Check it to use **Long Preamble**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

Packet-OVERDRIVE

This feature can enhance the performance in data transmission about 40%* more (by checking **Tx Burs**t). It is active only when both sides of Access Point and Station (in wireless client) invoke this function at the

same time. That is, the wireless client must support this feature and invoke the function, too.

Note: Vigor N61 wireless adapter supports this function. Therefore, you can use and install it into your PC for matching with Packet-OVERDRIVE (refer to the following picture of Vigor N61 wireless utility window, choose **Enable** for **TxBURST** on the tab of **Option**).

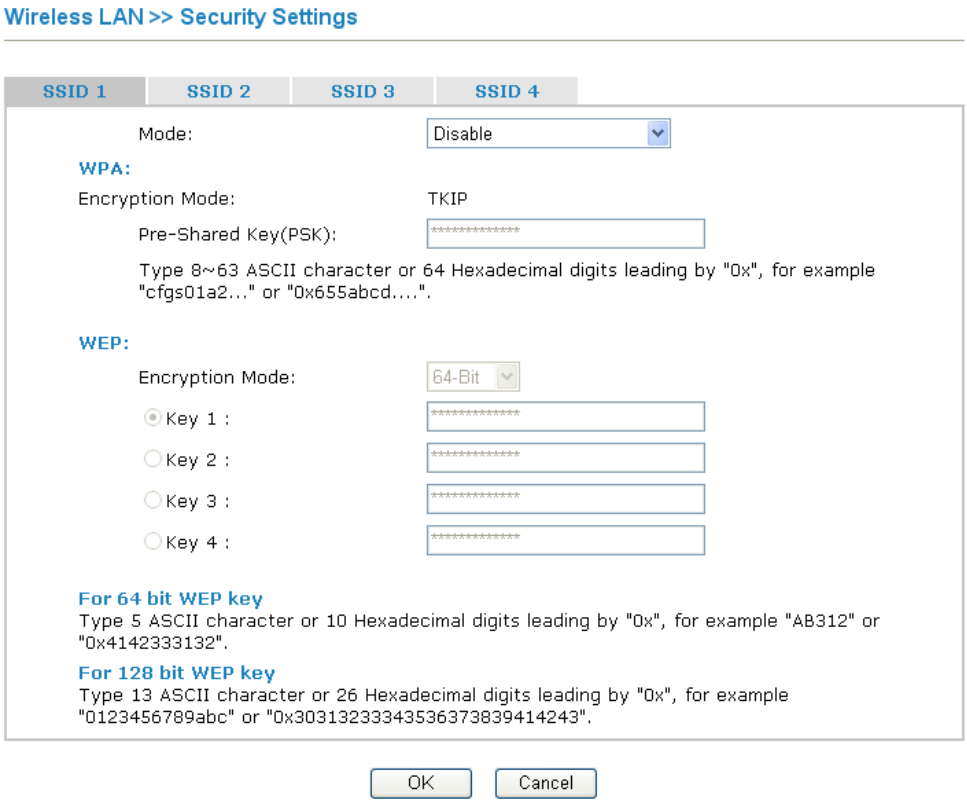


Rate Control It controls the data transmission rate through wireless connection.
Upload – Check Enable and type the transmitting rate for data upload. Default value is 30,000 kbps.
Download – Type the transmitting rate for data download. Default value is 30,000 kbps.

4.12.3 Security

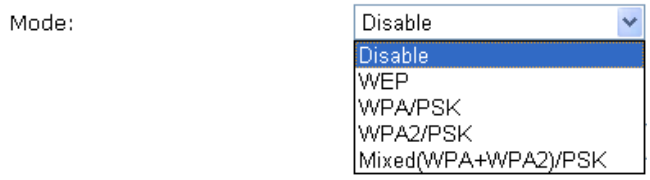
This page allows you to set security with different modes for SSID 1, 2, 3 and 4 respectively. After configuring the correct settings, please click **OK** to save and invoke it.

By clicking the **Security Settings**, a new web page will appear so that you could configure the settings of WEP and WPA.



Mode

There are several modes provided for you to choose.



Disable - Turn off the encryption mechanism.
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.

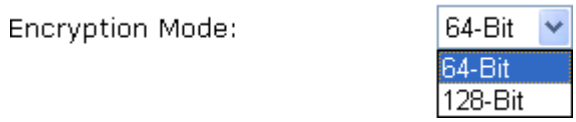
WPA

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...").
Type - Select from Mixed (WPA+WPA2) or WPA2 only.

Pre-Shared Key (PSK) - Either **8~63** ASCII characters, such as 012345678..(or 64 Hexadecimal digits leading by 0x, such as "0x321253abcde...").

WEP

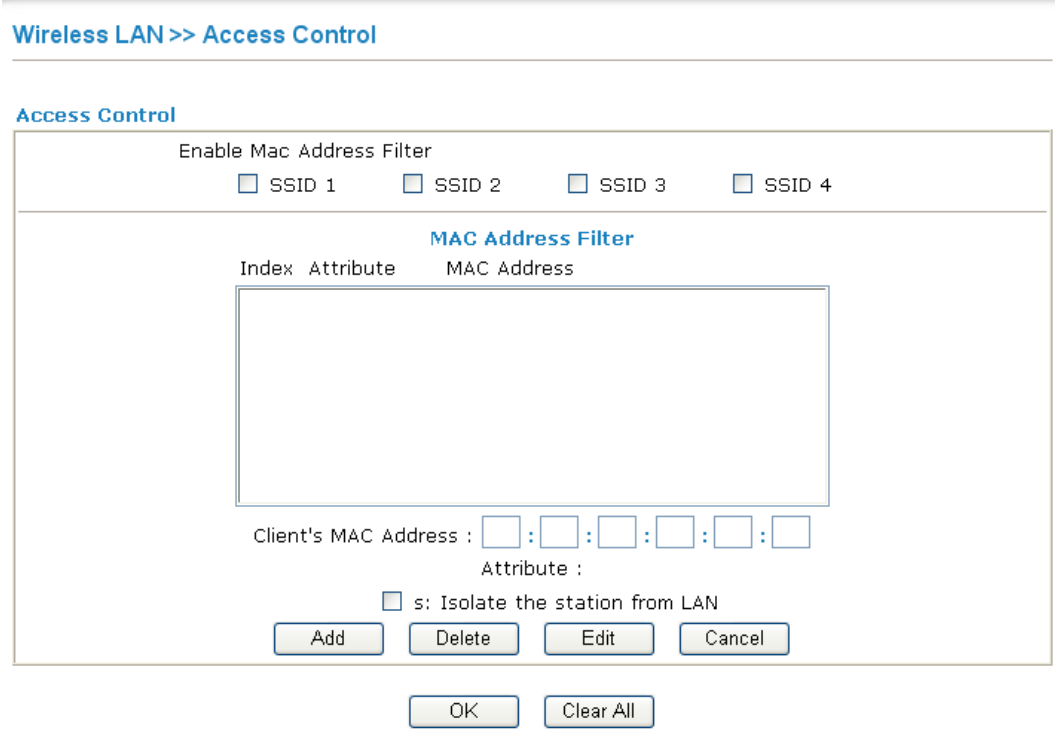
64-Bit - For 64 bits WEP key, either **5** ASCII characters, such as 12345 (or 10 hexadecimal digitals leading by 0x, such as 0x4142434445.)
128-Bit - For 128 bits WEP key, either **13** ASCII characters, such as ABCDEFGHIJKLM (or 26 hexadecimal digits leading by 0x, such as 0x41424344454647484 94A4B4C4D).



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.

4.12.4 Access Control

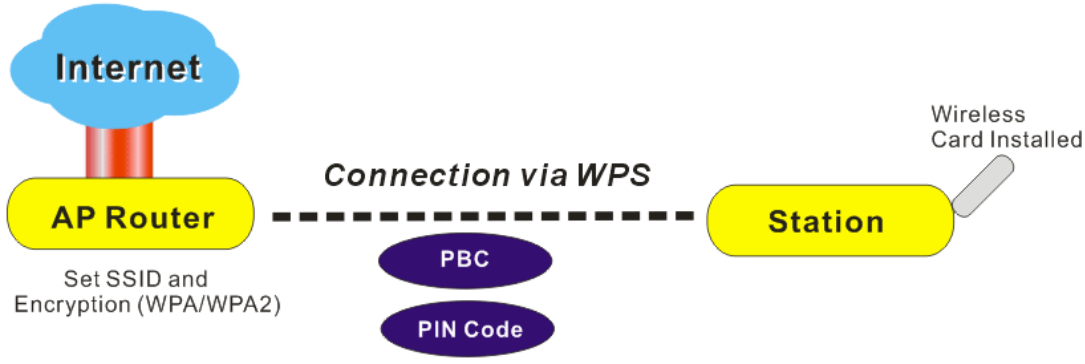
For additional security of wireless access, the **Access Control** facility allows you to restrict the network access right by controlling the wireless LAN MAC address of client. Only the valid MAC address that has been configured can access the wireless LAN interface. By clicking the **Access Control**,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



Enable Max Access Filter	Select to enable the MAC Address filter for wireless LAN identified with SSID 1 to 4 respectively. All the clients (expressed by MAC addresses) listed in the box can be grouped under different wireless LAN. For example, they can be grouped under SSID 1 and SSID 2 at the same time if you check SSID 1 and SSID 2.
MAC Address Filter	Display all MAC addresses that are edited before.
Client's MAC Address	Manually enter the MAC address of wireless client.
Attribute	**s: Isolate the station from LAN -** select to isolate the wireless connection of the wireless client of the MAC address from LAN.
Add	Add a new MAC address into the list.
Delete	Delete the selected MAC address in the list.
Edit	Edit the selected MAC address in the list.
Cancel	Give up the access control set up.
OK	Click it to save the access control list.
Clear All	Clean all entries in the MAC address list.

4.12.5 WPS

WPS (Wi-Fi Protected Setup) provides easy procedure to make network connection between wireless station and wireless access point (vigor router) with the encryption of WPA and WPA2.

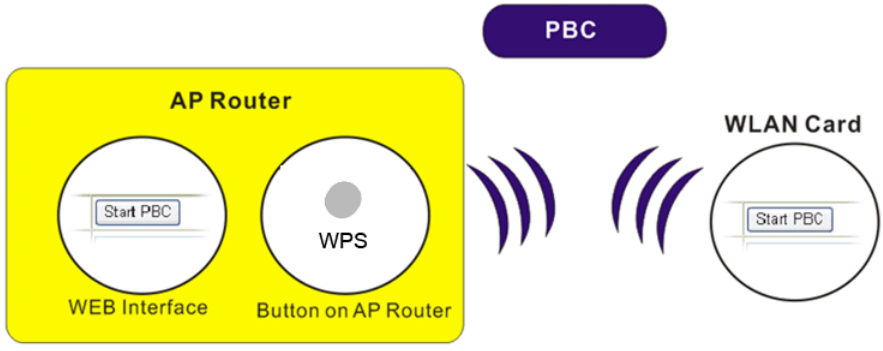


Note: Such function is available for the wireless station with WPS supported.

It is the simplest way to build connection between wireless network clients and vigor router. Users do not need to select any encryption mode and type any long encryption passphrase to setup a wireless client every time. He/she only needs to press a button on wireless client, and WPS will connect for client and router automatically.

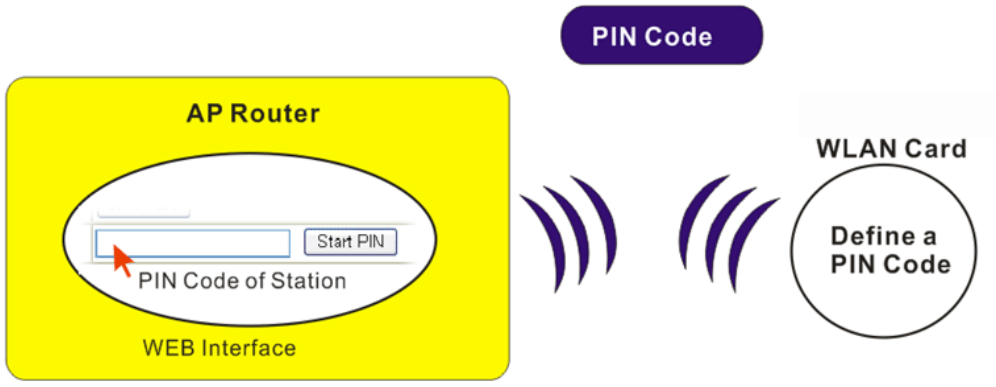
There are two methods to do network connection through WPS between AP and Stations: pressing the ***Start PBC*** button or using ***PIN Code***.

- On the side of Vigor 2710 series which served as an AP, press **WPS** button once on the front panel of the router or click **Start PBC** on web configuration interface. On the side of a station with network card installed, press **Start PBC** button of network card.

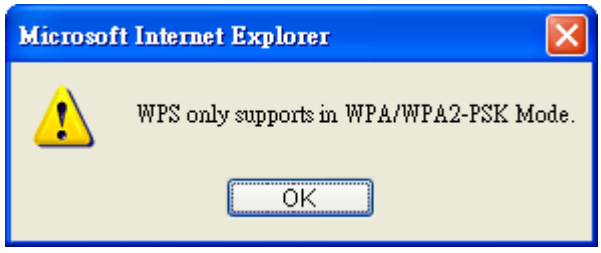


- If you want to use PIN code, you have to know the PIN code specified in wireless client. Then provide the PIN code of the wireless client you wish to connect to the

vigor router.

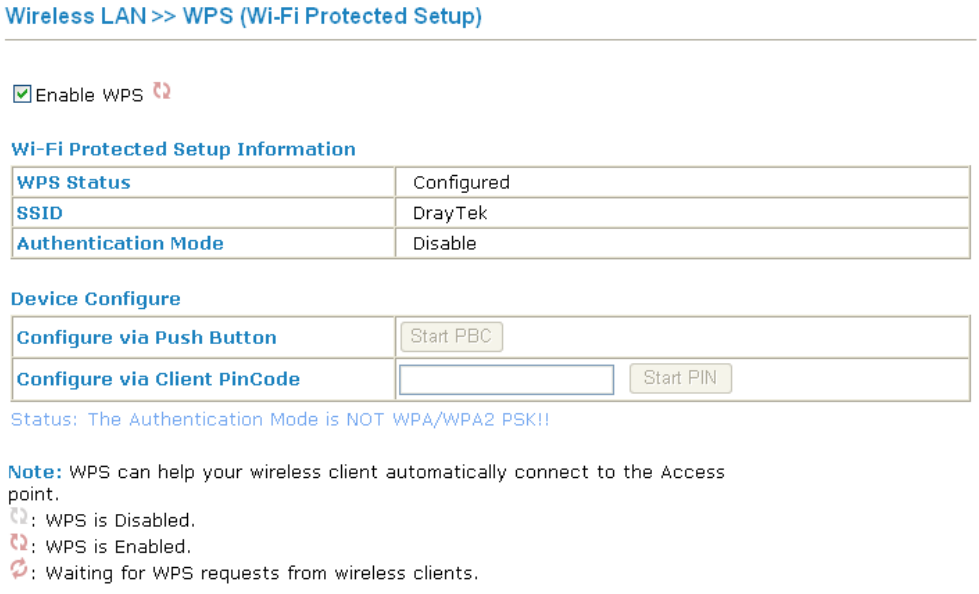


For WPS is supported in WPA-PSK or WPA2-PSK mode, if you do not choose such mode in **Wireless LAN>>Security**, you will see the following message box.



Please click **OK** and go back **Wireless LAN>>Security** to choose WPA-PSK or WPA2-PSK mode and access WPS again.

Below shows **Wireless LAN>>WPS** web page.



Enable WPS	Check this box to enable WPS setting.
WPS Status	Display related system information for WPS. If the wireless security (encryption) function of the router is properly configured, you can see 'Configured' message here.
SSID	Display the SSID1 of the router. WPS is supported by SSID1 only.

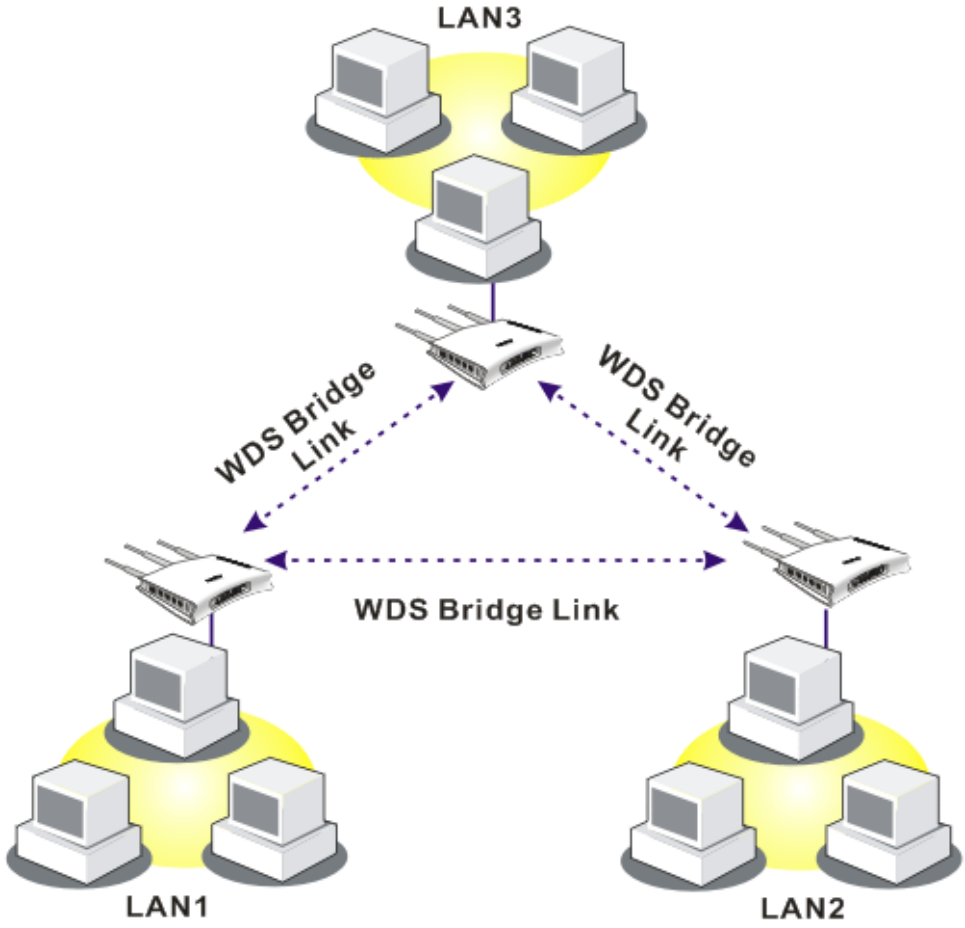
Authentication Mode	Display current authentication mode of the router. Only WPA2/PSK and WPA/PSK support WPS.
Configure via Push Button	Click **Start PBC** to invoke Push-Button style WPS setup procedure. The router will wait for WPS requests from wireless clients about two minutes. The WPS LED on the router will blink fast when WPS is in progress. It will return to normal condition after two minutes. (You need to setup WPS within two minutes)
Configure via Client PinCode	Please input the PIN code specified in wireless client you wish to connect, and click **Start PIN** button. The WLAN LED on the router will blink fast when WPS is in progress. It will return to normal condition after two minutes. (You need to setup WPS within two minutes)

4.12.6 WDS

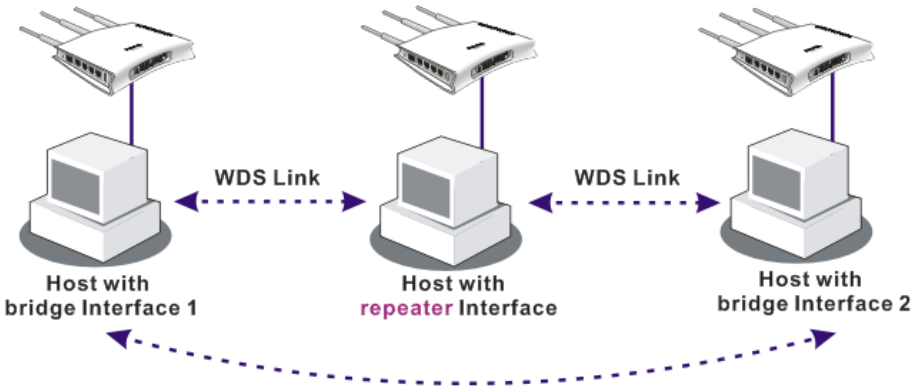
WDS means Wireless Distribution System. It is a protocol for connecting two access points (AP) wirelessly. Usually, it can be used for the following application:

- 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:

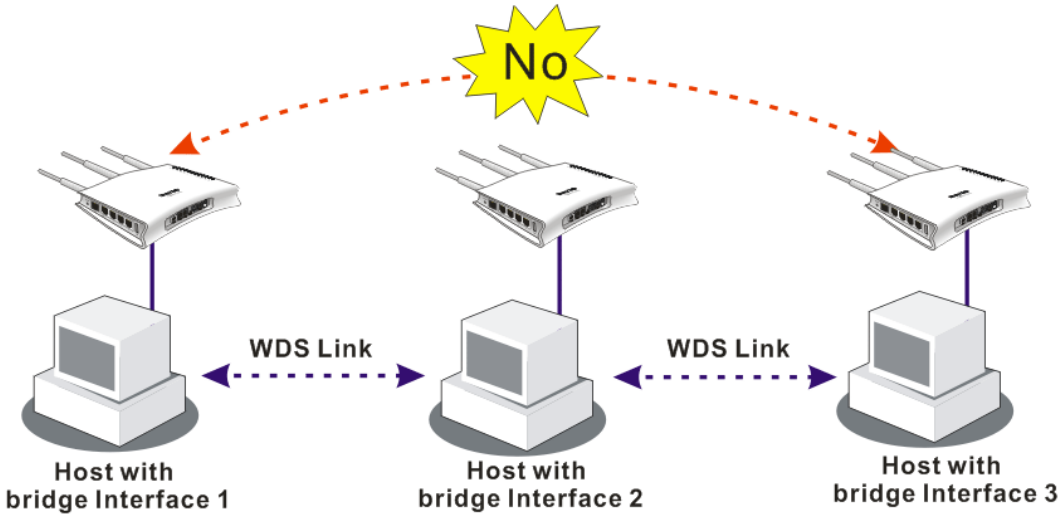


The application for the WDS-Repeater mode is depicted as below:

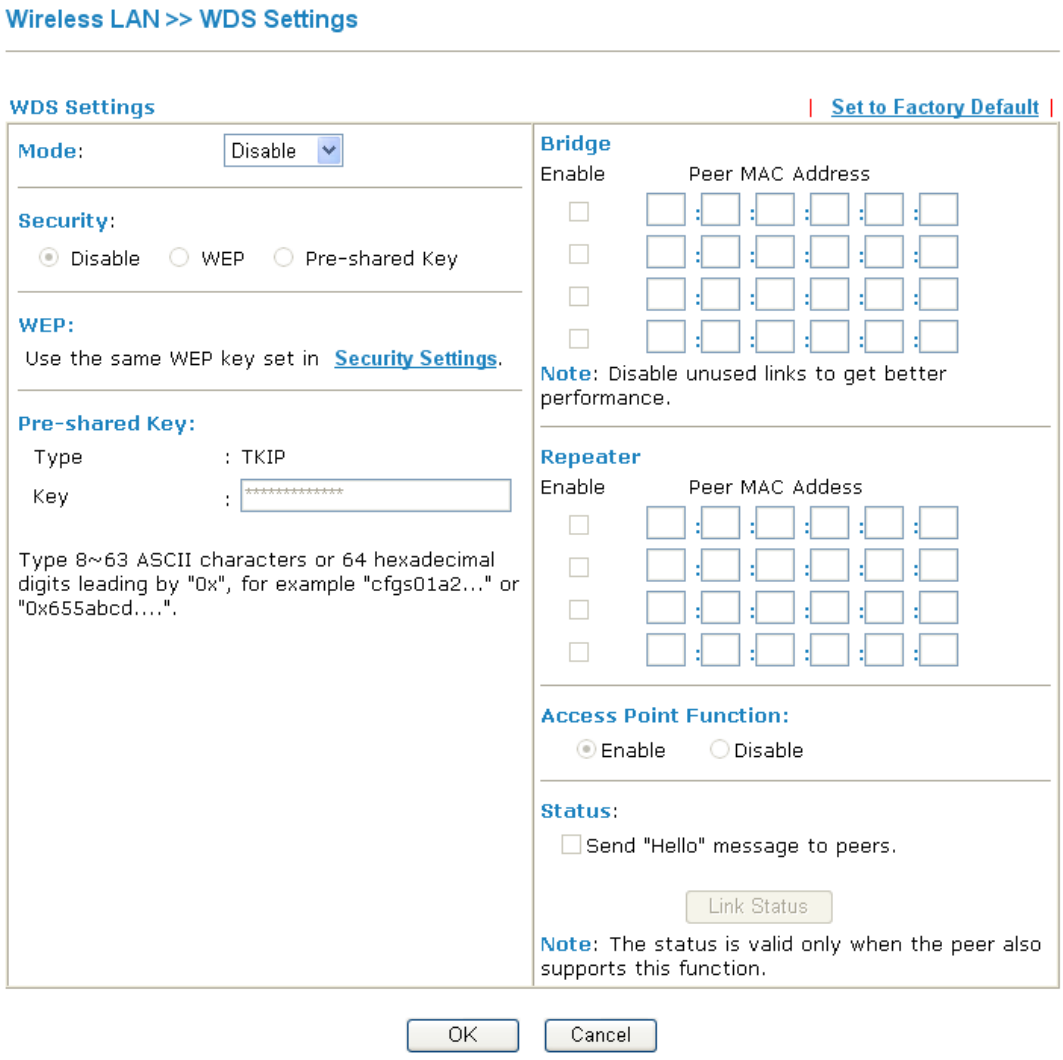


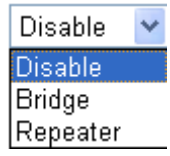
The major difference between these two modes is that: while in **Repeater** mode, the packets received from one peer AP can be repeated to another peer AP through WDS links. Yet in **Bridge** mode, packets received from a WDS link will only be forwarded to local wired or wireless hosts. In other words,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



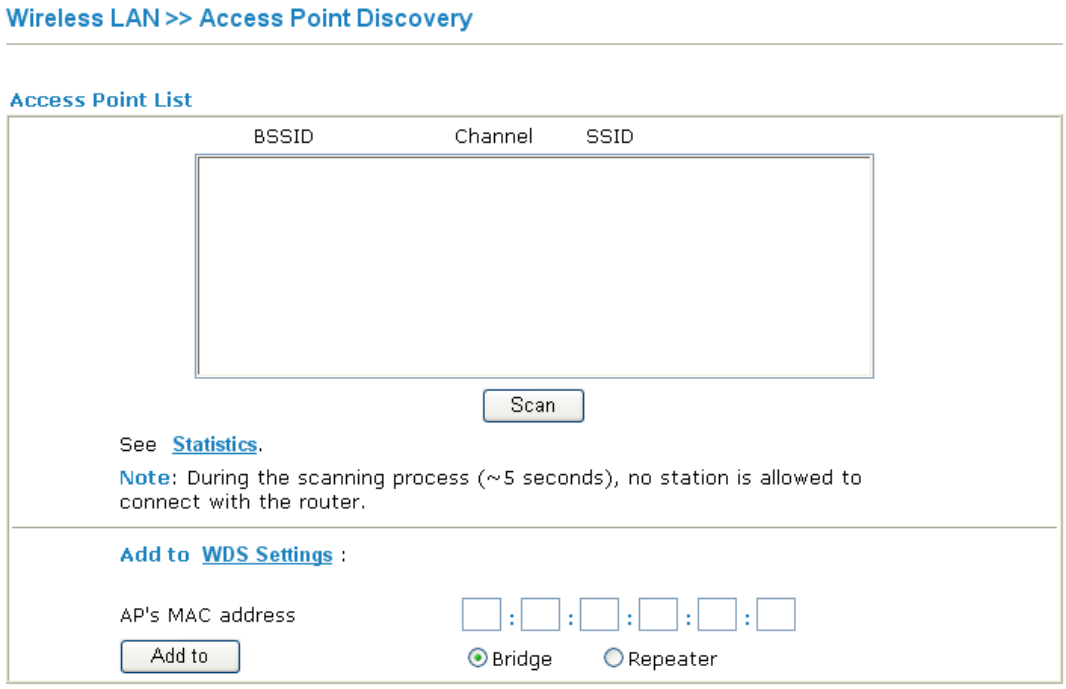
Mode	Choose the mode for WDS setting. **Disable** mode will not invoke any WDS setting. **Bridge** mode is designed to fulfill the first type of application. **Repeater** mode is for the second one. 
Security	There are three types for security, **Disable**, **WEP** and **Pre-shared key**. The setting 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.
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. Four 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. Four 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.

4.12.6 AP Discovery

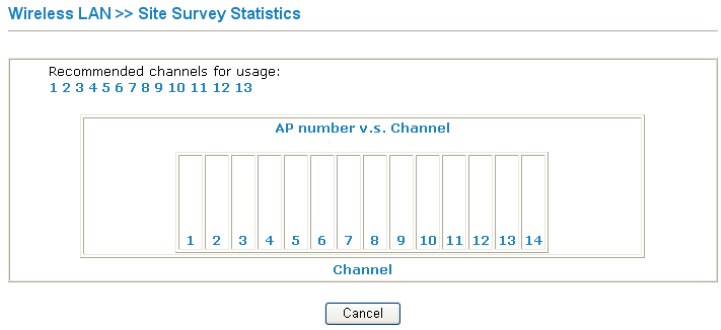
Vigor router can scan all regulatory channels and find working APs in the neighborhood. Based on the scanning result, users will know which channel is clean for usage. Also, it can be used to facilitate finding an AP for a WDS link. Notice that during the scanning process (about 5 seconds), no client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

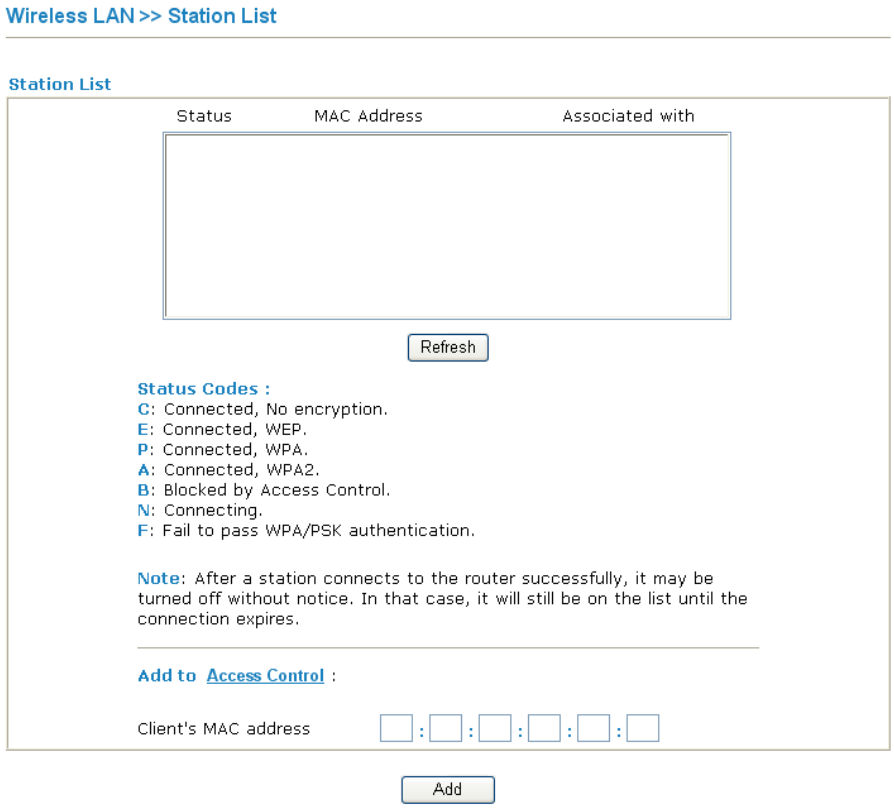
Statistics It displays the statistics for the channels used by APs.



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

4.12.7 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.



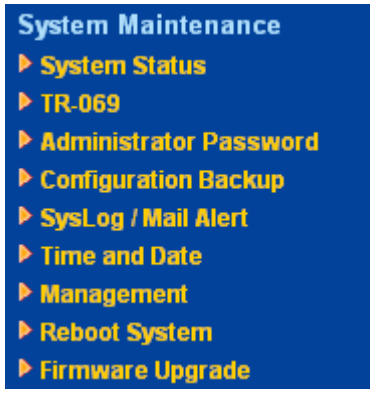
Refresh Click this button to refresh the status of station list.

Add Click this button to add current typed MAC address into **Access Control**.

4.13 System Maintenance

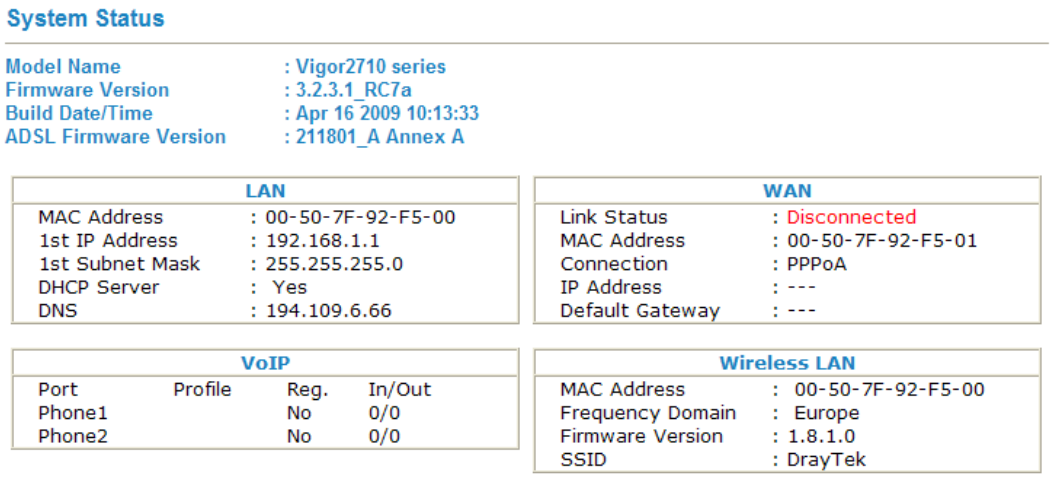
For the system setup, there are several items that you have to know the way of configuration: Status, Administrator Password, Configuration Backup, Syslog, Time setup, Reboot System, Firmware Upgrade.

Below shows the menu items for System Maintenance.



4.13.1 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.

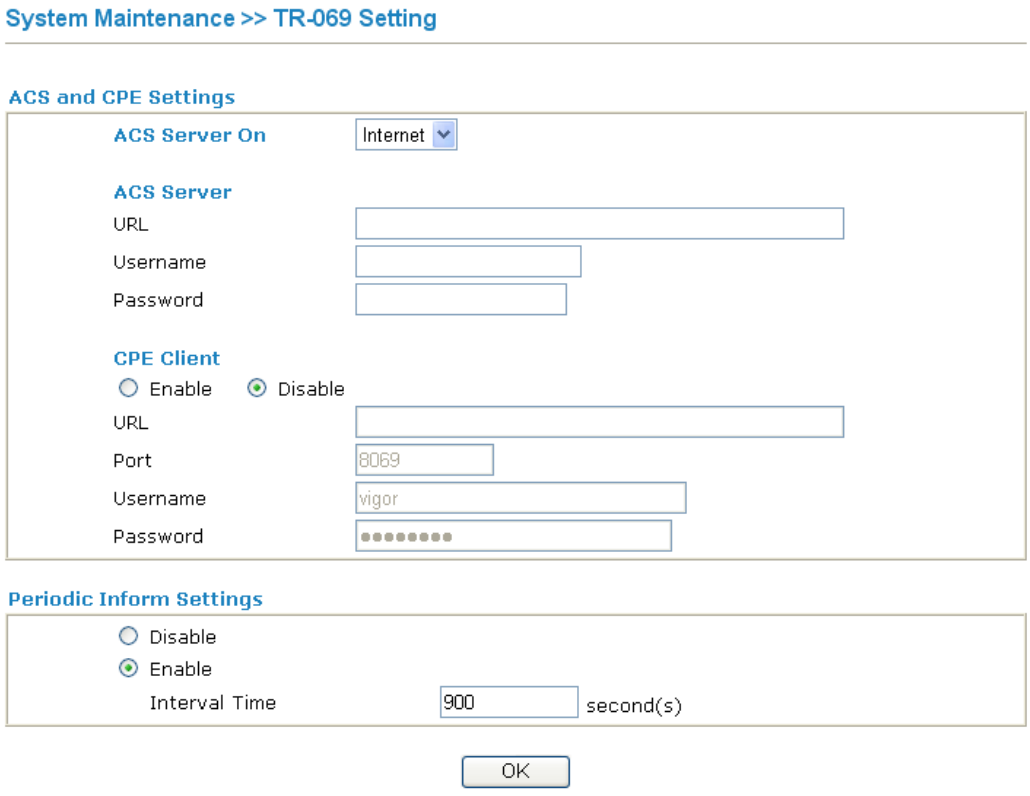


Model Name	Display the model name of the router.
Firmware Version	Display the firmware version of the router.
Build Date/Time	Display the date and time of the current firmware build.
ADSL Firmware Version	Display the ADSL firmware version.
***LAN*-------**	
MAC Address	Display the MAC address of the LAN Interface.
1st IP Address	Display the IP address of the LAN interface.
1st Subnet Mask	Display the subnet mask address of the LAN interface.

DHCP Server	Display the current status of DHCP server of the LAN interface.
DNS	Display the assigned IP address of the primary DNS.
WAN-------	
Link Status	Display current connection status.
MAC Address	Display the MAC address of the WAN Interface.
Connection	Display the connection type.
IP Address	Display the IP address of the WAN interface.
Default Gateway	Display the assigned IP address of the default gateway.
VoIP-------	
Port	Indicate the VoIP phone port.
Profile	Display the profile name for SIP account.
In/Out	Display the number for incoming/outgoing phone call.
Wireless LAN-------	
MAC Address	Display the MAC address of the wireless LAN.
Frequency Domain	It can be Europe (13 usable channels), USA (11 usable channels) etc. The available channels supported by the wireless products in different countries are various.
Firmware Version	It indicates information about equipped WLAN miniPCi card. This also helps to provide availability of some features that are bound with some WLAN miniPCi.
SSID	Display the SSID of the router.

4.13.2 TR-069

This device supports TR-069 standard. It is very convenient for an administrator to manage a TR-069 device through an Auto Configuration Server, e.g., VigorACS.



ACS Server On — Choose the interface for the router connecting to ACS server.

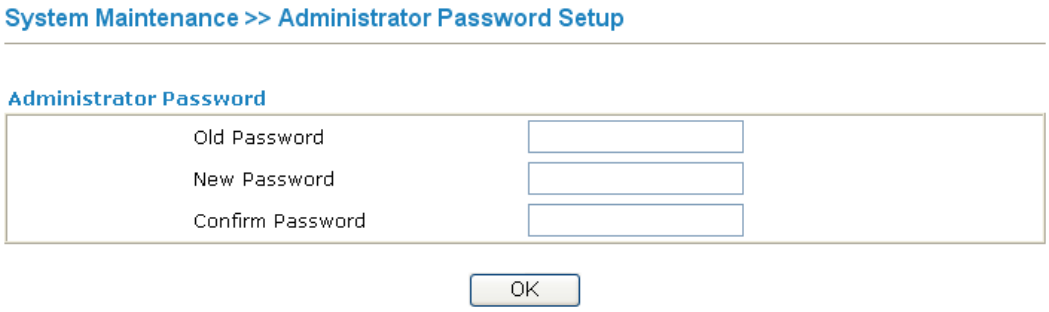
ACS Server — **URL/Username/Password –** Such data must be typed according to the ACS (Auto Configuration Server) you want to link. Please refer to Auto Configuration Server user's manual for detailed information.

CPE Client — It is not necessary for you to type them. Such information is useful for Auto Configuration Server.
Enable/Disable – Sometimes, port conflict might be occurred. To solve such problem, you might want to change port number for CPE. Please click Enable and change the port number.

Periodic Inform Settings — The default setting is **Enable**. Please set interval time or schedule time for the router to send notification to CPE. Or click **Disable** to close the mechanism of notification.

4.13.3 Administrator Password

This page allows you to set new password.



Old Password	Type in the old password. The factory default setting for password is **"admin"**.
New Password	Type in new password in this filed.
Confirm Password	Type in the new password again.

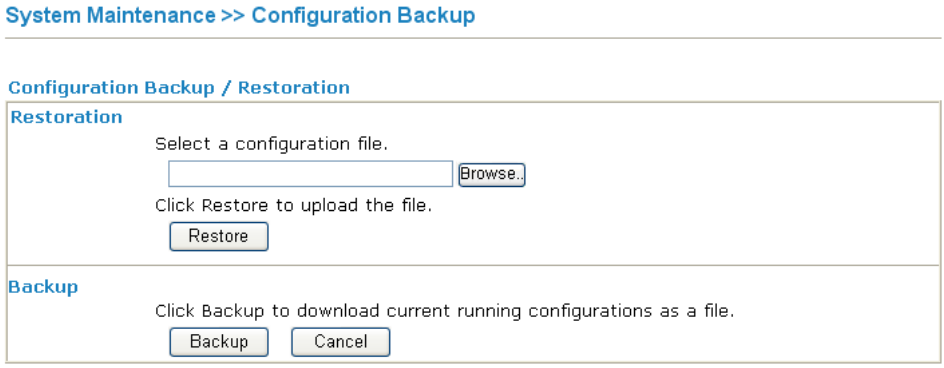
When you click OK, the login window will appear. Please use the new password to access into the web configurator again.

4.13.4 Configuration Backup

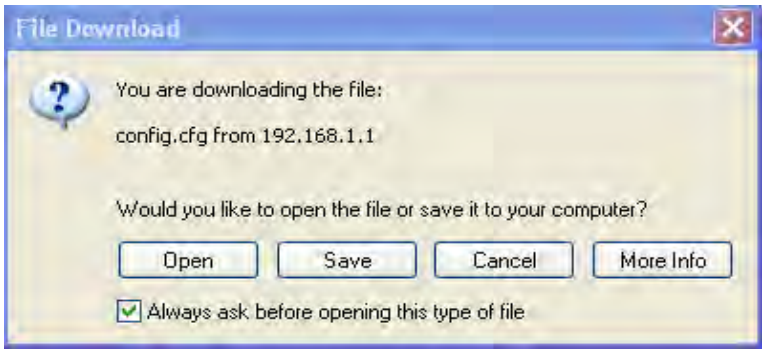
Backup the Configuration

Follow the steps below to backup your configuration.

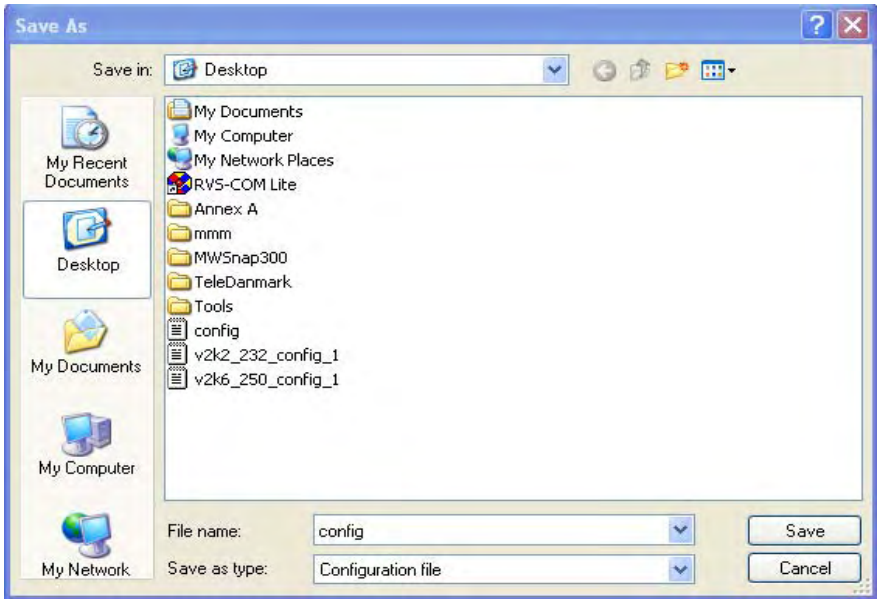
1. Go to **System Maintenance** >> **Configuration Backup**. The following windows will be popped-up, as shown below.



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



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



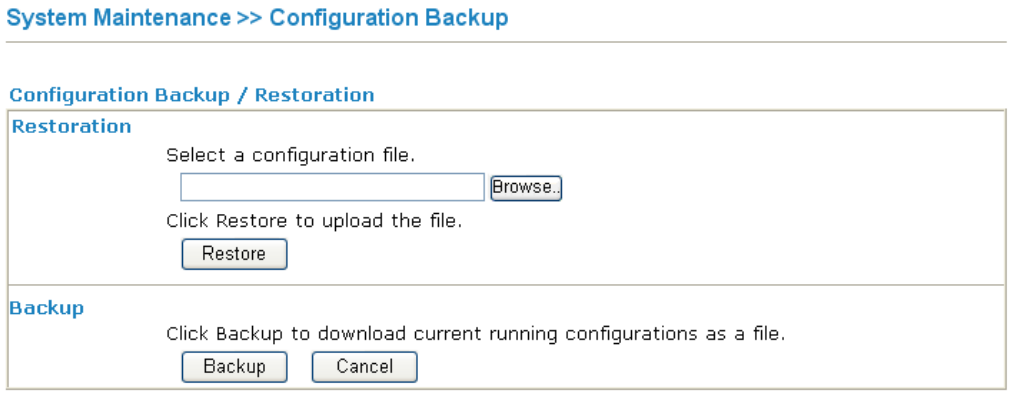
4. Click **Save** button, the configuration will download automatically to your computer as a file named **config.cfg**.

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

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

Restore Configuration

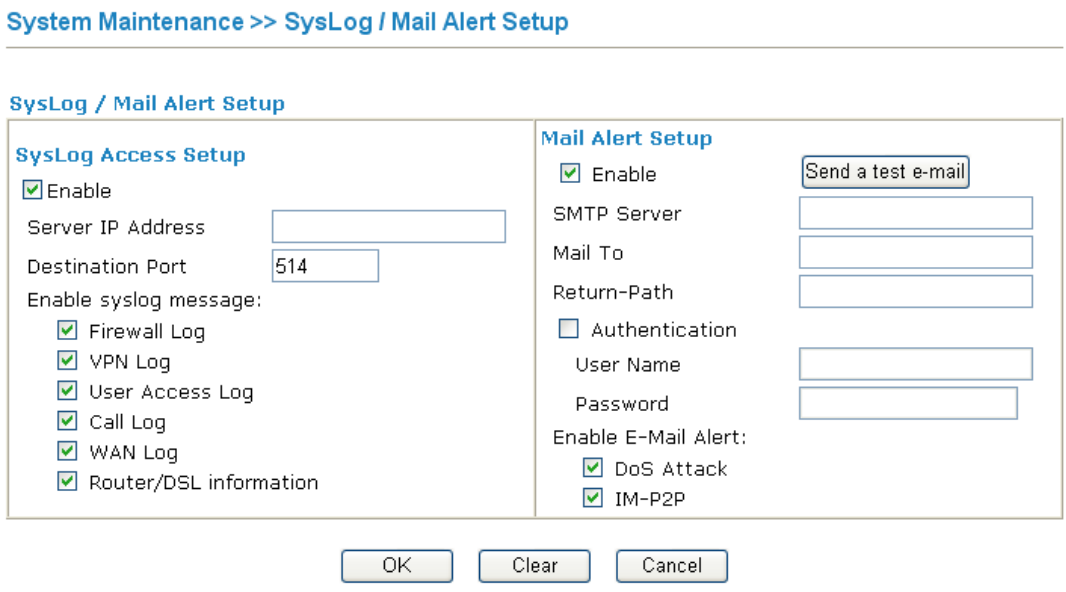
1. Go to **System Maintenance** >> **Configuration Backup**. The following windows will be popped-up, as shown below.



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

4.13.5 Syslog/Mail Alert

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



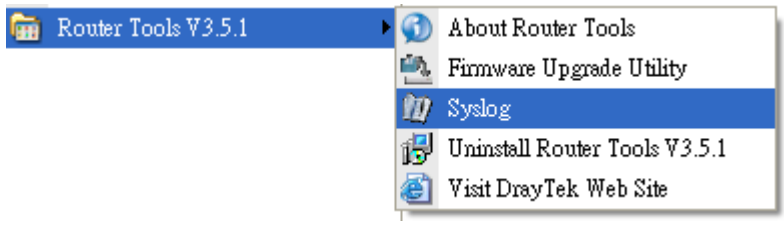
Enable (Syslog Access…)	Check "**Enable**" to activate function of syslog.
Syslog Server IP	The IP address of the Syslog server.
Destination Port	Assign a port for the Syslog protocol.
Enable syslog message	Check the box listed on this web page to send the corresponding message of firewall, VPN, User Access, Call, WAN, Router/DSL information to Syslog.
Enable (Alert Setup…)	Check "**Enable**" to activate function of mail alert.

Send a test e-mail	Make a simple test for the e-mail address specified in this page. Please assign the mail address first and click this button to execute a test for verify the mail address is available or not.
SMTP Server	The IP address of the SMTP server.
Mail To	Assign a mail address for sending mails out.
Return-Path	Assign a path for receiving the mail from outside.
Authentication	Check this box to activate this function while using e-mail application.
User Name	Type the user name for authentication.
Password	Type the password for authentication.
Enable E-mail Alert	Check the box to send alert message to the e-mail box while the router detecting the item(s) you specify here.

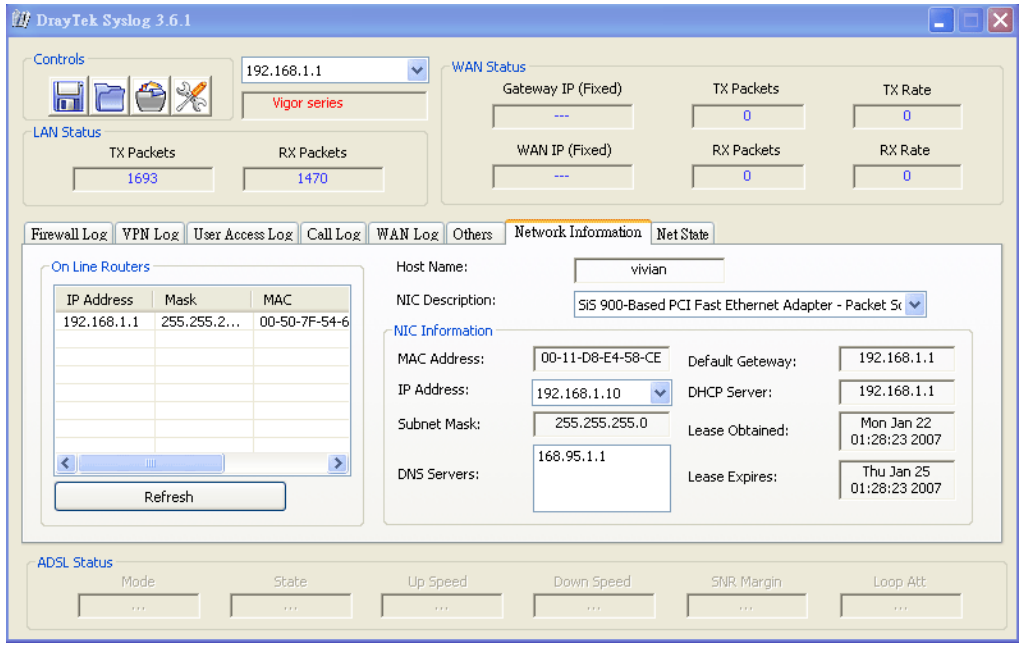
Click **OK** to save these settings.

For viewing the Syslog, please do the following:

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

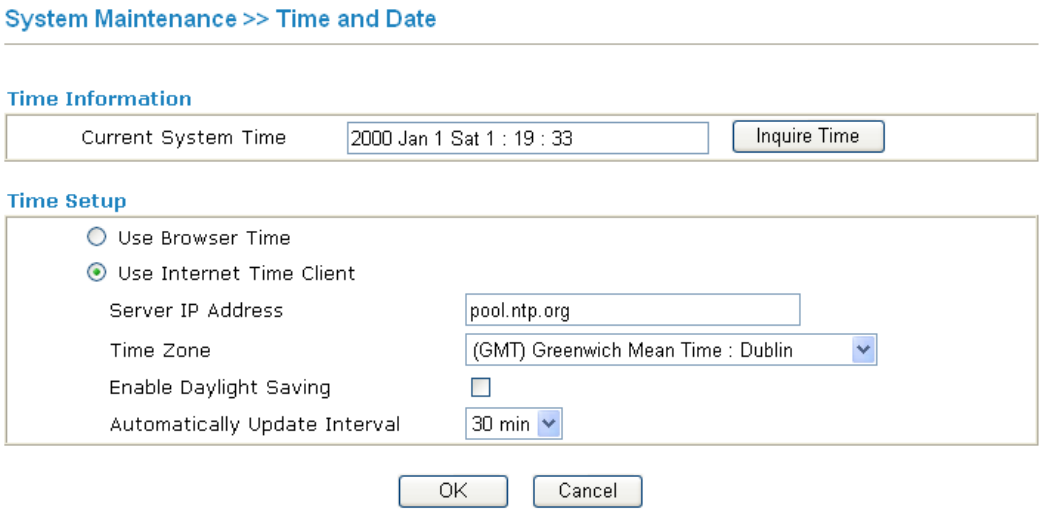


3. From the Syslog screen, select the router you want to monitor. Be reminded that in **Network Information**, select the network adapter used to connect to the router. Otherwise, you won't succeed in retrieving information from the router.



4.13.6 Time and Date

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

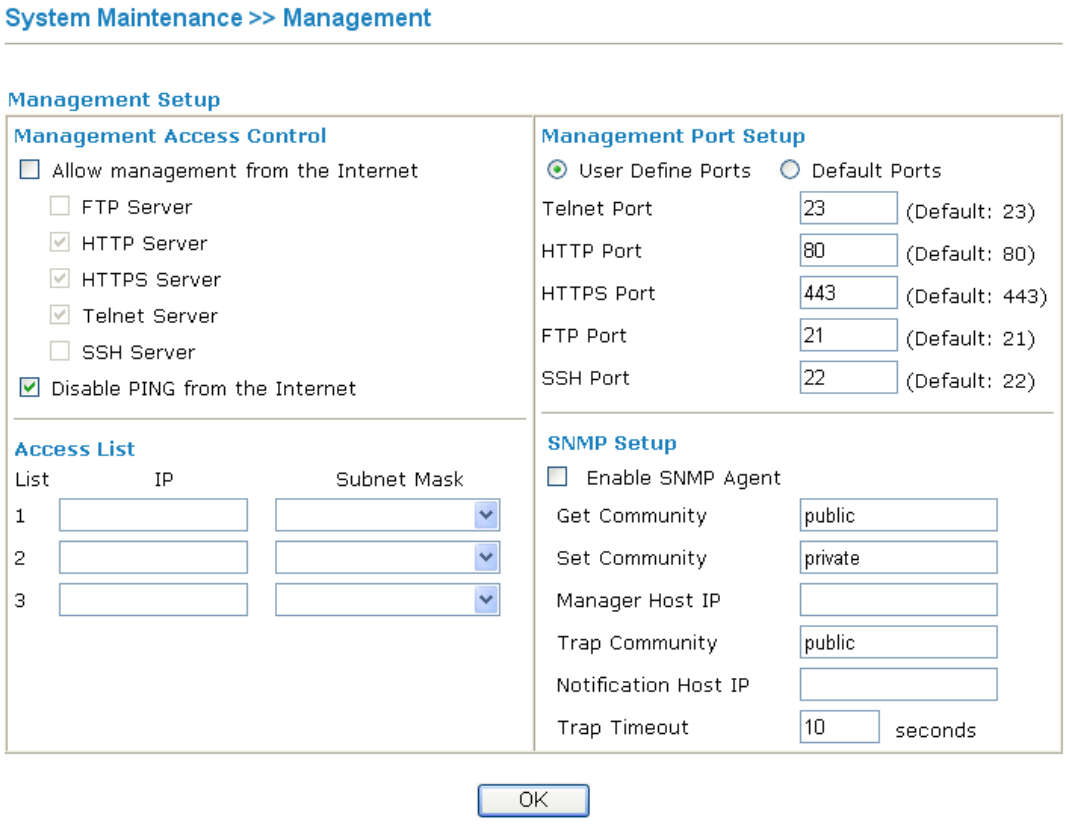


Current System Time	Click **Inquire Time** to get the current time.
Use Browser Time	Select this option to use the browser time from the remote administrator PC host as router's system time.
Use Internet Time	Select to inquire time information from Time Server on the Internet using assigned protocol.
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.

4.13.7 Management

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

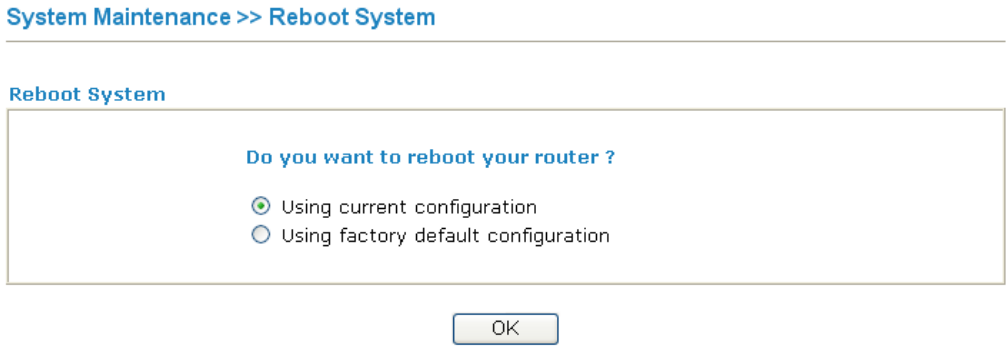


Allow management from the Internet	Enable the checkbox to allow system administrators to login from the Internet. There are several servers provided by the system to allow you managing the router from Internet. Check the box(es) to specify.
Disable PING from the Internet	Check the checkbox to reject all PING packets from the Internet. For security issue, this function is enabled by default.
Access List	You could specify that the system administrator can only login from a specific host or network defined in the list. A maximum of three IPs/subnet masks is allowed. **List IP** - Indicate an IP address allowed to login to the router. **Subnet Mask** - Represent a subnet mask allowed to login to the router.
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, HTTP and FTP 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.

4.13.8 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.

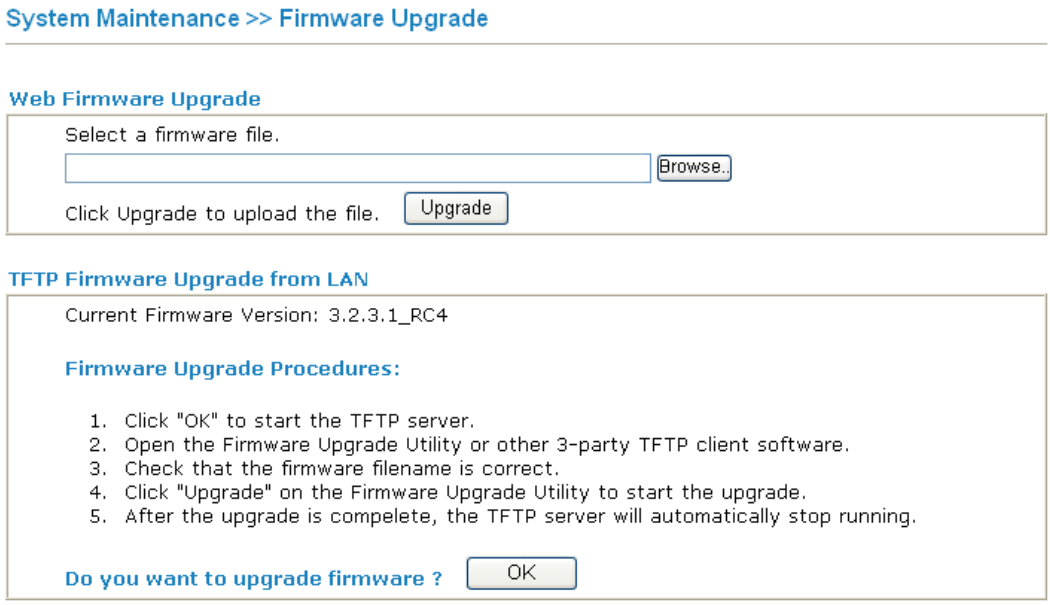
Note: When the system pops up Reboot System web page after you configure web settings, please click **OK** to reboot your router for ensuring normal operation and preventing unexpect errors of the router in the future.

4.13.9 Firmware Upgrade

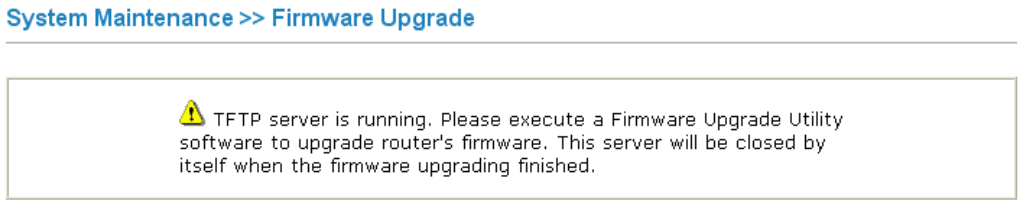
Before upgrading your router firmware, you need to install the Router Tools. The **Firmware Upgrade Utility** is included in the tools. The following web page will guide you to upgrade firmware by using an example. Note that this example is running over Windows OS (Operating System).

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

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



Click **OK**. The following screen will appear. Please execute the firmware upgrade utility first.

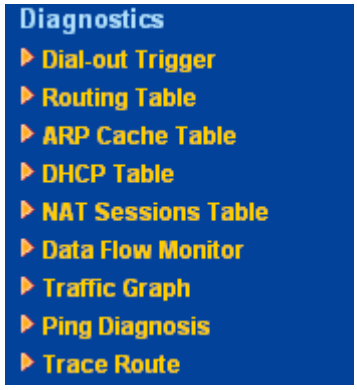


For the detailed information about firmware update, please go to Chapter 4.

4.14 Diagnostics

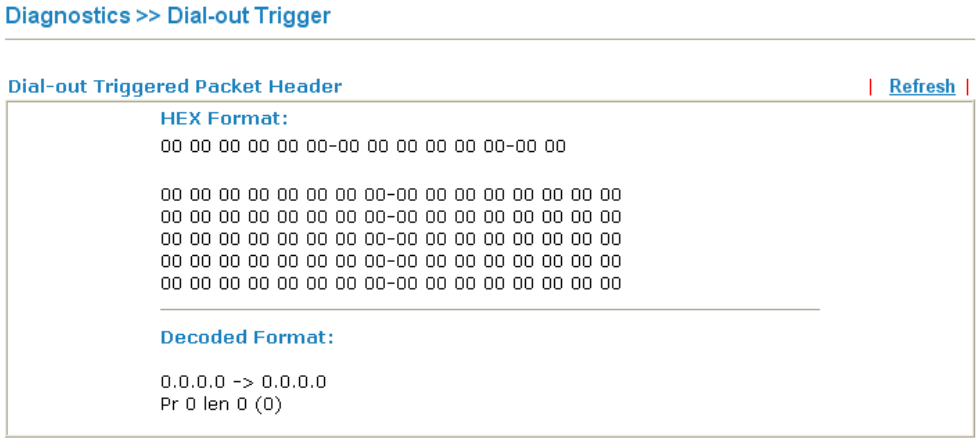
Diagnostic Tools provide a useful way to **view** or **diagnose** the status of your Vigor router.

Below shows the menu items for Diagnostics.



4.14.1 Dial-out Trigger

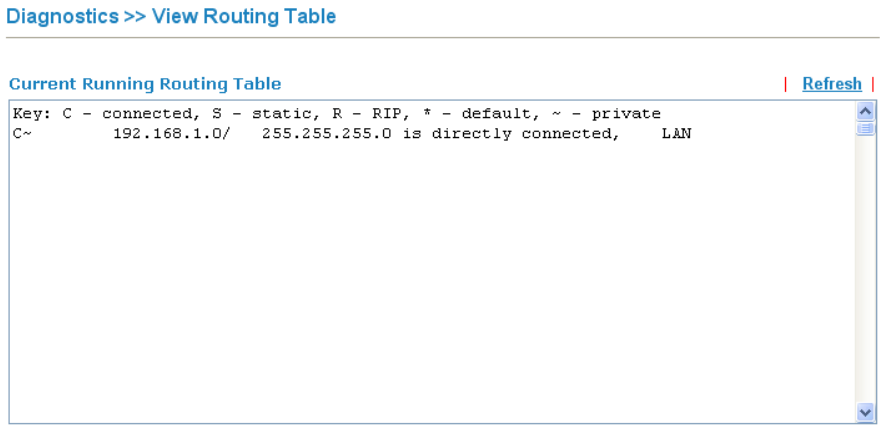
Click **Diagnostics** and click **Dial-out Trigger** to open the web page. The internet connection (e.g., PPPoE, PPPoA, etc) is triggered by a package sending from the source IP address.



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.

4.14.2 Routing Table

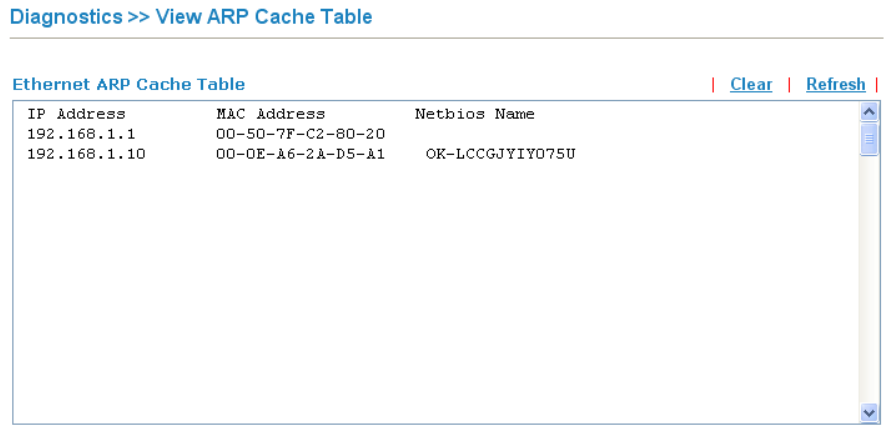
Click **Diagnostics** and click **Routing Table** to open the web page.



Refresh	Click it to reload the page.

4.14.3 ARP Cache Table

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

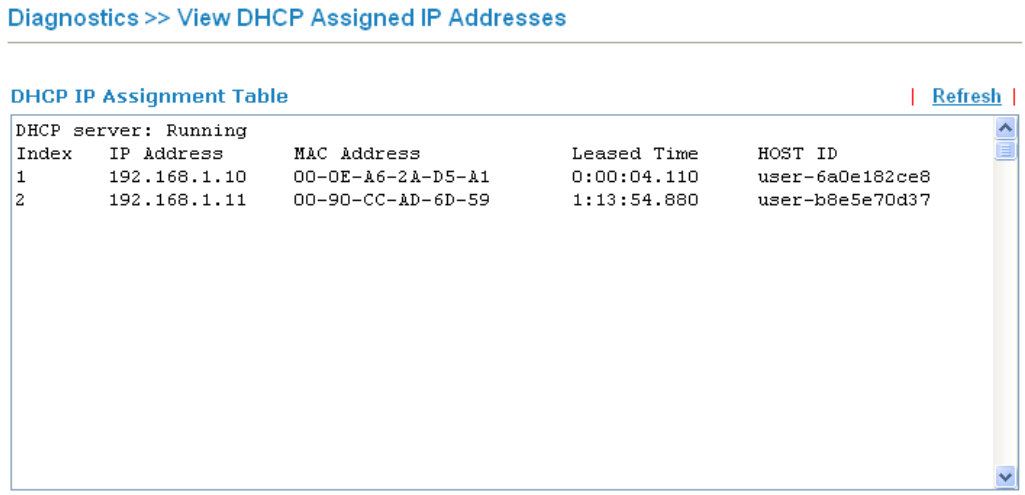


Refresh	Click it to reload the page.
Clear	Click it to clear the whole table.

4.14.4 DHCP Table

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

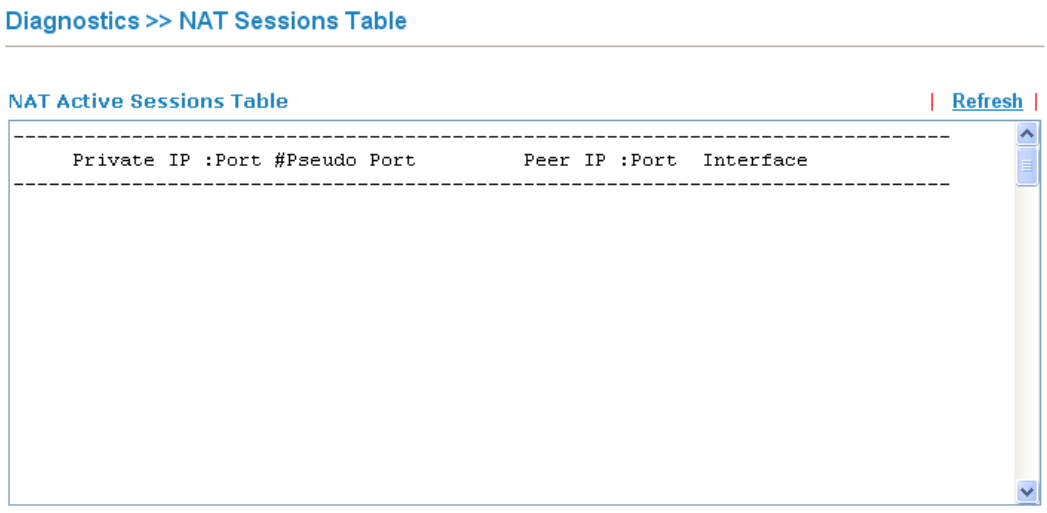
Click **Diagnostics** and click **DHCP Table** to open the web page.



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.

4.14.5 NAT Sessions Table

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

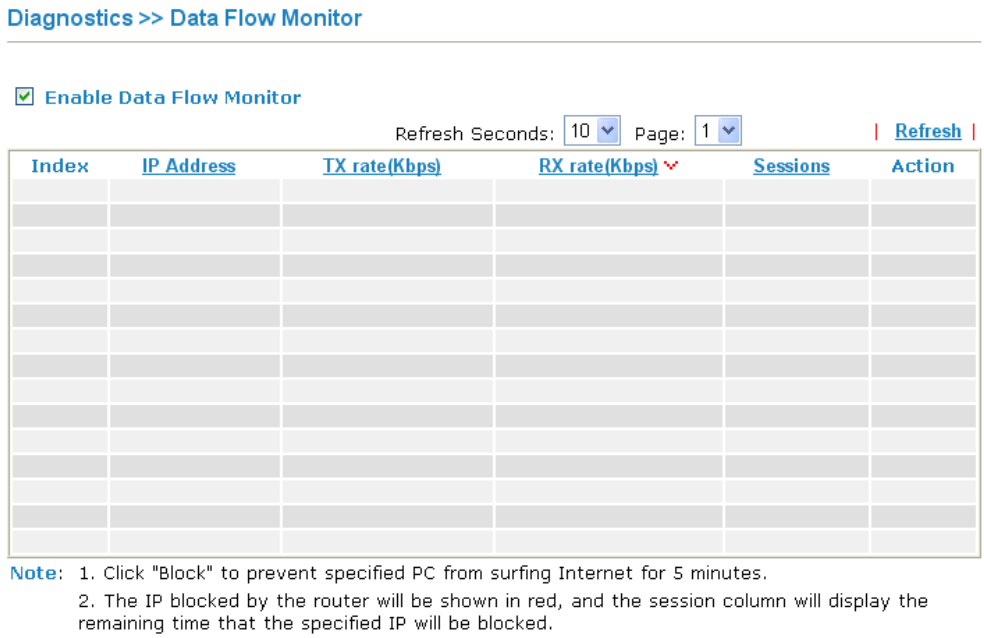


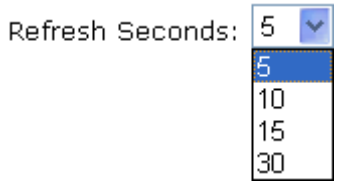
Private IP:Port	It indicates the source IP address and port of local PC.
#Pseudo Port	It indicates the temporary port of the router used for NAT.
Peer IP:Port	It indicates the destination IP address and port of remote host.
Interface	It displays the representing number for different interface.
Refresh	Click it to reload the page.

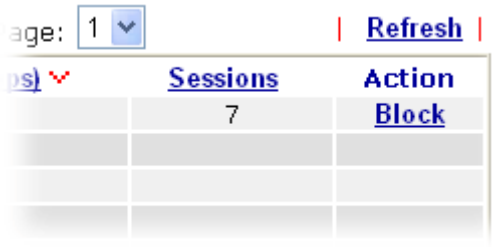
4.14.6 Data Flow Monitor

This page displays the running procedure for the IP address monitored and refreshes the data in an interval of several seconds. The IP address listed here is configured in Bandwidth Management. You have to enable IP bandwidth limit and IP session limit before invoke Data Flow Monitor. If not, a notification dialog box will appear to remind you enabling it.

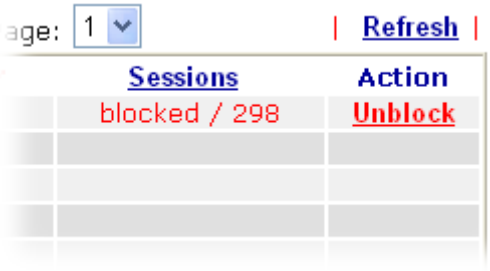
Click **Diagnostics** and click **Data Flow Monitor** to open the web page. You can click **IP Address**, **TX rate**, **RX rate** or **Session** link for arranging the data display.



Enable Data Flow Monitor	Check this box to enable this function.
Refresh Seconds	Use the drop down list to choose the time interval of refreshing data flow that will be done by the system automatically. 
Refresh	Click this link to refresh this page manually.
Index	Display the number of the data flow.
IP Address	Display the IP address of the monitored device.
TX rate (kbps)	Display the transmission speed of the monitored device.
RX rate (kbps)	Display the receiving speed of the monitored device.
Sessions	Display the session number that you specified in Limit Session web page.
Action	**Block** - can prevent specified PC accessing into Internet within 5 minutes.

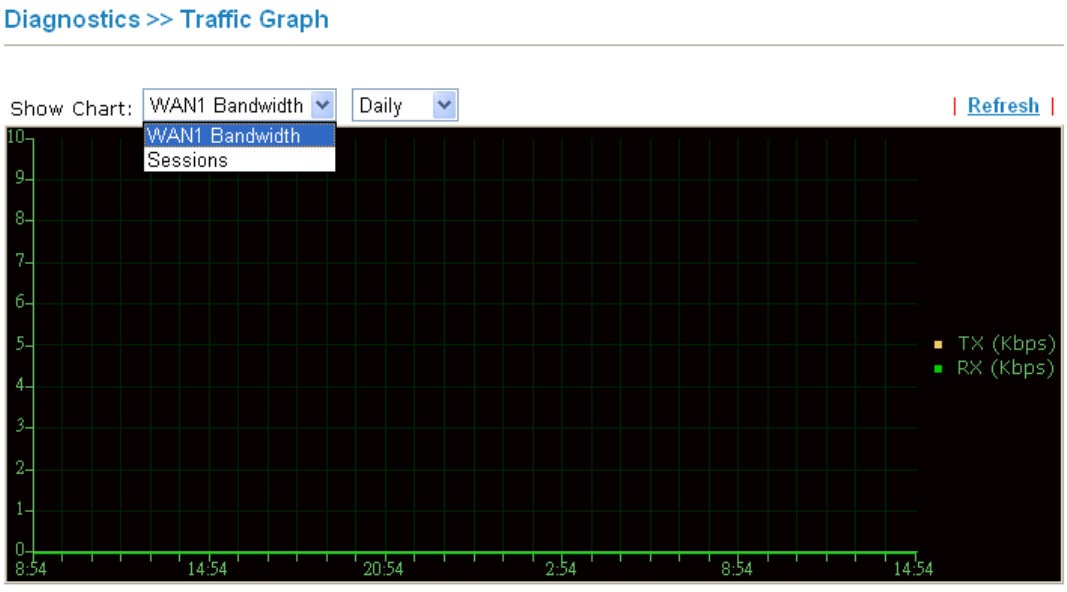


Unblock – the device with the IP address will be blocked in five minutes. The remaining time will be shown on the session column.



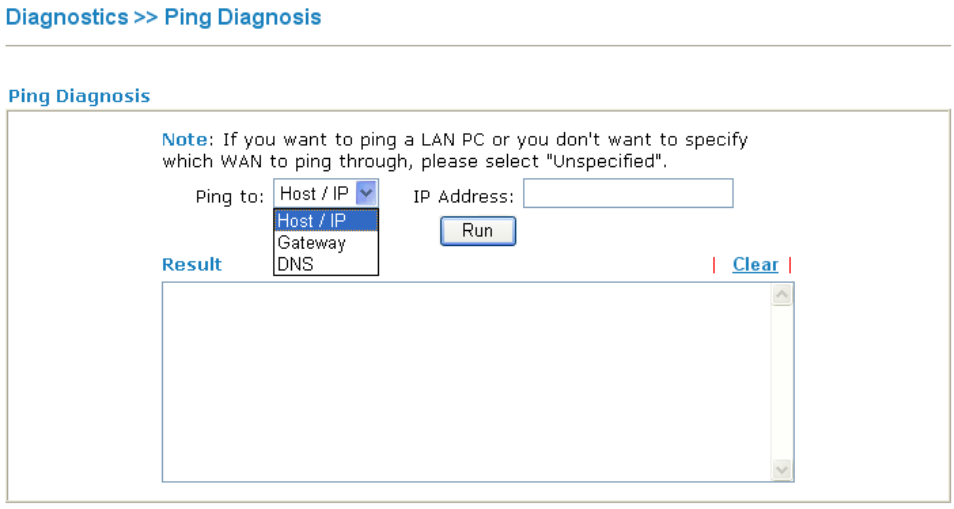
4.14.7 Traffic Graph

Click **Diagnostics** and click **Traffic Graph** to pen the web page. Choose WAN1 Bandwidth, Sessions, daily or weekly for viewing different traffic graph. Click **Refresh** to renew the graph at any time.



4.14.8 Ping Diagnosis

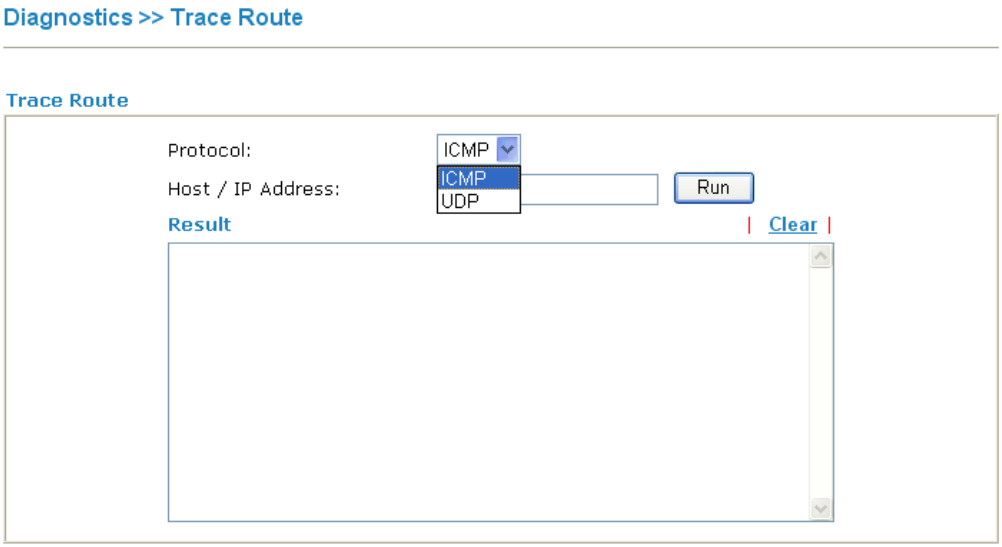
Click **Diagnostics** and click **Ping Diagnosis** to pen the web page.



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

4.14.9 Trace Route

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

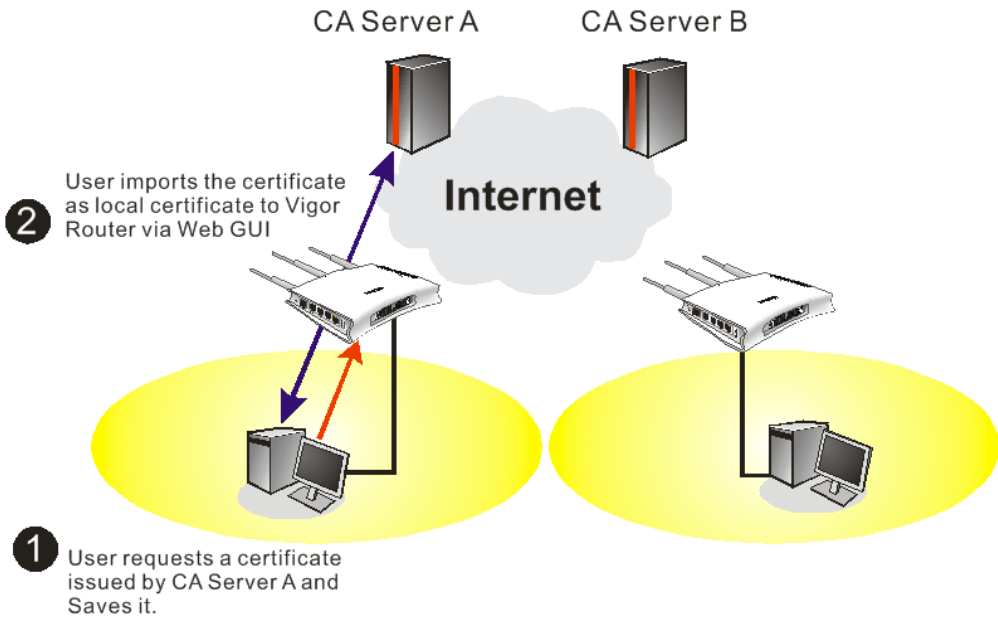


Protocol	Use the drop down list to choose the interface that you want to ping through.
Host/IP Address	It indicates the IP address of the host.
Run	Click this button to start route tracing work.
Clear	Click this link to remove the result on the window.

This page is left blank.

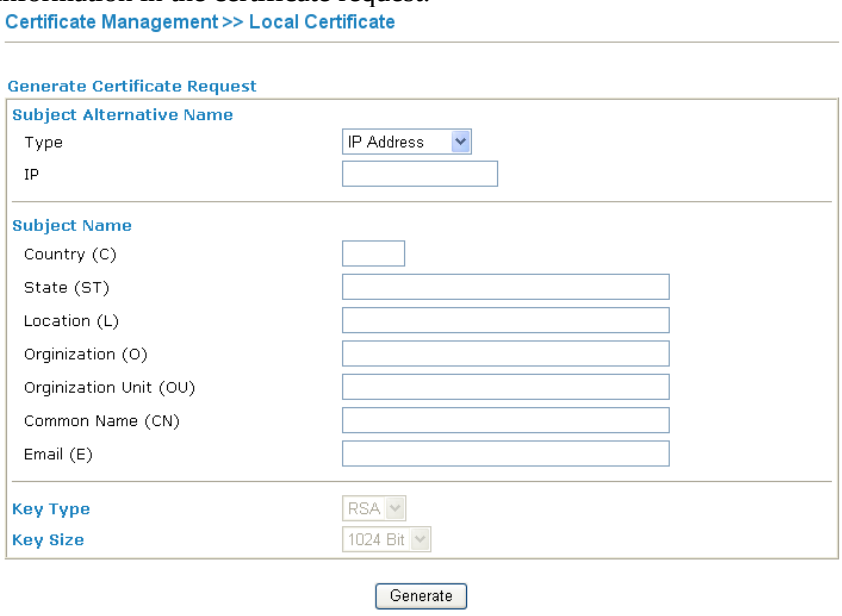
5 Application and Examples

5.1 Request a certificate from a CA server on Windows CA Server

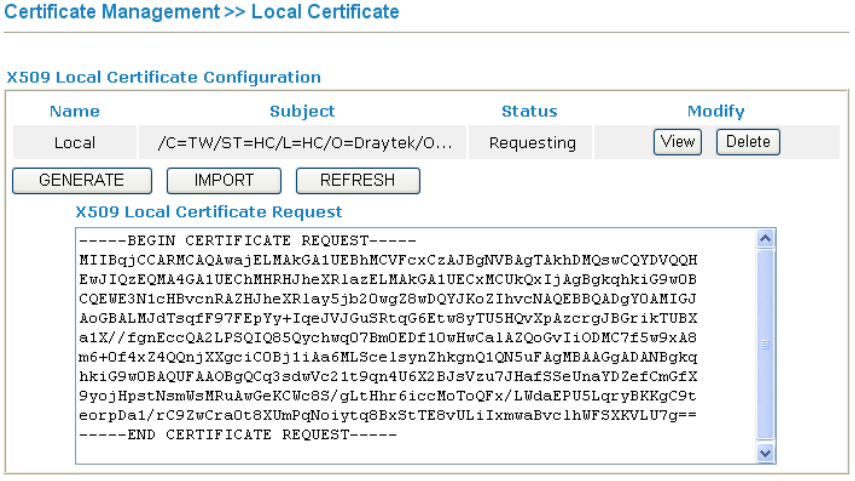


1. Go to **Certificate Management** and choose **Local Certificate**.

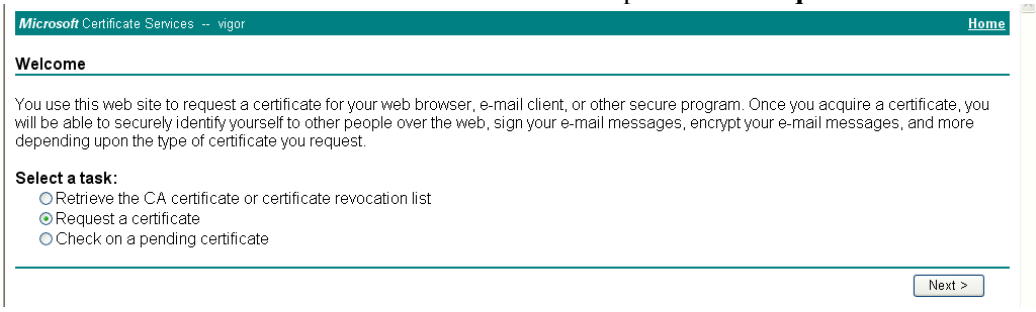
2. You can click **GENERATE** button to start to edit a certificate request. Enter the information in the certificate request.



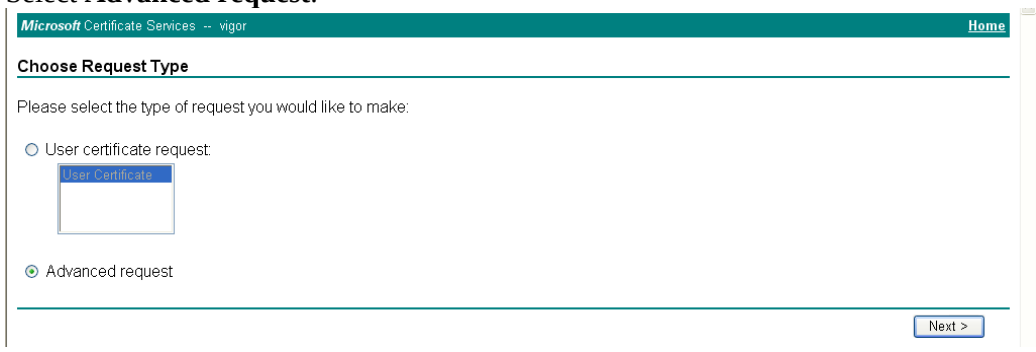
3. Copy and save the X509 Local Certificate Requet as a text file and save it for later use.



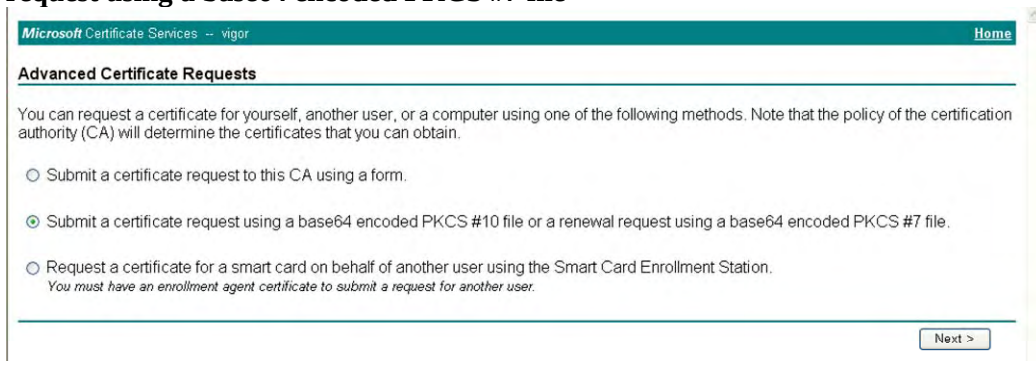
4. Connect to CA server via web browser. Follow the instruction to submit the request. Below we take a Windows 2000 CA server for example. Select **Request a Certificate**.



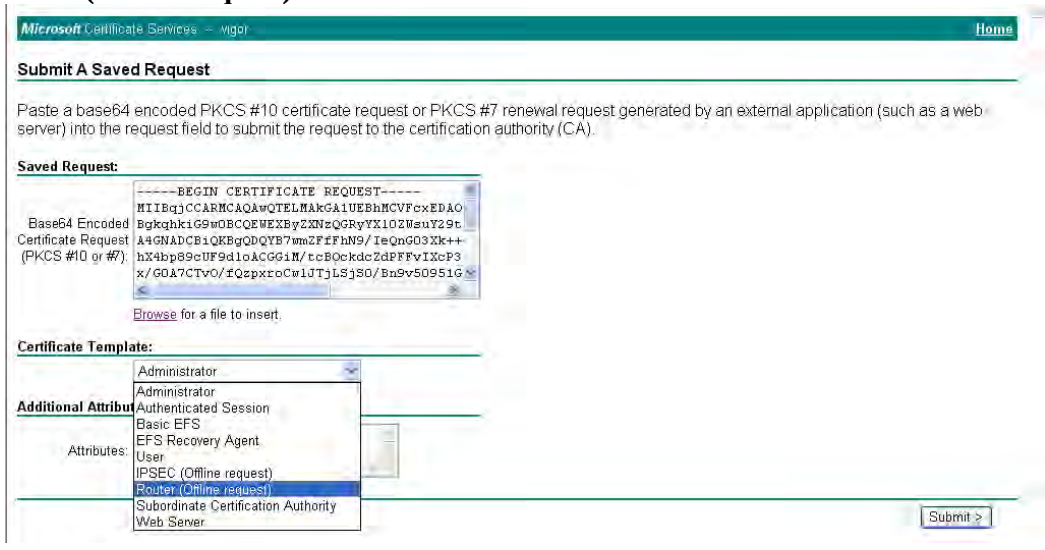
Select **Advanced request**.



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 Requet text file. Select **Router (Offline request)** or **IPSec (Offline request)** below.



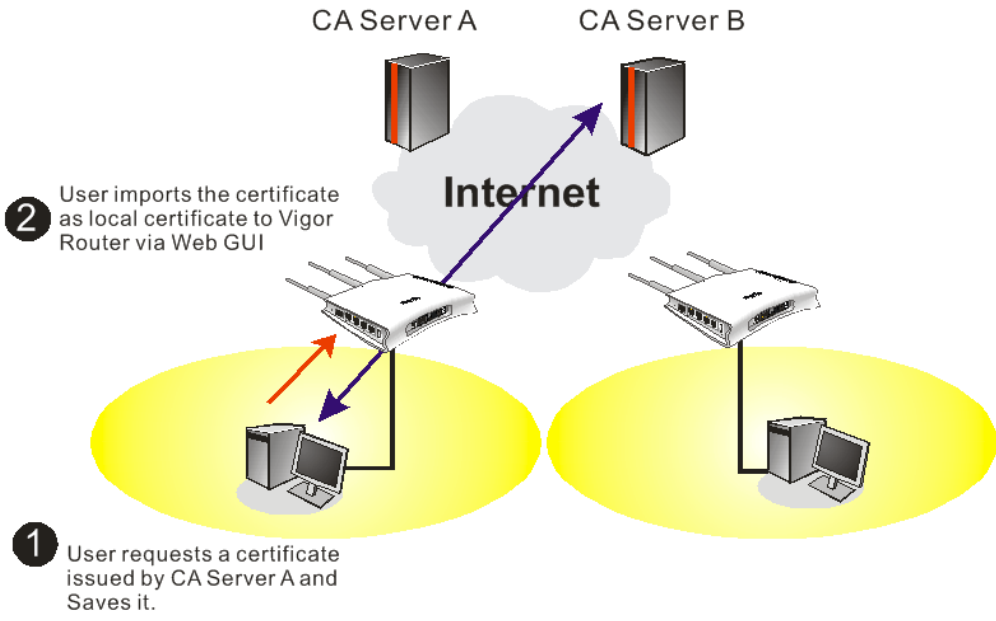
Then you have done the request and the server now issues you a certificate. Select **Base 64 encoded** certificate and **Download CA certificate**. Now you should get a certificate (.cer file) and save it.

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

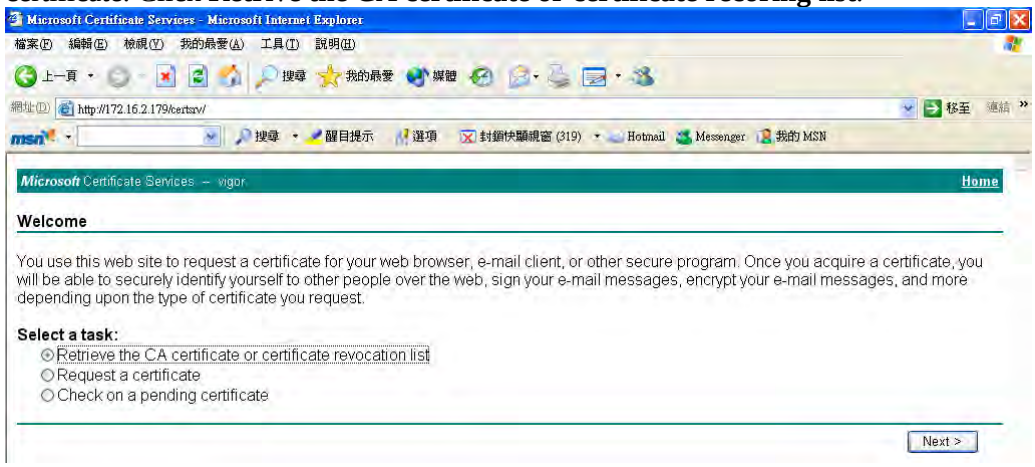
and you will find the below window showing "------BEGINE CERTIFICATE------....."

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

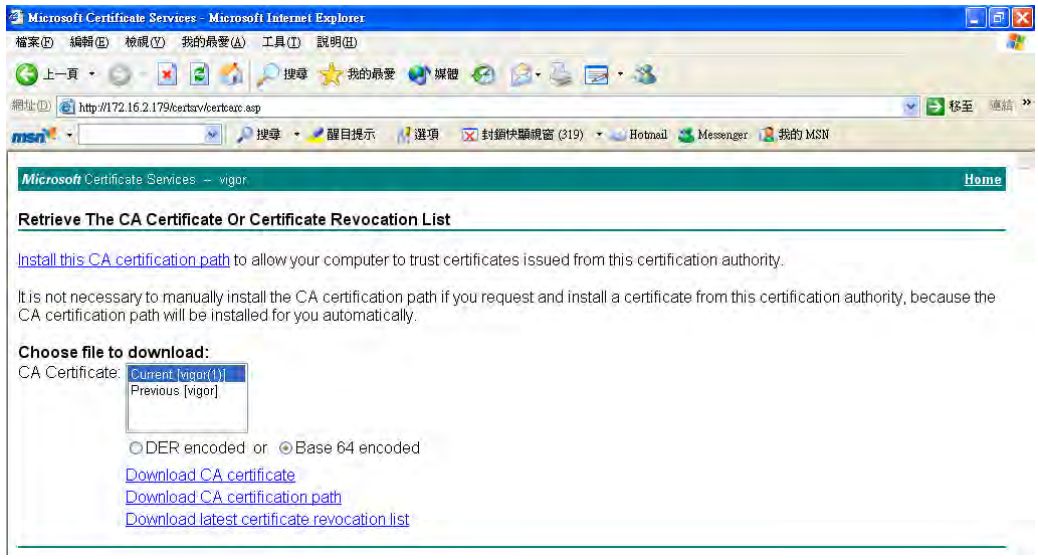
5.2 Request a CA Certificate and Set as Trusted on Windows CA Server



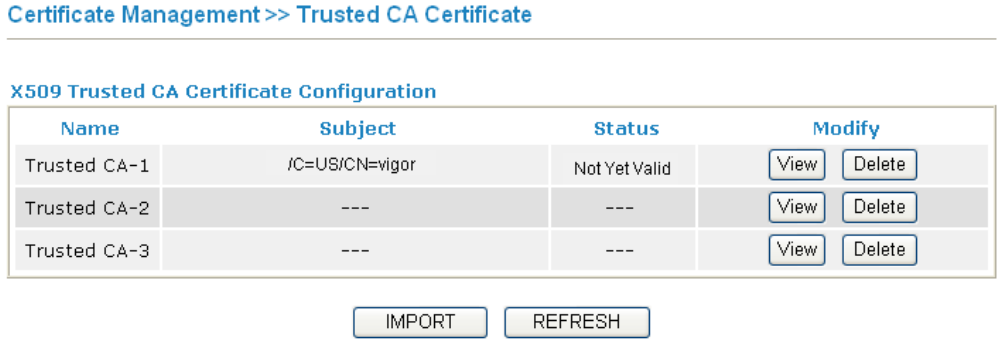
1. Use web browser connecting to the CA server that you would like to retrieve its CA certificate. Click **Retrive the CA certificate or certificate recoring list**.



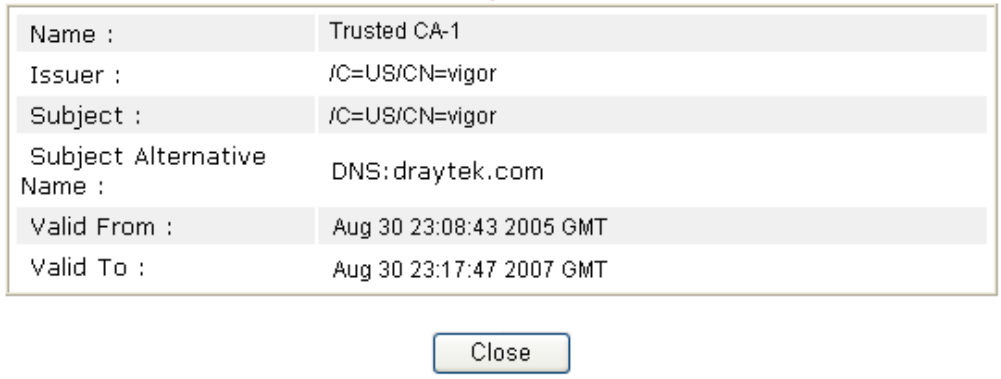
2. In **Choose file to download**, click CA Certificate **Current** and **Base 64 encoded,** and **Download CA certificate** to save the .cer. file.



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.

5.3 Calling Scenario for VoIP function

5.3.1 Calling via SIP Sever

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

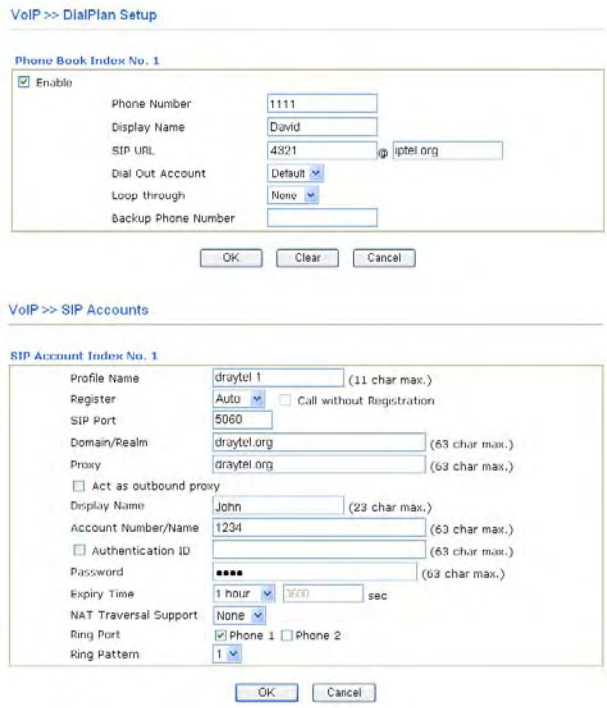
John's SIP URL: 1234@draytel.org, David's SIP URL: 4321@iptel.org

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: unhecked
Display Name: John
Account Number/Name: 1234
Authentication ID: unchecked
Password: ****
Expiry Time: (use default value)

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

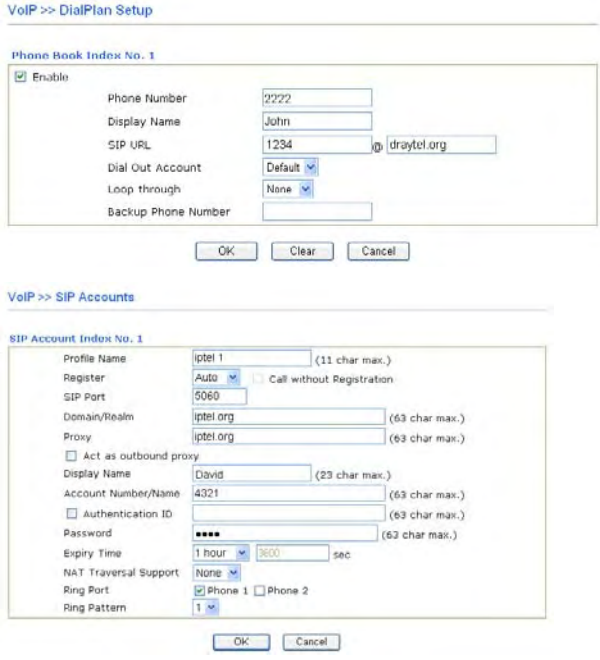


John calls David ---
He picks up the phone and dials 1111#. (DialPlan Phone Number for David)

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.

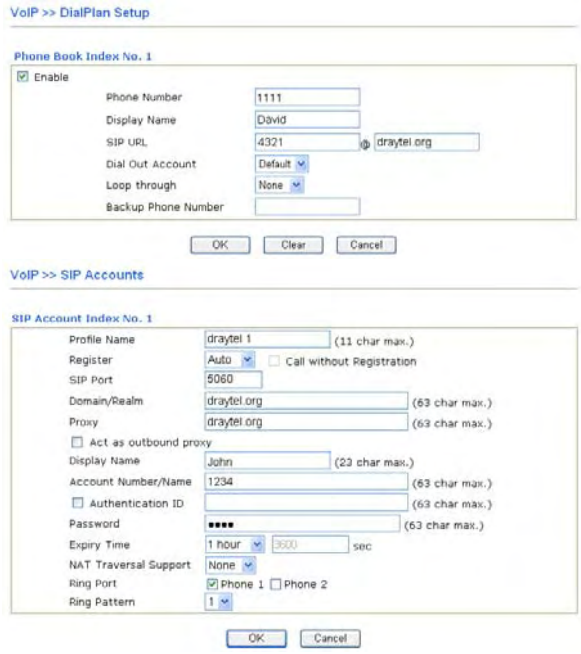
John's SIP URL: 1234@draytel.org , David's SIP URL: 4321@draytel.org

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)

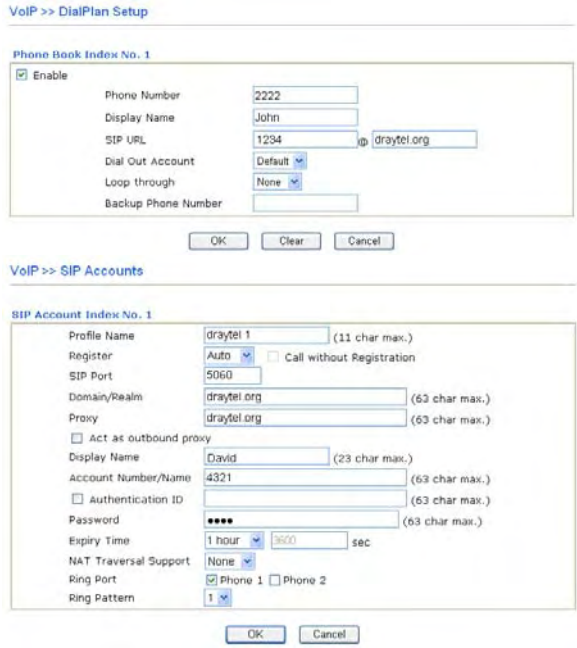


John calls David
He picks up the phone and dials 1111#. (DialPlan Phone Number for David) Or,
He picks up the phone and dials 4321#. (David's Account Name)

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)

5.3.2 Peer-to-Peer Calling

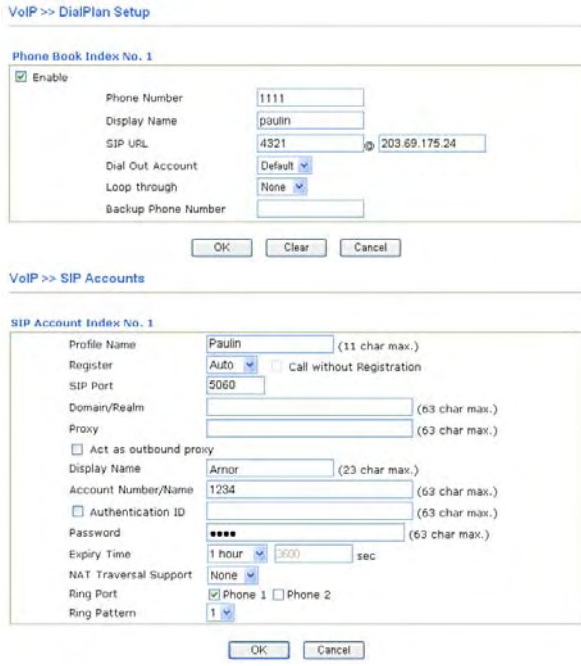
Example 3: Arnor and Paulin have Vigor routers respectively. They can call each other *without* SIP Registrar. First they must have each other's IP address and assign an Account Name for the port used for calling.

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)

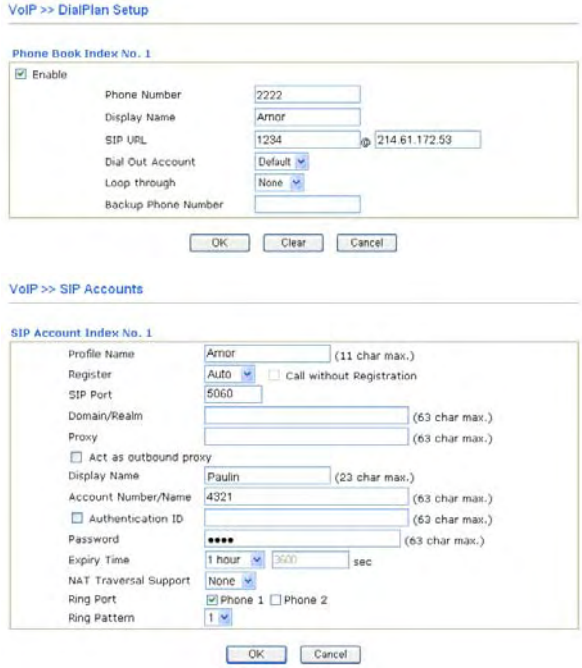


Arnor calls Paulin
He picks up the phone and dials **1111#**. (DialPlan Phone Number for Arnor)

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
Acco4unt Name: 4321
Authentication ID: unchecked
Password: (blank)
Expiry Time: (use default value)

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

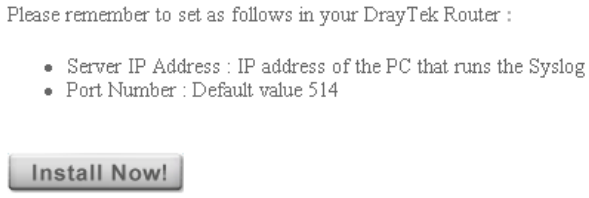


Paulin calls Arnor
He picks up the phone and dials **2222#** (DialPlan Phone Number for John)

5.4 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.

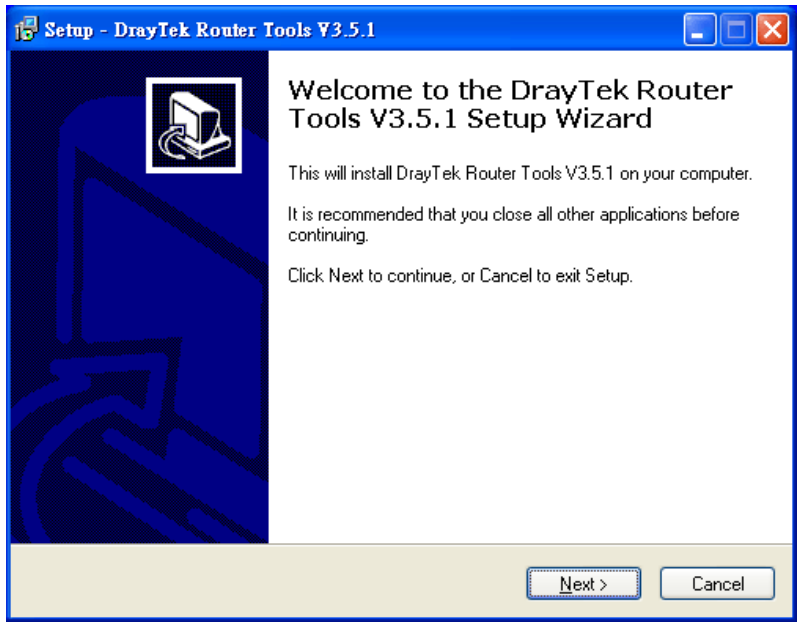


4. The file **RTSxxx.exe** will be asked to copy onto your computer. Remember the place of storing the execution file.
5. Go to **www.draytek.com** to find out the newly update firmware for your router.
6. Access into **Support Center** >> **Downloads**. Find out the model name of the router and click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

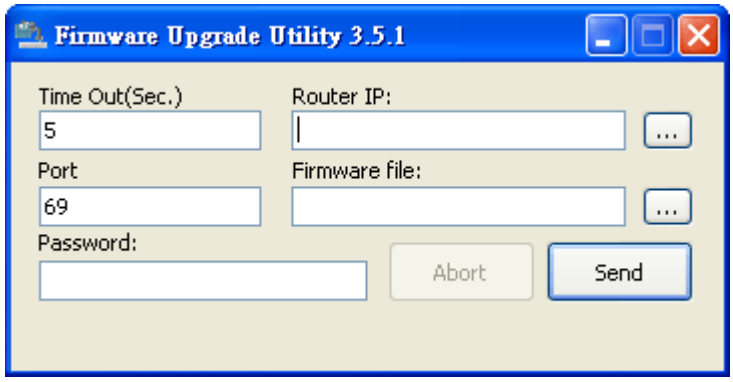
Tools Name	Released Date	Version	OS	Support Model	Download
Router Tools	21/12/2006	3.5.1	MS-Windows	All Model	zip
Smart VPN Client	18/08/2006	3.2.6	MS-Windows	All Model	zip
LPR	27/06/2005	1.0	MS-Windows	For Print Function	zip
VTA	15/09/2005	2.8	Windows2000/XP	For ISDN Model	zip
DialPlan	26/01/2006	2.5_lite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

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.

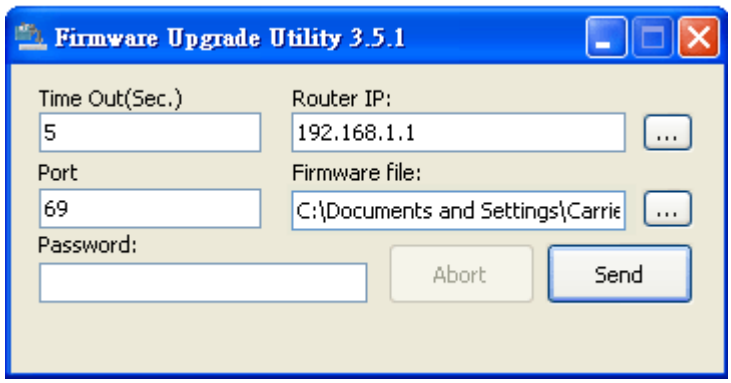
9. Double click on the icon of router tool. The setup wizard will appear.



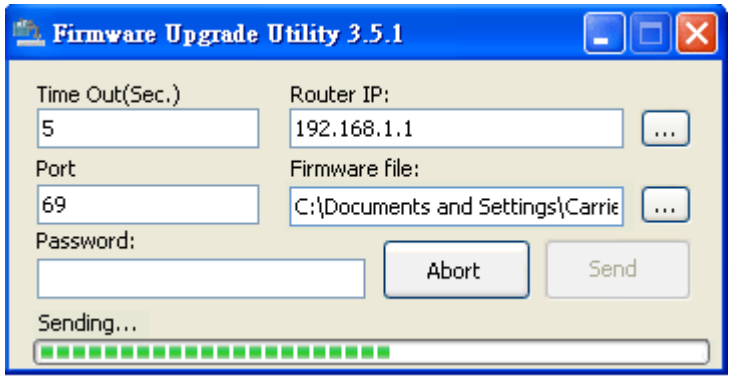
10. Follow the onscreen instructions to install the tool. Finally, click **Finish** to end the installation.
11. From the **Start** menu, open **Programs** and choose **Router Tools XXX** >> **Firmware Upgrade Utility**.



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.

6 Trouble Shooting

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

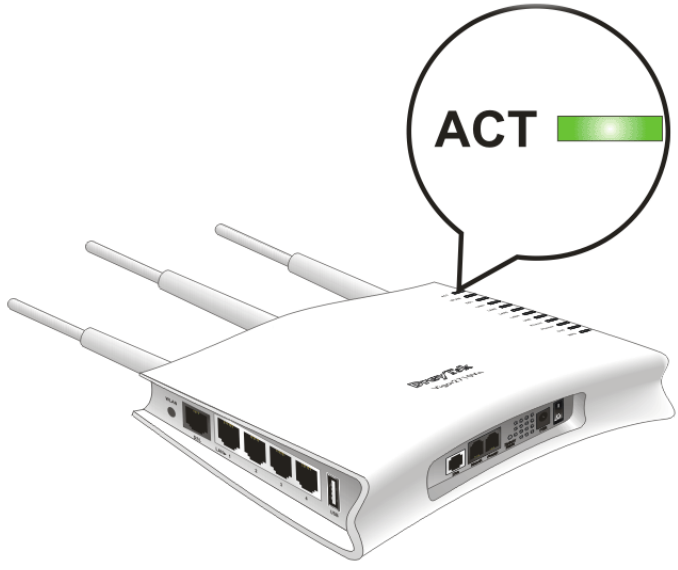
- Checking the hardware status.
- Checking the network connection settings on your computer.
- Pinging the router from your computer.
- Check online status.
- Resetting the router to factory default settings.

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

6.1 Checking the Hardware Status

Follow the steps below to verify the hardware status.

1. Check the power line and WLAN/LAN cable connections.
   Refer to "**1.3 Hardware Installation"** for details.
2. Turn on the router. Make sure the **ACT LED** blink once per second and the correspondent **LAN LED** is bright.



3. If not, it means that there is something wrong with the hardware status. Simply back to **"1.3 Hardware Installation"** to execute the hardware installation again. And then, try again.

6.2 Checking the Network Connection Settings on Your Computer

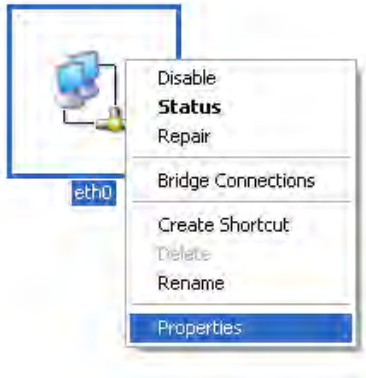
Sometimes the link failure occurs due to the wrong network connection settings. After trying the above section, if the link is stilled failed, please do the steps listed below to make sure the network connection settings is OK.

For Windows

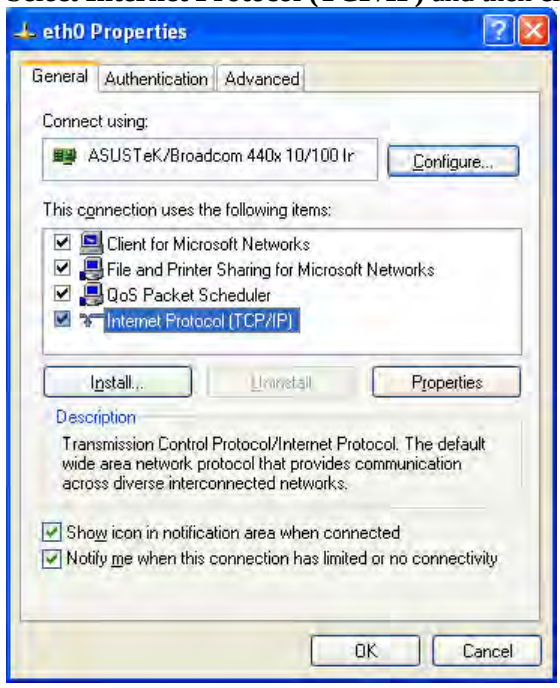
> The example is based on Windows XP. As to the examples for other operation systems, please refer to the similar steps or find support notes in **www.draytek.com**.

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

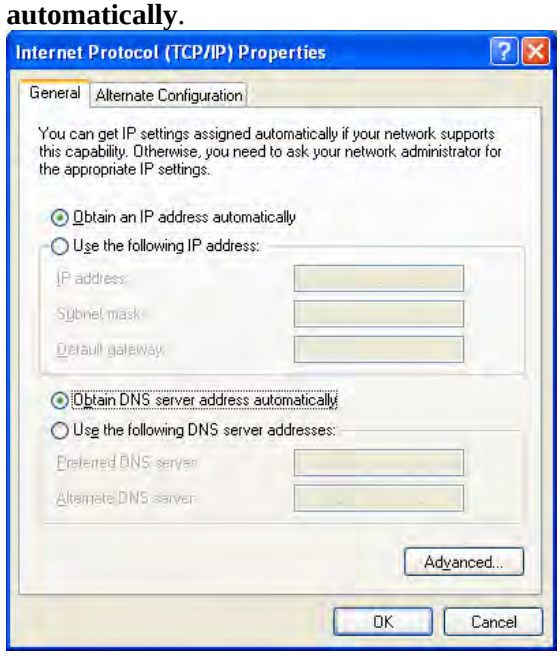
2. Right-click on **Local Area Connection** and click on **Properties**.



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

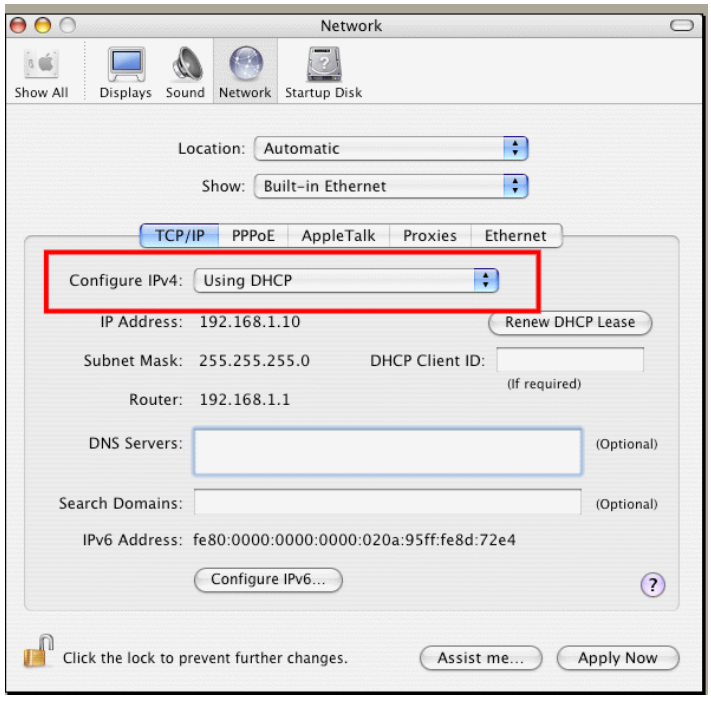


4. Select **Obtain an IP address automatically** and **Obtain DNS server address automatically**.



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.



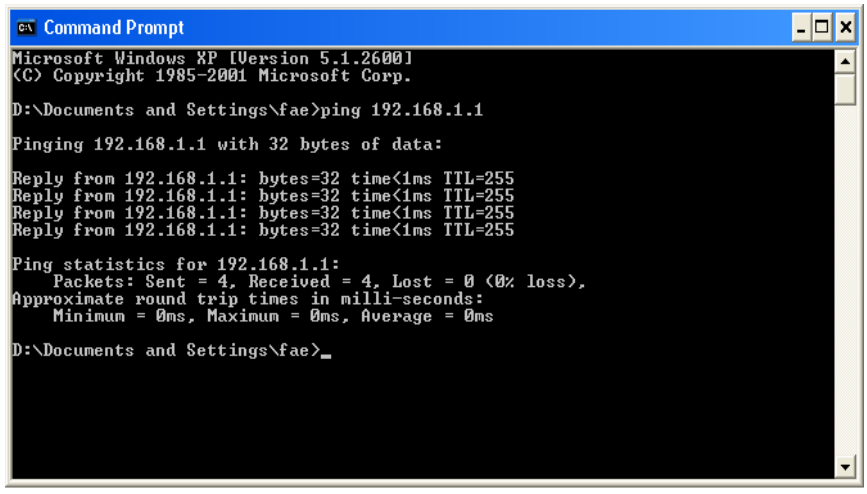
6.3 Pinging the Router from Your Computer

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

Please follow the steps below to ping the router correctly.

For Windows

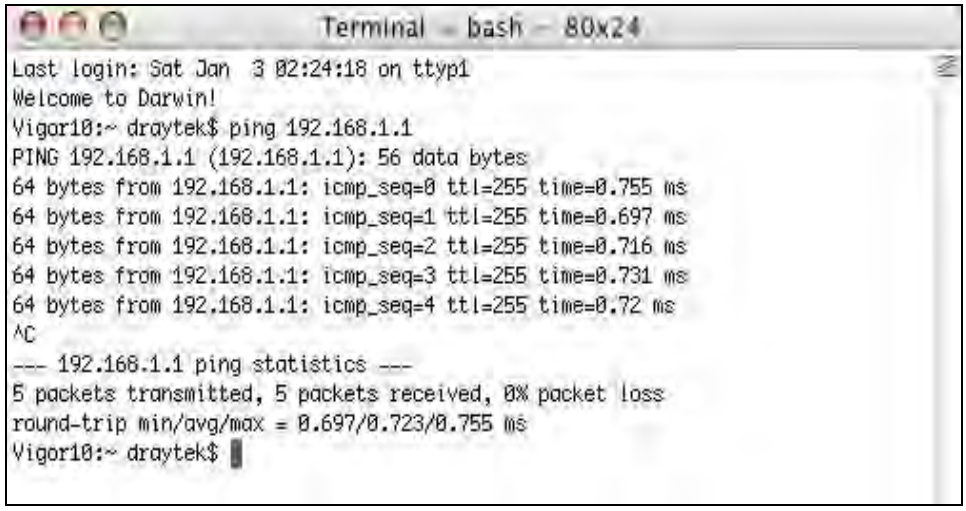
1. Open the **Command** Prompt window (from **Start menu> Run**).
2. Type **command** (for Windows 95/98/ME) or **cmd** (for Windows NT/ 2000/XP/Vista). The DOS command dialog will appear.



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.

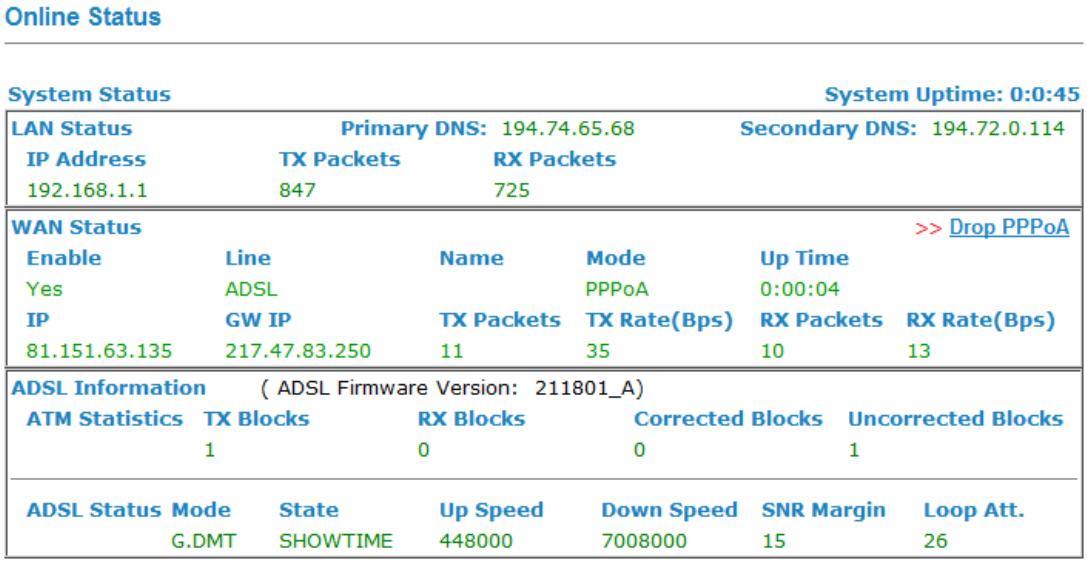
For MacOs (Terminal)

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.



6.4 Check Online Status Page

Go to online status page and check if WAN status shows connected and is in green, if not please check the Internet connection configuration guide in section 2.4 to check the configuration for Internet connectivity.



6.5 Resetting the Router to Factory Default Settings

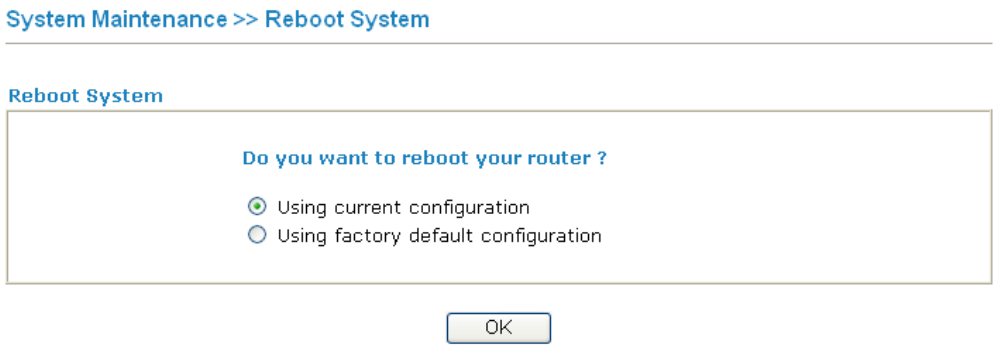
Sometimes, a wrong connection can be improved by returning to the default settings. Try to reset the router by software or hardware.

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

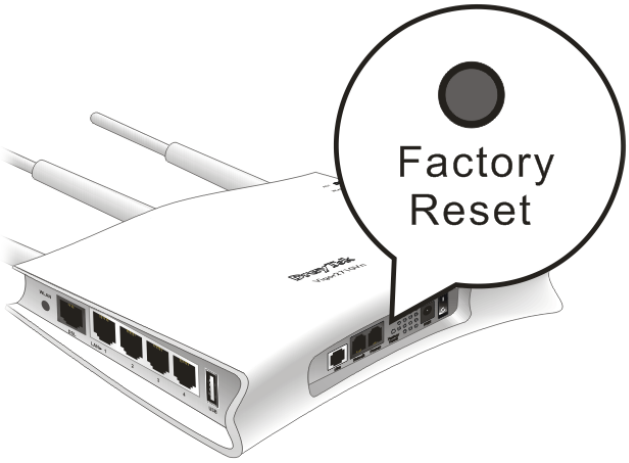
You can reset the router to factory default via Web page.

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.

6.6 Technical Support

If you need further assistance with configuration or troubleshooting of your Vigor 2710 series, please visit www.support.draytek.co.uk.