DrayTek

Vigor*IPPBX* 3510 Series

Your reliable networking solutions partner

User's Guide

V.2.0

Vigor*IPPBX* 3510 Series
User's Guide

Version: 2.0

Firmware Version: V3.5.5

Date: 19/11/2010

Copyright Information

Copyright Declarations

Copyright 2010 All rights reserved. This publication contains information that is protected by copyright. No part may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language without written permission from the copyright holders.

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 will be regularly upgraded. Please consult the DrayTek web site for more information on newest firmware, tools and documents.

http://www.draytek.com

European Community Declarations

Manufacturer: DrayTek Corp.
Address: No. 26, Fu Shing Road, HuKou Township, HsinChu Industrial Park, Hsin-Chu County, Taiwan 303
Product: VigorIPPBX 3510

DrayTek Corp. declares that VigorIPPBX 3510 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 A and EN55024/Class A.

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

Regulatory Information

Federal Communication Commission Interference Statement

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

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

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

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

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

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

This product is designed for the ISDN and POTS network throughout the EC region and Switzerland. Please see the user manual for the applicable networks on your product.

Table of Contents

Chapter 1: Preface 1

1.1 Web Configuration Buttons Explanation 1

1.2 LED Indicators and Connectors 2

1.3 Hardware Installation 4

1.3.1 Introduction for FXS/FXO/ISDN TE/ISDN NT Module 5

1.4 Printer Installation 7

Chapter 2: Configuring Basic Settings 13

2.1 Changing Password 13

2.2 Quick Start Wizard 15

2.2.1 PPPoE 16

2.2.2 PPTP/L2TP 18

2.2.3 Static IP 20

2.2.4 DHCP 21

2.3 IPPBX Wizard 22

2.3.1 Extension & Group Setup 22

2.3.2 SIP Trunk Setup 24

2.3.3 Office Hours Setup 25

2.4 Service Activation Wizard 26

2.5 Online Status 30

2.6 Saving Configuration 31

2.7 Support Area 31

Chapter 3: Applications 33

3.1 Versatile PSTN and VoIP Trunk 33

3.2 Cost-effective Extendability by Integrated Analog-telephone Adapter (for 24 Conventional Analog Phones) & POE-switch for IP-based phones 35

3.3 ISDN Application via ISDN Trunk 37

3.4 ISDN Application with All ISDN TE Ports 38

3.5 ISDN Application with 4 ISDN TE and 2 ISDN TE/ 2 ISDN NT Ports 39

Chapter 4: Other Applications 41

4.1 Create a LAN-to-LAN Connection Between Remote Office and Headquarter 41

4.2 Create a Remote Dial-in User Connection Between the Teleworker and Headquarter 48

4.3 QoS Setting Example 52

4.4 LAN – Created by Using NAT 56

4.5 Upgrade Firmware for VigorIPPBX 3510 58

4.6 Backup and Restore Settings for VigorIPPBX 3510 60

4.6.1 Backup the Configuration Settings 60
4.6.2 Restore the Configuration Settings 64
4.7 Request a certificate from a CA server on Windows CA Server 68
4.8 Request a CA Certificate and Set as Trusted on Windows CA Server 72
4.9 Creating an Account for MyVigor 74

Chapter 5: Reference - Advanced Web Configuration 81
5.1 WAN 81
5.1.1 Basics of Internet Protocol (IP) Network 81
5.1.2 Network Connection by 3G USB Modem 82
5.1.3 General Setup 82
5.1.4 Internet Access 85
5.1.5 Load-Balance Policy 92
5.2 LAN 94
5.2.1 Basics of LAN 94
5.2.2 General Setup 96
5.2.3 Static Route 99
5.2.4 VLAN 101
5.2.5 Bind IP to MAC 103
5.3 NAT 104
5.3.1 Port Redirection 105
5.3.2 DMZ Host 107
5.3.3 Open Ports 110
5.4 Firewall 115
5.4.1 Basics for Firewall 115
5.4.2 General Setup 117
5.4.3 Filter Setup 119
5.4.4 DoS Defense 126
5.5 Objects Settings 129
5.5.1 IP Object 129
5.5.2 IP Group 131
5.5.3 Service Type Object 132
5.5.4 Service Type Group 133
5.5.5 Keyword Object 134
5.5.6 Keyword Group 135
5.5.7 File Extension Object 136
5.6 CSM 137
5.6.1 APP Enforcement Profile 139
5.6.2 URL Content Filter Profile 143
5.6.3 Web Content Filter Profile 147

5.7 Bandwidth Management 151
5.7.1 Sessions Limit 151
5.7.2 Bandwidth Limit 152
5.7.3 Quality of Service 153
5.8 Applications 160
5.8.1 Dynamic DNS 160
5.8.2 Schedule 162
5.8.3 RADIUS 164
5.8.4 UPnP 165
5.8.5 IGMP 167
5.8.6 Wake on LAN 168
5.9 VPN and Remote Access 169
5.9.1 Remote Access Control 169
5.9.2 PPP General Setup 170
5.9.3 IPSec General Setup 171
5.9.4 IPSec Peer Identity 172
5.9.5 Remote Dial-in User 174
5.9.6 LAN to LAN 177
5.9.7 Connection Management 184
5.10 Certificate Management 185
5.10.1 Local Certificate 185
5.10.2 Trusted CA Certificate 187
5.10.3 Certificate Backup 188
5.11 IP PBX 188
5.11.1 Extension 189
5.11.2 Line Setting 192
5.11.3 Dial Plan 198
5.11.4 PBX System 203
5.11.5 PBX Status 221
5.12 USB Application 222
5.12.1 USB General Settings 222
5.12.2 USB User Management 224
5.12.3 File Explorer 226
5.12.4 USB Disk Status 227
5.12.5 Syslog Explorer 227
5.13 System Maintenance 229
5.13.1 System Status 229
5.13.2 TR-069 231
5.13.3 Administrator Password 232
5.13.4 Configuration Backup 232

5.13.5 Syslog/Mail Alert 233
5.13.6 Time and Date 236
5.13.7 Management 237
5.13.8 Reboot System 238
5.13.9 Firmware Upgrade 239
5.13.10 Activation 239
5.14 Diagnostics 241
5.14.1 Dial-out Trigger 241
5.14.2 Routing Table 242
5.14.3 ARP Cache Table 242
5.14.4 DHCP Table 243
5.14.5 NAT Sessions Table 243
5.14.6 Ping Diagnosis 244
5.14.7 Data Flow Monitor 245
5.14.8 Traffic Graph 246
5.14.9 Trace Route 247

Chapter 6: Trouble Shooting 249
6.1 Checking If the Hardware Status Is OK or Not 249
6.2 Checking If the Network Connection Settings on Your Computer Is OK or Not 250
6.3 Pinging the Router from Your Computer 252
6.4 Checking If the ISP Settings are OK or Not 253
6.5 Backing to Factory Default Setting If Necessary 255
6.6 Contacting Your Dealer 255

Appendix: Hardware Specifications 257

Chapter 1: Preface

VigorIPPBX 3510 is a broadband router with WAN interface. It provides policy-based load-balance, fail-over and BOD (Bandwidth on Demand), also it integrates IP layer QoS, NAT session/bandwidth management to help users control works well with large bandwidth.

By adopting hardware-based VPN platform and hardware encryption of AES/DES/3DS, the router increases the performance of VPN greatly, and offers several protocols (such as IPSec/PPTP/L2TP) with up to 32 VPN tunnels.

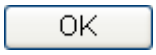
The object-based design used in SPI (Stateful Packet Inspection) firewall allows users to set firewall policy with ease. CSM (Content Security Management) provides users control and management in IM (Instant Messenger) and P2P (Peer to Peer) more efficiency than before. By the way, DoS/DDoS prevention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

VigorIPPBX 3510 can provide up to 100 extensions setup to let all registered IP phones in LAN or remote sites around the world to have unlimited free calls through Internet. Moreover, VigorIPPBX 3510 is able to establish multiple networking architectures corresponding to your current desire and future needs of growing communication. Its ISDN/PSTN compatibility lets you move from simple VoIP solution such as IP phone and Softphone to integrate with comprehensive networking infrastructure, such as ISDN and Analog phone line any time you need.

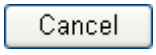
Object-based firewall is flexible and allows your network be safe. In addition, through VoIP function, the communication fee for you and remote people can be reduced.

1.1 Web Configuration Buttons Explanation

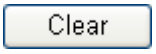
Several main buttons appeared on the web pages are defined as the following:



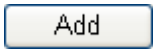
Save and apply current settings.



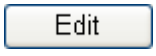
Cancel current settings and recover to the previous saved settings.



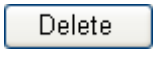
Clear all the selections and parameters settings, including selection from drop-down list. All the values must be reset with factory default settings.



Add new settings for specified item.



Edit the settings for the selected item.



Delete the selected item with the corresponding settings.

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

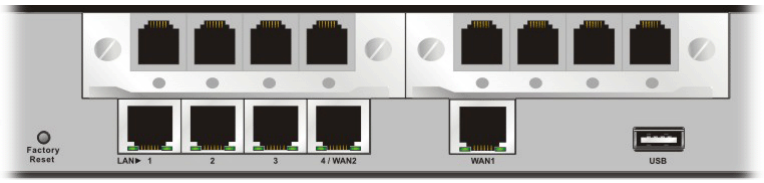
1.2 LED Indicators and Connectors

Before you use the Vigor router, please get acquainted with the LED indicators and connectors first. The displays of LED indicators and connectors for the routers are different slightly. The following sections will introduce them respectively.

Description for LED

LED		Status	Explanation
PWR (Power)		On	The router is powered on.
		Off	The router is powered off.
ACT (Activity)		Blinking	The router is powered on and running normally.
		Off	The router is not ready or failed.
WAN		On	The WAN connection is ready.
		Blinking	It will blink while transmitting data.
CDR		On	CDR utility has been installed and is recording.
		Off	CDR utility has not been installed or is unable to record.
USB		On	A USB device is connected and active.
		Blinking	The data is transmitting.
MSF		Blinking	Storage (NAND flash or USB disk) is full.
VPN		On	The VPN tunnel is active.
CSM		On	The profiles of CSM (Content Security Management) for IM/P2P, URL Content Filter, Web Content Filter application is enabled from **Firewall >> General Setup**. (These profiles can be established under **CSM** menu).
QoS		On	The QoS function is active.
LED on Connector			
LAN 1/2/3/4	Left LED (Green)	On	The port is connected.
		Off	The port is disconnected.
		Blinking	The data is transmitting.
	Right LED (Green)	On	The port is connected with 100Mbps.
		Off	The port is connected with 10Mbps.
WAN 1	Left LED (Green)	On	The port is connected.
		Off	The port is disconnected.
		Blinking	The data is transmitting.
	Right LED (Green)	On	The port is connected with 100Mbps.
		Off	The port is connected with 10Mbps.

Description for Connectors



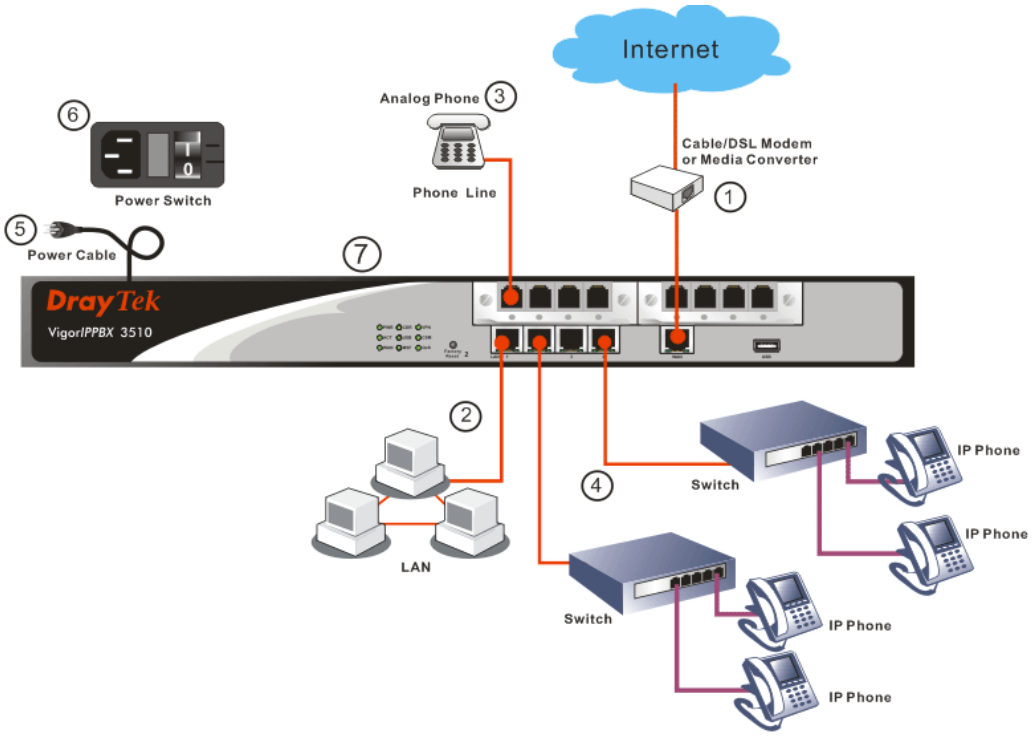
Interface	Description
Factory Reset	Restore the default settings. Usage: Turn on the router (ACT LED is blinking). Press the hole and keep for more than 5 seconds. When you see the ACT LED begins to blink rapidly than usual, release the button. Then the router will restart with the factory default configuration.
FXS	Connecter for telephone set.
FXO	Connecter for FXS interface of PABX.
LAN (1-4)	Connecters for local networked devices.
WAN 2/1	Connecter for remote networked devices.
USB	Connecter for a USB device (for 3G USB Modem or printer).
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 cable Modem/DSL Modem/Media Converter to WAN port of router with Ethernet cable (RJ-45).
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 PBX function). For the model without phone ports, skip this step.
4. Connect IP Phone(s) via VigorSwitch to this router.
5. 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.
6. Power on the device by pressing down the power switch on the rear panel.
7. The system starts to initiate. After completing the system test, the **PWR** and **ACT** LEDs will light up and start blinking.

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



1.3.1 Introduction for FXS/FXO/ISDN TE/ISDN NT Module

VigorIPPBX 3510 has two expansion slots; each slot can be plugged into 4-port PSTN card, ISDN-NTTE or ISDN-TE card. The PSTN card involves two kinds of interface: FXS and FXO. The ISDN-NTTE card involves two kinds of interface: NT for port 1 and 3; TE or NT (user configurable) for port 2 and 4. And ISDN-TE card involves 4-port TE mode. You can deploy different PSTN/ISDN applications according to the requirements.

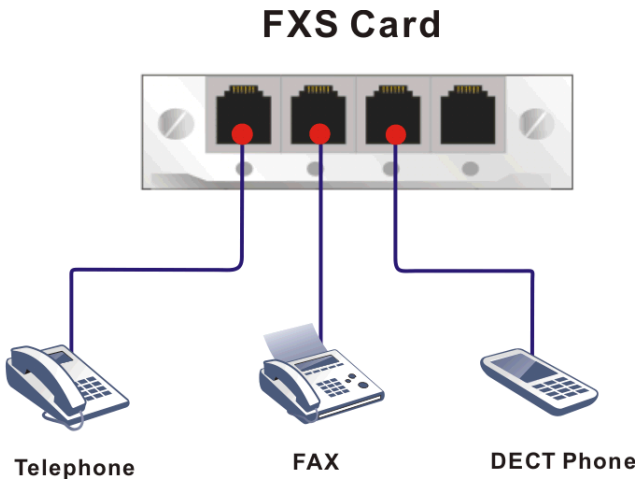
FXS and FXO

FXS (Foreign eXchange Station) and FXO (Foreign eXchange Office) are assembled with a pair. A telecommunications line from an FXO device must be connected to an FXS device. Similarly, an FXS device must be connected to an FXO device. For example, PSTN is FXS equipment, and a telephone is FXO equipment.

As for VigorIPPBX 3510, it is more special because it has both FXS and FXO devices at the same time. It can connect to the phone line to act as FXO equipment; and it can connect to telephones to act as FXS equipment.

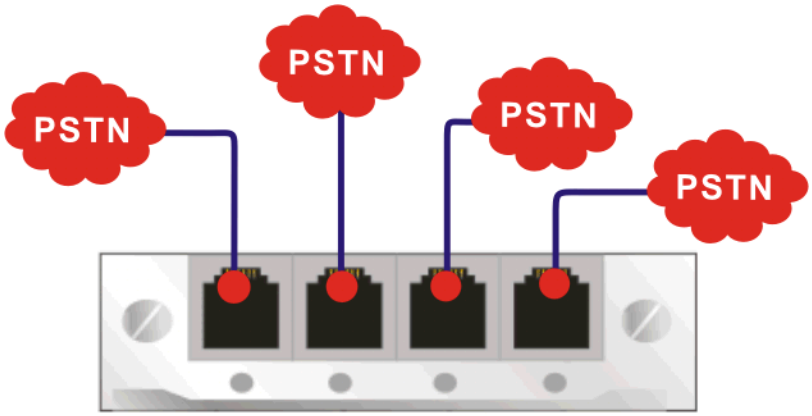
FXS card

This card can connect to the telephone, FAX machine, DECT Phone, and so on.



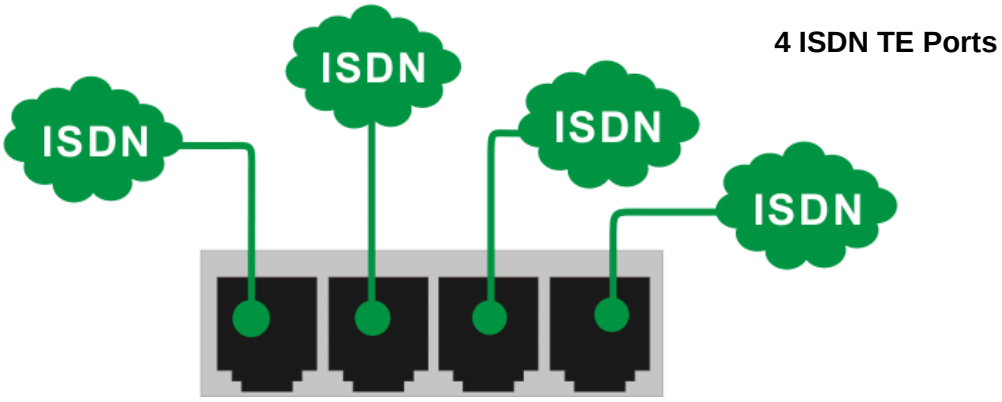
FXO card

This card can connect to PSTN lines and extension lines of PBX

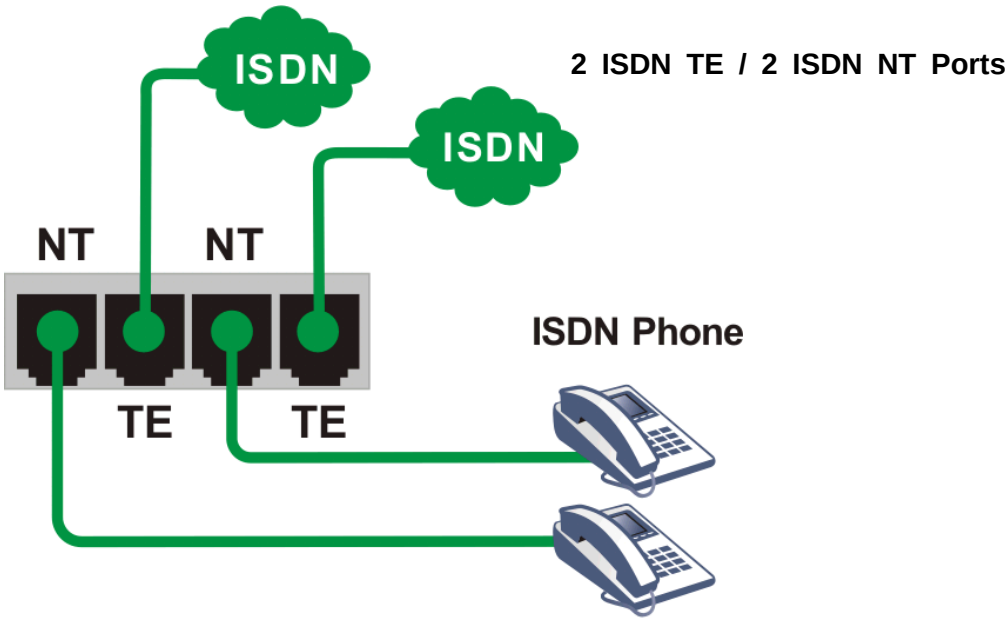


ISDN NT (S0) and TE

NT means Network Terminal. The ISDN port in NT mode is a port that used to connect general ISDN phones. And TE means Terminal Equipment. The ISDN port in TE mode is a port that used to connect ISDN line or ISDN PBX.



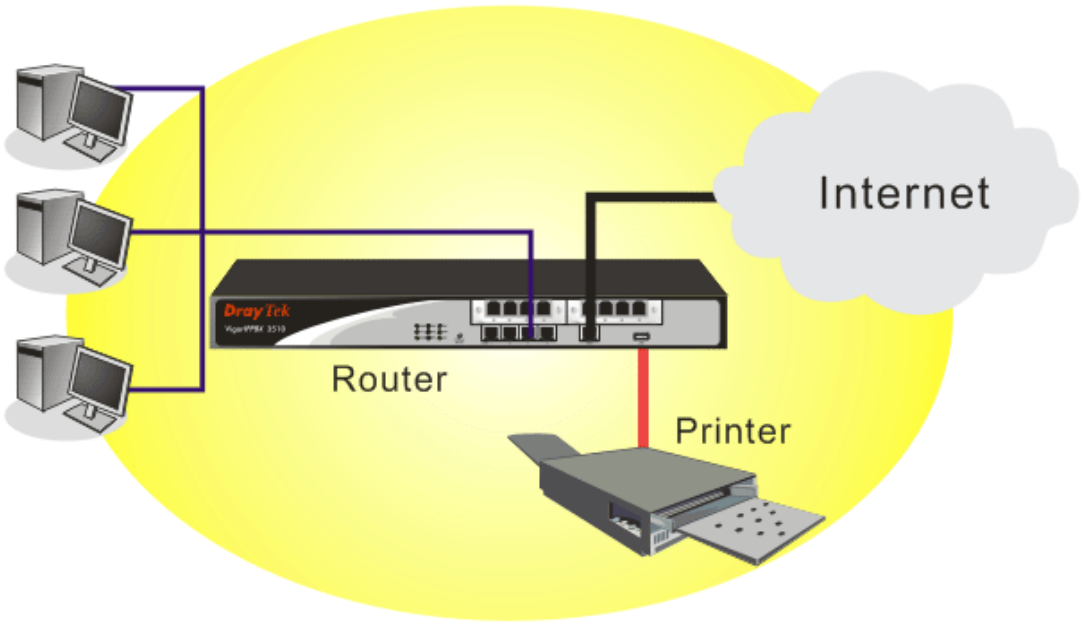
As for the Private Branch Exchange (PBX), it is more special because it has both ISDN-NT and ISDN-TE devices at the same time. It can connect to the ISDN line to act as ISDN-TE equipment; and it can connect to ISDN telephones to act as ISDN-NT equipment.



Based on the characteristics described above that the ISDN NT equipment and the ISDN TE equipment must connect with each other, please pay special attention when you use ISDN NT card and ISDN TE card.

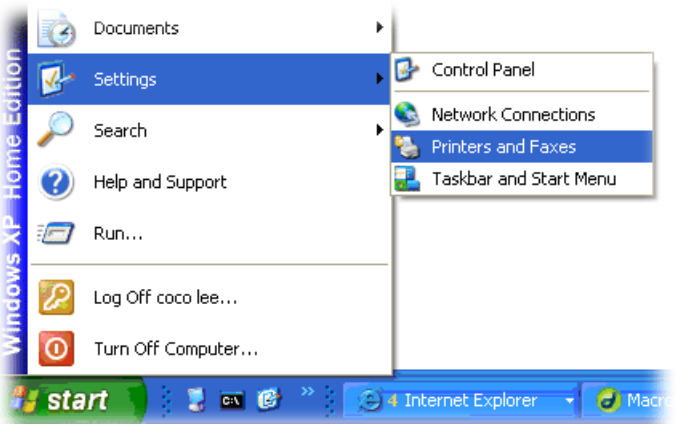
1.4 Printer Installation

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

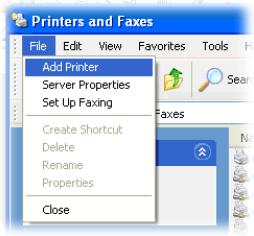


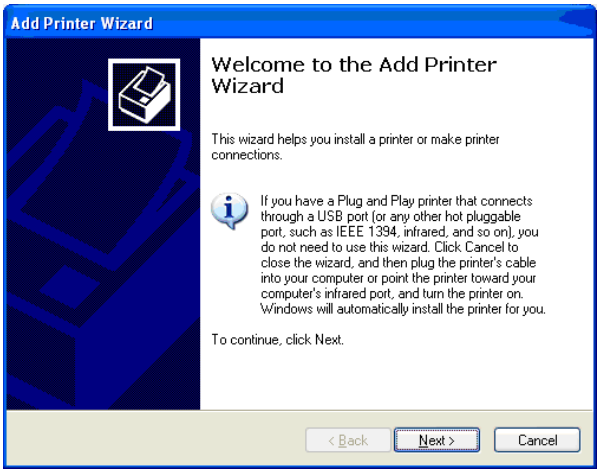
Before using it, please follow the steps below to configure settings for connected computers.

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

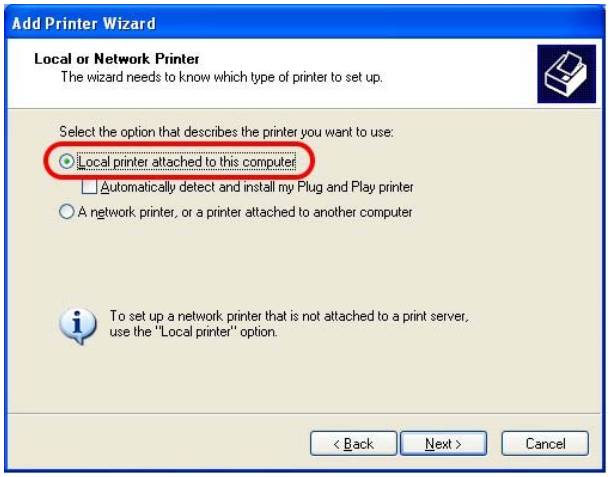


3. Open **File->Add a New Computer**. A welcome dialog will appear. Please click **Next**.

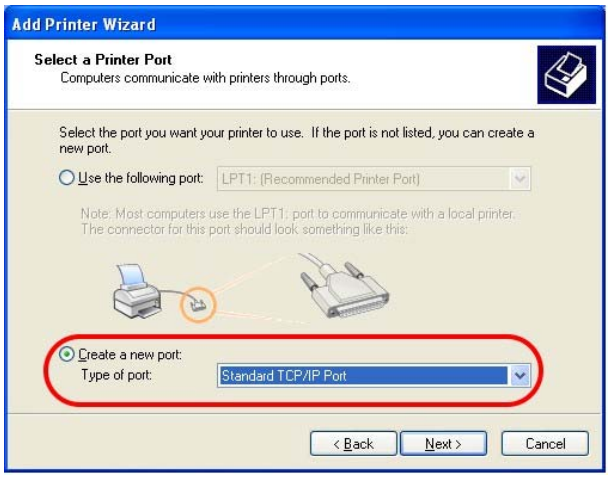




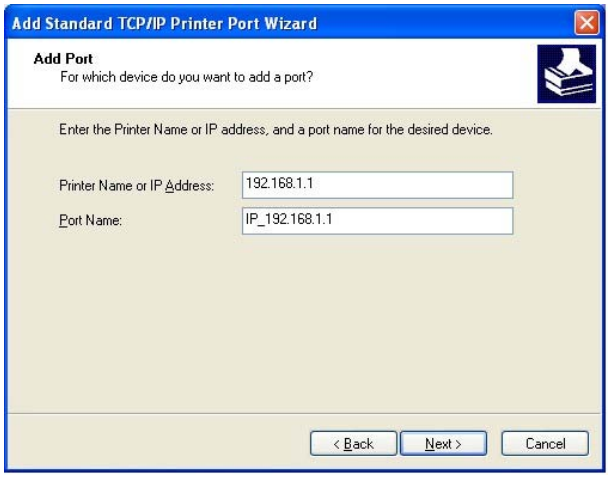
4. Click Local printer attached to this computer and click Next.



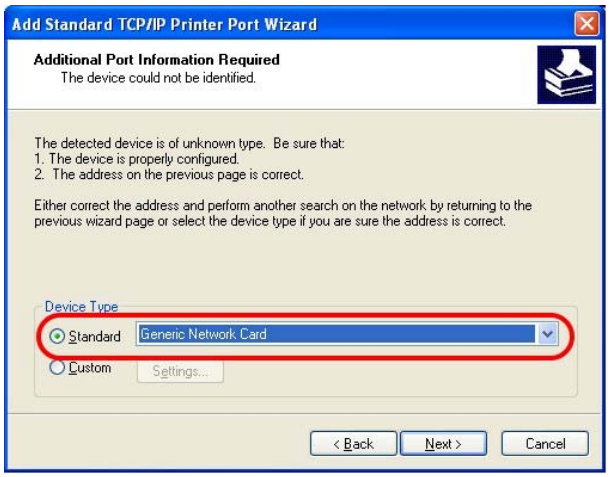
5. In this dialog, choose **Create a new port Type of port** and use the drop down list to select **Standard TCP/IP Port**. Click **Next**.



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**.

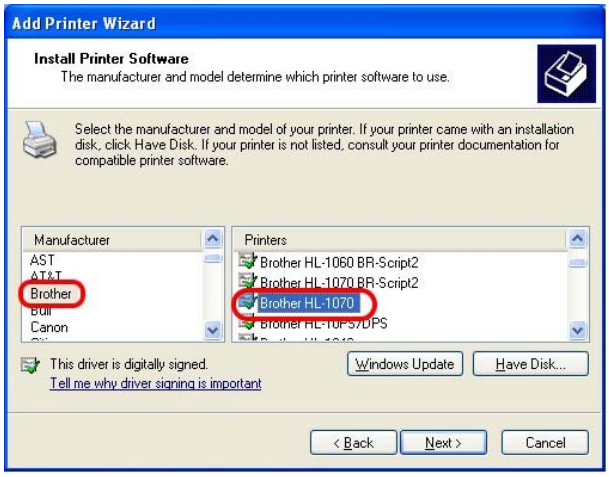


7. Click Standard and choose Generic Network Card.

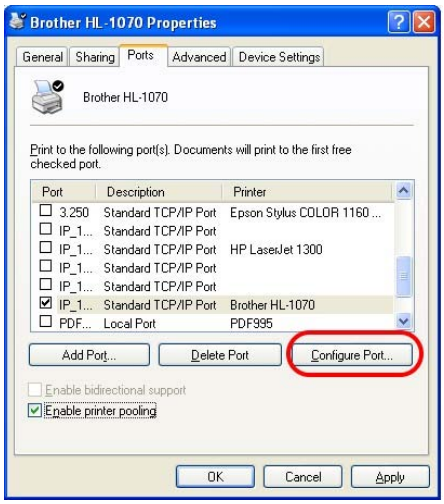


8. Then, in the following dialog, click **Finish**.

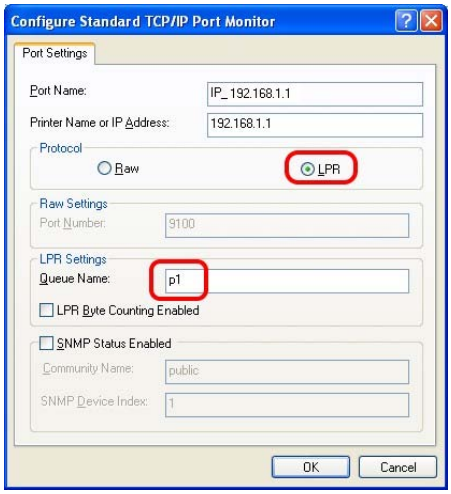
9. Now, your system will ask you to choose right name of the printer that you installed onto the router. Such step can make correct driver loaded onto your PC. When you finish the selection, click **Next**.



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.

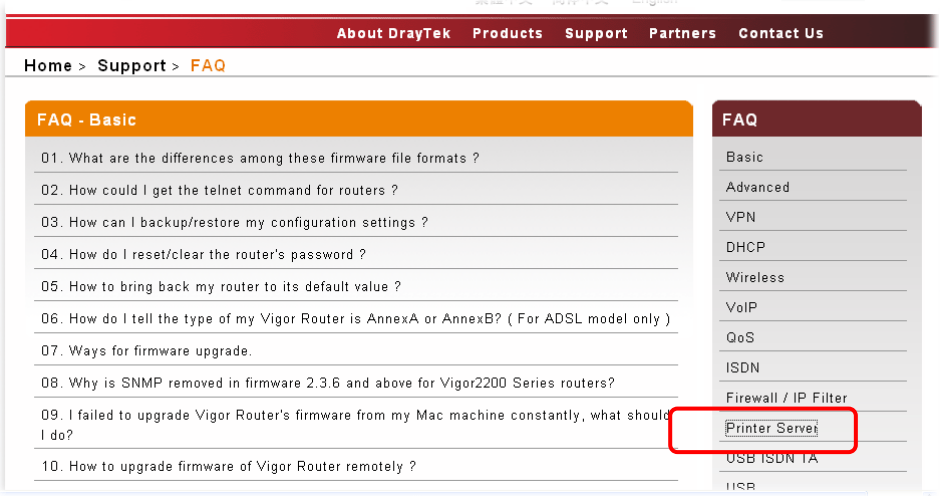


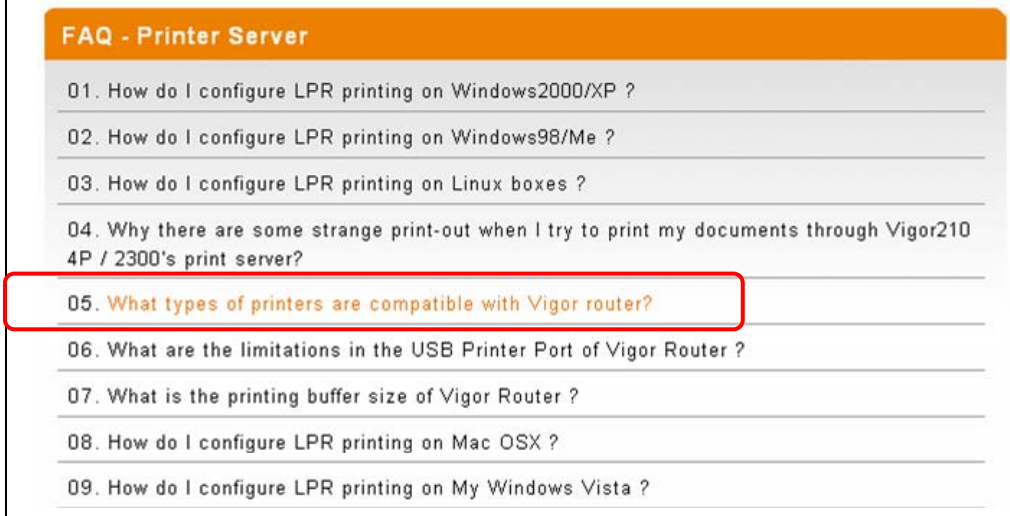
11. Select "**LPR**" on Protocol, type **p1** (number 1) as Queue Name. Then click **OK**. Next please refer to the red rectangle for choosing the correct protocol and LPR name.



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.

Chapter 2: Configuring Basic Settings

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

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

2.1 Changing Password

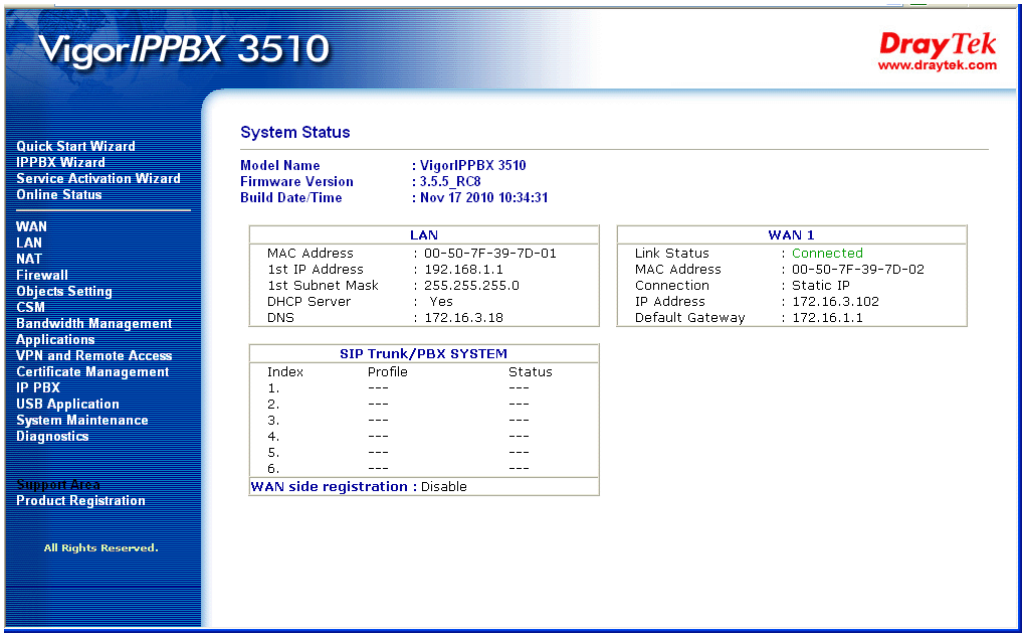
To change the password for this device, you have to access into the web browse with default password first.

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

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

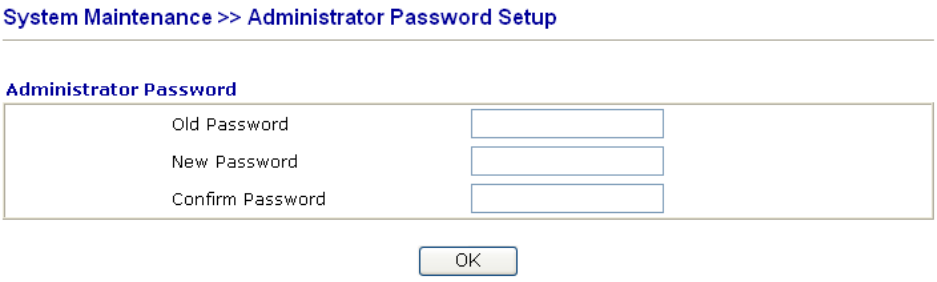
2. Open a web browser on your PC and type **http://192.168.1.1.** A pop-up window will open to ask for username and password. Please type “admin” as the username and leave blank for the password on the window. Next click **OK** for next screen.

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



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

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

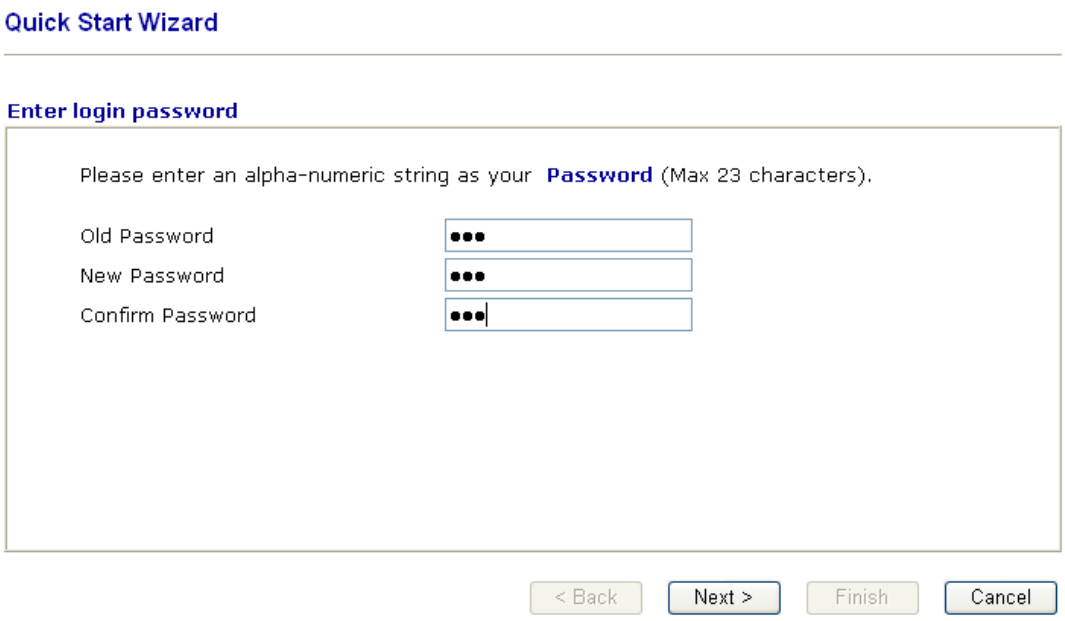


5. Enter the login password (the default is blank) on the field of **Old Password**. Type **New Password** and **Confirm Password**. Then click **OK** to continue.

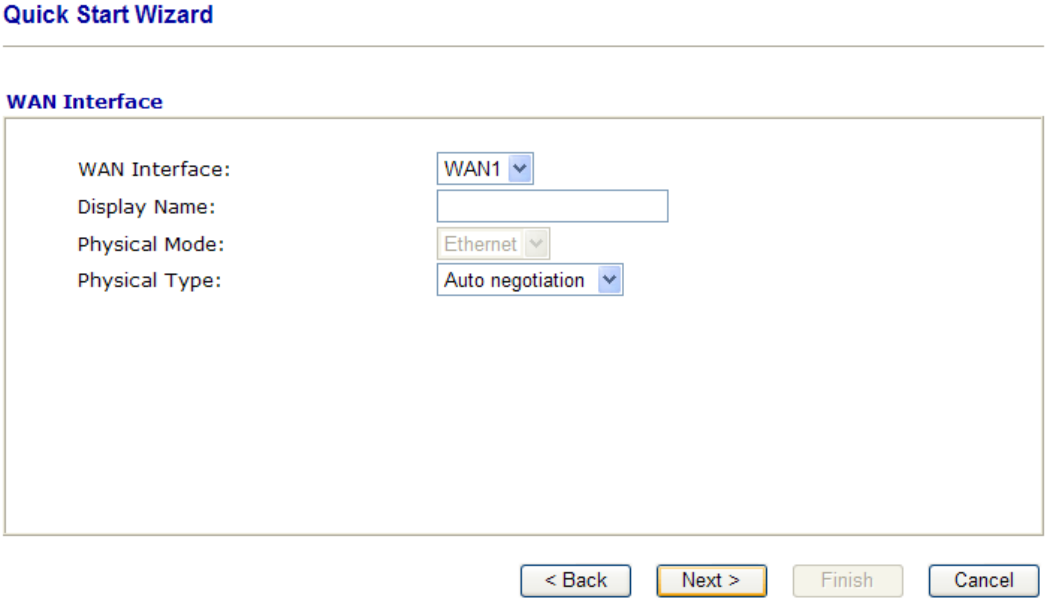
6. Now, the password has been changed. Next time, use the new password to access the Web Configurator for this router.

2.2 Quick Start Wizard

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

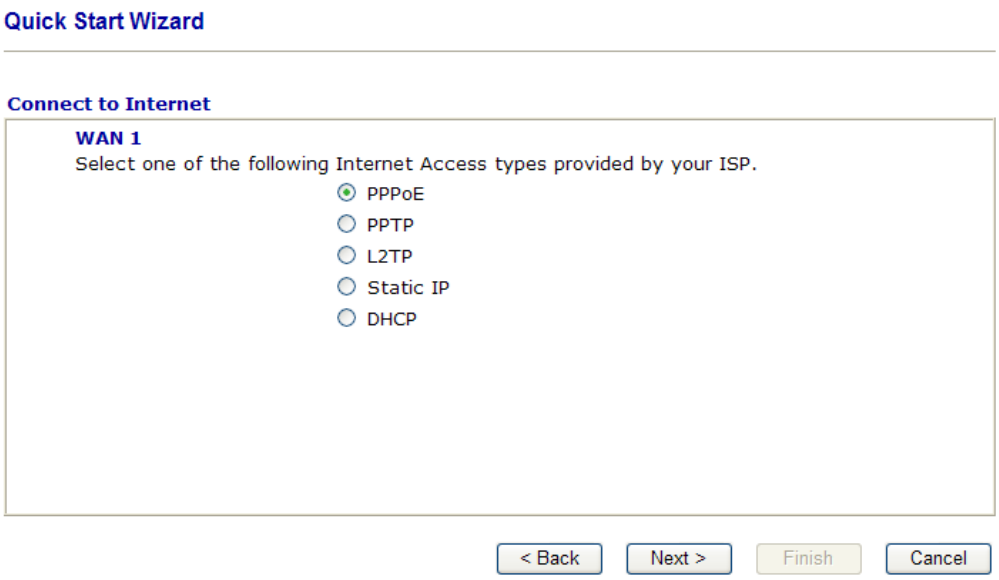


On the next page as shown below, please select the WAN interface that you use. Choose **Auto negotiation** as the physical type for your router. Then click **Next** for next step.



WAN Interface	Specify which interface you use for network connection.
Display Name	Type the name for this router.
Physical Mode	If you choose WAN2, you can specify Ethernet or 3G USB Modem as the physical mode.
Physical Type	Choose the physical type you desired. The default setting is **Auto negotiation**.

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



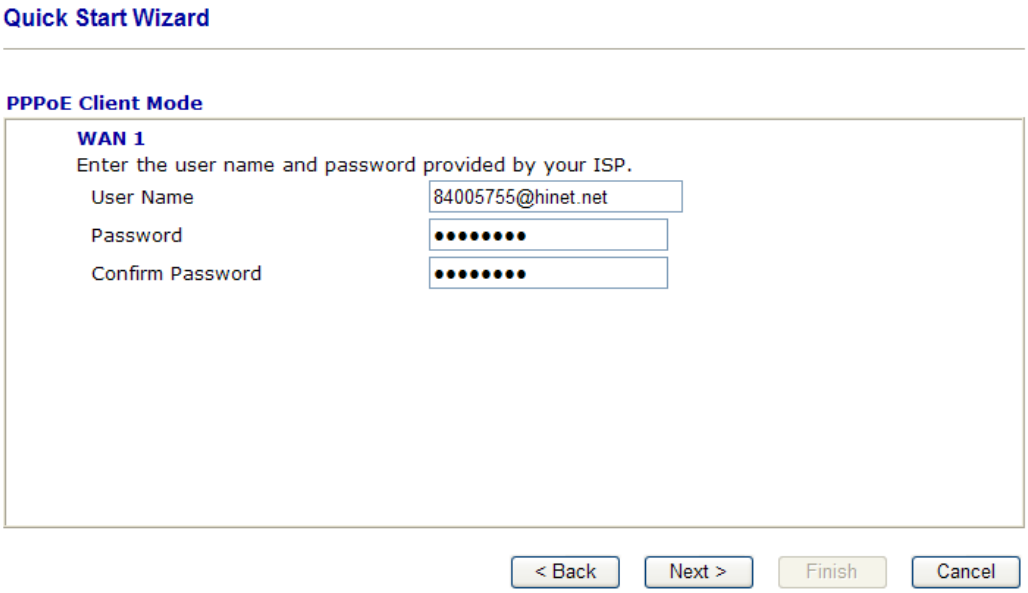
In the **Quick Start Wizard**, you can configure the router to access the Internet with different protocol/modes such as **PPPoE**, **PPTP, L2TP**, **Static IP** or **DHCP**. The router supports the WAN interface for Internet access.

2.2.1 PPPoE

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

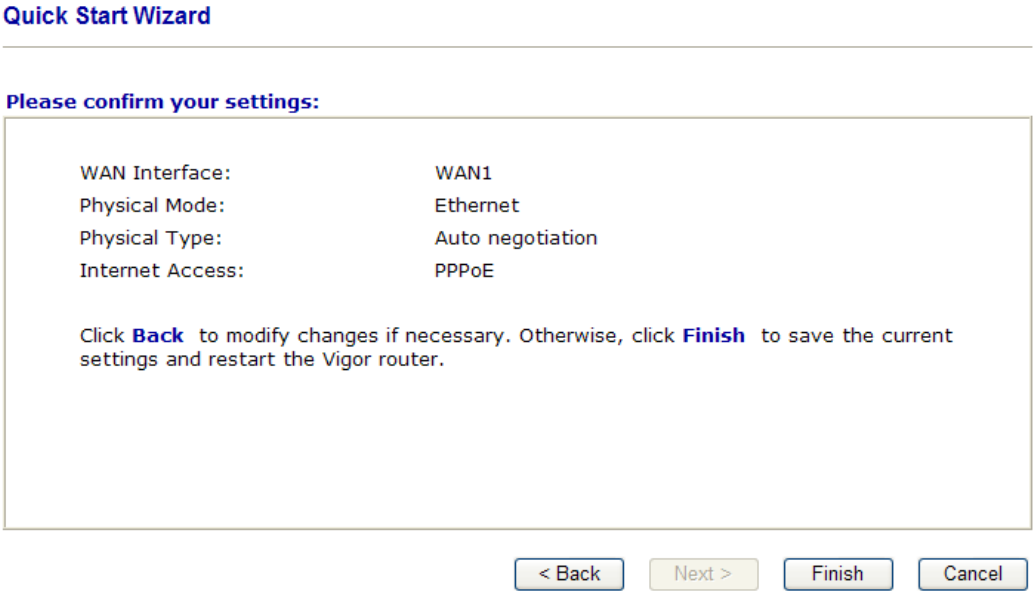
PPPoE is used for most of modem users. All local users can share one PPPoE connection for accessing the Internet. Your service provider will provide you information about user name, password, and authentication mode.

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



User Name	Assign a specific valid user name provided by the ISP.
Password	Assign a valid password provided by the ISP.
Confirm Password	Retype the password.

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

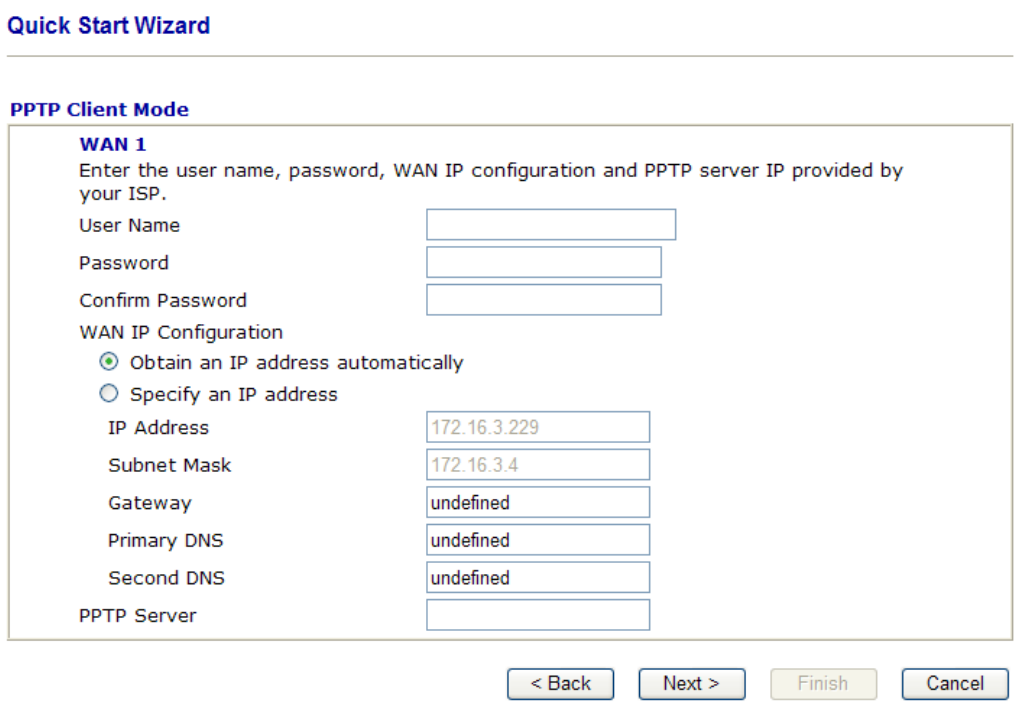


Click **Finish.** A page of **Quick Start Wizard Setup OK!!!** will appear. Then, the system status of this protocol will be shown.

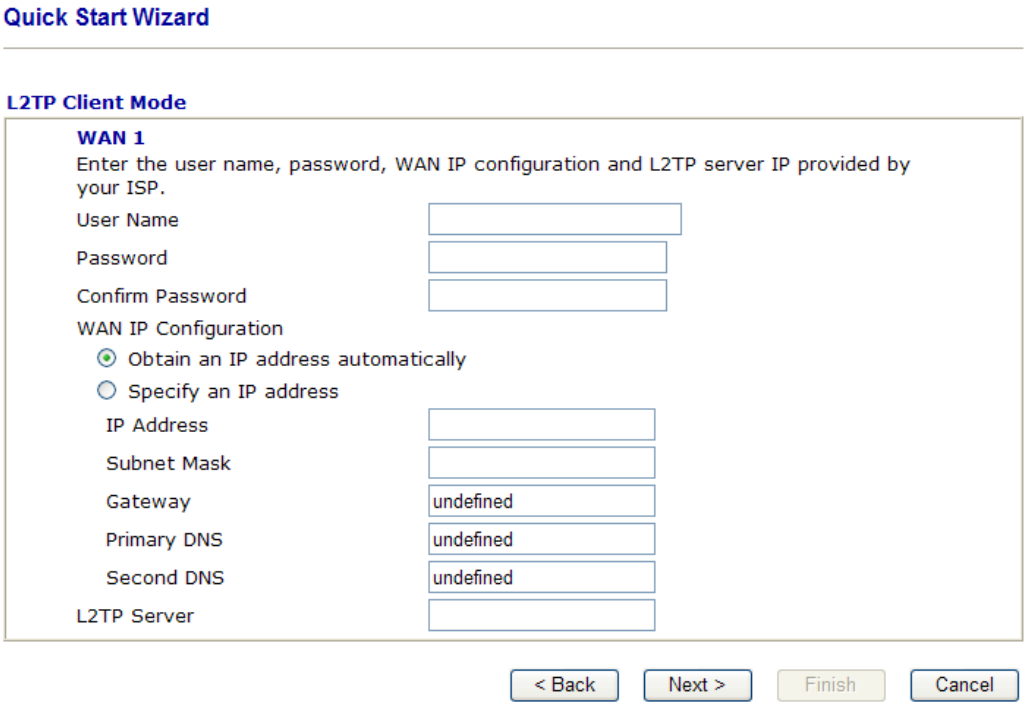
2.2.2 PPTP/L2TP

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

PPTP Setting ---



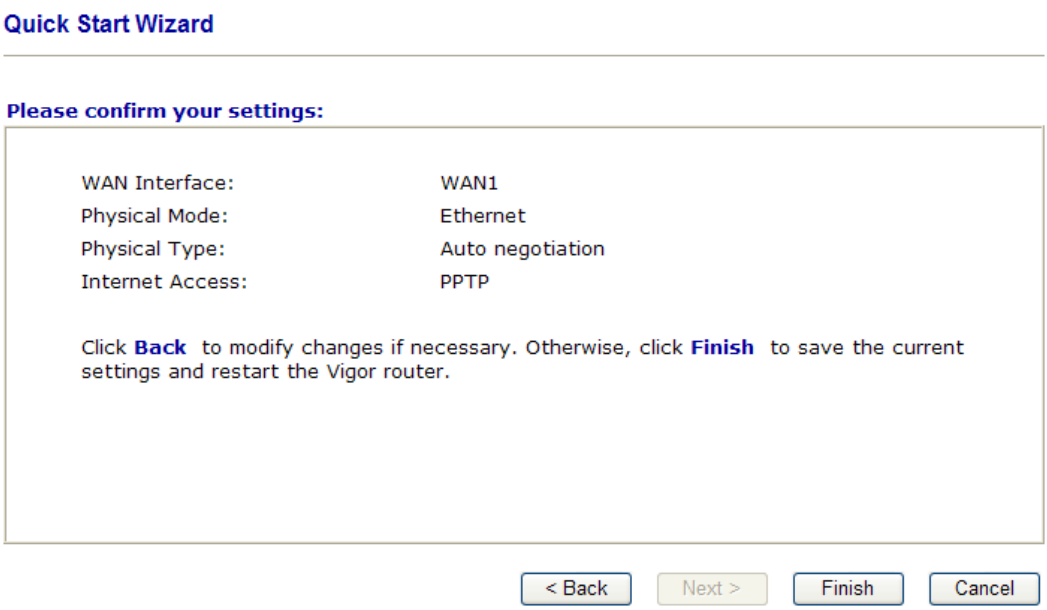
L2TP Setting ---



User Name	Assign a specific valid user name provided by the ISP.
Password	Assign a valid password provided by the ISP.
Confirm Password	Retype the password.

Obtain an IP address automatically	Click it to obtain the IP address automatically.
Specify an IP address	Click it to specify some data manually. **IP Address** – Type the IP address. **Subnet Mask** – Type the subnet mask **Gateway –** Type the gateway of the router. **Primary DNS** – Type the primary DNS address **Secondary DNS** – Type the secondary DNS if required. **PPTP/L2TP Server** – Type the IP address of the PPTP/L2TP Server.

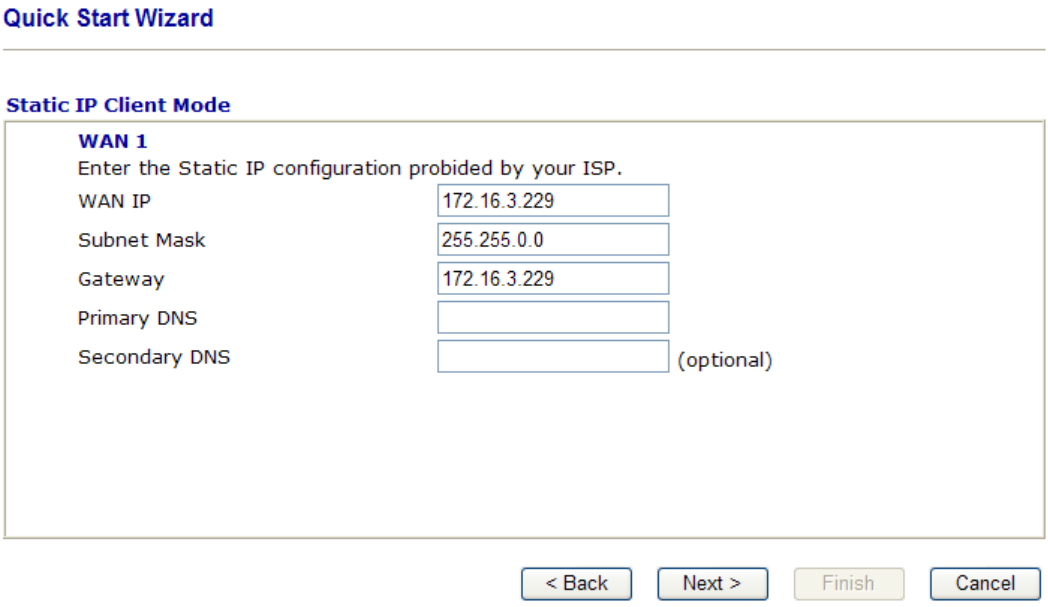
Click **Next** for viewing summary of such connection.



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

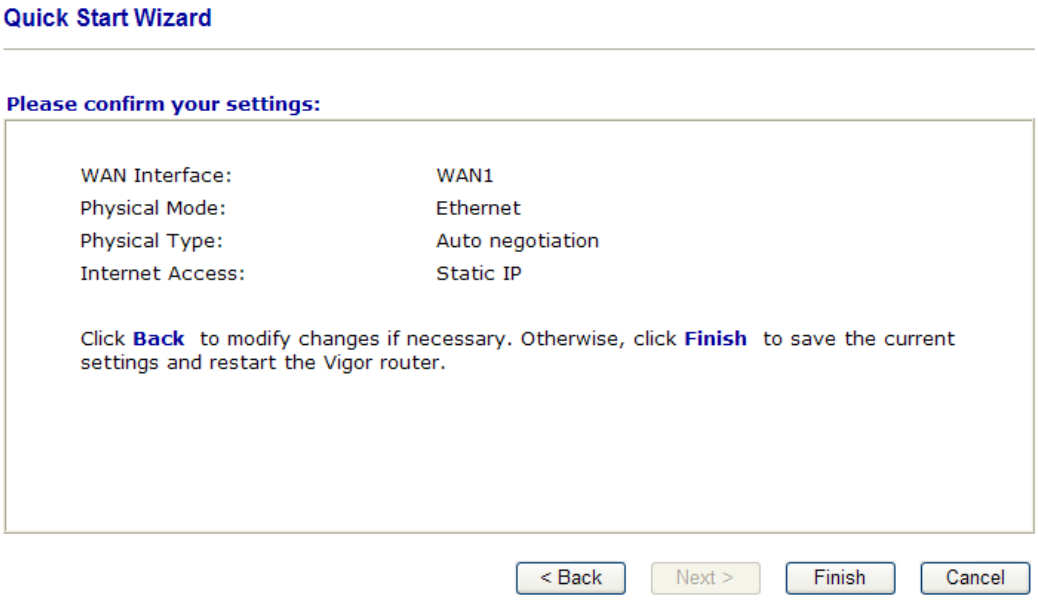
2.2.3 Static IP

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



WANIP Address	Type the IP address.
Subnet Mask	Type the subnet mask.
Gateway	Type the gateway IP address.
Primary/Secondary DNS	Type in the primary IP address for the router if you want to use **Static IP** mode. If necessary, type in secondary IP address for necessity in the future.

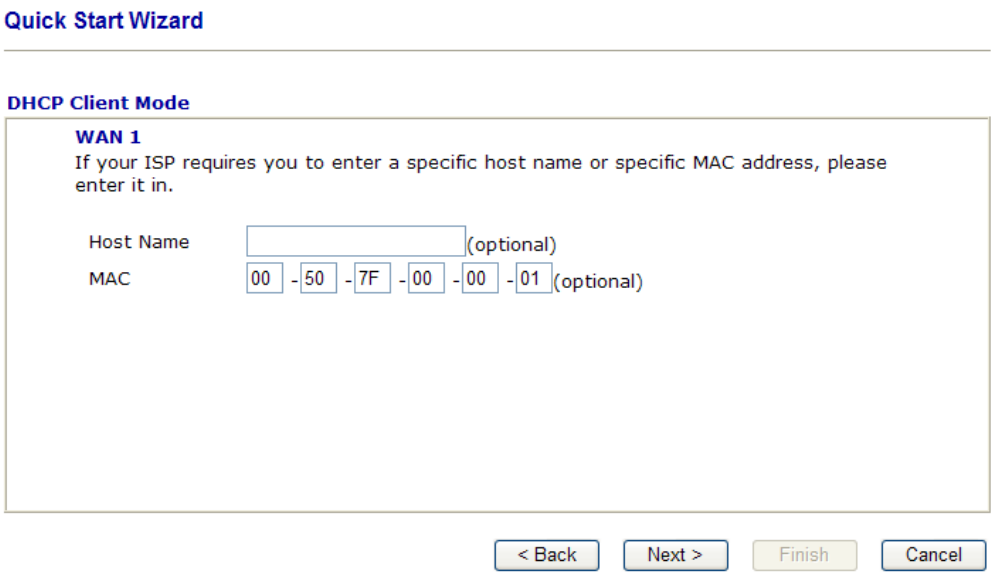
After finishing the settings in this page, click **Next** to see the following page.



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

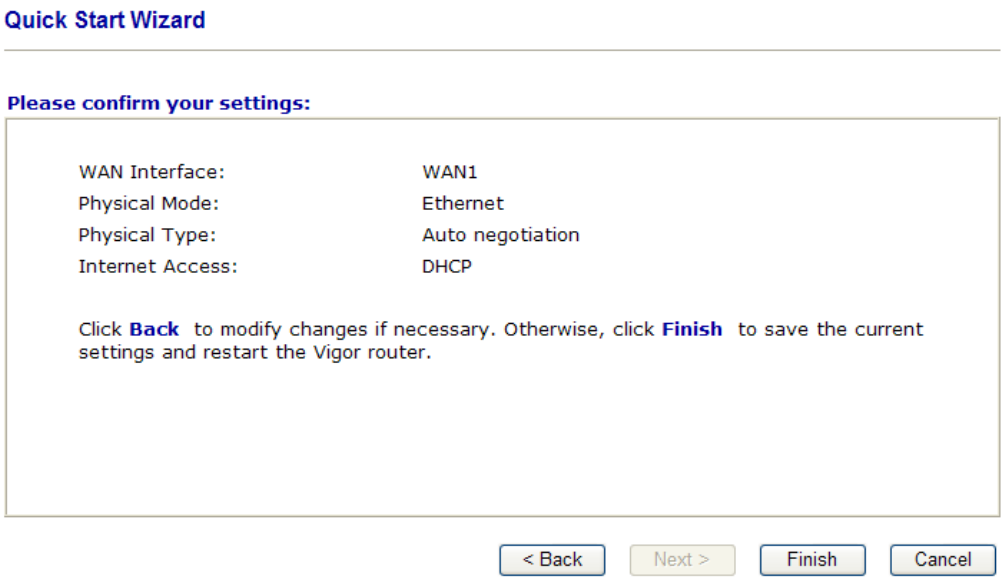
2.2.4 DHCP

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



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

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

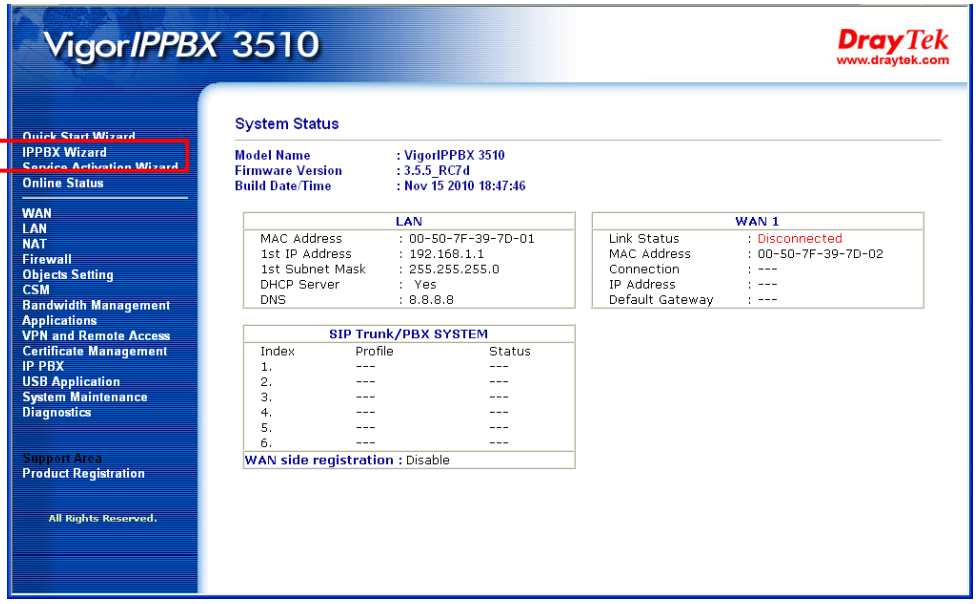


Click **Finish.** A page of **Quick Start Wizard Setup OK!!!** will appear. Then, the system status of this protocol will be shown.

Quick Start Wizard Setup OK !!!

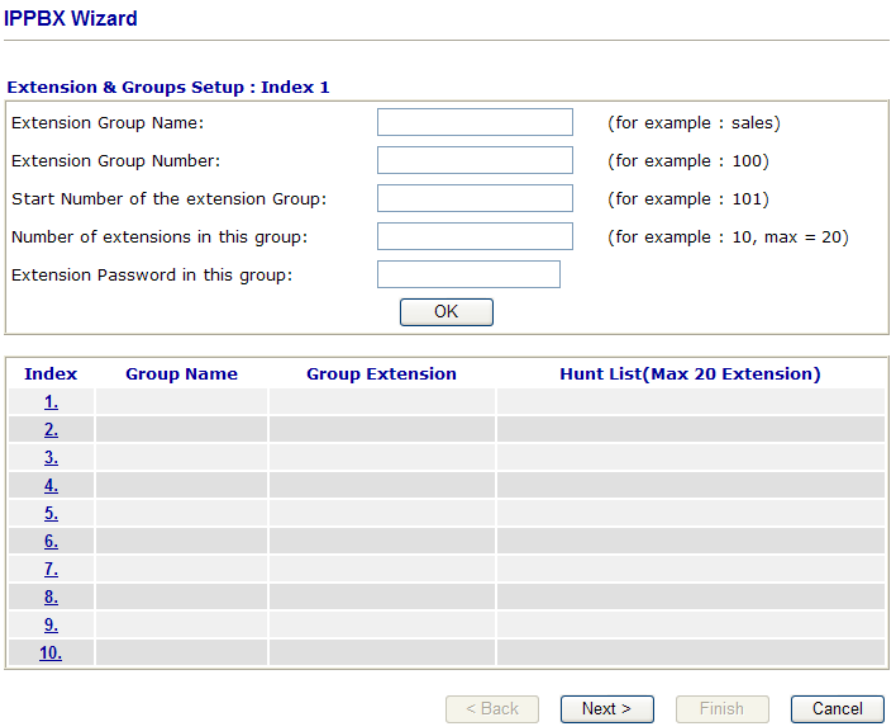
2.3 IPPBX Wizard

IPPBX Wizard can guide the user to configure the required settings for this router within several steps. All the settings, also, can be configured by using **IP PBX** menu. However, the wizard is the most convenient and easy method for users.



2.3.1 Extension & Group Setup

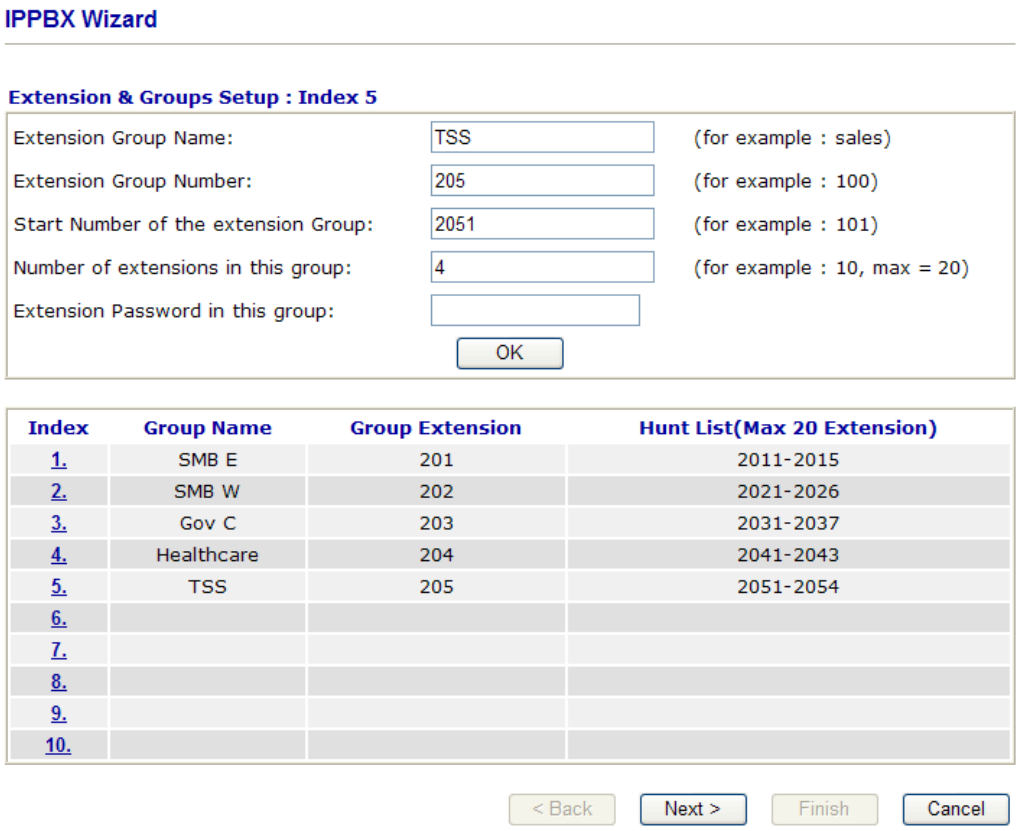
Click **IPPBX Wizard**. You can get the first screen as shown below.



Extension Group Name	Type a name as a display for this extension group.
Extension Group Number	Type the number of extension for such group.
Start Number of the extension Group	Type the start extension number for such group.
Number of extension in this group	Type the total number of the extension for such group.
Extension Password in this group	Type the password. All the extensions in this group that need to register to IPPBX respectively must use such password for the registration.

When you finish the settings of group name, group number, start number, number of extension fields, please click **OK** to save them. The new added group will be displayed on the screen. You can set 10 groups for using in different conditions. Then click **Next** to access into next web page.

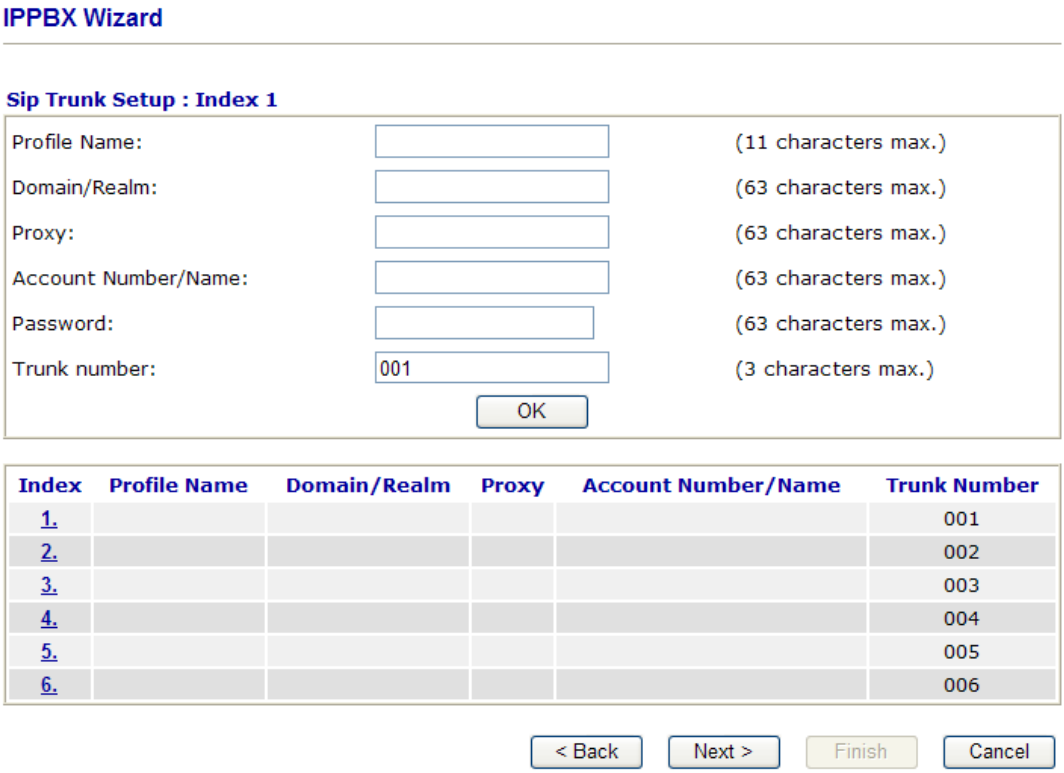
Below shows an example for your reference:



After finishing the extension & group setup, please click **Next**.

2.3.2 SIP Trunk Setup

This page allows you to set profiles for six SIP outside lines at one time.



Profile Name — Type a name for this profile for identifying.

Domain/Realm — Set the domain name or IP address of the SIP Registrar server.

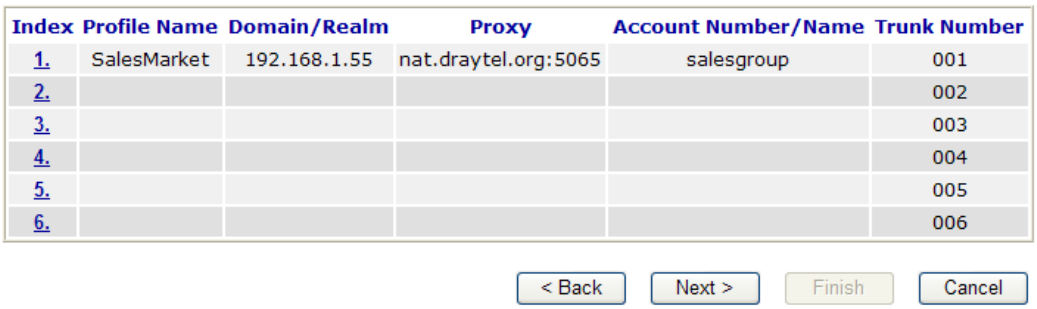
Proxy — Set domain name or IP address of SIP proxy server. By the time you can type **:port number** after the domain name to specify that port as the destination of data transmission (e.g., **nat.draytel.org:5065**)

Account Number/Name — Enter your account name of SIP Address.

Password — Type the password which will be used in registration for SIP service for this profile.

Trunk Number — There are two ways to dial outside lines for an extension number. First, dial a short number and wait for a while. When dial tone appears, please dial the real outside line number. Second, dial a short number and then the real outside line number without waiting for dial tone. The short number is defined here as Trunk Number.

When you finish the settings of profile name, domain/realm, proxy, account number/name, password and trunk number fields, please click **OK** to save them. The new added profile will be displayed on the screen.



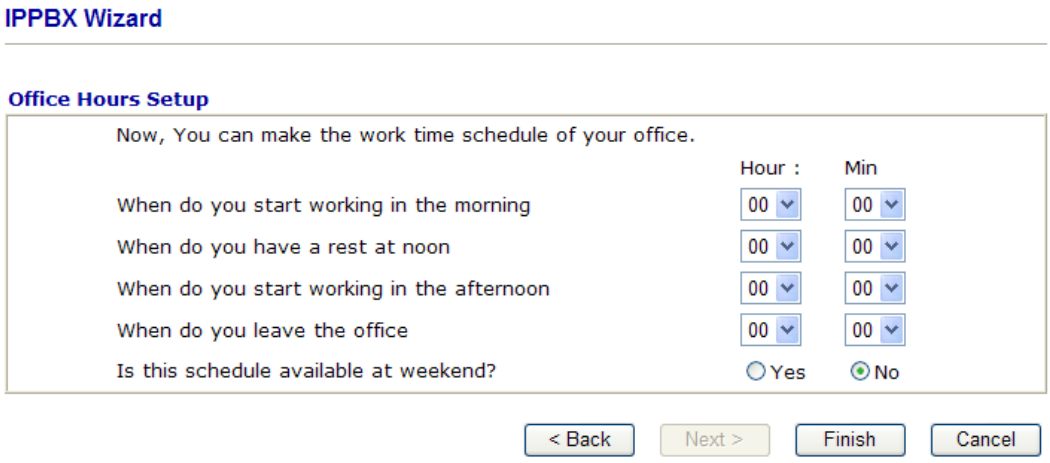
Index	Profile Name	Domain/Realm	Proxy	Account Number/Name	Trunk Number
1.	SalesMarket	192.168.1.55	nat.draytel.org:5065	salesgroup	001
2.					002
3.					003
4.					004
5.					005
6.					006

< Back | Next > | Finish | Cancel

You can set 6 profiles for using in different conditions. Then click **Next** to access into next web page.

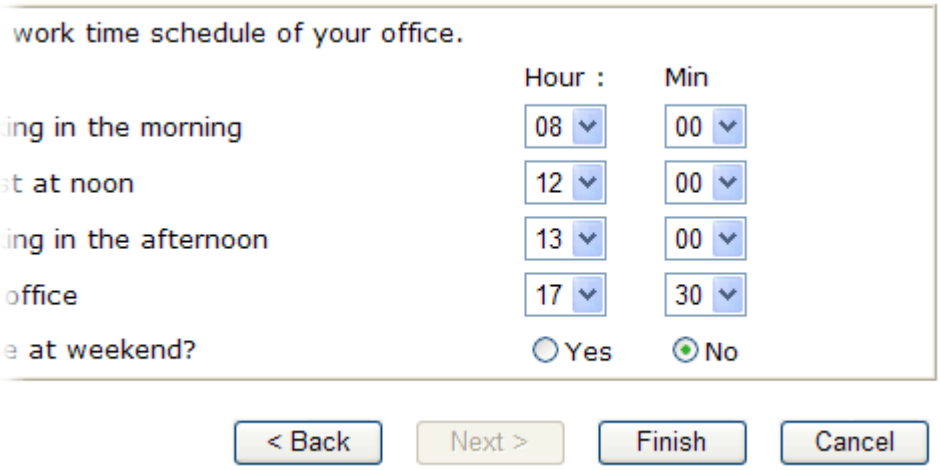
2.3.3 Office Hours Setup

This page allows you to set office hours including starting point, ending point on duty day(s).



When do you start working in the morning	Use the drop down menu to choose the time as the starting point in the morning.
When do you have a rest at noon	Use the drop down menu to choose the time as the ending point in the morning.
When do you start working in the afternoon	Use the drop down menu to choose the time as the starting point in the afternoon.
When do you leave the office	Use the drop down menu to choose the time as the ending point in the afternoon.
Is this schedule available at the weekend	If such schedule will be available in the weekend, simply click **Yes**, otherwise, click **No**.

When you finish the settings, click **Finish** to save the settings and exit the wizard.



2.4 Service Activation Wizard

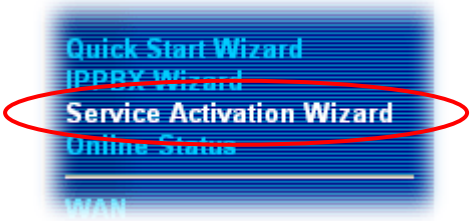
Service Activation Wizard can guide you to set WCF (Web Content Feature) feature with a quick way.

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

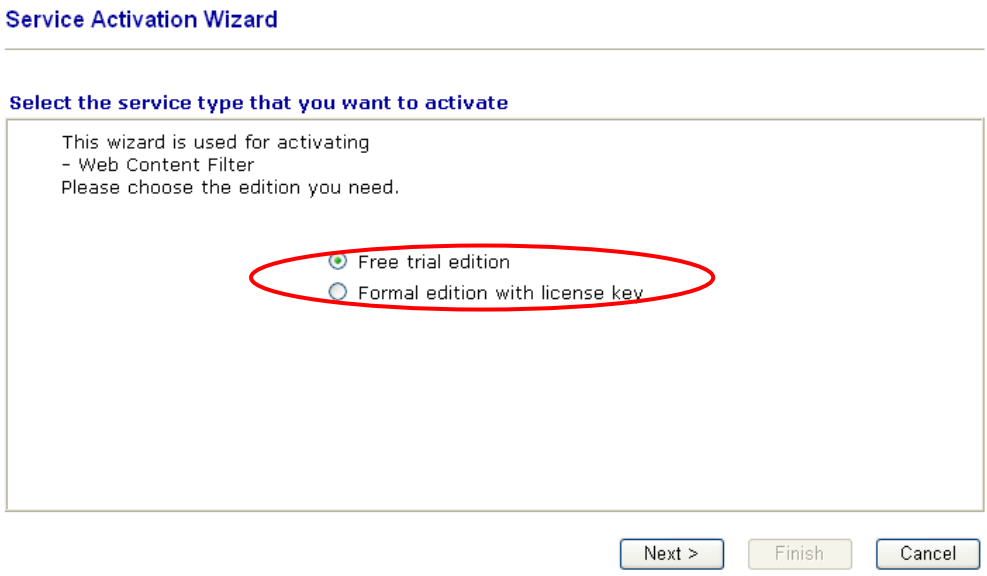
Service Activation Wizard is a tool which allows you to use trial version or update the license of WCF directly without accessing into the server (***MyVigor***) located on http://myvigor.draytek.com. For using Web Content Filter Profile, please refer to section **5.6.3 Web Content Filter Profile** for detailed information.

Now, please follow the steps listed below to activate WCF feature for your router.

1. Open **Service Activation Wizard**.



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

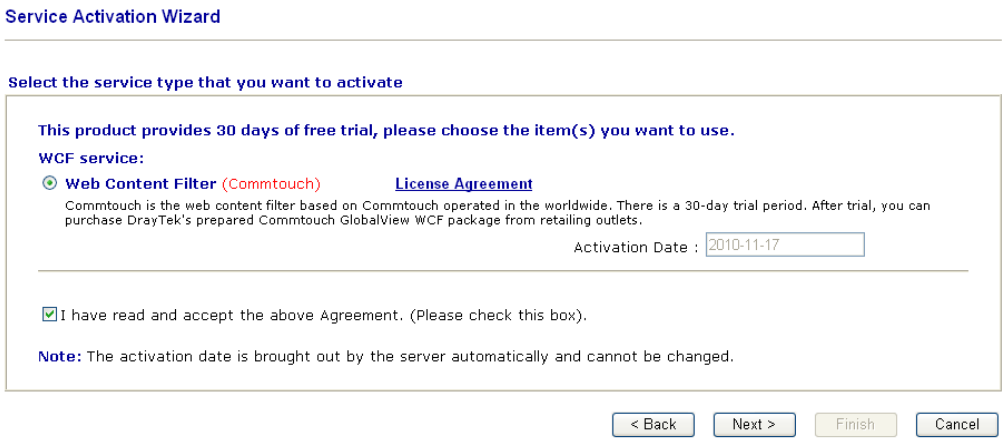


Free trial edition: it offers a period of trial for you to get acquainted with WCF function.

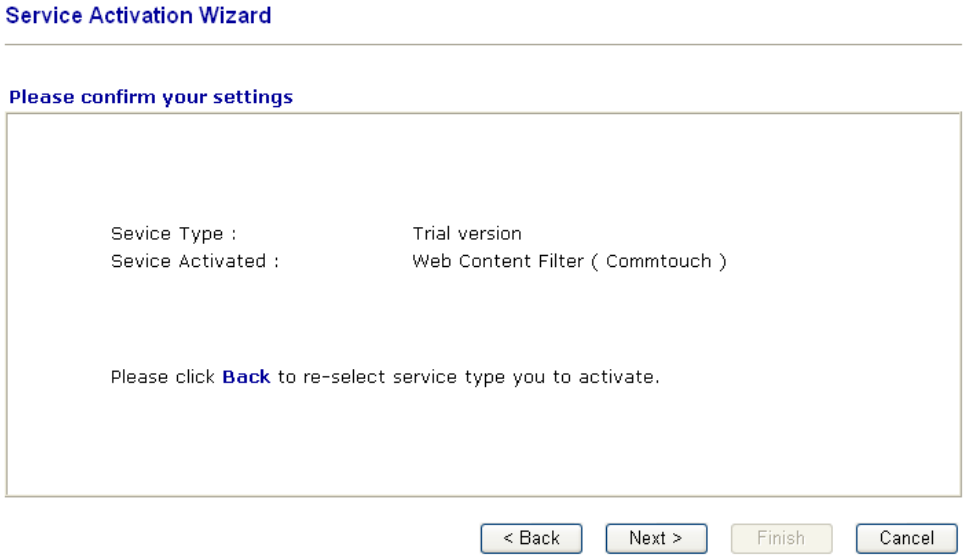
Formal edition with license key: you can extend the license valid time manually.

Note: If you activate **Formal edition with license key** first, the free trial edition will be invalid.

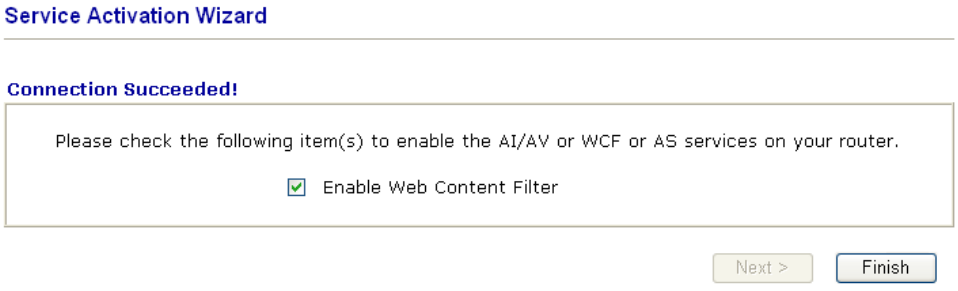
3. In the following page, please check the box of **I have read and accept the above agreement**. When you finish the selection, please click **Next**.



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



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



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

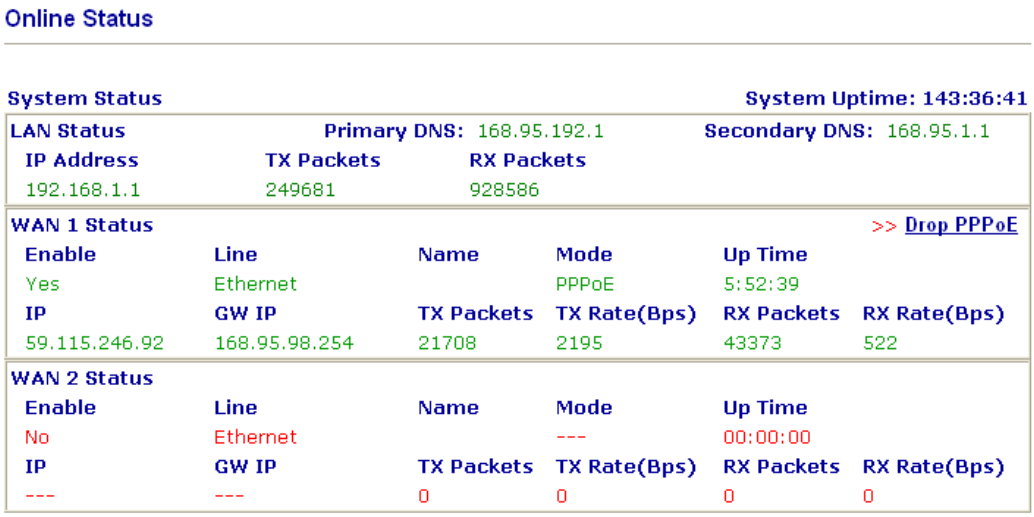
> **Note:** The service will be activated and applied as the default rule configured in **Firewall>>General Setup**.

6. Now, the web page will display the service that you have activated according to your selection. The valid time for the free trial of these services is one month.

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

2.5 Online Status

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



Detailed explanation is shown below:

Primary DNS Display the IP address of the primary DNS.

Secondary DNS Display the IP address of the secondary DNS.

LAN Status

IP Address Display the IP address of the LAN interface.

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

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

WAN Status

Enable Display if such WAN interface is enabled or not.

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

Name Display the name set in WAN page.

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

Up Time Display the total uptime of the interface.

IP Display the IP address of the WAN interface.

GW IP Display the IP address of the default gateway.

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

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

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

RX Rate Display the speed of received octets at the WAN interface.

Note: The words in green mean that the WAN connection of that interface is ready for accessing Internet; the words in red mean that the WAN connection of that interface 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.

2.7 Support Area

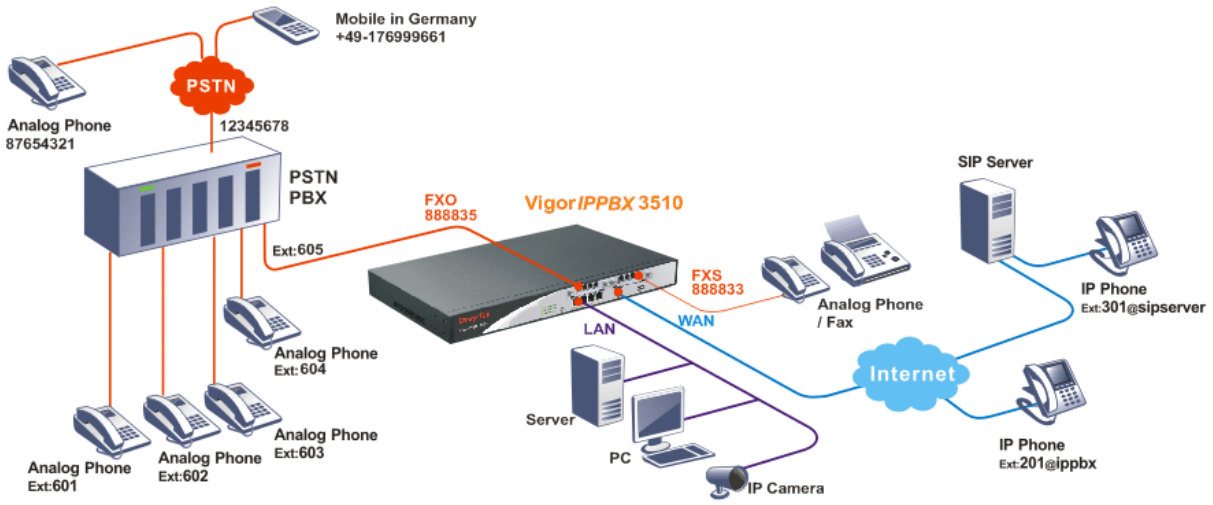
When you click the menu item under **Support Area**, you will be guided to visit www.draytek.com and open the corresponding pages directly.

This page is left blank.

Chapter 3: Applications

This chapter shows several scenarios for your reference to configure IP PBX for different purposes.

3.1 Versatile PSTN and VoIP Trunk

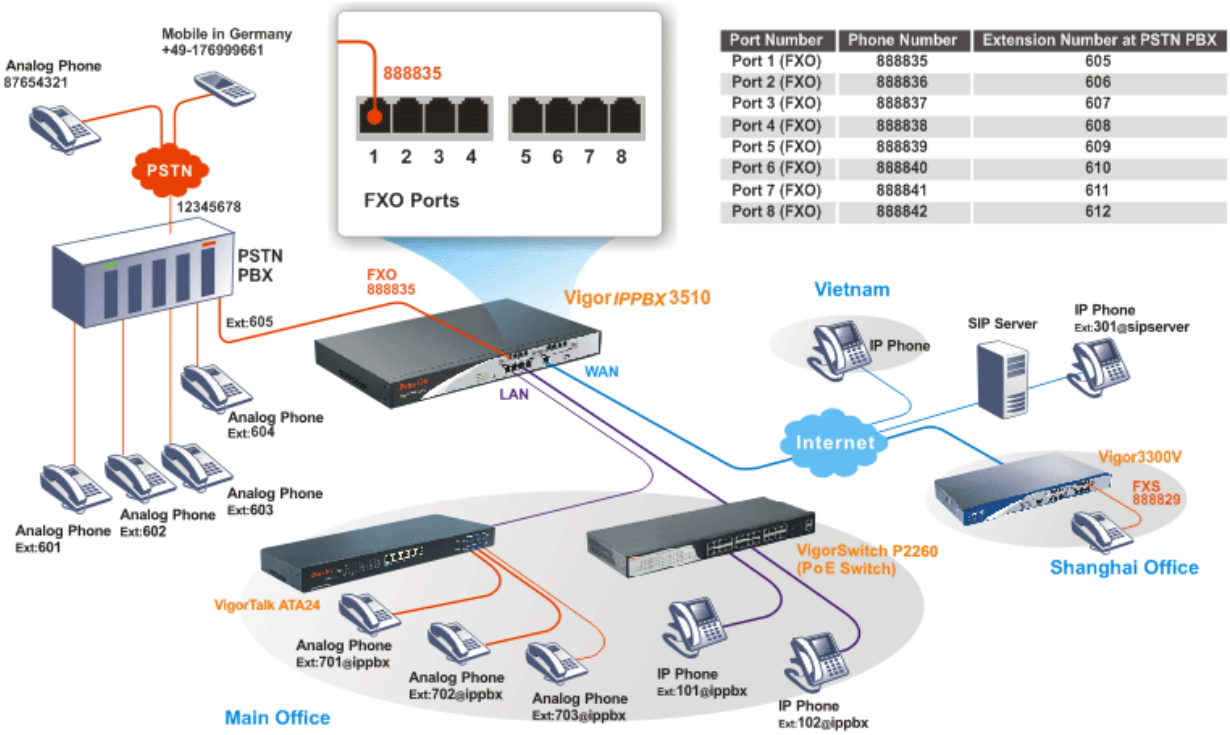


- The establishment of IP registration is made through WAN port.
- The remote IP -based phone with ext. 301 is registered at a SIP server.
- The remote IP -based phone with ext. 201 is registered at remote site.
- The analog phone or fax machine is connected to FXS module. The said VoIP No. is 888833.
- The PSTN PBX is with PSTN line No. 12345678. The remote analog phone line is No. 87654321. The remote mobile phone is with No. +49-176999661.
- The analog phones with ext. No.601, 602, 603, 604 are connected to PSTN PBX. Connect one FXO port to PSTN PBX's inside line. The extension No. 605 line is assigned to the FXO port on FXO module.
- The analog phone (connected to FXS module) made a call to remote mobile (+49-176999661): Press 888835#. After getting through you will hear the dial tone, press outside line 0 and then press the mobile number +49-176999661.
- The IP phone with ext. No. 201 made a call to remote analog phone (No. 87654321): Press 888835#. After getting through you will hear the dial tone, press outside line 0 and then press the PSTN number 87654321.
- The mobile No. +49-176999661 made a call to IP Phone with ext. No.201: Press 12345678. After getting through you will hear the auto reply from the PBX, then

press the extension No. 605. After getting through you can hear the dial tone, then press ext. No. 201.

- The analog phone with ext. No. 602 made a call to IP phone with extension No. 301: Press extension No. **605.** After getting through you will hear the dial tone, then press the ext. No. 301.

3.2 Cost-effective Extendability by Integrated Analog-telephone Adapter (for 24 Conventional Analog Phones) & POE-switch for IP-based phones



Port Number	Phone Number	Extension Number at PSTN PBX
Port 1 (FXO)	888835	605
Port 2 (FXO)	888836	606
Port 3 (FXO)	888837	607
Port 4 (FXO)	888838	608
Port 5 (FXO)	888839	609
Port 6 (FXO)	888840	610
Port 7 (FXO)	888841	611
Port 8 (FXO)	888842	612

- The establishment of IP registration is made through WAN port.
- The remote IP -based phone with ext. 301 is registered at a SIP server.
- The remote IP -based phone with ext. 201 is registered at remote site.
- The PSTN PBX is with PSTN line No. 12345678. The remote analog phone line is No. 87654321. The remote mobile phone is with No. +49-176999661.
- The analog phones with ext. No.601, 602, 603, 604 are connected to PSTN PBX. Connect 8 FXO ports to PSTN PBX's inside line.

  FXO 1 port: with extension No. 605 [Phone No. 88835]

  FXO 2 port: with extension No. 606 [Phone No. 88836]

  FXO 3 port: with extension No. 607 [Phone No. 88837]

  FXO 4 port: with extension No. 608 [Phone No. 88838]

  FXO 5 port: with extension No. 609 [Phone No. 88839]

  FXO 6 port: with extension No. 610 [Phone No. 88840]

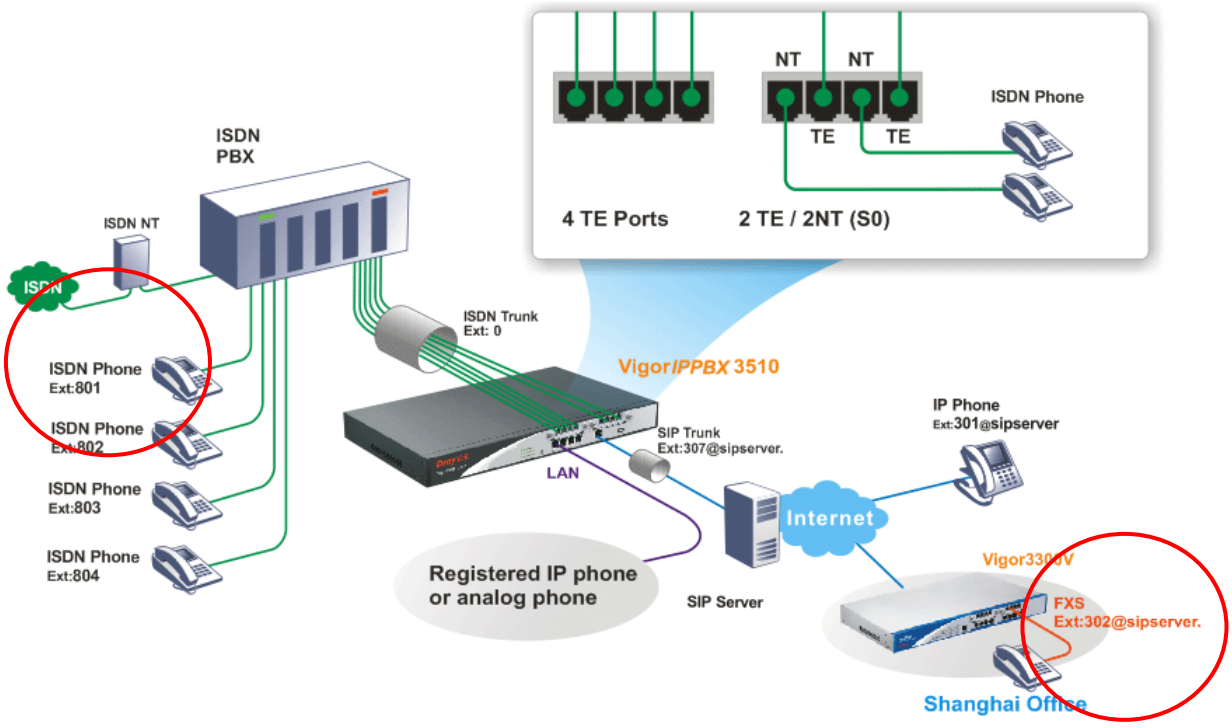
  FXO 7 port: with extension No. 611 [Phone No. 88841]

  FXO 8 port: with extension No. 612 [Phone No. 88842]

- The IP phone with ext. No. 201 made a call to remote analog phone (No. 87654321): Press 888835#. After getting through you will hear the dial tone, press outside line **0** and then press the PSTN number 87654321.
- The analog phone with VoIP number 88829 in Shanghai made a call to the remote mobile No. (+49-176999661): Press 888842#. After getting through you will hear the dial tone, press outside line **0** and then press the mobile No. +49-176999661.
- The mobile No. +49-176999661 made a call to IP Phone with ext. No.201: Press 12345678. After getting through you will hear the auto reply from the PBX, then press the extension No. 611. After getting through you can hear the dial tone, then press ext. No. 201.
- The analog phone with ext. No. 602 made a call to IP phone with extension No. 703: Press extension No. **609.** After getting through you will hear the dial tone, then press the ext. No. 703.
- The analog phone with VoIP number 88829 in Shanghai made a call to the analog phone (ext. No.604): Press 888838#. After getting through you will hear the dial tone, then press the ext. No. 604.

Device	WAN IP	Port Number	Phone Number	Extension Number at PSTN PBX
VigorIPPBX 3510	220.135.240.20	Port 1 (FXO)	888835	605
		Port 2 (FXO)	888836	606
		Port 3 (FXO)	888837	607
		Port 4 (FXO)	888838	608
		Port 5 (FXO)	888839	609
		Port 6 (FXO)	888840	610
		Port 7 (FXO)	888841	611
		Port 8 (FXO)	888842	612
Vigor3300V	61.31.167.135	Port 1 (FXS)	888829	

3.3 ISDN Application via ISDN Trunk



- The establishment of IP registration is made through WAN port.
- Ext. 307 and 302 are registered at a SIP server.
- The remote IP-based phone with ext. 301 is registered at a SIP server, too.
- The ISDN Phone with ext. No.801, 802, 803, and 804 are connected to ISDN PBX.

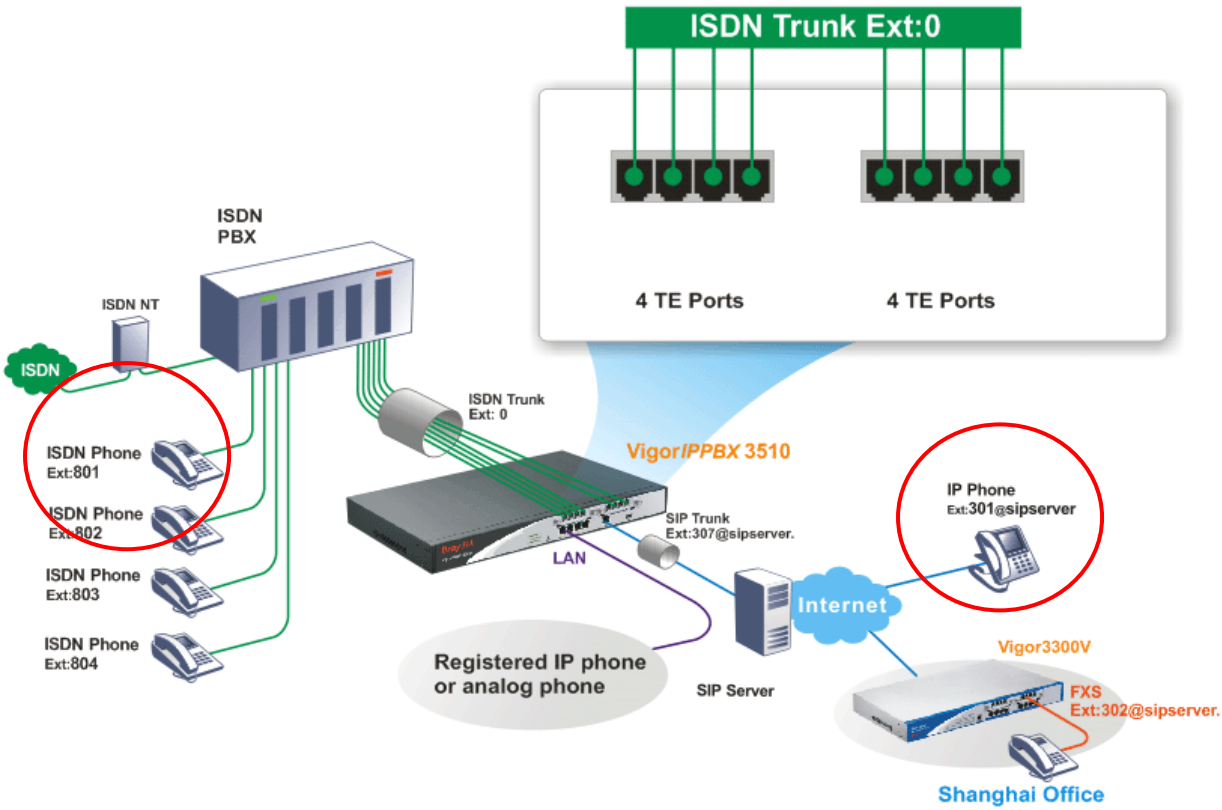
  ISDN Phone: with extension No. 801

  ISDN Phone: with extension No. 802

  ISDN Phone: with extension No. 803

  ISDN Phone: with extension No. 804
- The analog phone with VoIP number 302 in Shanghai made a call to the remote ISDN Phone (Ex:801): Dial to SIP trunk number 307; then dial ISDN trunk number 0 to connect to ISDN PBX. After getting through you can hear the dial tone, press ext. No. 801.

3.4 ISDN Application with All ISDN TE Ports



- The establishment of IP registration is made through WAN port.
- Ext. 307 and 302 are registered at a SIP server.
- The remote IP-based phone with ext. 301 is registered at a SIP server.
- The ISDN Phone with ext. No.801, 802, 803, and 804 are connected to ISDN PBX.

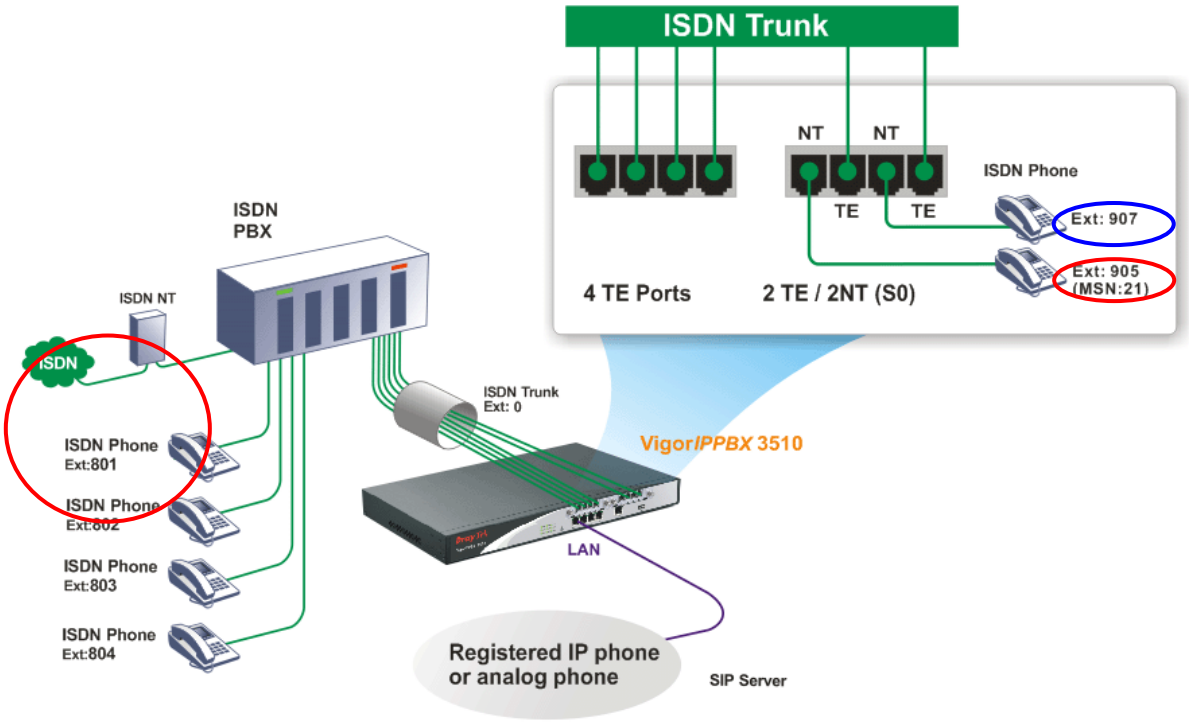
  ISDN Phone: with extension No. 801

  ISDN Phone: with extension No. 802

  ISDN Phone: with extension No. 803

  ISDN Phone: with extension No. 804
- The IP phone with ext. 301 on Internet made a call to the remote ISDN Phone (Ex: 801): Dial to SIP trunk number 307; then dial ISDN trunk number 0 to connect to ISDN PBX. After getting through you can hear the dial tone, press ext. No. 801.

3.5 ISDN Application with 4 ISDN TE and 2 ISDN TE/ 2 ISDN NT Ports



- The establishment of IP registration is made through WAN port.
- The ISDN Phone with ext. No.801, 802, 803, and 804 are connected to ISDN PBX.

  ISDN Phone: with extension No. 801

  ISDN Phone: with extension No. 802

  ISDN Phone: with extension No. 803

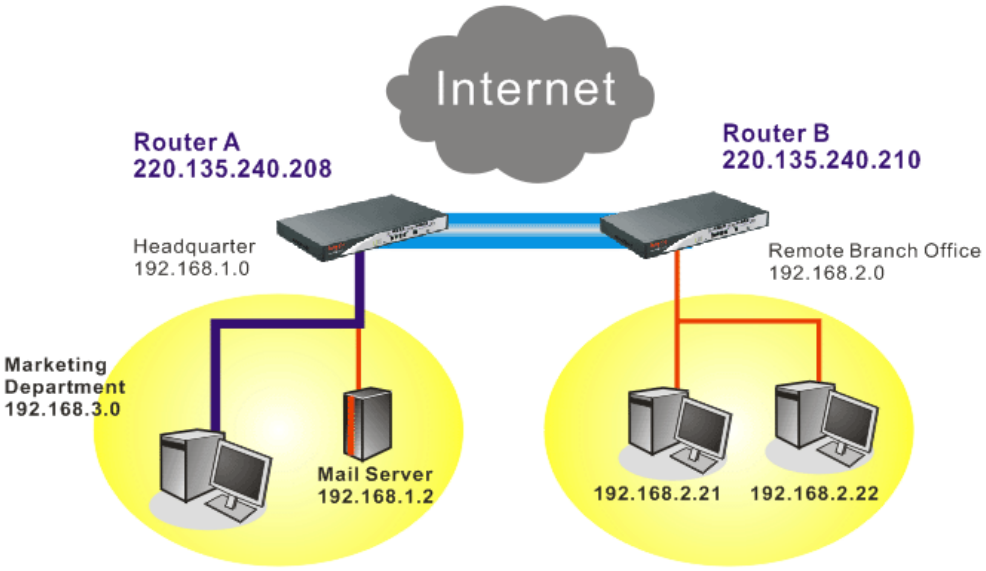
  ISDN Phone: with extension No. 804
- The ISDN phone with ext. 905 (with MSN No. 21) on VigorIPPBX 3510 made a call to the remote ISDN Phone (Ex:801): Dial ISDN trunk number 0 to connect to ISDN PBX. After getting through you can hear the dial tone, press ext. No. 801.
- The ISDN phone with ext. 907 (without MSN number) on VigorIPPBX 3510 made a call to the remote ISDN Phone (Ex: 801): Dial ISDN trunk number 0 to connect to ISDN PBX. After getting through you can hear the dial tone, press ext. No. 801.

This page is left blank.

Chapter 4: Other Applications

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

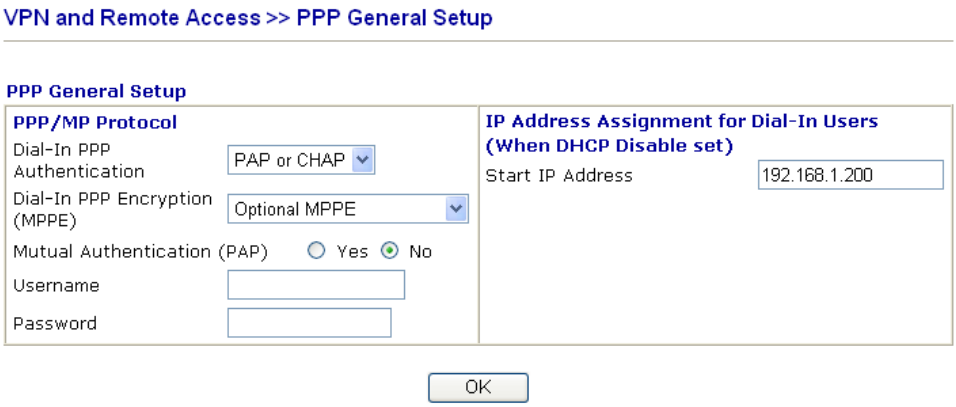
The most common case is that you may want to connect to network securely, such as the remote branch office and headquarter. According to the network structure as shown in the below illustration, you may follow the steps to create a LAN-to-LAN profile. These two networks (LANs) should NOT have the same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



Settings in Router A in headquarter:

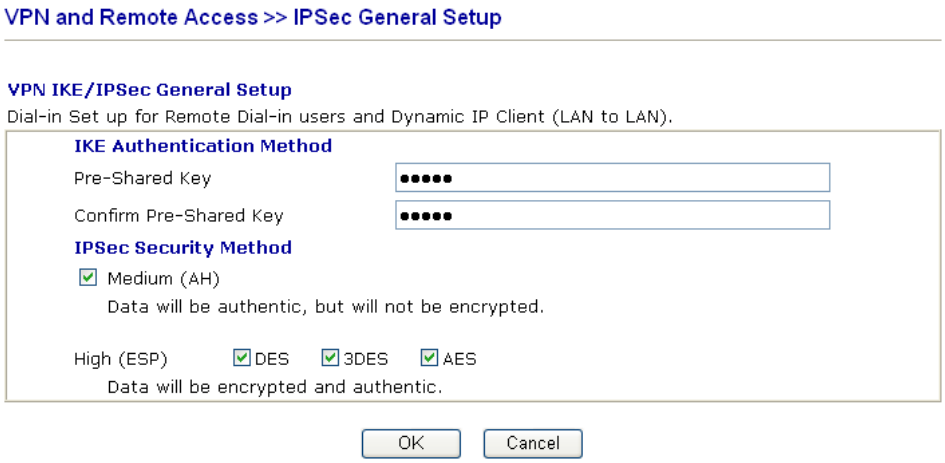
1. Go to **VPN and Remote Access** and select **Remote Access Control** to enable the necessary VPN service and click **OK**.

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

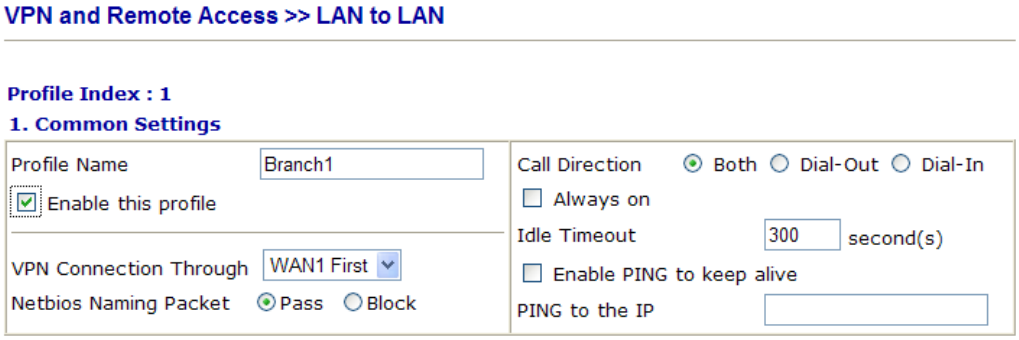


For using **IPSec**-based service, such as IPSec or L2TP with IPSec Policy, you have to

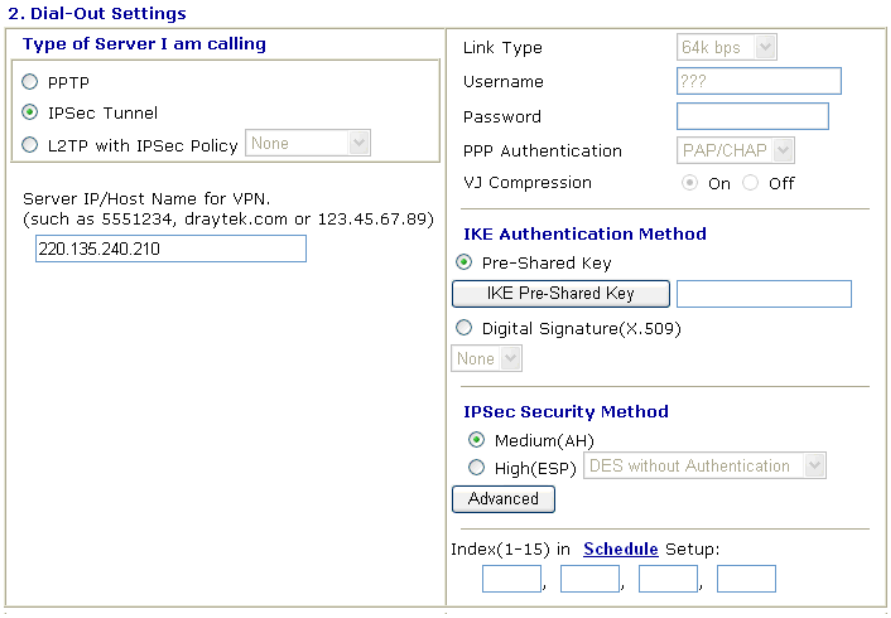
set general settings in **IPSec General Setup**, such as the pre-shared key that both parties have known.



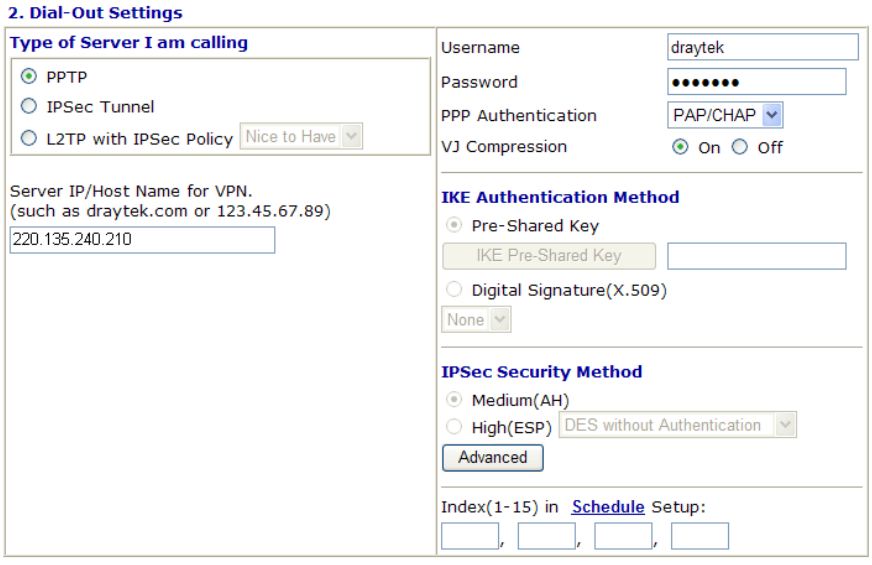
3. Go to **LAN-to-LAN**. Click on one index number to edit a profile.
4. Set **Common Settings** as shown below. You should enable both of VPN connections because any one of the parties may start the VPN connection.



5. Set **Dial-Out Settings** as shown below to dial to connect to Router B aggressively with the selected Dial-Out method.
If an ***IPSec-based*** service is selected, you should further specify the remote peer IP Address, IKE Authentication Method and IPSec Security Method for this Dial-Out connection.

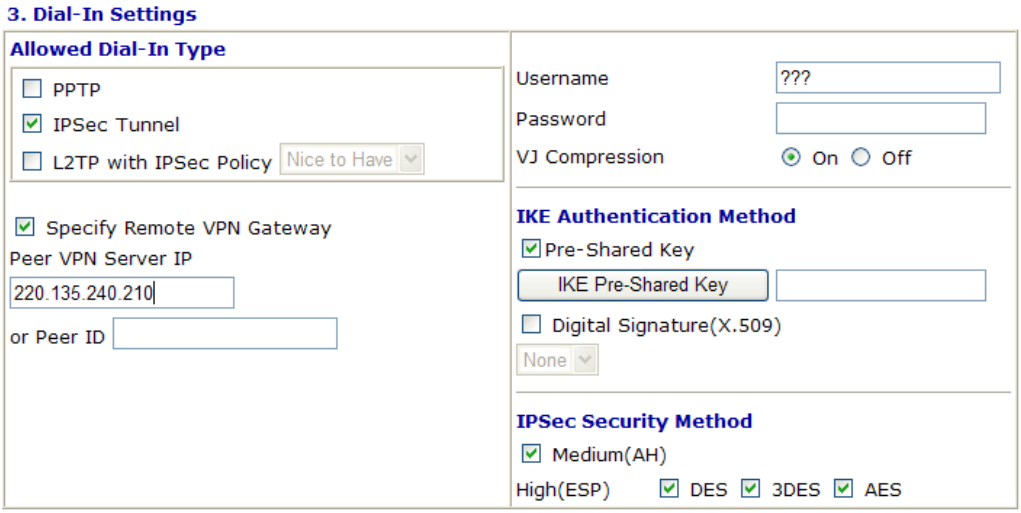


If a ***PPP-based service*** is selected, you should further specify the remote peer IP Address, Username, Password, PPP Authentication and VJ Compression for this Dial-Out connection.

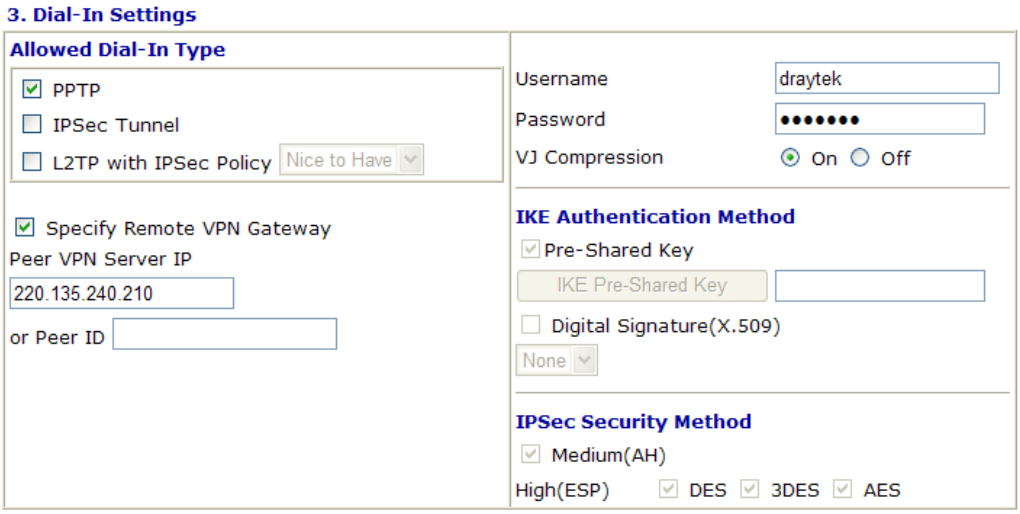


6. Set **Dial-In settings** to as shown below to allow Router B dial-in to build VPN connection.

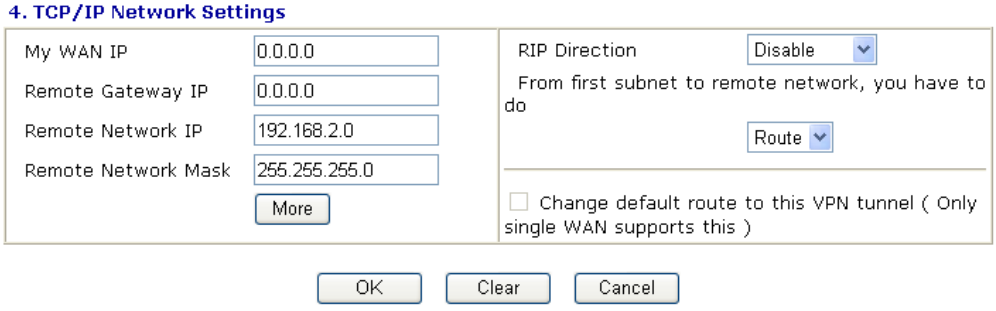
If an ***IPSec-based*** service is selected, you may further specify the remote peer IP Address, IKE Authentication Method and IPSec Security Method for this Dial-In connection. Otherwise, it will apply the settings defined in **IPSec General Setup** above.



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

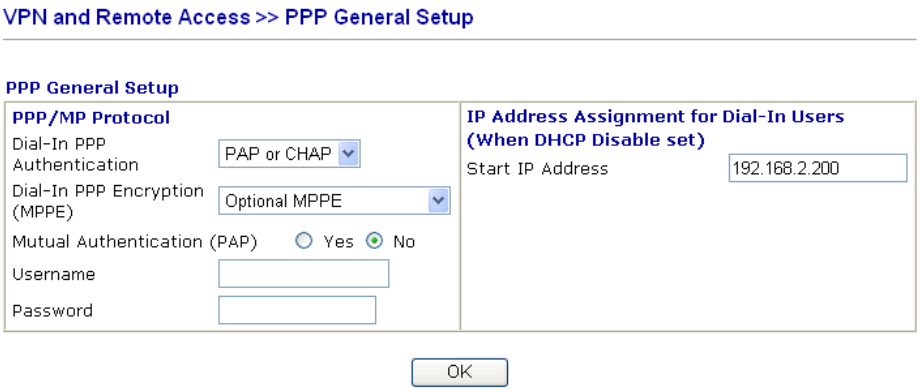


7. At last, set the remote network IP/subnet in **TCP/IP Network Settings** so that Router A can direct the packets destined to the remote network to Router B via the VPN connection.

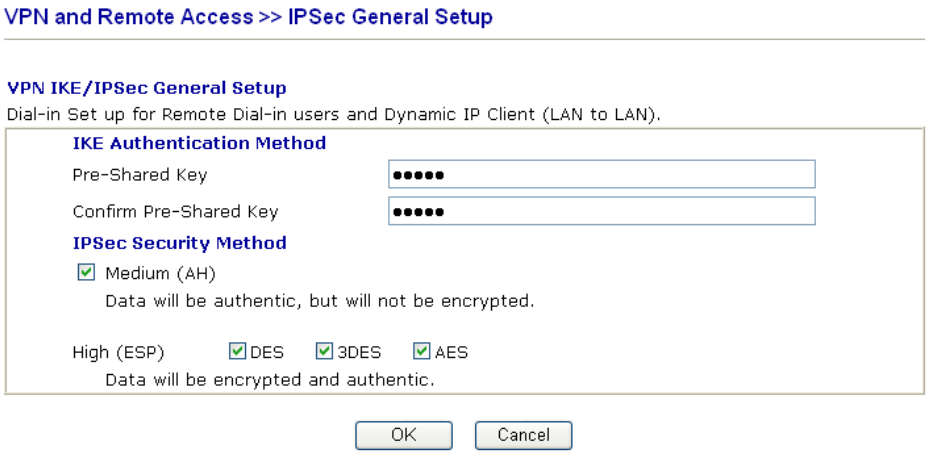


Settings in Router B in the remote office:

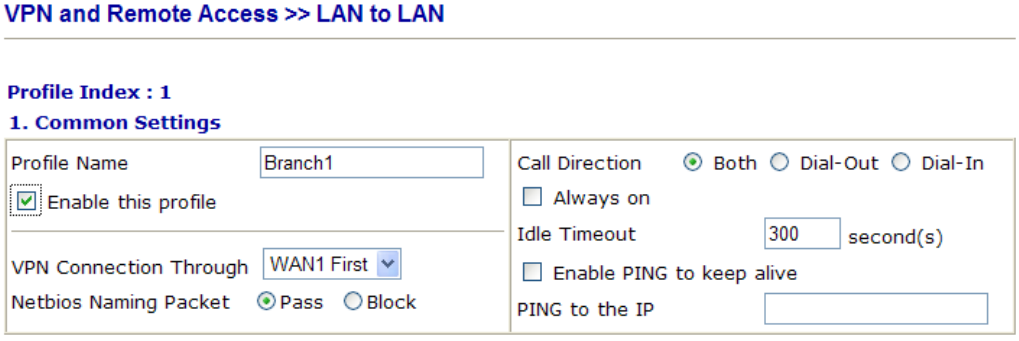
1. Go to **VPN and Remote Access** and select **Remote Access Control** to enable the necessary VPN service and click **OK**.
2. Then, for using **PPP based** services, such as PPTP, L2TP, you have to set general settings in **PPP General Setup**.



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

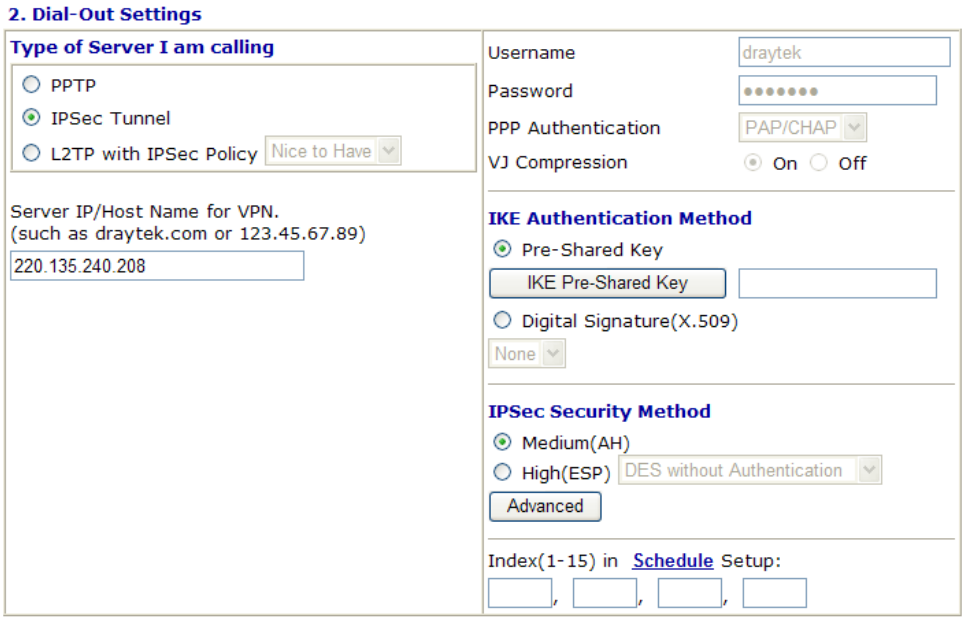


3. Go to **LAN-to-LAN**. Click on one index number to edit a profile.
4. Set **Common Settings** as shown below. You should enable both of VPN connections because any one of the parties may start the VPN connection.

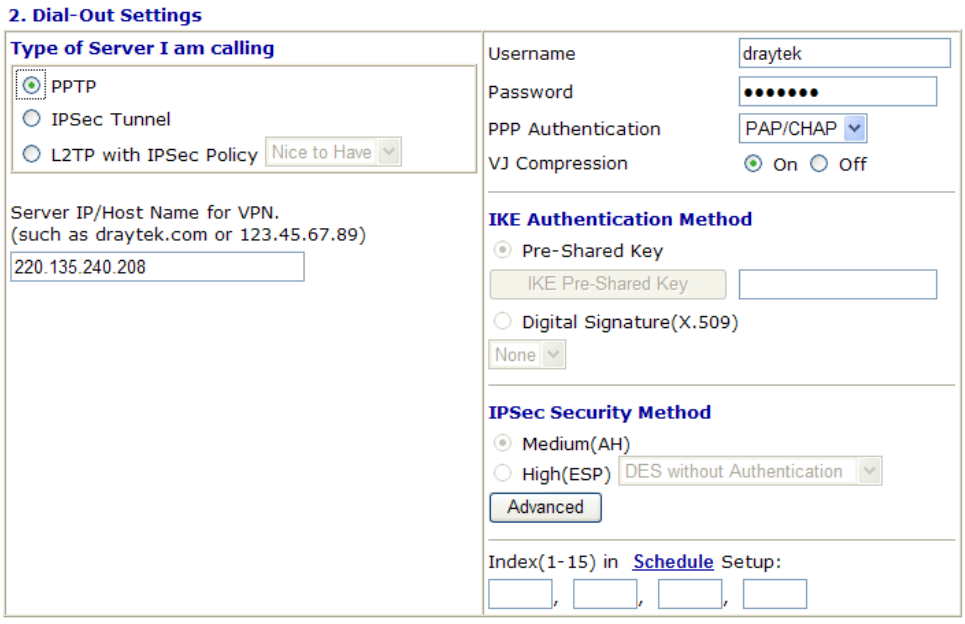


5. Set **Dial-Out Settings** as shown below to dial to connect to Router B aggressively with the selected Dial-Out method.

   If an ***IPSec-based*** service is selected, you should further specify the remote peer IP Address, IKE Authentication Method and IPSec Security Method for this Dial-Out connection.

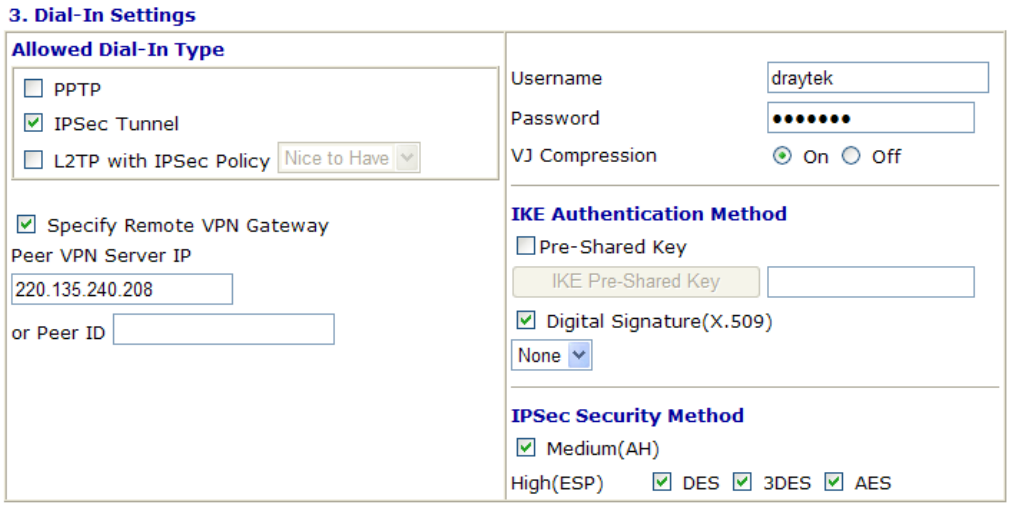


   If a ***PPP-based*** service is selected, you should further specify the remote peer IP Address, Username, Password, PPP Authentication and VJ Compression for this Dial-Out connection.

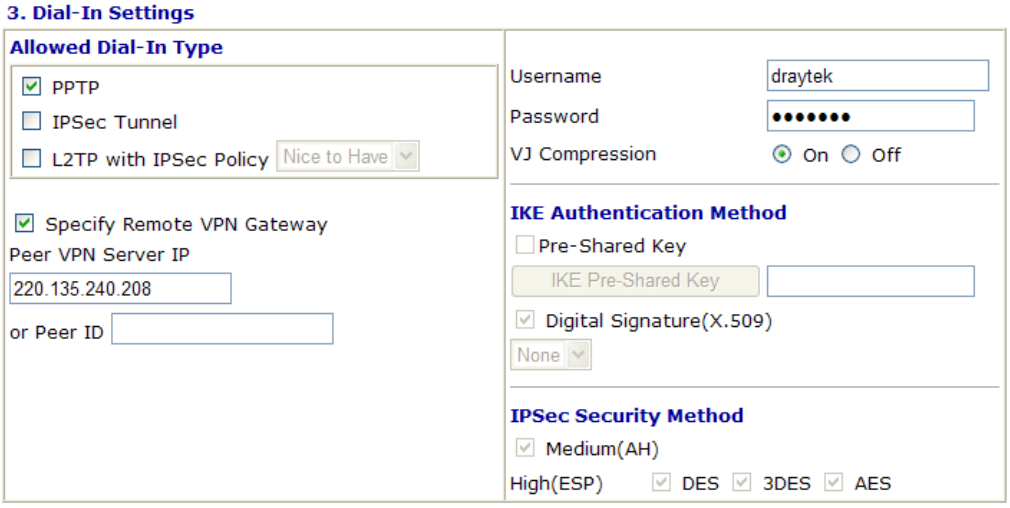


6. Set **Dial-In settings** to as shown below to allow Router A dial-in to build VPN connection.

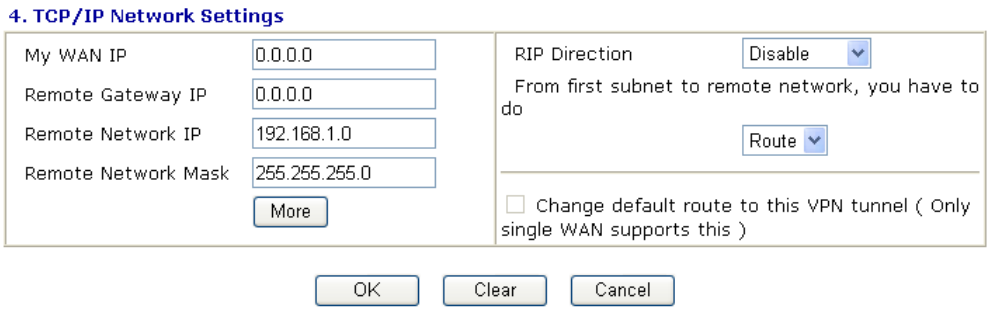
   If an ***IPSec-based*** service is selected, you may further specify the remote peer IP Address, IKE Authentication Method and IPSec Security Method for this Dial-In connection. Otherwise, it will apply the settings defined in **IPSec General Setup** above.



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

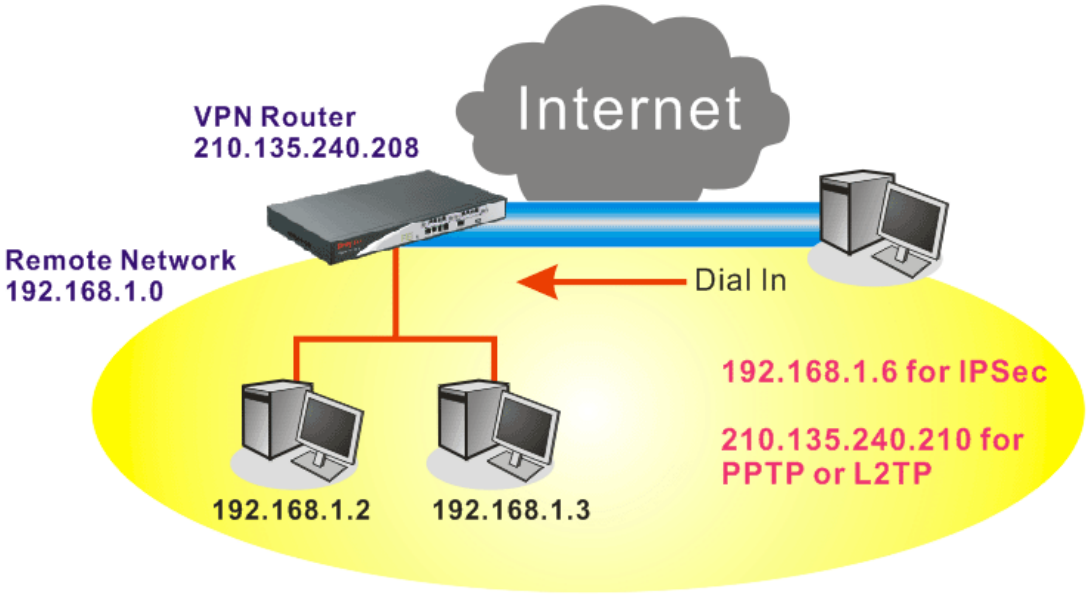


7. At last, set the remote network IP/subnet in **TCP/IP Network Settings** so that Router B can direct the packets destined to the remote network to Router A via the VPN connection.



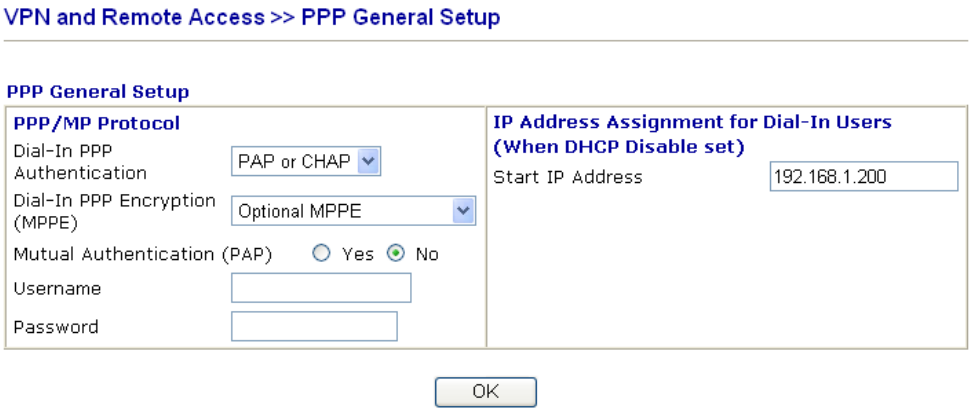
4.2 Create a Remote Dial-in User Connection Between the Teleworker and Headquarter

The other common case is that you, as a teleworker, may want to connect to the enterprise network securely. According to the network structure as shown in the below illustration, you may follow the steps to create a Remote User Profile and install Smart VPN Client on the remote host.

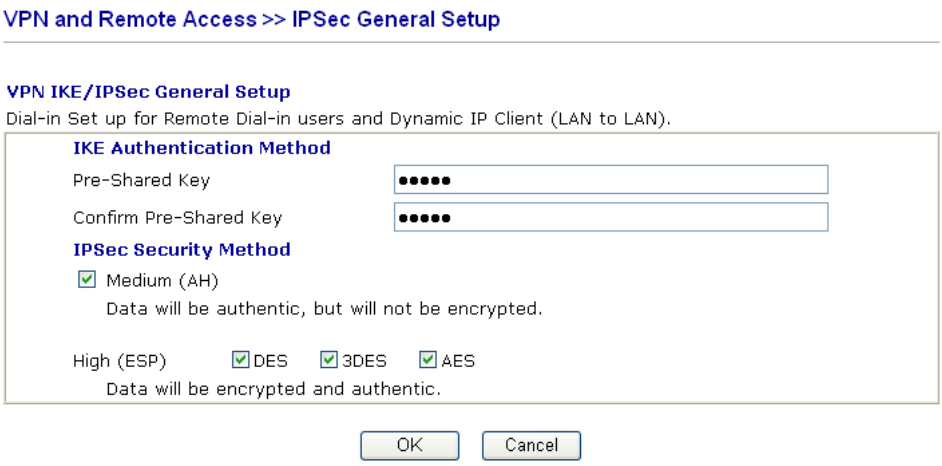


Settings in VPN Router in the enterprise office:

1. Go to **VPN and Remote Access** and select **Remote Access Control** to enable the necessary VPN service and click **OK**.
2. Then, for using PPP based services, such as PPTP, L2TP, you have to set general settings in **PPP General Setup**.

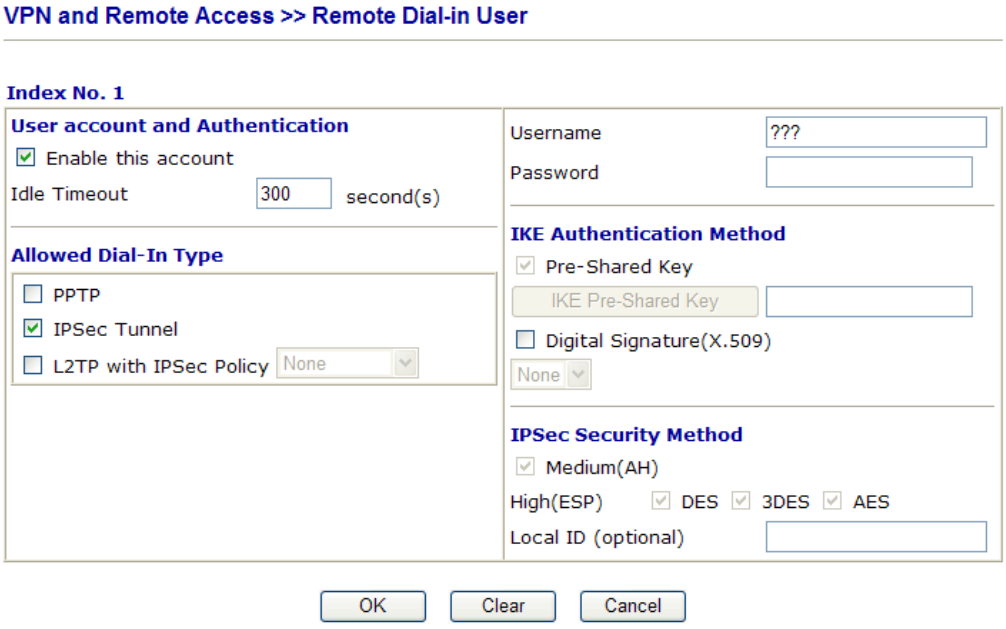


For using IPSec-based service, such as IPSec or L2TP with IPSec Policy, you have to set general settings in **IKE/IPSec General Setup**, such as the pre-shared key that both parties have known.

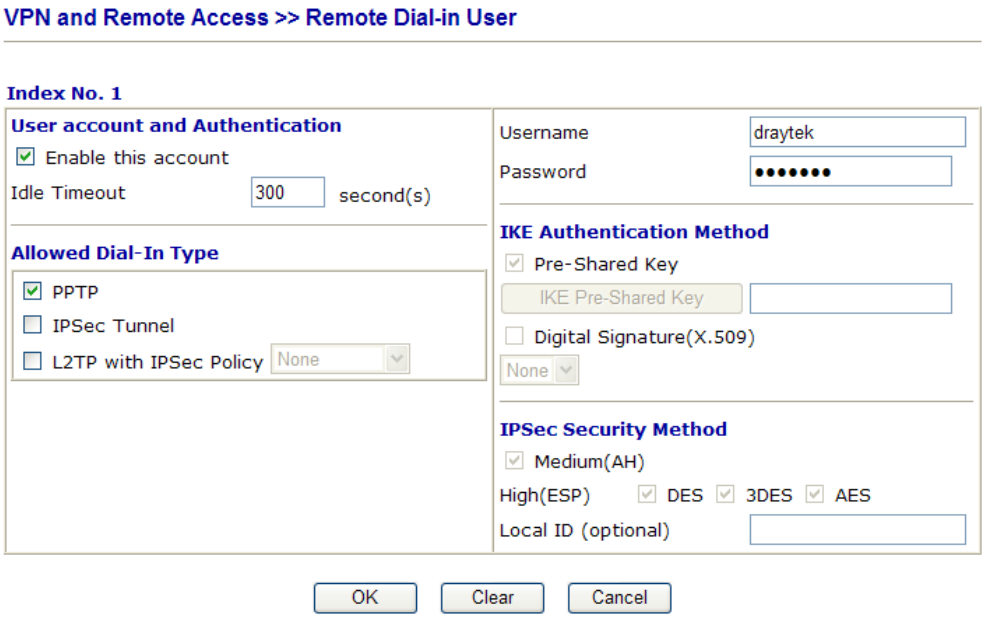


3. Go to **Remote Dial-In User**. Click on one index number to edit a profile.
4. Set **Dial-In** settings to as shown below to allow the remote user dial-in to build VPN connection.

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



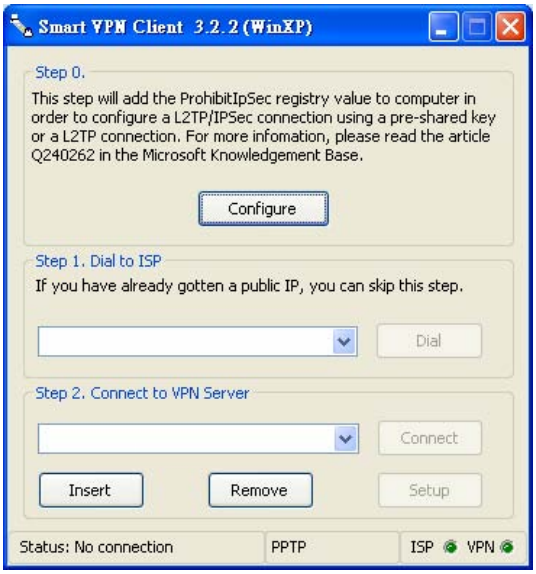
   If a ***PPP-based*** service is selected, you should further specify the remote peer IP Address, Username, Password, and VJ Compression for this Dial-In connection.



Settings in the remote host:

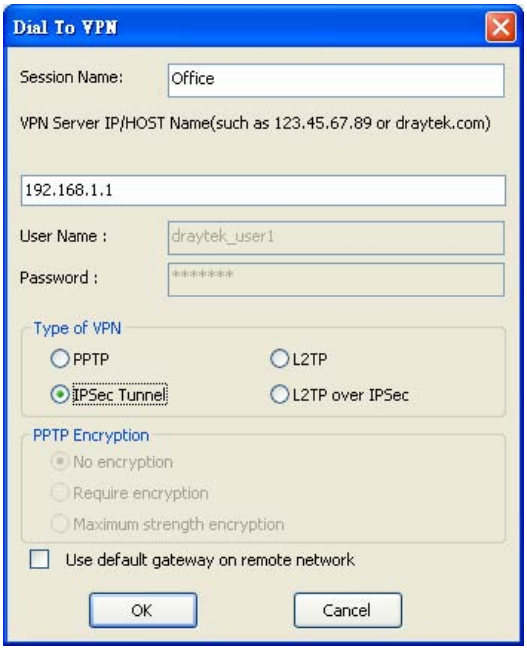
1. For Win98/ME, you may use "Dial-up Networking" to create the PPTP tunnel to Vigor router. For Win2000/XP, please use "Network and Dial-up connections" or “Smart VPN Client”, complimentary software to help you create PPTP, L2TP, and L2TP over IPSec tunnel. You can find it in CD-ROM in the package or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

2. After successful installation, for the first time user, you should click on the **Step 0. Configure** button. Reboot the host.

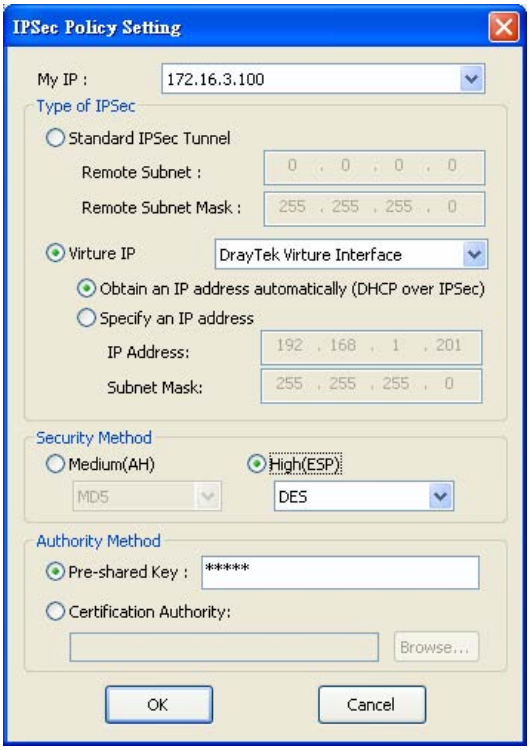


3. In **Step 2. Connect to VPN Server**, click **Insert** button to add a new entry.

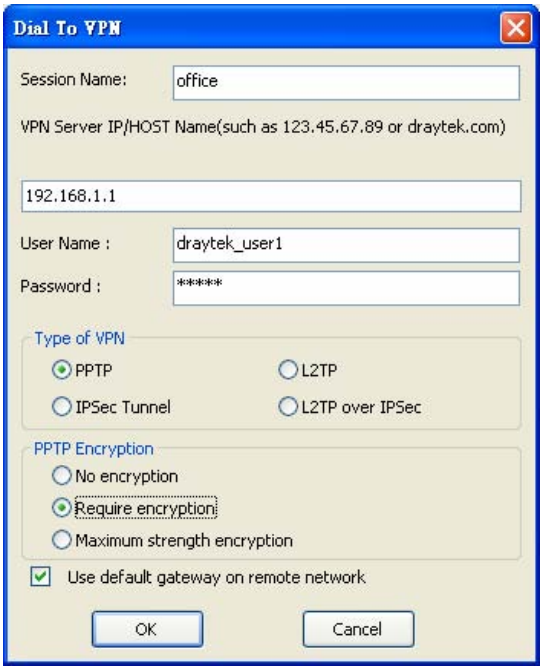
   If an IPSec-based service is selected as shown below,



You may further specify the method you use to get IP, the security method, and authentication method. If the Pre-Shared Key is selected, it should be consistent with the one set in VPN router.



If a PPP-based service is selected, you should further specify the remote VPN server IP address, Username, Password, and encryption method. The User Name and Password should be consistent with the one set up in the VPN router. To use default gateway on remote network means that all the packets of remote host will be directed to VPN server then forwarded to Internet. This will make the remote host seem to be working in the enterprise network.

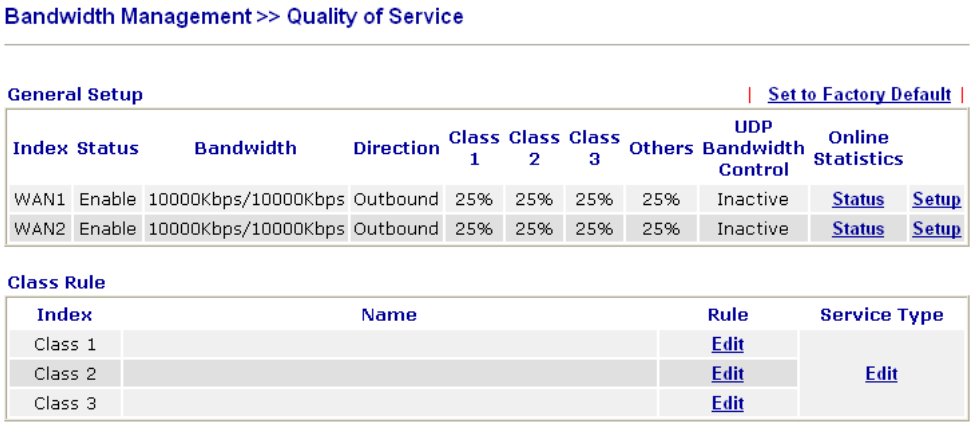


4. Click **Connect** button to build connection. When the connection is successful, you will find a green light on the right down corner.

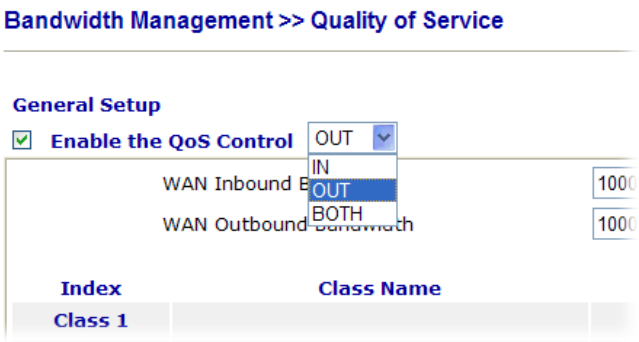
4.3 QoS Setting Example

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

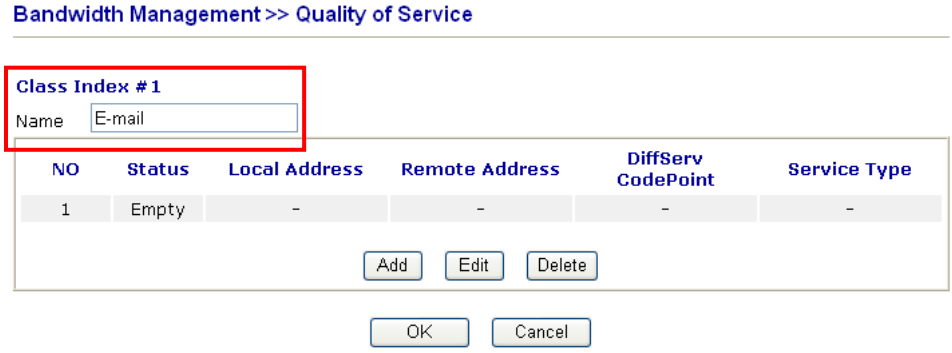
1. Go to **Bandwidth Management>>Quality of Service.**



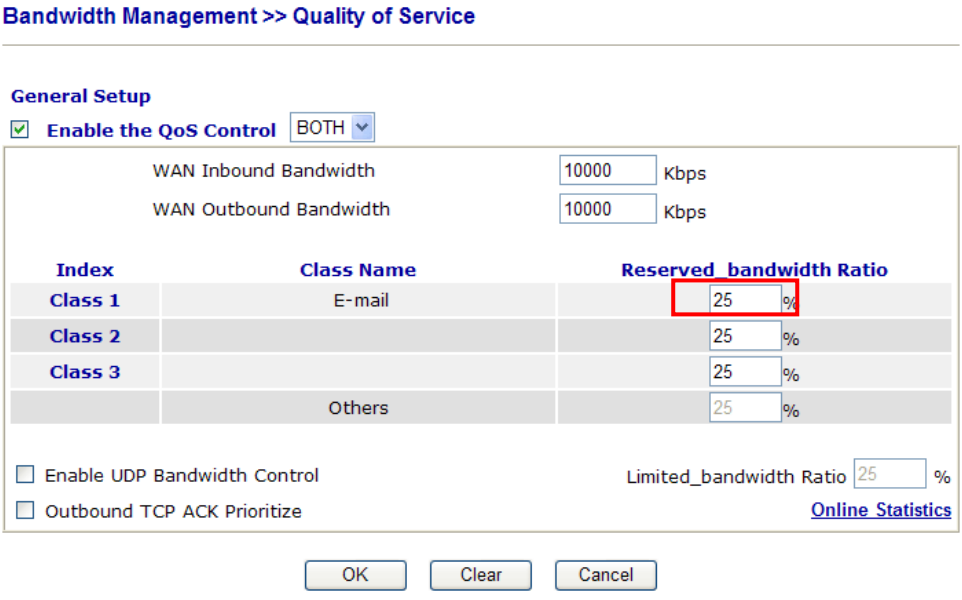
2. Click **Setup** link of WAN 1. Make sure the QoS Control on the left corner is checked. And select **BOTH** in **Direction**.



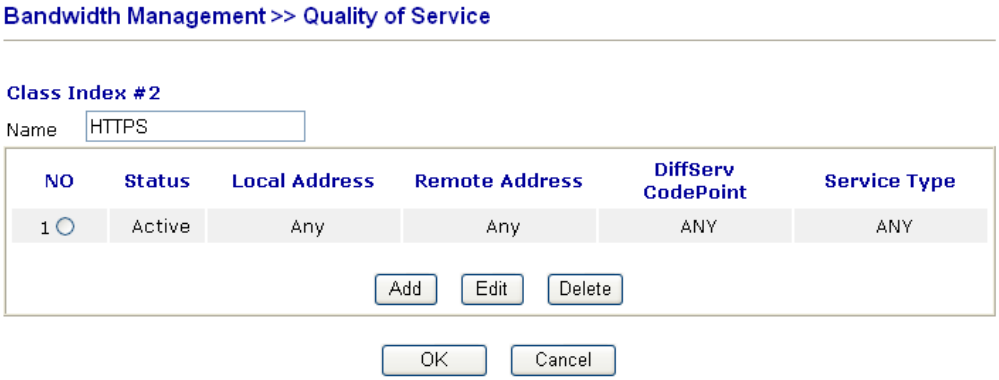
3. Return to previous page. Enter the Name of Index Class 1 by clicking **Edit** link. Type the name "**E-mail**" for Class 1.



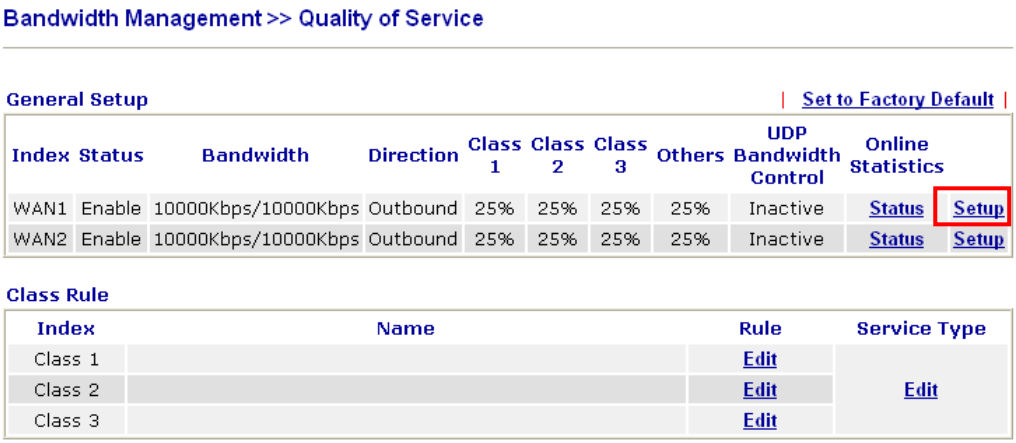
4. For this index, the user will set reserved bandwidth (e.g., 25%) for **E-mail** using protocol POP3 and SMTP.



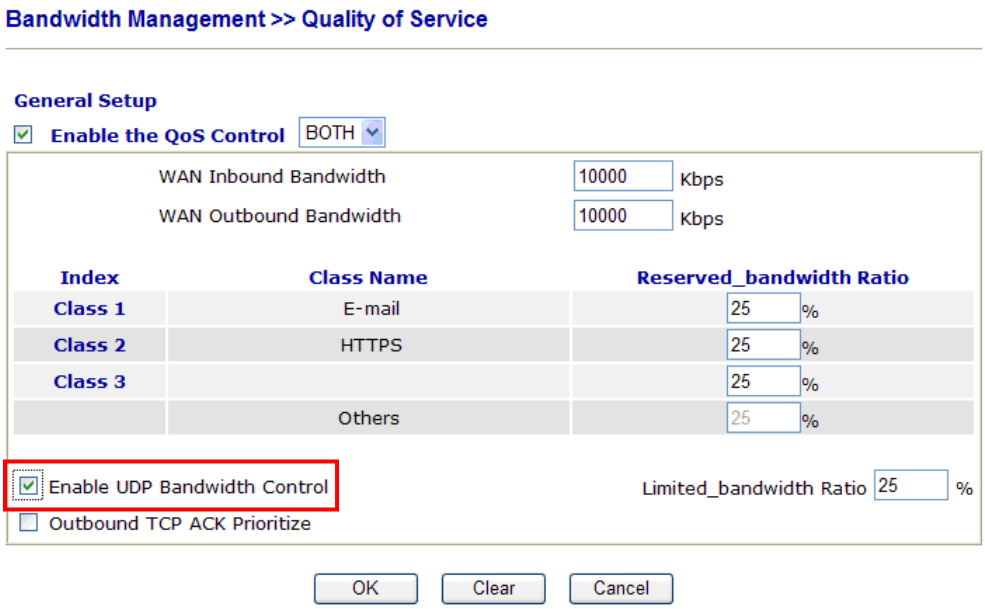
5. Return to previous page. Enter the Name of Index Class 2 by clicking **Edit** link. In this index, the user will set reserved bandwidth for **HTTPS**. And click **OK**.



6. Click **Setup** link for WAN1.

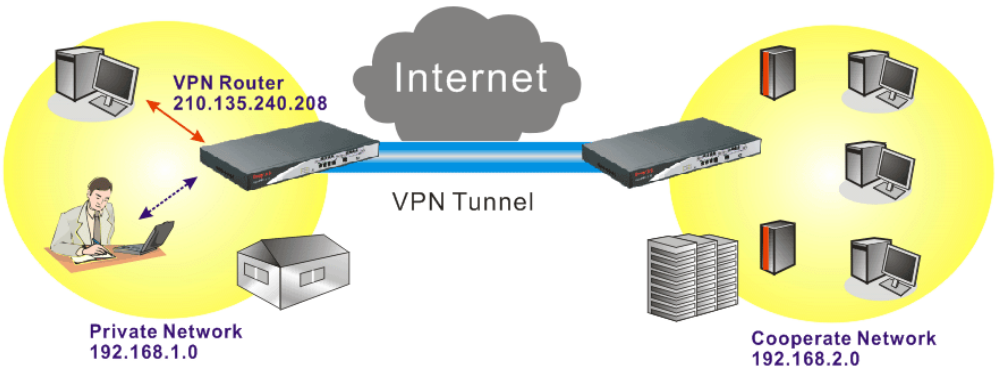


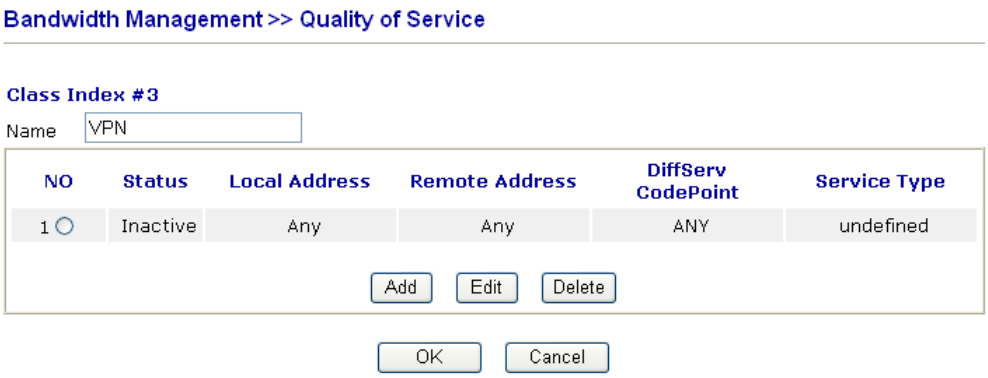
7. Check **Enable UDP Bandwidth Control** on the bottom to prevent enormous UDP traffic of VoIP influent other application. Click **OK**.



8. If the worker has connected to the headquarter using host to host VPN tunnel. (Please refer to Chapter 3 VPN for detail instruction), he may set up an index for it. Enter the

Class Name of Index 3. In this index, he will set reserved bandwidth for 1 VPN tunnel.



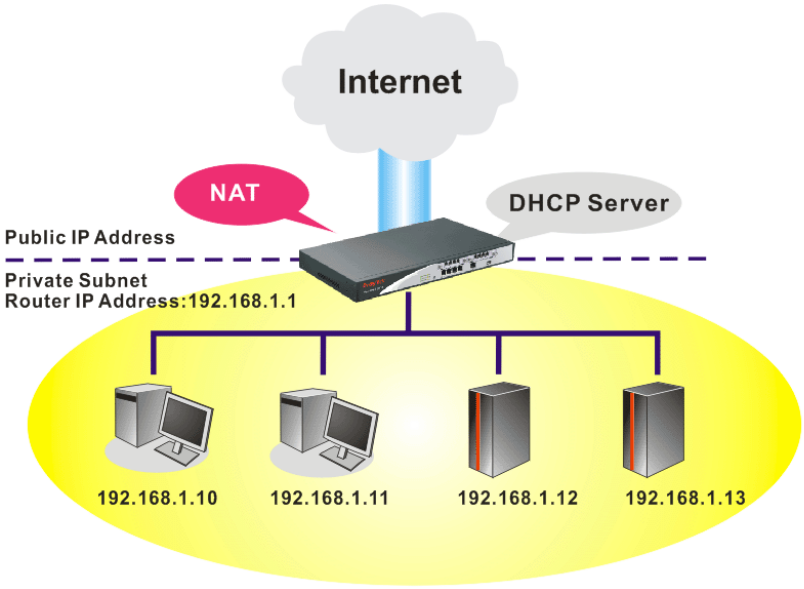


9. Click **Edit** to open the following window. Check the **ACT** box, first.

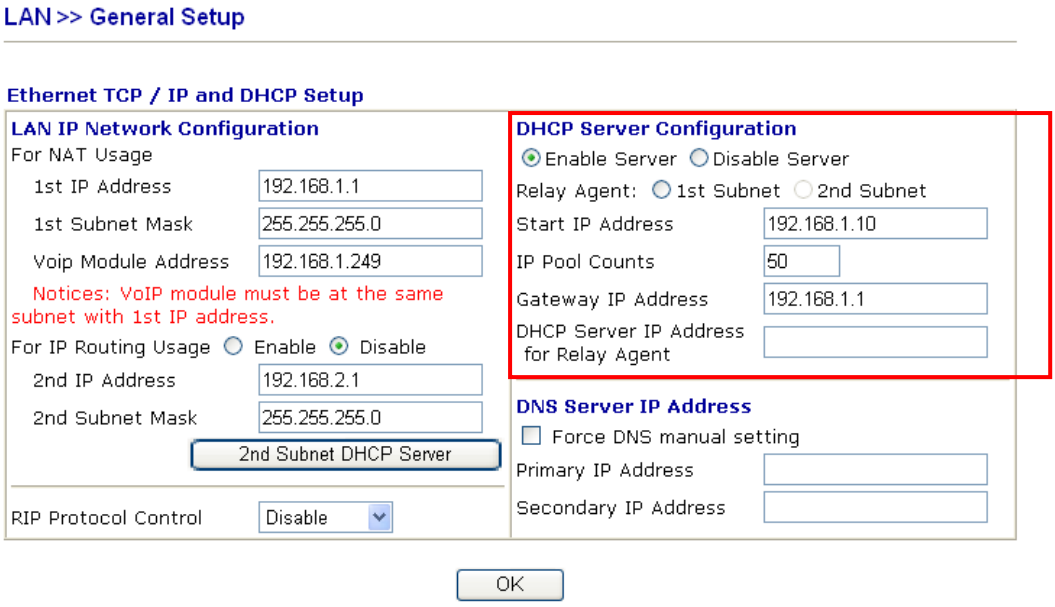
10. Then click **Edit** of **Local Address** to set a worker's subnet address. Click **Edit** of **Remote Address** to set headquarter's IP address. Leave other fields and click **OK**.

4.4 LAN – Created by Using NAT

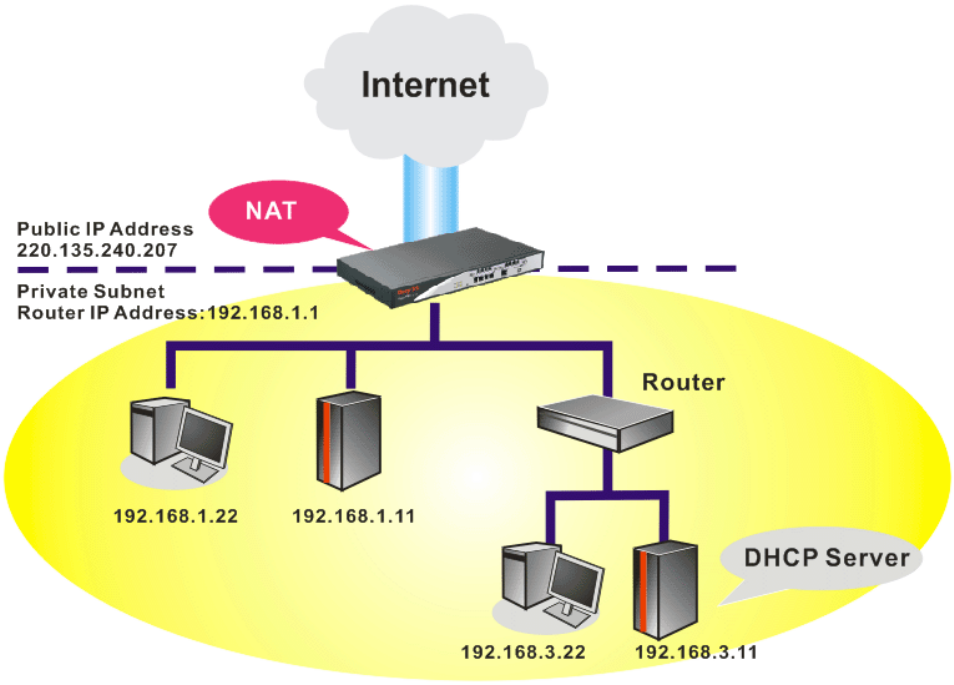
An example of default setting and the corresponding deployment are shown below. The default Vigor router private IP address/Subnet Mask is 192.168.1.1/255.255.255.0. The built-in DHCP server is enabled so it assigns every local NATed host an IP address of 192.168.1.x starting from 192.168.1.10.



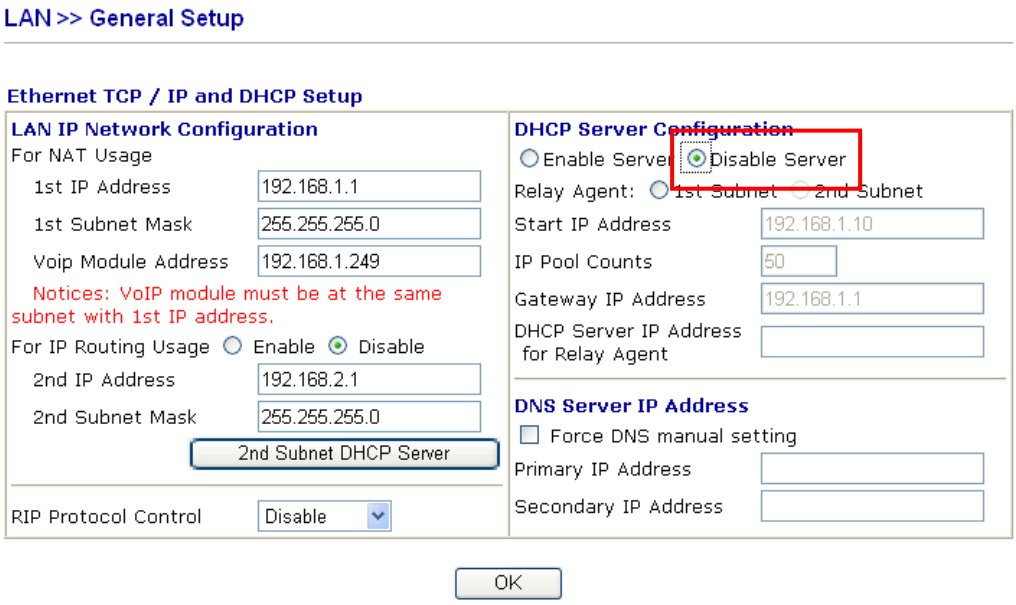
You can just set the settings wrapped inside the red rectangles to fit the request of NAT usage.



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



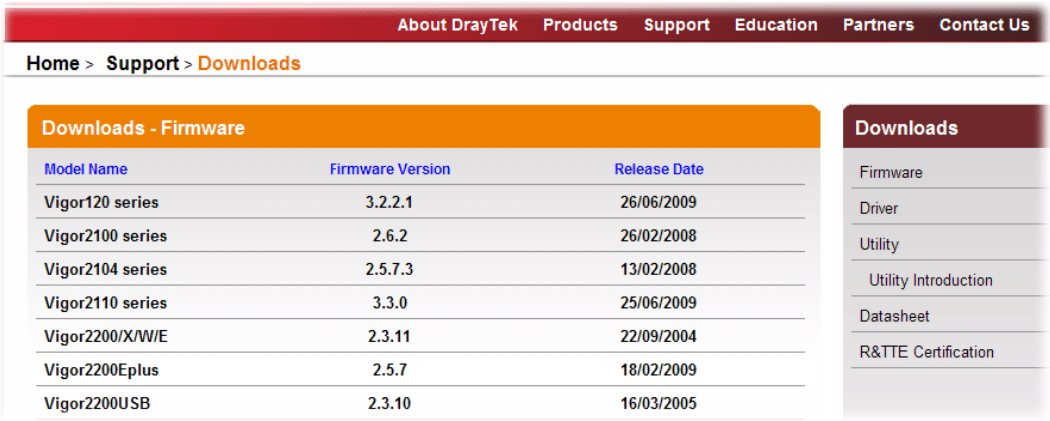
You can just set the settings wrapped inside the red rectangles to fit the request of NAT usage.



4.5 Upgrade Firmware for VigorIPPBX 3510

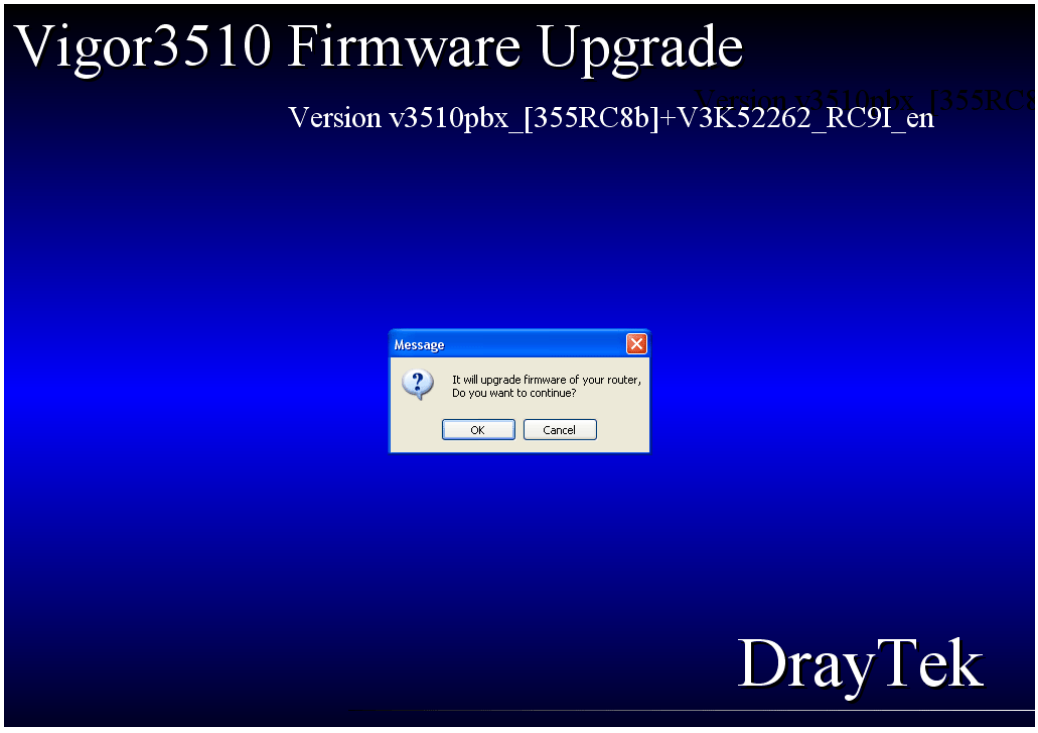
Please do the following:

1. Go to **www.draytek.com.**
2. Access into **Support >> Downloads**. Please click the model name of VigorIPPBX 3510 and click on it to download the firmware execution file.

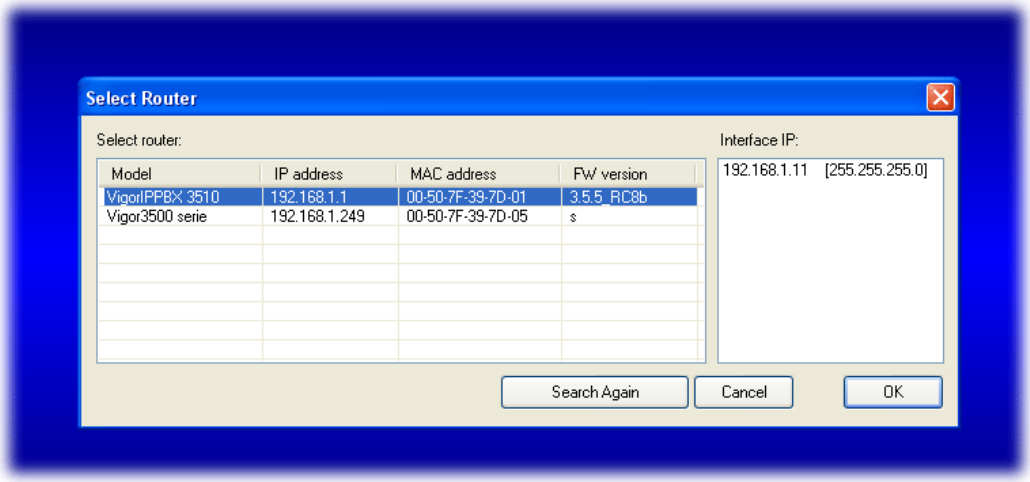


3. Locate the **AutoFwUp_VXXX** file that you downloaded from the website.

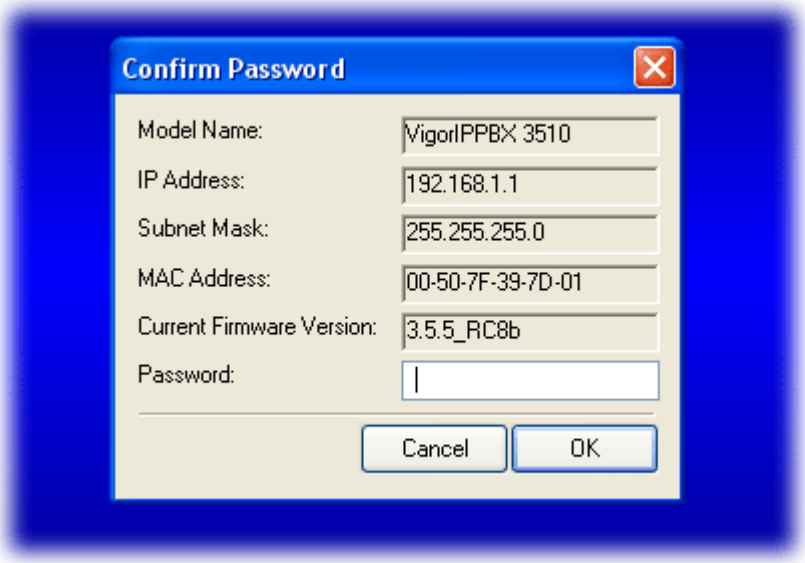
4. Double-click the execution file of **AutoFwUp_VXXX** to run the program. The following screen will appear. Click **OK**.



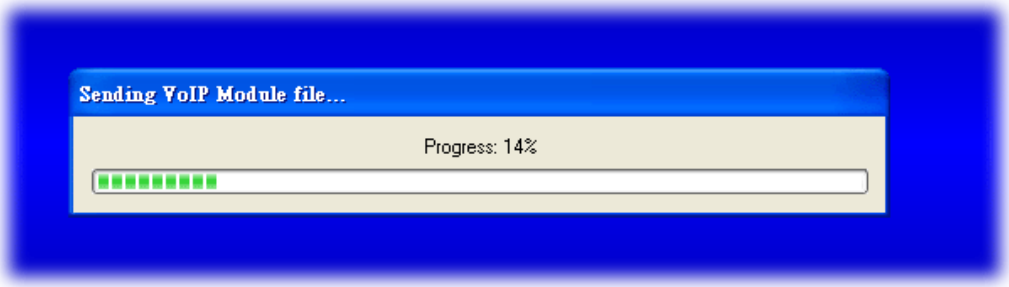
5. In the dialog of **Select Router**, choose VigorIPPBX 3510 and click **OK**.



6. In the **Confirm Password** dialog, please type the password that you use to login Vigor router and click **OK**. If there is no password needed, click **OK** directly.



7. Next, the system will start to upgrade the firmware for the router automatically.



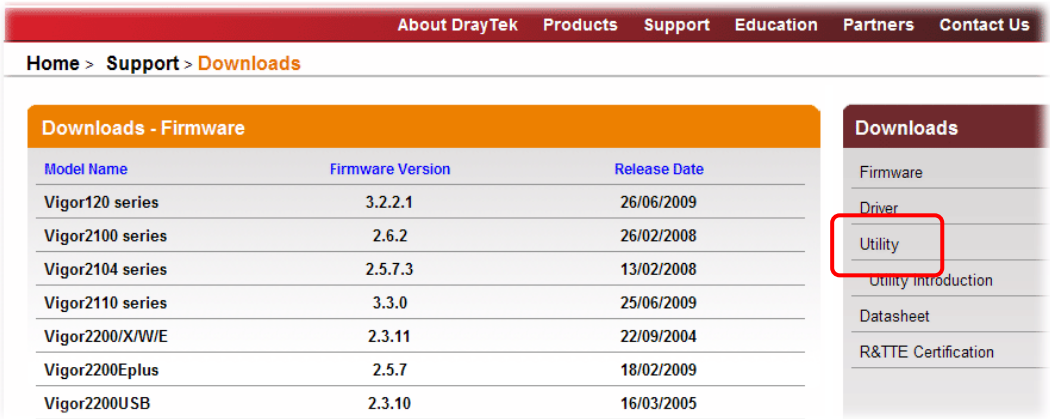
8. Please wait for several minutes. When the following dialog appear, please click OK.

9. Now, the firmware upgrade has been finished.

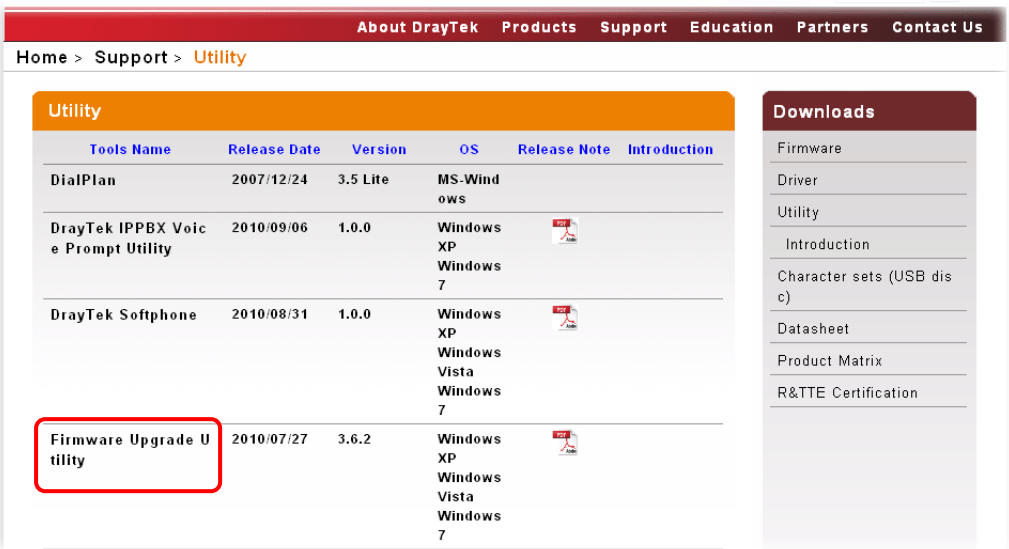
4.6 Backup and Restore Settings for VigorIPPBX 3510

4.6.1 Backup the Configuration Settings

1. Go to **www.draytek.com.**
2. Access into **Support >> Downloads**. Please find out **Utility** menu and click it. Search the model you have (i.e., VigorIPPBX 3510) and click on it to download the newly update firmware for your router.

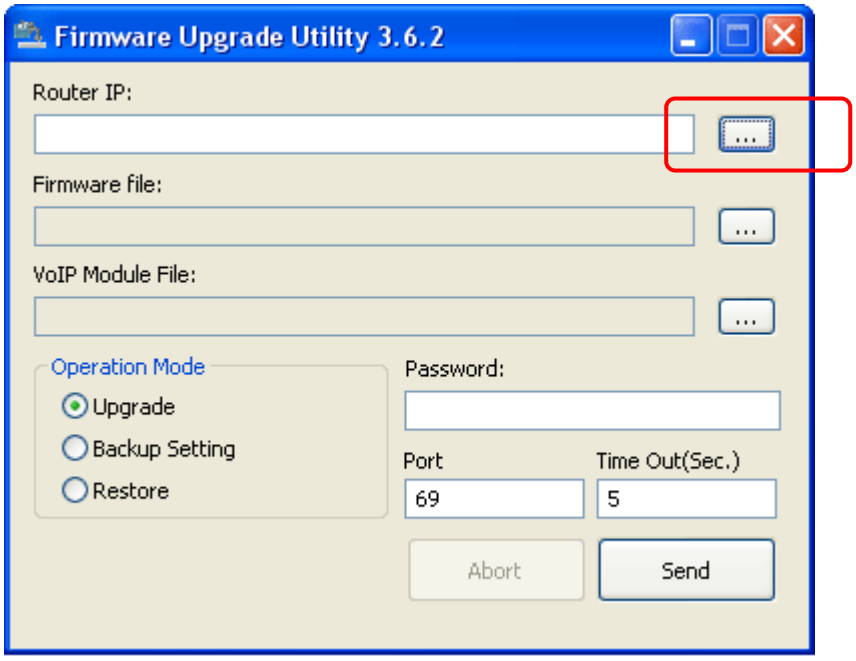


3. Click on the link of **Firmware Upgrade Utility** to download the tool. After downloading the file, please decompressed it onto your host.

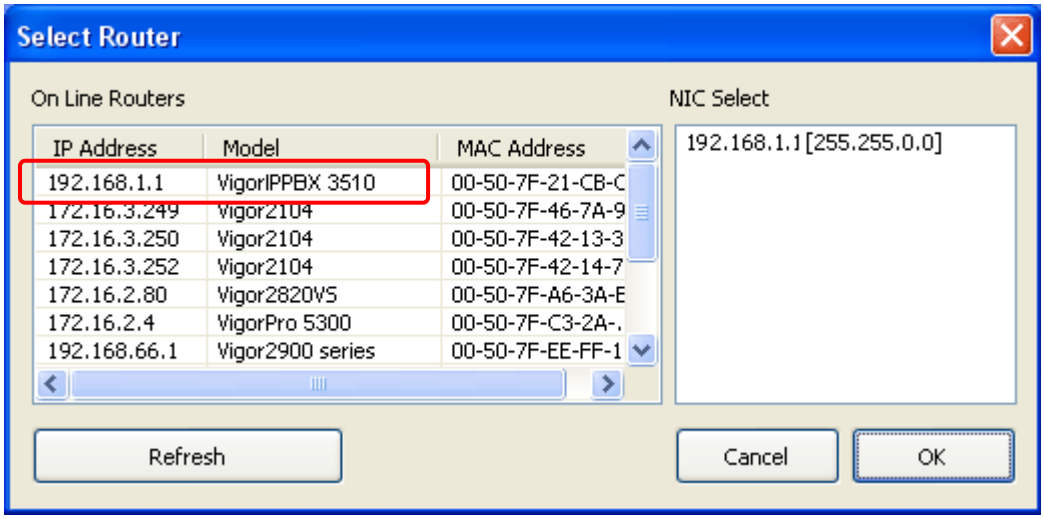


4. Double click on the **FrmUpg** icon.

5. The Firmware Upgrade Utility will appear as follows:

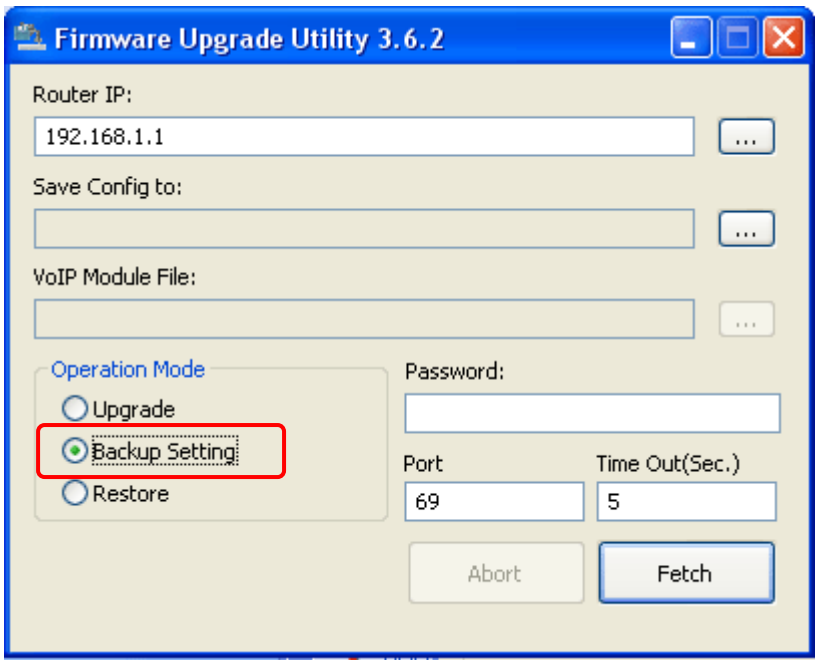


6. Click the browse ... button of **Router IP** to search the IP address (e.g., 192.168.1.1) of VigorIPPBX 3510. Click **OK**.

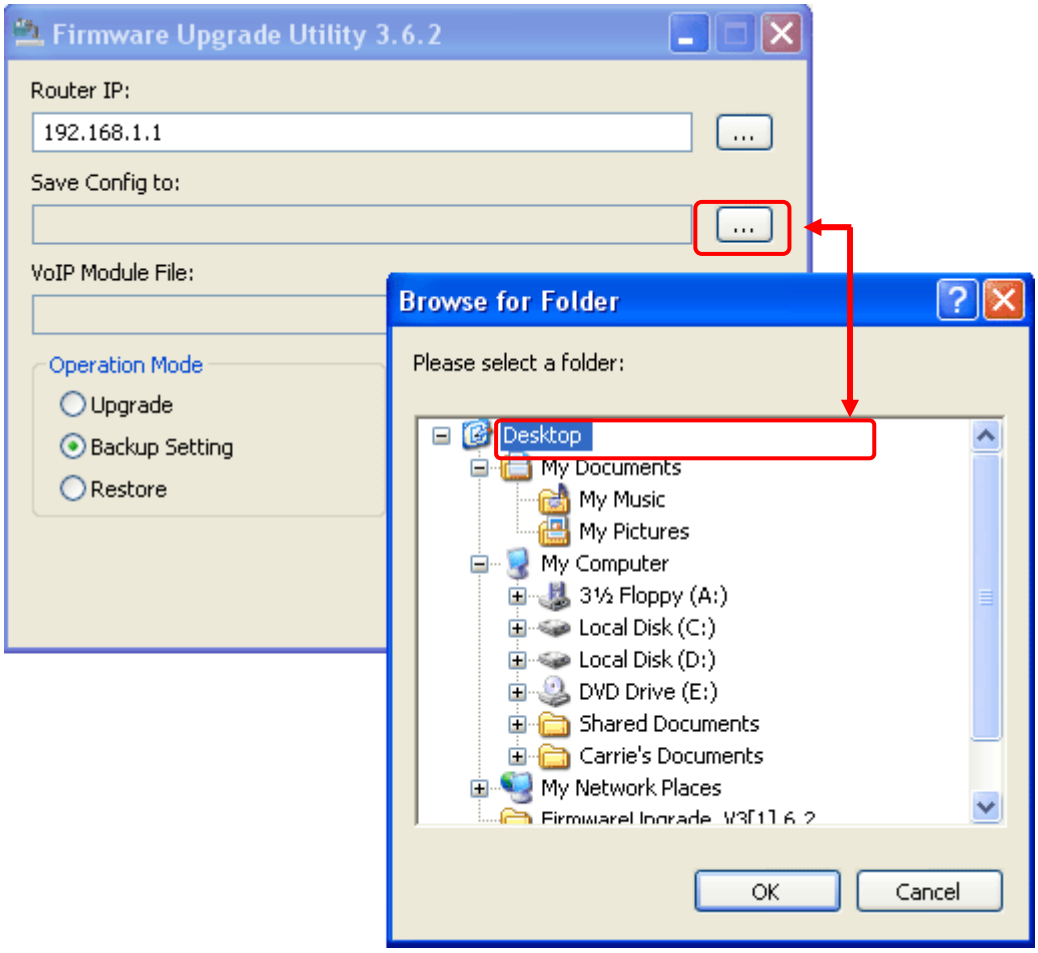


Note: Do not type the IP address in the field of **Router IP** directly.

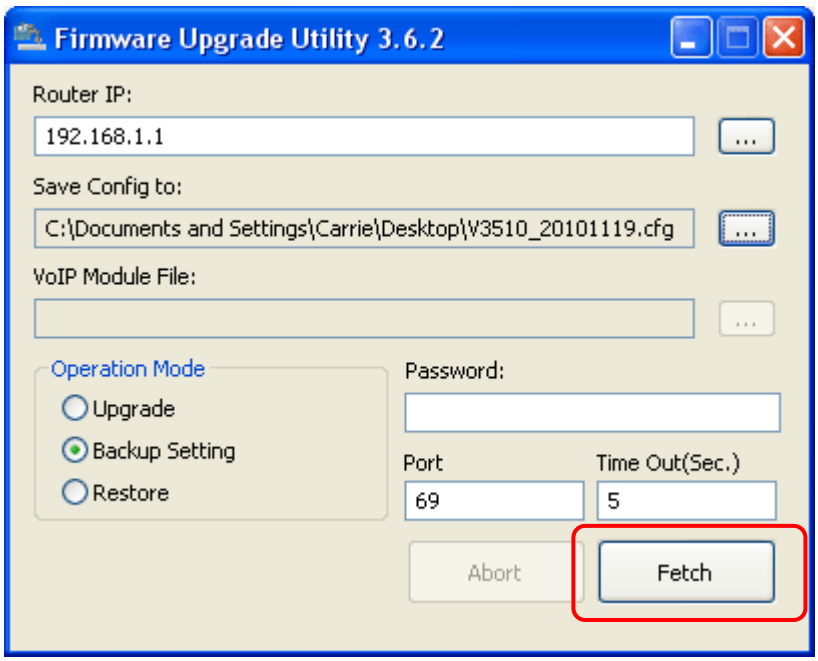
7. Choose **Backup Setting** as the **Operation Mode**.



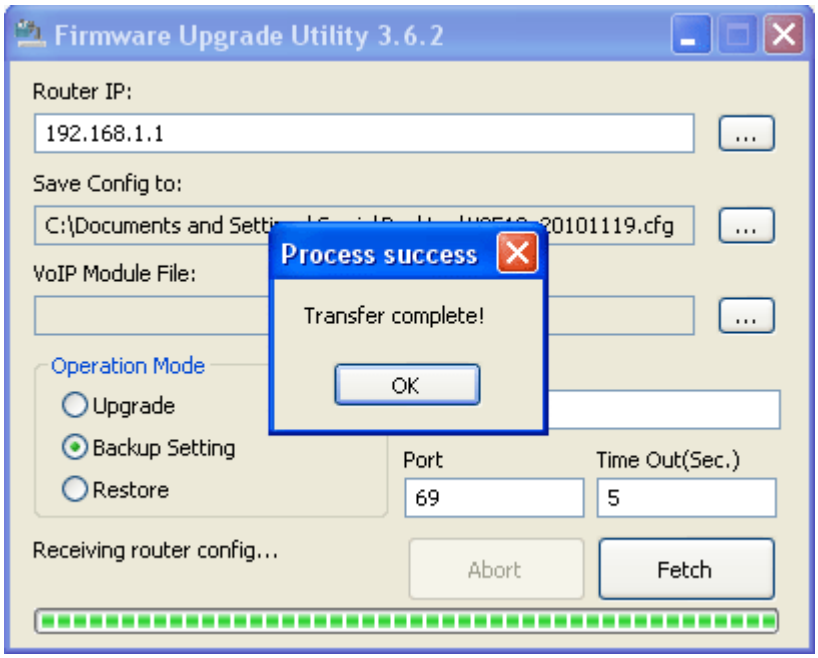
8. Next, click the browse button of **Save Config to** for specifying the place that the configuration file stored. Click **OK**.



9. Next, click **Fetch.**



10. When it is finished, the following dialog will appear.

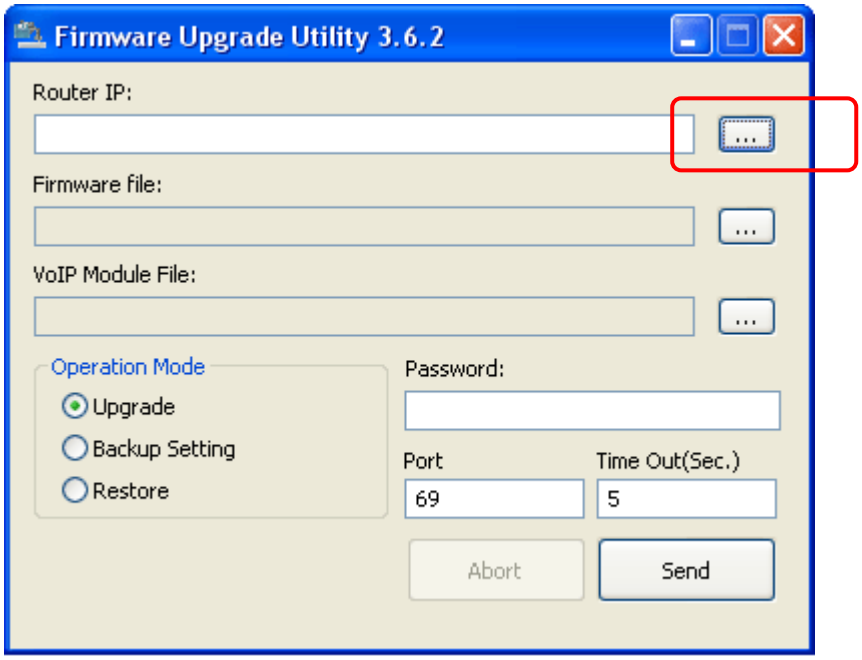


11. Now, the configuration files (with the file name like V3510_XXXX, V35VoipMoudule_XXXX) will be stored in your host.

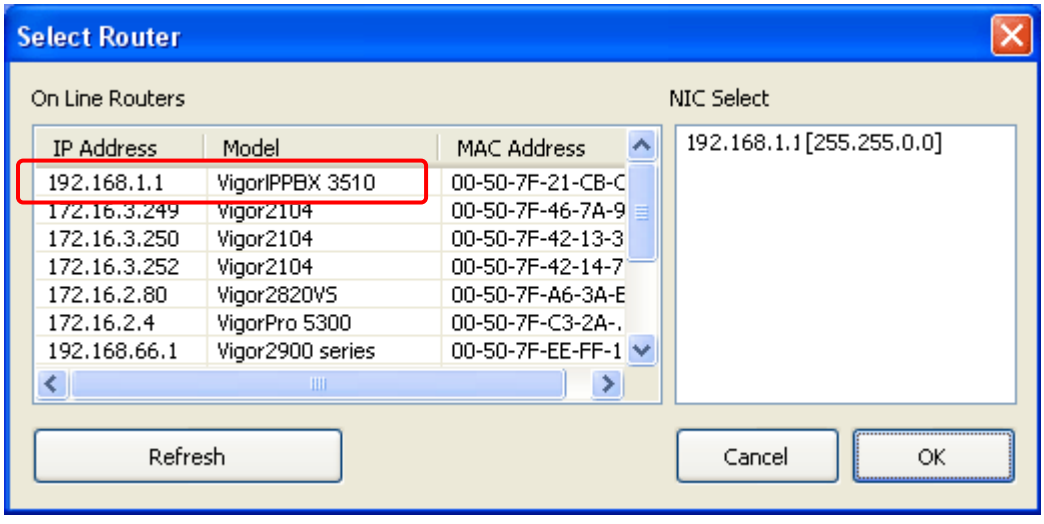
4.6.2 Restore the Configuration Settings

1. Double click on the **FrmUpg** icon.

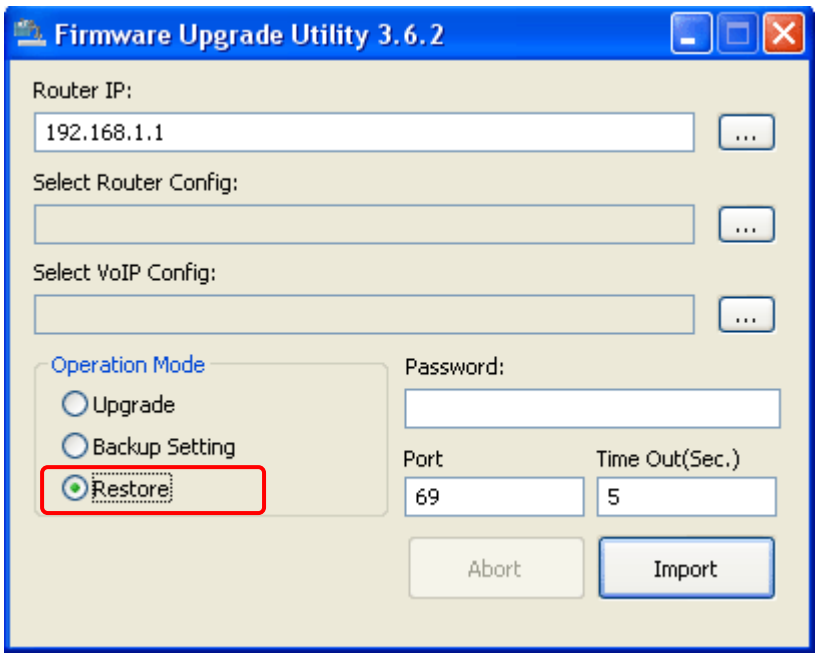
2. The Firmware Upgrade Utility will appear as follows:



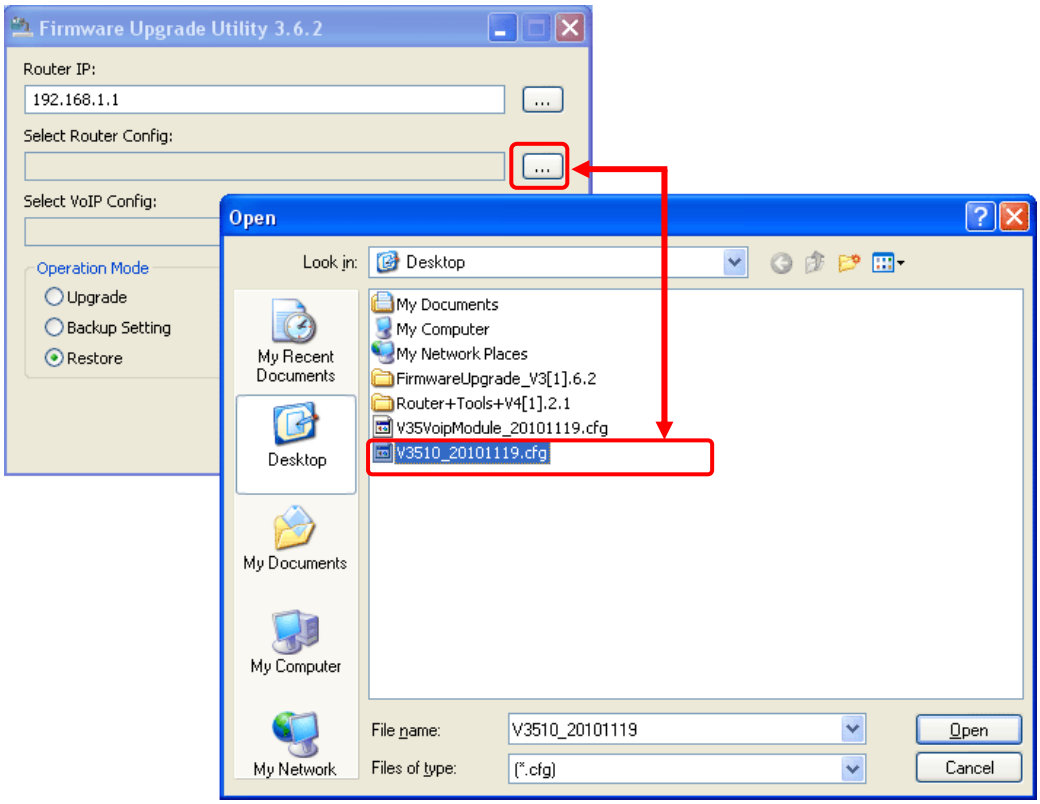
3. Click the browse ... button of **Router IP** to search the IP address (e.g., 192.168.1.1) of VigorIPPBX 3510. Click **OK**.



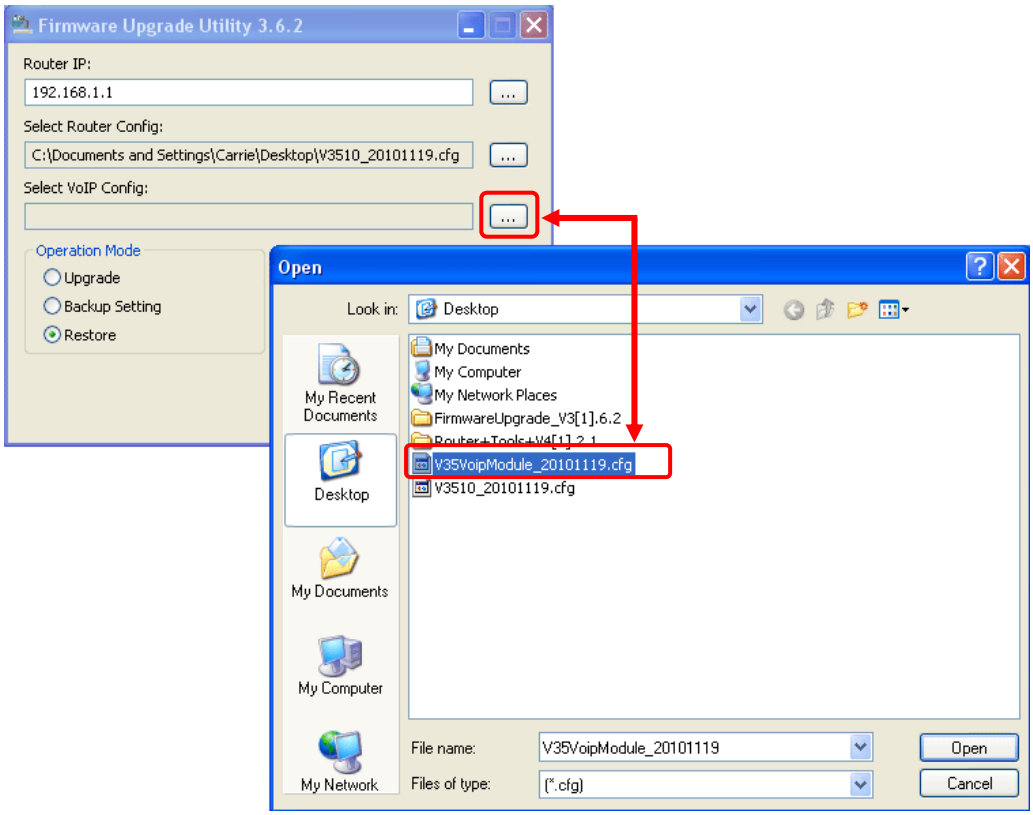
4. Choose **Restore** as the **Operation Mode**.



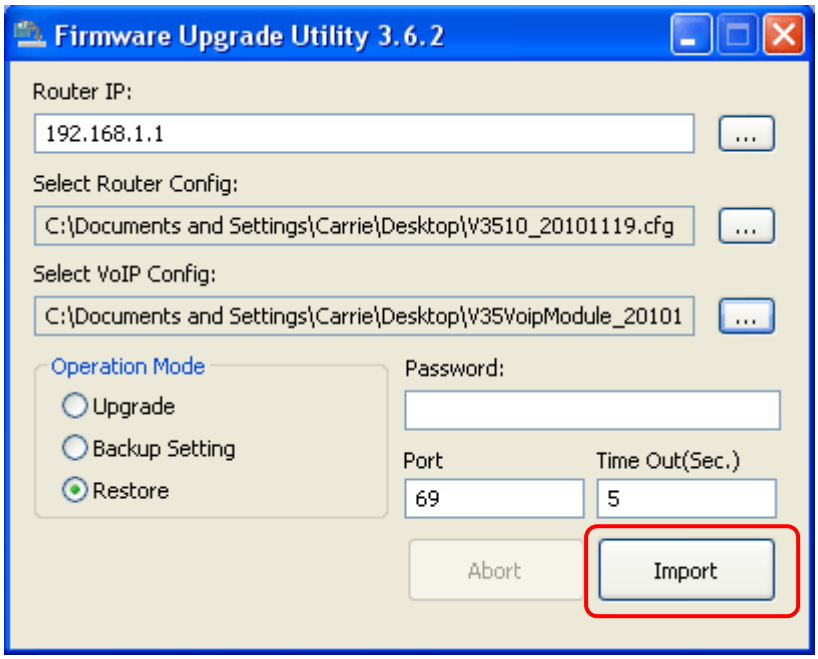
5. Click the browse ... button of **Select Router Config** to locate the configuration file.



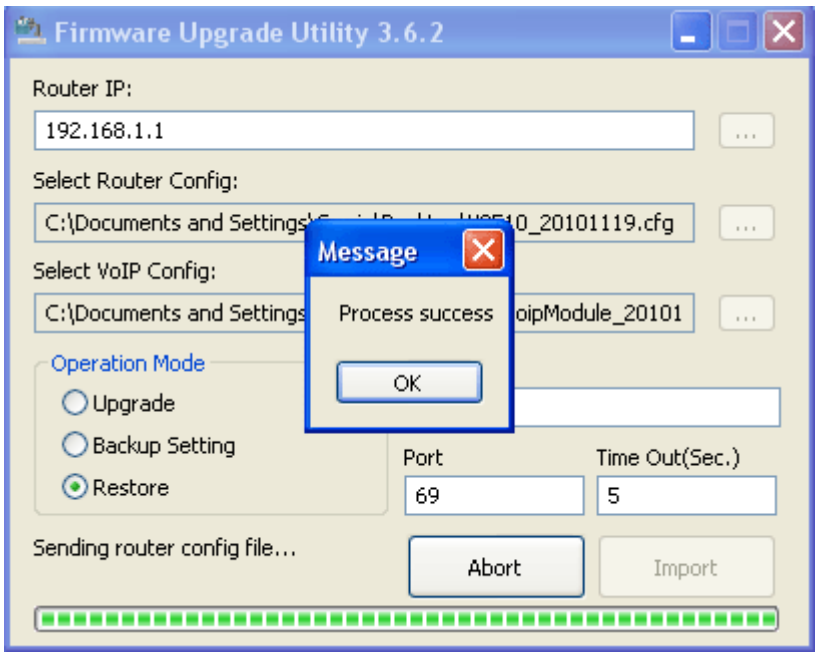
6. Next, click the browse button of **Select VoIP Config** to locate the module file for the router. Choose the file of V3K52262_XXXXXXX and click **Open**.



7. Next, click **Import**.

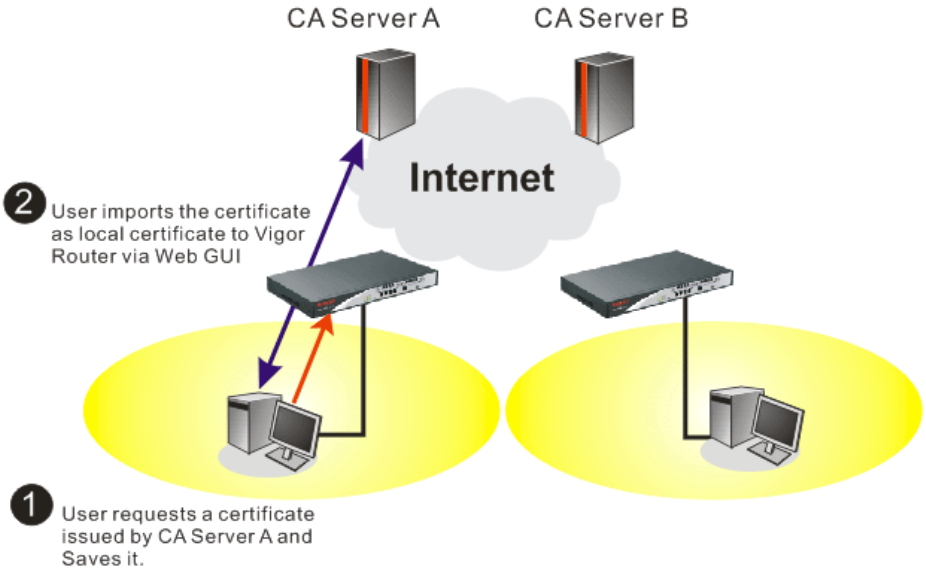


8. When it is finished, the following dialog will appear.



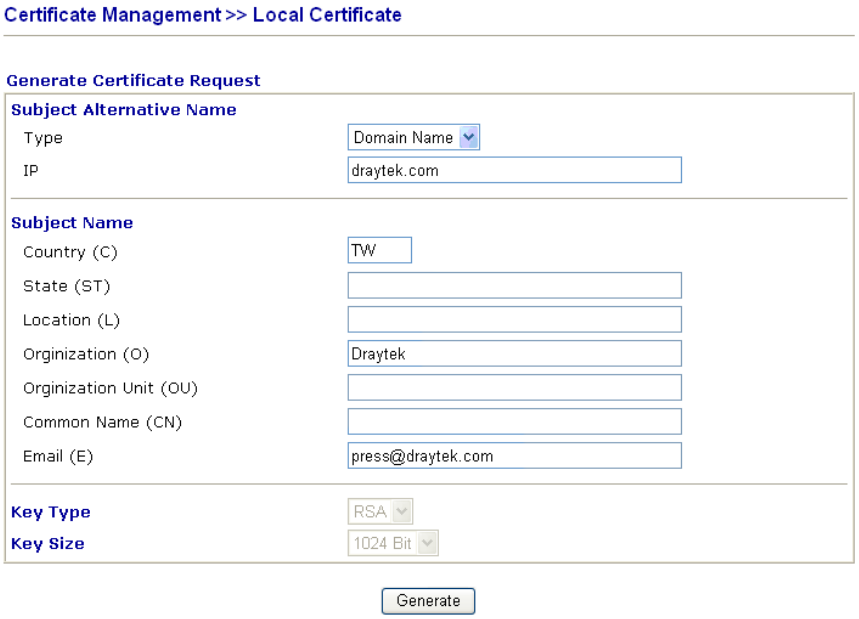
9. Now, the configuration files have been restored to your router.

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

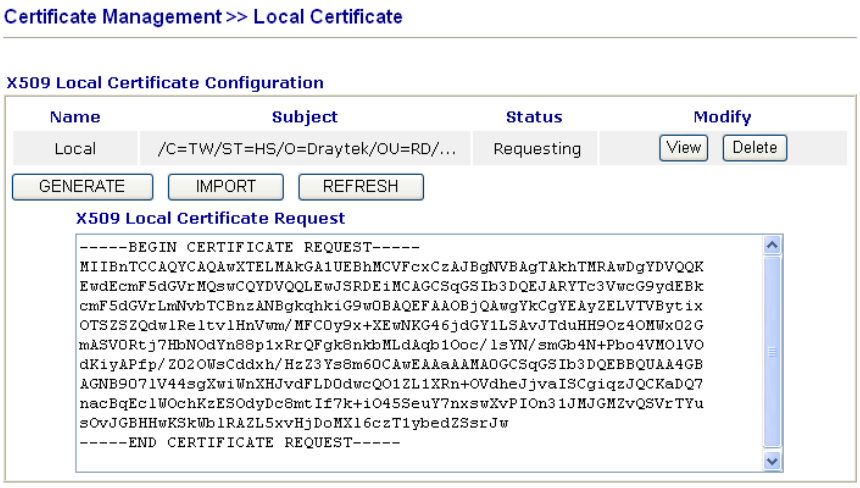


1. Go to **Certificate Management** and choose **Local Certificate**.

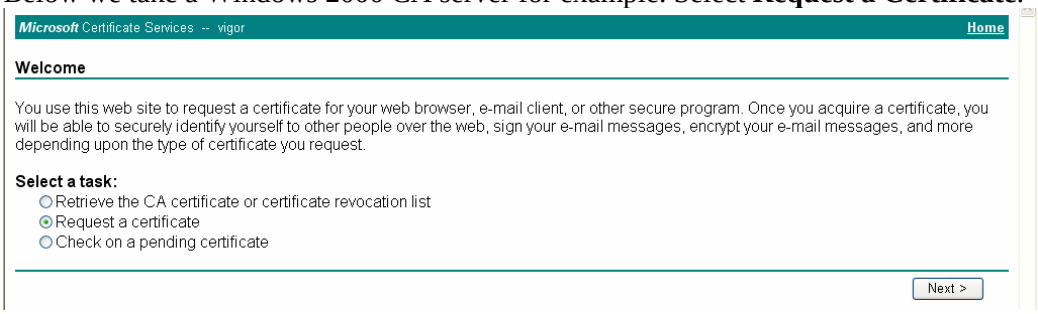
2. You can click **GENERATE** button to start to edit a certificate request. Enter the information in the certificate request.



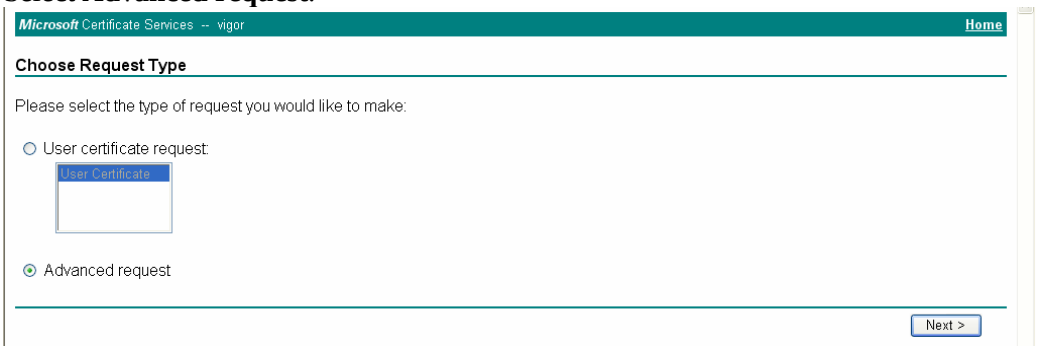
3. Copy and save the X509 Local Certificate Requet as a text file and save it for later use.



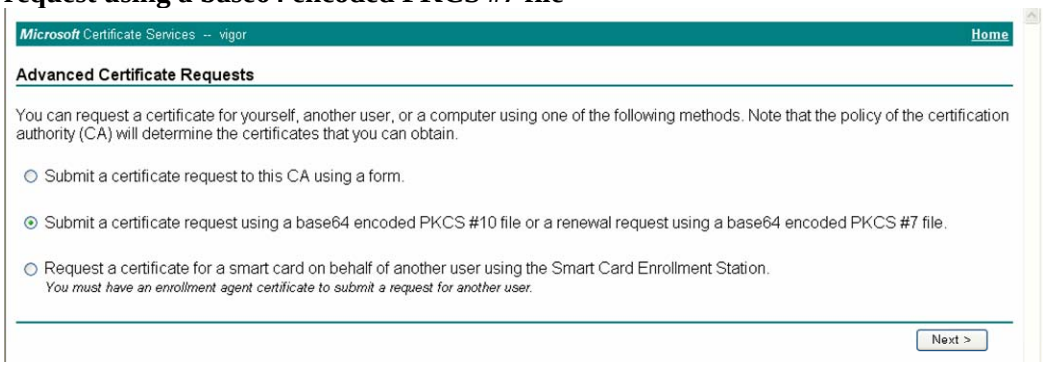
4. Connect to CA server via web browser. Follow the instruction to submit the request. Below we take a Windows 2000 CA server for example. Select **Request a Certificate**.



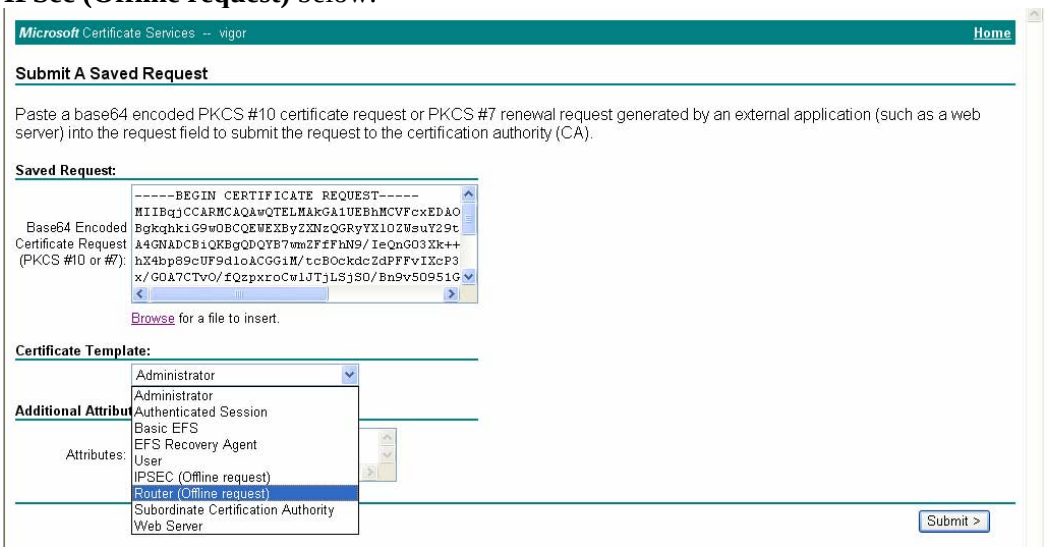
Select **Advanced request**.



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

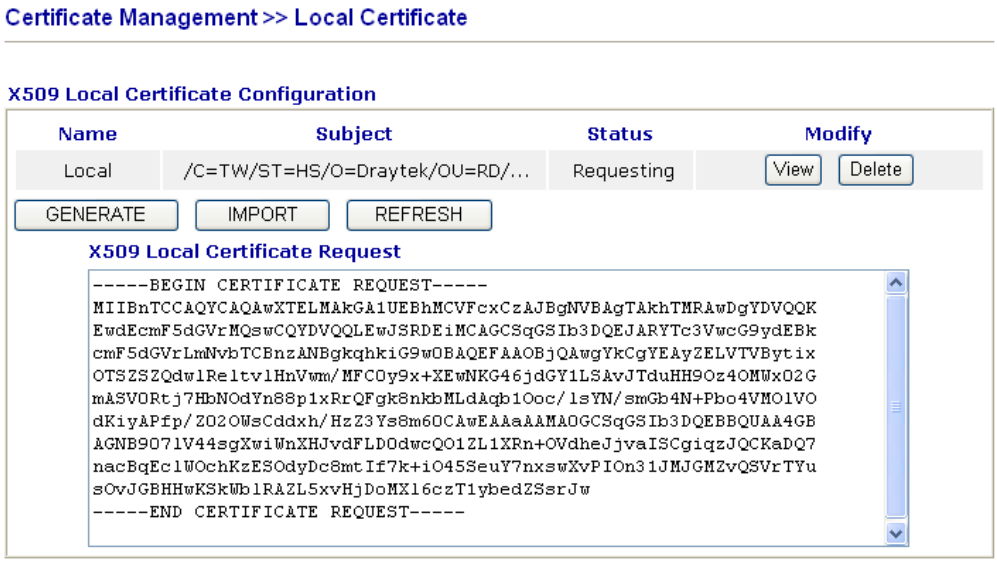


Import the X509 Local Certificate Request text file. Select **Router (Offline request)** or **IPSec (Offline request)** below.



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

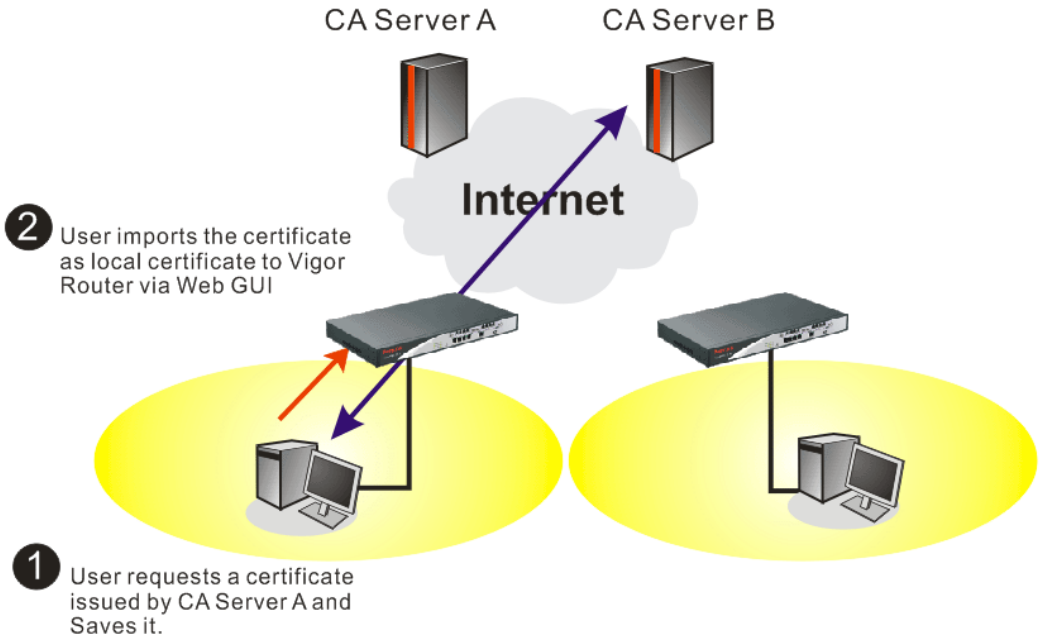
5. Back to Vigor router, go to **Local Certificate**. Click **IMPORT** button and browse the file to import the certificate (.cer file) into Vigor router. When finished, click refresh and you will find the below window showing "------END CERTIFICATE REQUEST------"



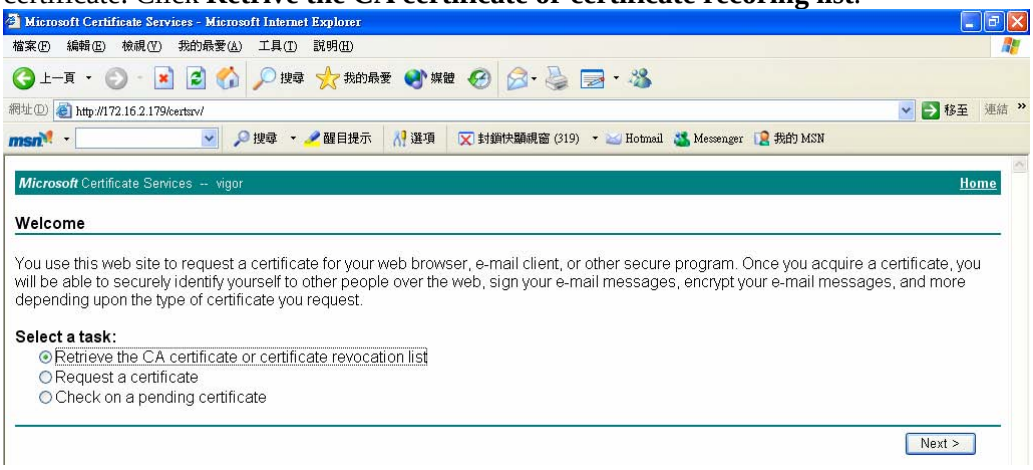
6. You may review the detail information of the certificate by clicking **View** button.

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

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

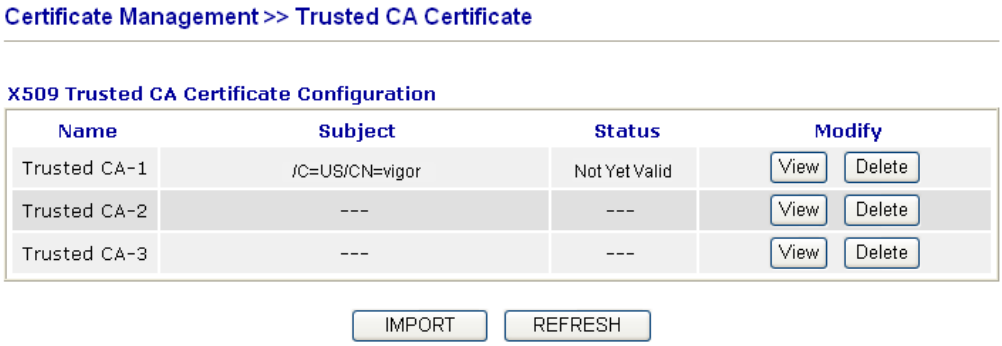


1. Use web browser connecting to the CA server that you would like to retrieve its CA certificate. Click **Retrive the CA certificate or certificate recoring list**.

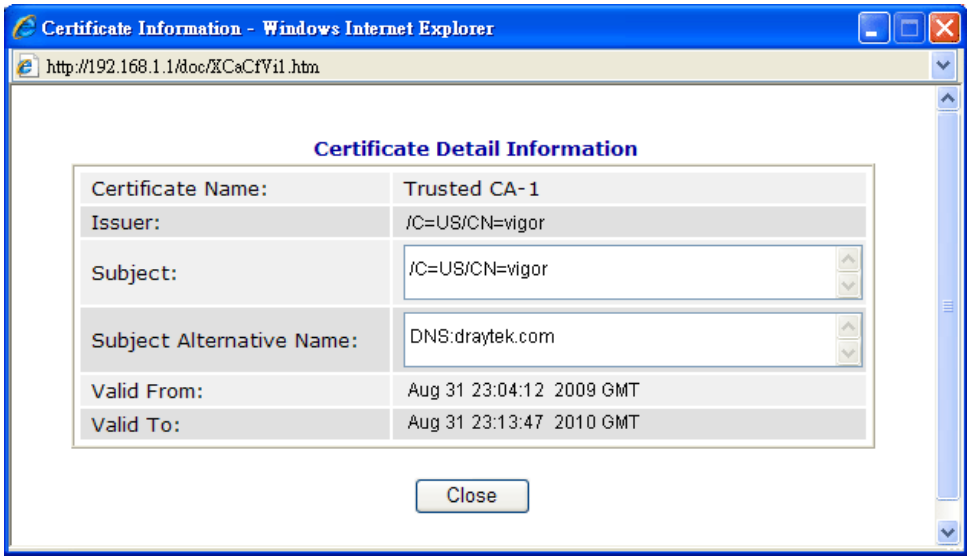


2. In **Choose file to download**, click CA Certificate **Current** and **Base 64 encoded,** and **Download CA certificate** to save the .cer. file.

3. Back to Vigor router, go to **Trusted CA Certificate**. Click **IMPORT** button and browse the file to import the certificate (.cer file) into Vigor router. When finished, click refresh and you will find the below illustration.



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



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

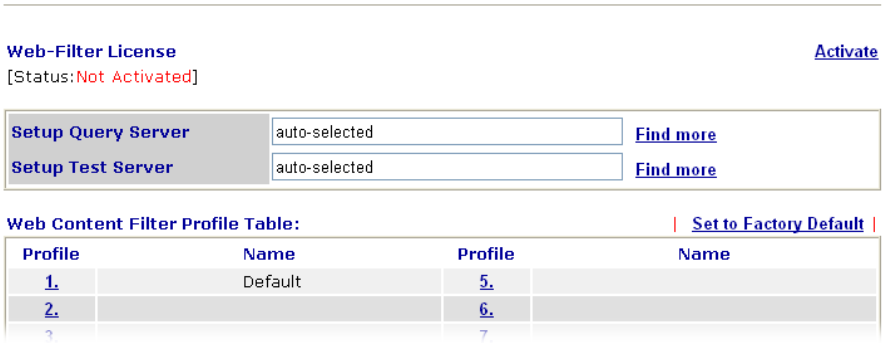
4.9 Creating an Account for MyVigor

The website of MyVigor (a server located on http://myvigor.draytek.com) provides useful service (e.g., Web Content Filter) to filter the web pages for protecting your system.

To access into MyVigor for getting more information, please create an account for MyVigor first.

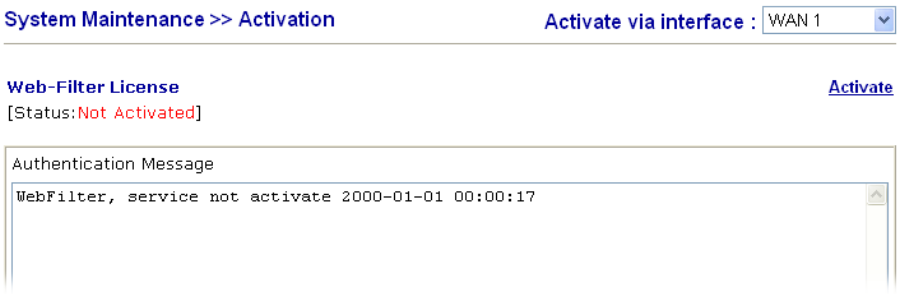
4.9.1 Creating an Account via Vigor Router

1. Click **CSM>> Web Content Filter Profile**. The following page will appear.



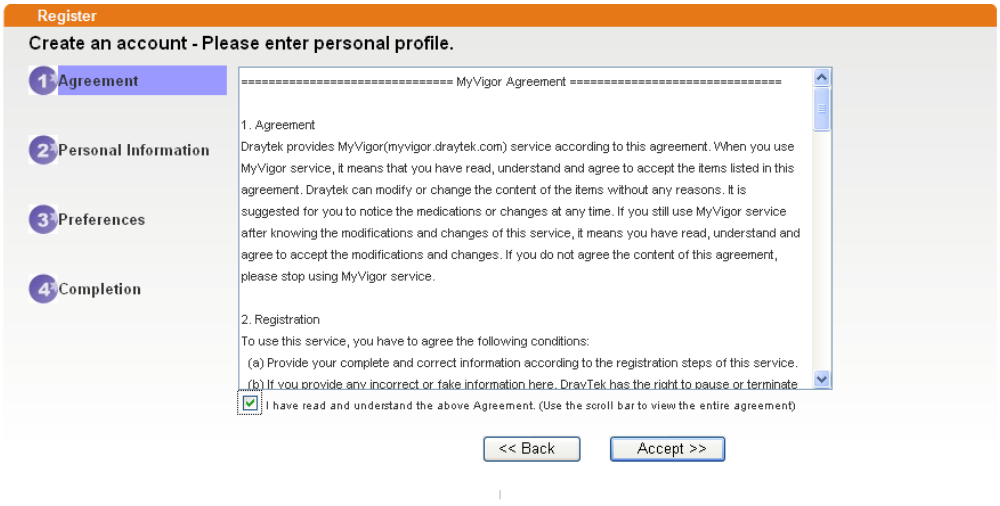
Or

Click **System Maintenance>>Activation** to open the following page.

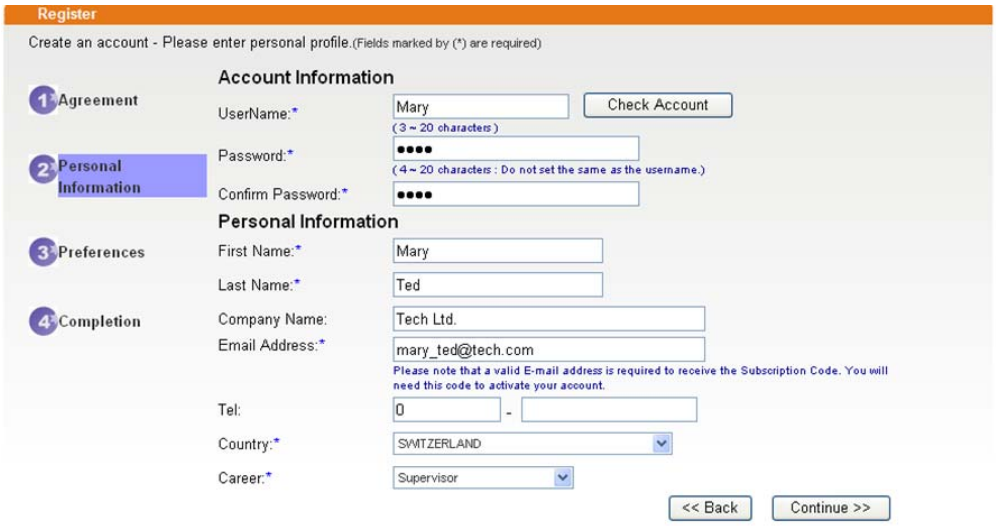


2. Click the **Activate** link. A login page for MyVigor web site will pop up automatically.

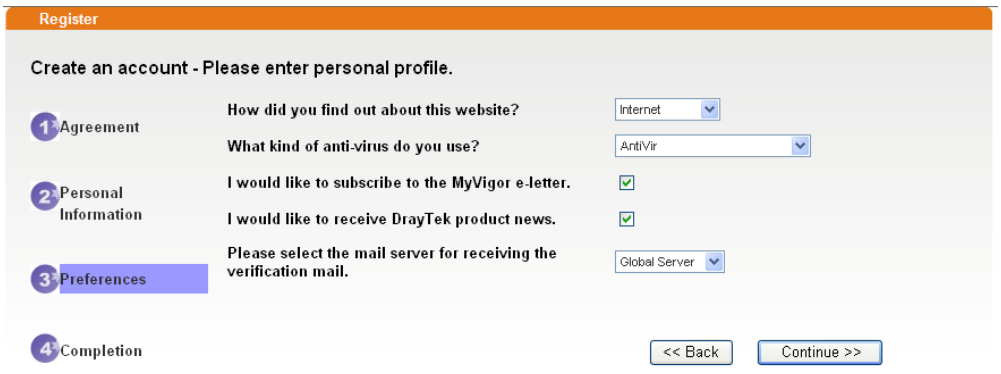
3. Click the link of **Create an account now**.
4. Check to confirm that you accept the Agreement and click **Accept**.



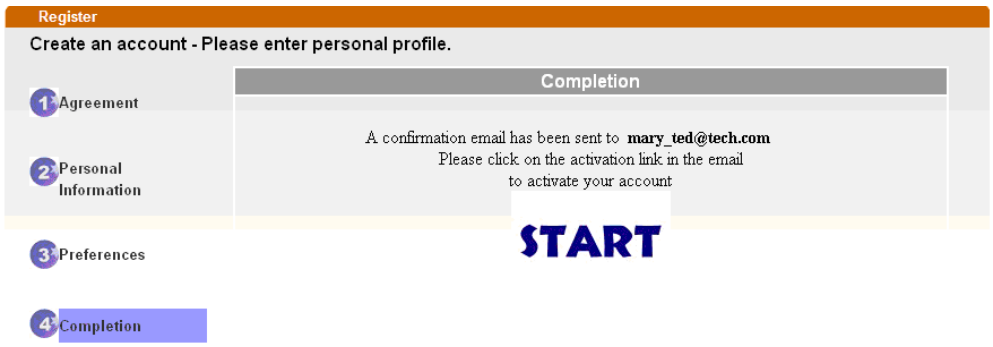
5. Type your personal information in this page and then click **Continue**.



6. Choose proper selection and click **Continue**.



7. Now you have created an account successfully. Click START.



8. Check to see the confirmation ***email*** with the title of **New Account Confirmation Letter from myvigor.draytek.com**.

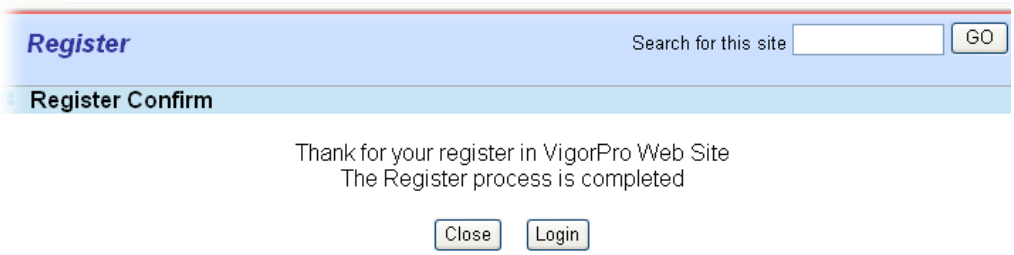
****** This is an automated message from myvigor.draytek.com.******

Thank you (**Mary**) for creating an account.

Please click on the activation link below to activate your account

Link : Activate my Account

9. Click the **Activate my Account** link to enable the account that you created. The following screen will be shown to verify the register process is finished. Please click **Login**.

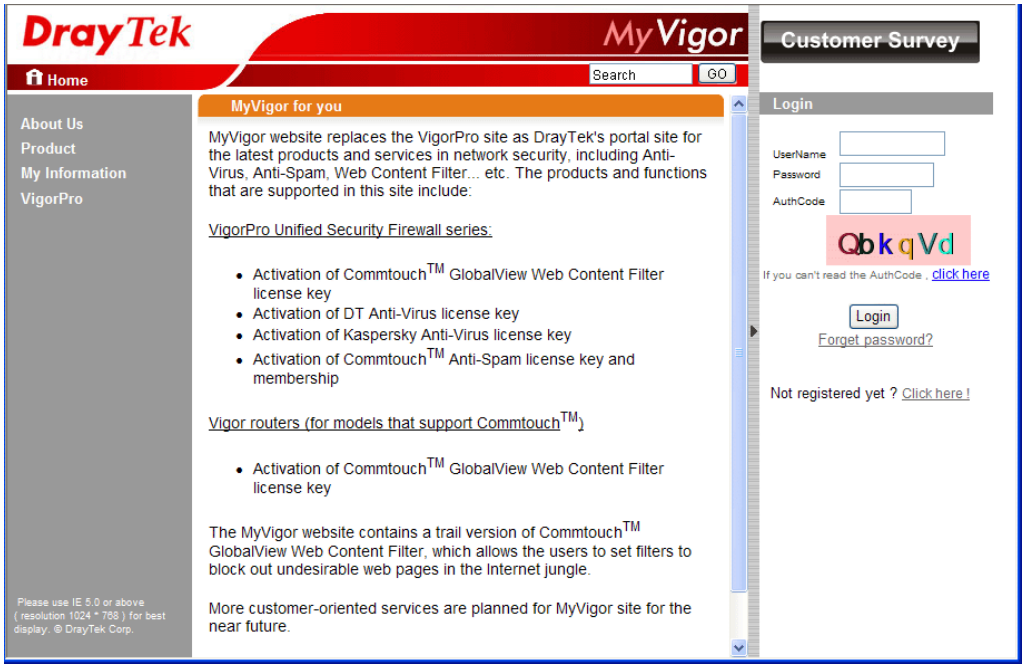


10. When you see the following page, please type in the account and password (that you just created) in the fields of **UserName** and **Password**.

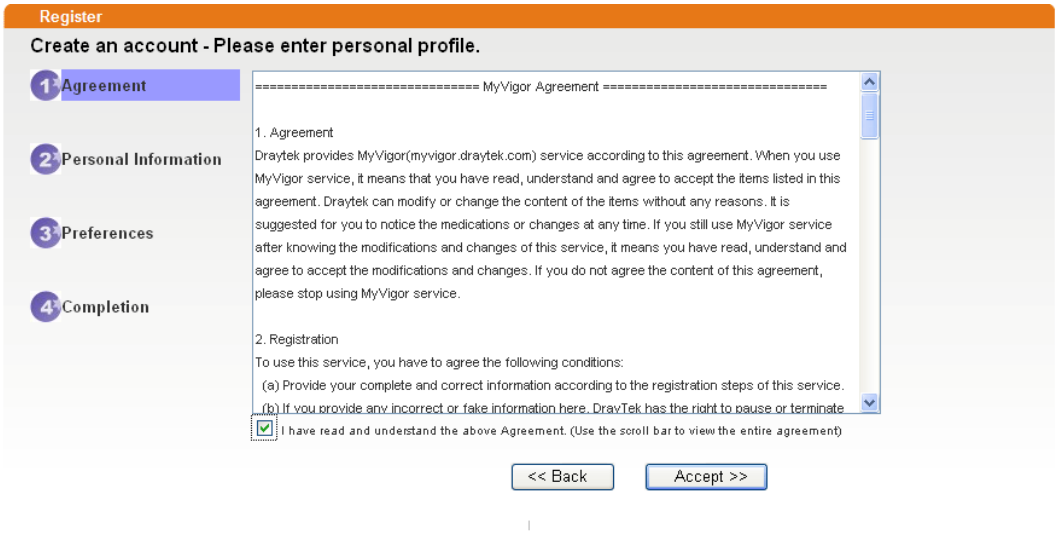
11. Now, click **Login**. Your account has been activated. You can access into MyVigor server to activate the service (e.g., WCF) that you want.

4.9.2 Creating an Account via MyVigor Web Site

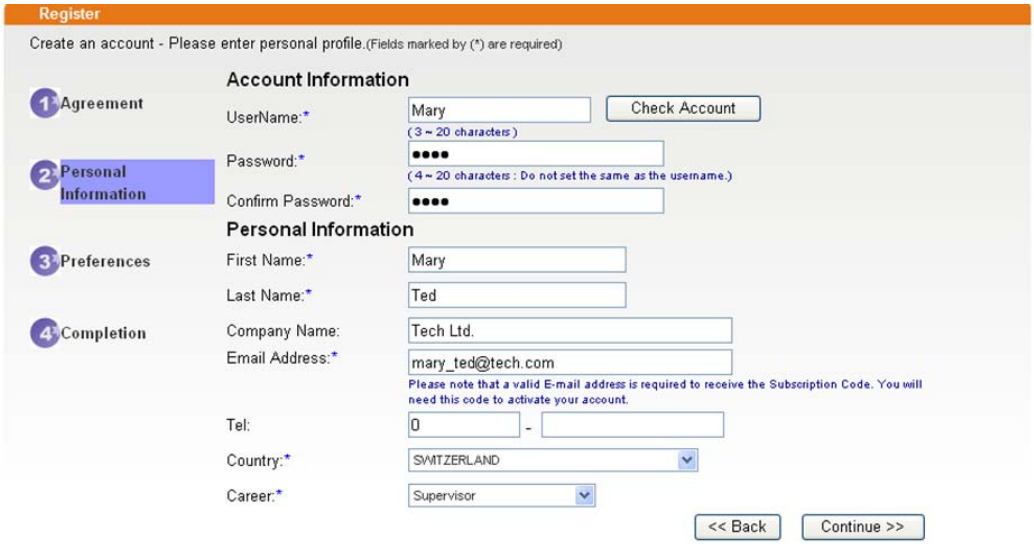
1. Access into http://myvigor.draytek.com. Find the line of **Not registered yet?**. Then, click the link **Click here!** to access into next page.



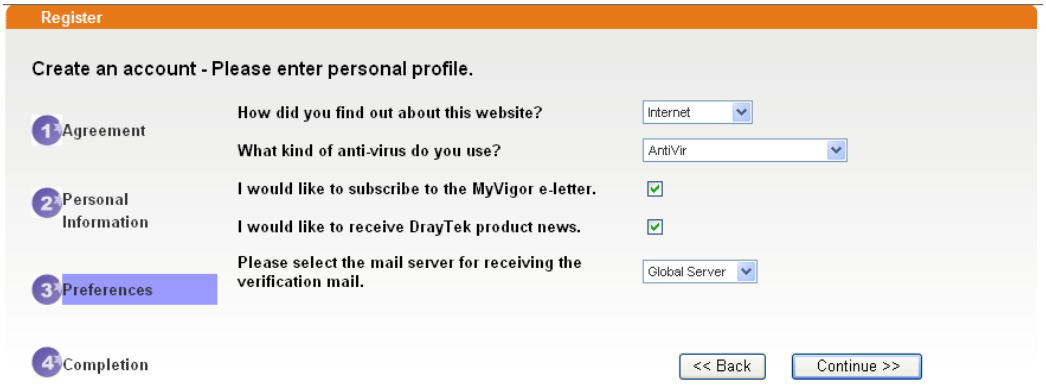
2. Check to confirm that you accept the Agreement and click **Accept**.



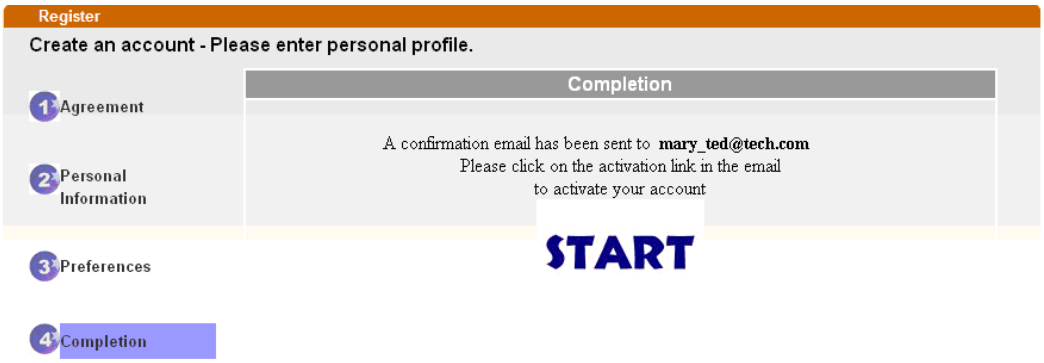
3. Type your personal information in this page and then click **Continue**.



4. Choose proper selection and click **Continue**.



5. Now you have created an account successfully. Click START.



6. Check to see the confirmation ***email*** with the title of **New Account Confirmation Letter from myvigor.draytek.com**.

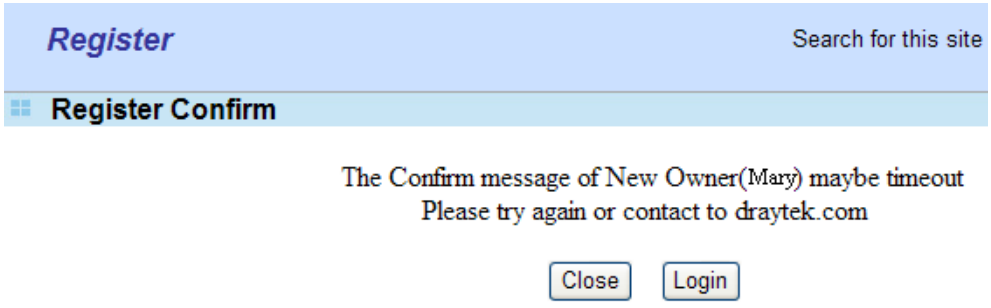
****** This is an automated message from myvigor.draytek.com.******

Thank you (**Mary**) for creating an account.

Please click on the activation link below to activate your account

Link : Activate my Account

7. Click the **Activate my Account** link to enable the account that you created. The following screen will be shown to verify the register process is finished. Please click **Login**.



8. When you see the following page, please type in the account and password (that you just created) in the fields of **UserName** and **Password**. Then type the code in the box of Auth Code according to the value displayed on the right side of it.

Now, click **Login**. Your account has been activated. You can access into MyVigor server to activate the service (e.g., WCF) that you want.

Chapter 5: Reference - Advanced Web Configuration

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

5.1 WAN

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

5.1.1 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 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

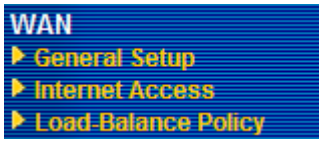
via **PAP** or **CHAP** with **RADIUS** authentication system. And your IP address, DNS server, and other related information will usually be assigned by your ISP.

5.1.2 Network Connection by 3G USB Modem

For 3G mobile communication through Access Point is popular more and more, VigorIPPBX 3510 adds the function of 3G network connection for such purpose. By connecting 3G USB Modem to the USB port of VigorIPPBX 3510, it can support HSDPA/UMTS/EDGE/GPRS/GSM and the future 3G standard (HSUPA, etc). VigorIPPBX 3510 with 3G USB Modem allows you to receive 3G signals at any place such as your car or certain location holding outdoor activity and share the bandwidth for using by more people. Users can use four LAN ports on the router to access Internet.

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

Below shows the menu items for Internet Access.



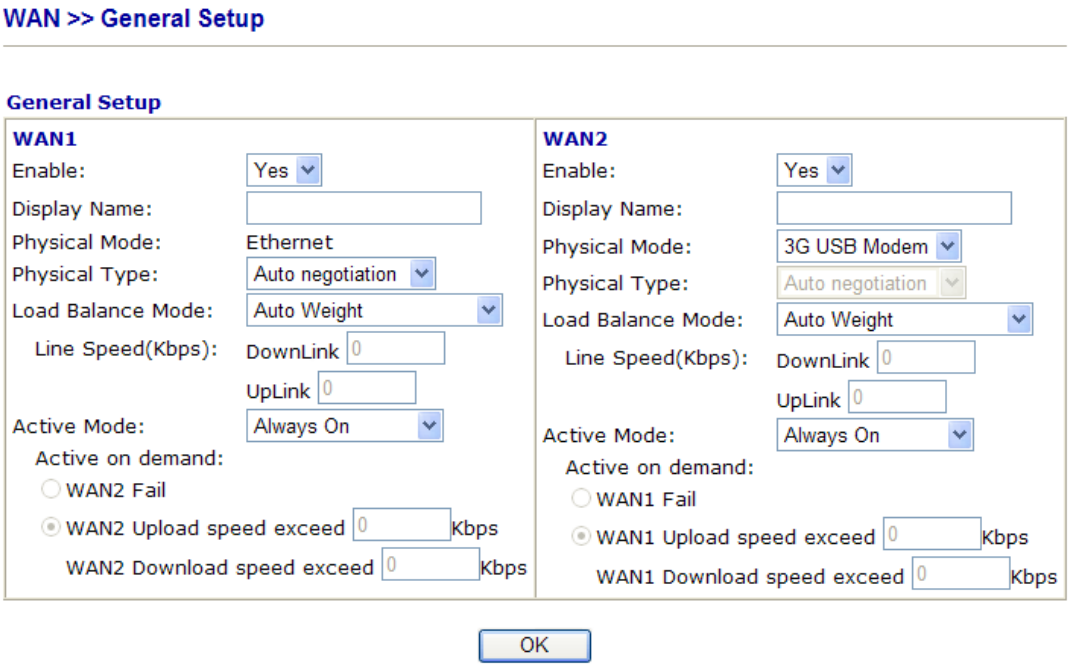
5.1.3 General Setup

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

This router supports dual WAN function. It allows users to access Internet and combine the bandwidth of the dual WAN to speed up the transmission through the network. Each WAN port (WAN1- through WAN port/WAN2- through LAN4 port) can connect to different ISPs, Even if the ISPs use different technology to provide telecommunication service (such as Cable modem, etc.). If any connection problem occurred on one of the ISP connections, all the traffic will be guided and switched to the normal communication port for proper operation. Please configure WAN1 and WAN2 settings.

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

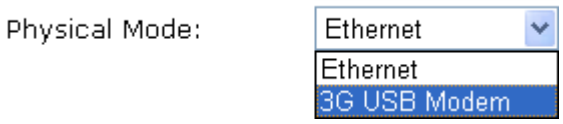
Note: In default, WAN1 is enabled. WAN2 is optional.



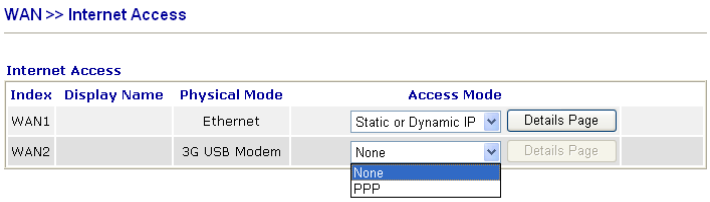
Enable Choose **Yes** to invoke the settings for this WAN interface. Choose **No** to disable the settings for this WAN interface.

Display Name Type the description for the WAN1/WAN2 interface.

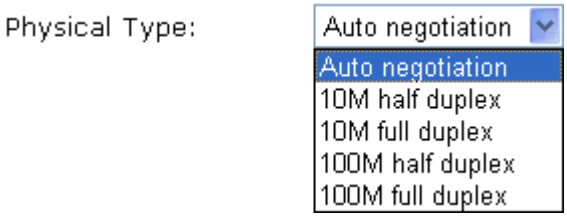
Physical Mode For WAN1, the physical connection is done and fixed through Ethernet port; yet the physical connection for WAN2 is done through an Ethernet port (P4) or USB port.



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

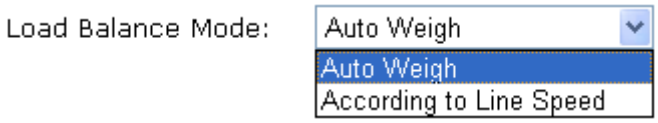


Physical Type You can change the physical type for WAN2 or choose **Auto negotiation** for determined by the system.



Load Balance Mode

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

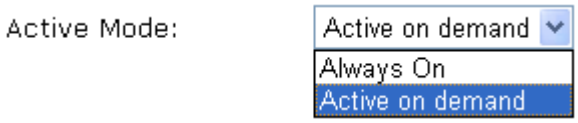


Line Speed

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

Active Mode

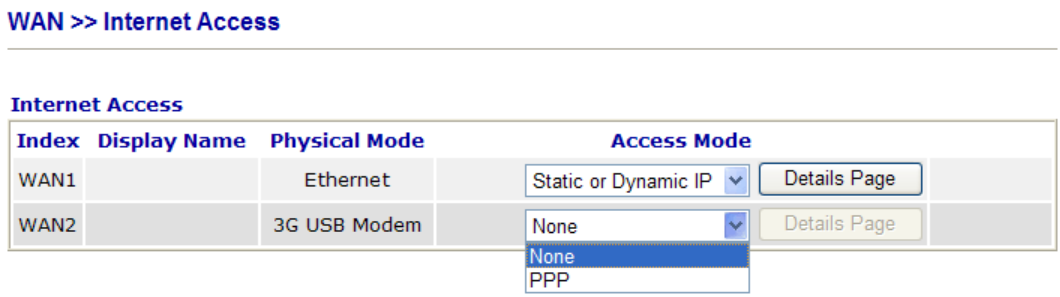
Choose **Always On** to make the WAN connection (WAN1/WAN2) being activated always; or choose **Active on demand** to make the WAN connection (WAN1/WAN2) activated if it is necessary.

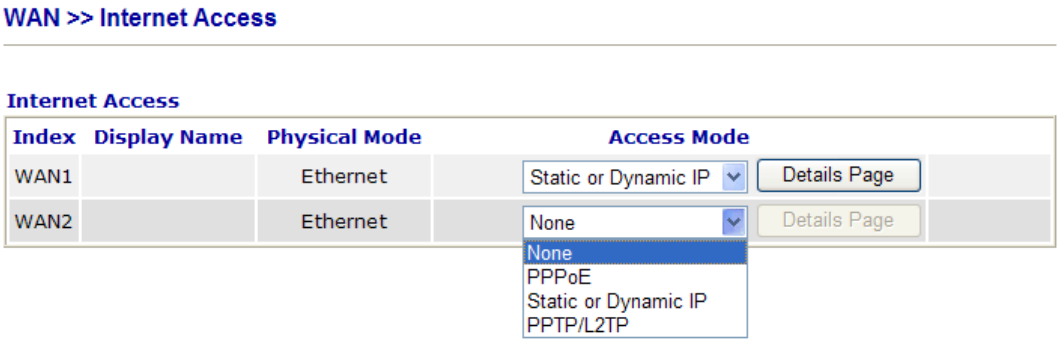


If you choose Active on demand, the Idle Timeout will be available for you to set for PPPoE and PPTP access modes in the Details Page of WAN>>Internet Access. In addition, there are three selections for you to choose for different purposes.
WAN1 Fail – It means the connection for WAN2 will be activated when WAN1 is failed.
WAN1 Upload speed exceed XX kbps – It means the connection for WAN2 will be activated when WAN1 Upload speed exceed certain value that you set in this box for 15 seconds.
WAN1 Download speed exceed XX kbps– It means the connection for WAN2 will be activated when WAN1 Download speed exceed certain value that you set in this box for 15 seconds.
WAN2 Fail – It means the connection for WAN1 will be activated when WAN2 is failed.
WAN2 Upload speed exceed XX kbps – It means the connection for WAN1 will be activated when WAN2 Upload speed exceed certain value that you set in this box for 15 seconds.
WAN2 Download speed exceed XX kbps– It means the connection for WAN1 will be activated when WAN2 Download speed exceed certain value that you set in this box for 15 seconds.

5.1.4 Internet Access

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



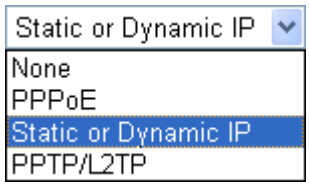


Index It shows the WAN modes that this router supports. WAN1 is the default WAN interface for accessing into the Internet. WAN2 is the optional WAN interface for accessing into the Internet when WAN 1 is inactive for some reason.

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

Physical Mode It shows the physical connection for WAN1 (Ethernet) /WAN2 (Ethernet or 3G USB Modem) according to the real network connection.

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

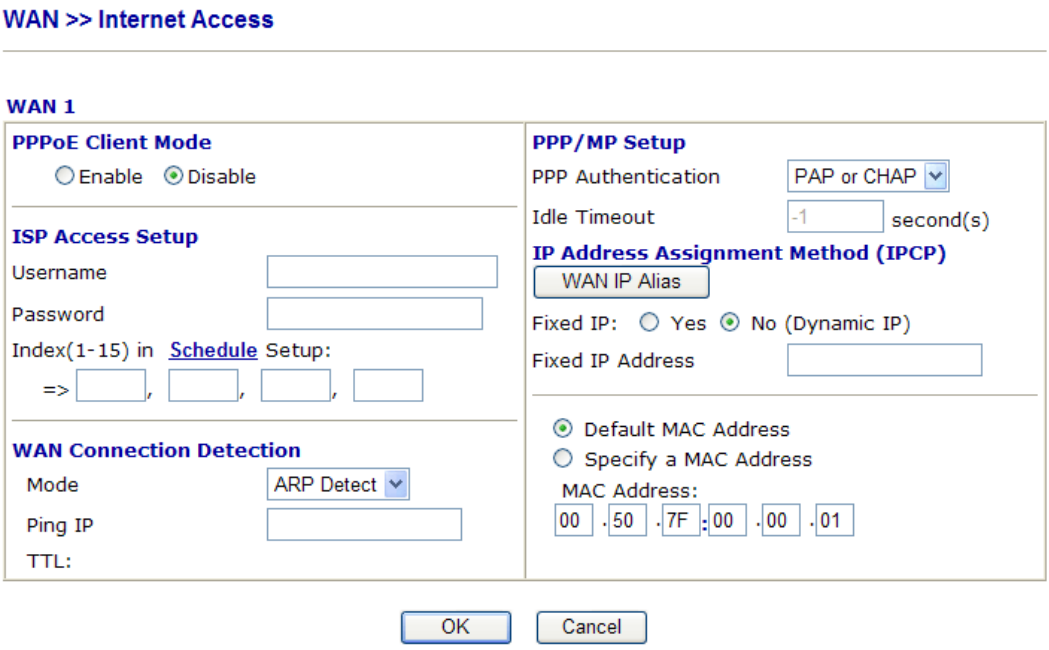


There are three access modes provided for PPPoE, Static or Dynamic IP and PPTP/L2TP.

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

Details Page for PPPoE

To use **PPPoE** as the accessing protocol of the internet, please choose **Internet Access** from **WAN** menu. Then, select **PPPoE** mode for WAN2. 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.

ISP Access Setup Enter your allocated username, password and authentication parameters according to the information provided by your ISP.
Username – Type in the username provided by ISP in this field.
Password – Type in the password provided by ISP in this field.
Index (1-15) in Schedule Setup - You can type in four sets of time schedule for your request. All the schedules can be set previously in **Application – Schedule** web page and you can use the number that you have set in that web page.

WAN Connection Detection Such function allows you to verify whether network connection is alive or not through ARP Detect or Ping Detect.
Mode – Choose **ARP Detect** or **Ping Detect** for the system to execute for WAN detection.
Ping IP – If you choose Ping Detect as detection mode, you have to type IP address in this field for pinging.
TTL (Time to Live) – Displays value for your reference. TTL value is set by telnet command.

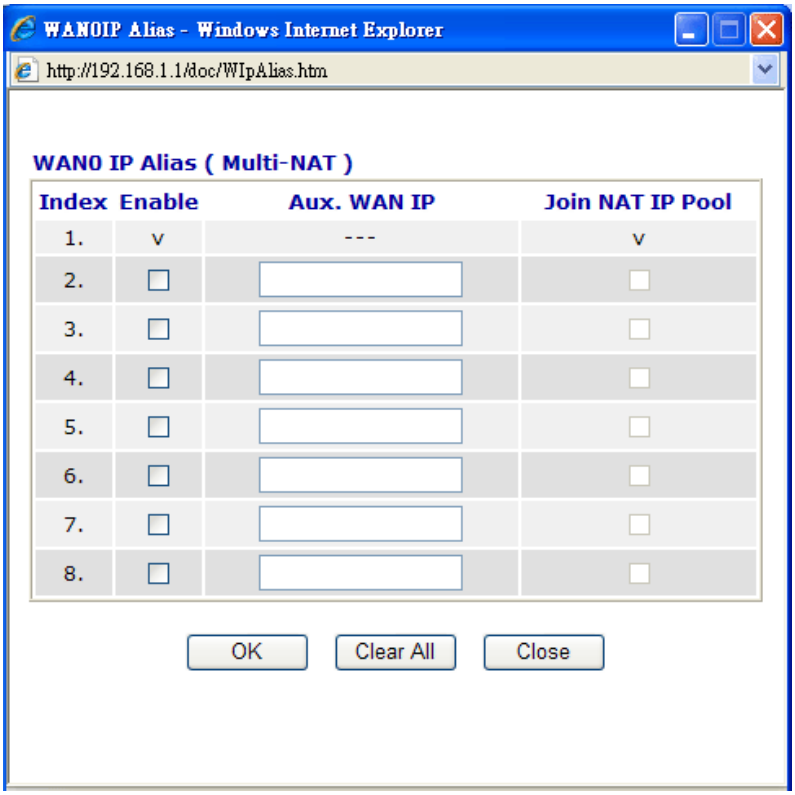
PPP/MP Setup **PPP Authentication** – Select **PAP only** or **PAP or CHAP** for PPP. If you want to connect to Internet all the time, you can check **Always On**.

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

IP Address Assignment Method (IPCP)

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

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



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

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

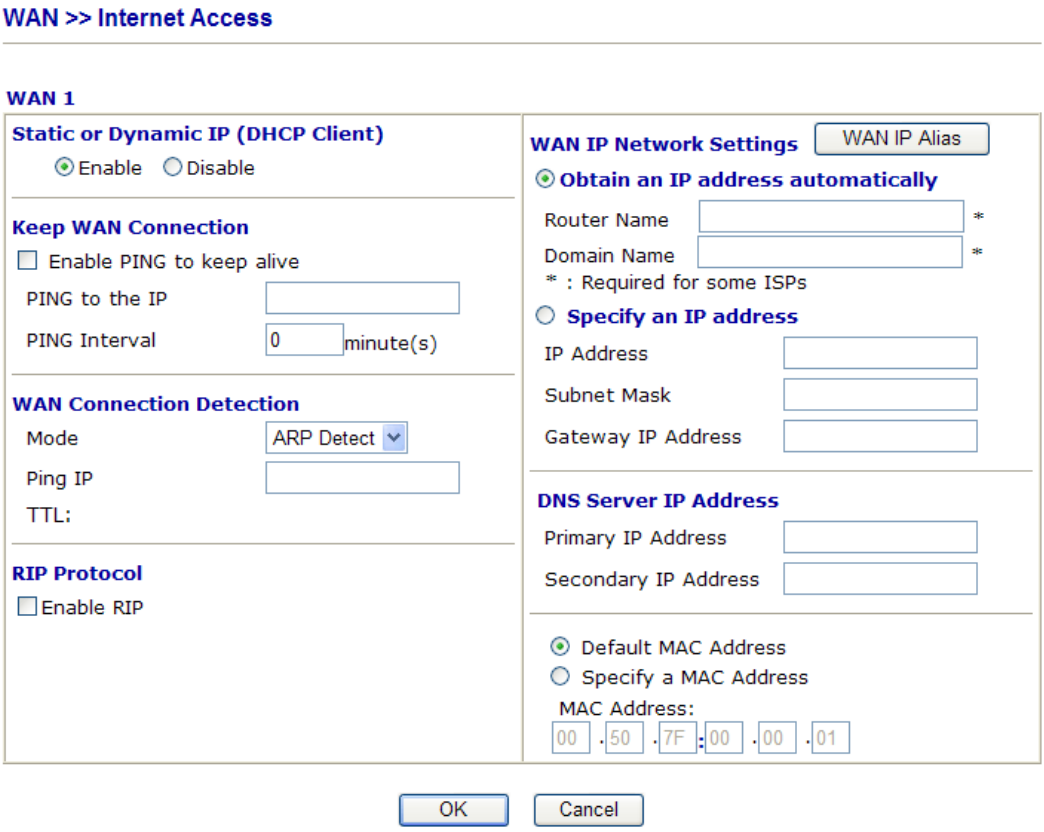
Specify a MAC Address – Type the MAC address for the router manually.

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

Details Page for Static or Dynamic IP

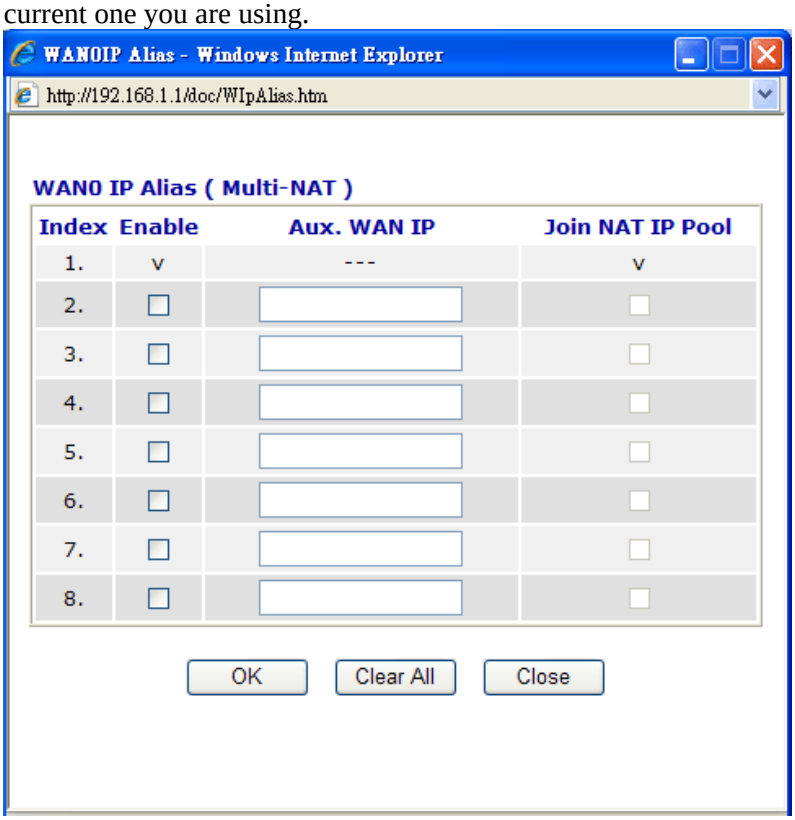
For static IP mode, you usually receive a fixed public IP address or a public subnet, namely multiple public IP addresses from your DSL or Cable ISP service providers. In most cases, a Cable service provider will offer a fixed public IP, while a DSL service provider will offer a public subnet. If you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

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



Access Control	Click **Enable** for activating this function. If you click **Disable**, this function will be closed and all the settings that you adjusted in this page will be invalid.
Keep WAN Connection	Normally, this function is designed for Dynamic IP environments because some ISPs will drop connections if there is no traffic within certain periods of time. Check **Enable PING to keep alive** box to activate this function. **PING to the IP** - If you enable the PING function, please specify the IP address for the system to PING it for keeping alive. **PING Interval** - Enter the interval for the system to execute the PING operation.
WAN Connection Detection	Such function allows you to verify whether network connection is alive or not through ARP Detect or Ping Detect. **Mode** – Choose **ARP Detect** or **Ping Detect** for the system to execute for WAN detection. **Ping IP** – If you choose Ping Detect as detection mode, you have to type IP address in this field for pinging. **TTL (Time to Live)** – Displays value for your reference. TTL value is set by telnet command.
RIP Protocol	Routing Information Protocol is abbreviated as RIP（RFC1058）specifying how routers exchange routing tables information. Click **Enable RIP** for activating this function.
WAN IP Network Settings	This group allows you to obtain an IP address automatically and allows you type in IP address manually.

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



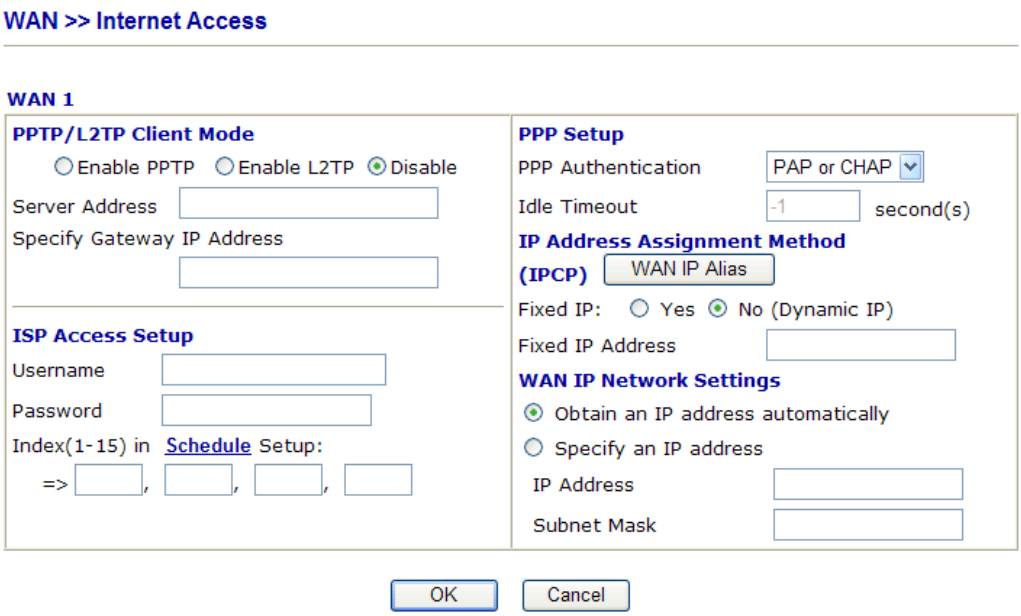
Obtain an IP address automatically – Click this button to obtain the IP address automatically if you want to use **Dynamic IP** mode.
Router Name: Type in the router name provided by ISP.
Domain Name: Type in the domain name that you have assigned.
Specify an IP address – Click this radio button to specify some data if you want to use **Static IP** mode.
IP Address: Type the IP address.
Subnet Mask: Type the subnet mask.
Gateway IP Address: Type the gateway IP address.
Default MAC Address : Click this radio button to use default MAC address for the router.
Specify a MAC Address: Some Cable service providers specify a specific MAC address for access authentication. In such cases you need to click the **Specify a MAC Address** and enter the MAC address in the MAC Address field.

DNS Server IP Address

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

Details Page for PPTP/L2TP

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



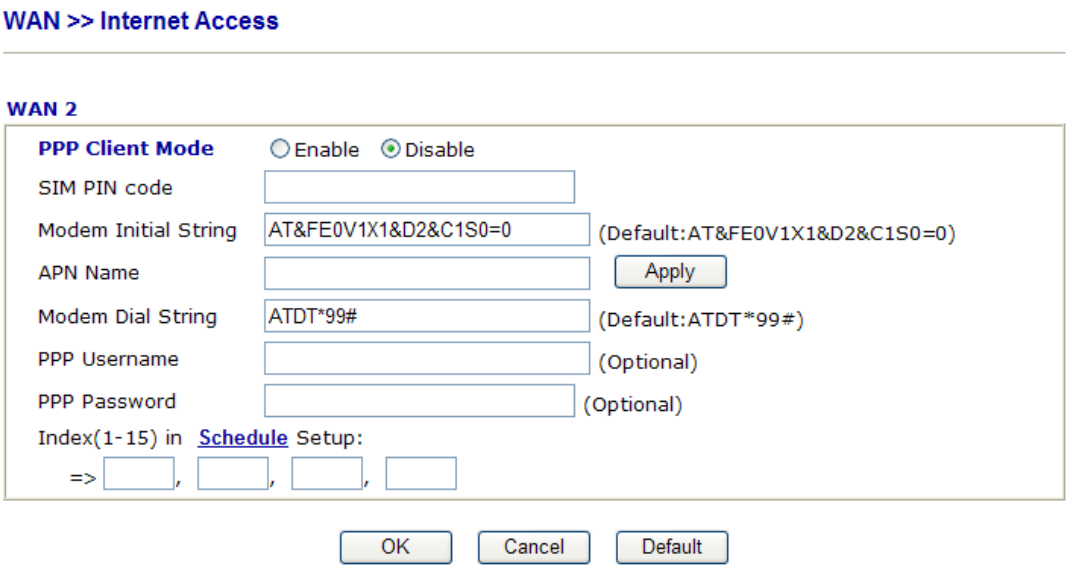
PPTP/L2TP Client Mode	**Enable PPTP-** Click this radio button to enable a PPTP client to establish a tunnel on the WAN interface. **Enable L2TP** - Click this radio button to enable a L2TP client to establish a tunnel on the WAN interface. **Disable** – Click this radio button to close the connection through PPTP or L2TP. **Server Address** - Specify the IP address of the PPTP/L2TP server if you enable PPTP/L2TP client mode. **Specify Gateway IP Address** – Specify the gateway IP address for DHCP server.
ISP Access Setup	**Username** -Type in the username provided by ISP in this field. **Password** -Type in the password provided by ISP in this field. **Index (1-15) in Schedule Setup -** You can type in four sets of time schedule for your request. All the schedules can be set previously in **Application – Schedule** web page and you can use the number that you have set in that web page.
PPP Setup	**PPP Authentication** - Select **PAP only** or **PAP or CHAP** for PPP. **Idle Timeout** - Set the timeout for breaking down the Internet after passing through the time without any action.
IP Address Assignment Method(IPCP)	**Fixed IP** - Usually ISP dynamically assigns IP address to you each time you connect to it and request. In some case, your ISP provides service to always assign you the same IP address whenever you request. In this case, you can fill in this IP address in the Fixed IP field. Please contact your ISP before you want to use this function. Click **Yes** to use this function and type in a fixed IP address in the box. **Fixed IP Address** -Type a fixed IP address.
WAN IP Network	**Obtain an IP address automatically** – Click this button to obtain

Settings the IP address automatically.

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

Details Page for PPP

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



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

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

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

APN Name APN means Access Point Name which is provided and required by some ISPs. Type the name and click Apply.

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

PPP Username Type the PPP username (optional).

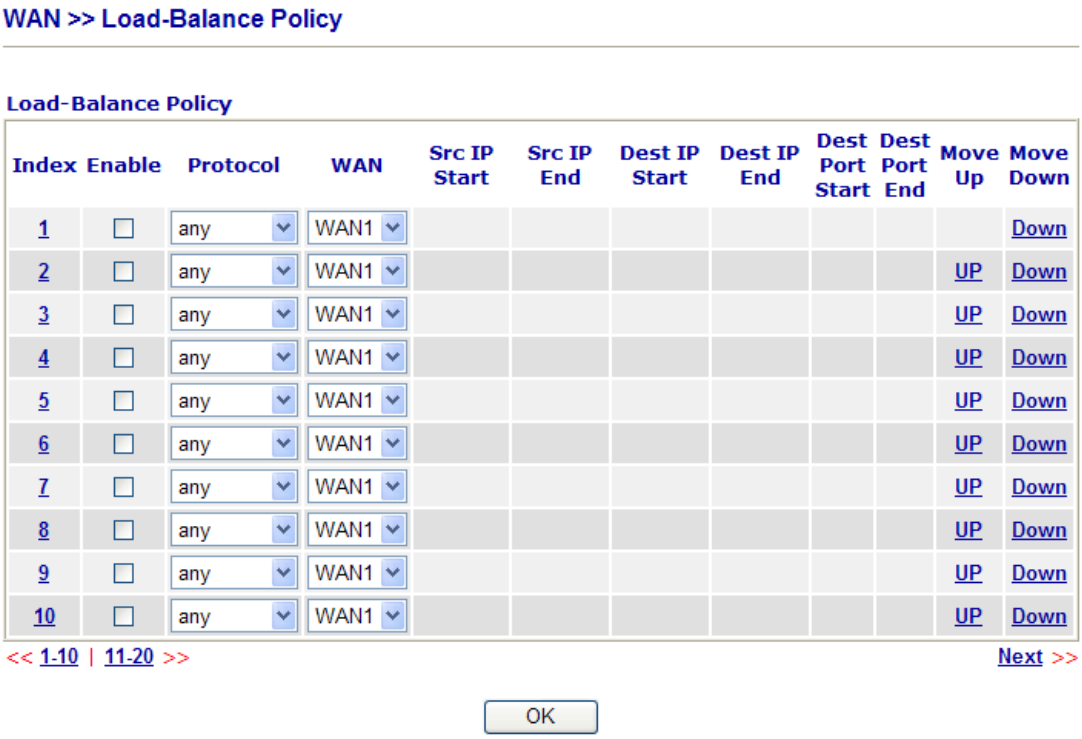
PPP Password Type the PPP password (optional).

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

5.1.5 Load-Balance Policy

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

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



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

Enable Check this box to enable this policy.

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

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

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

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

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

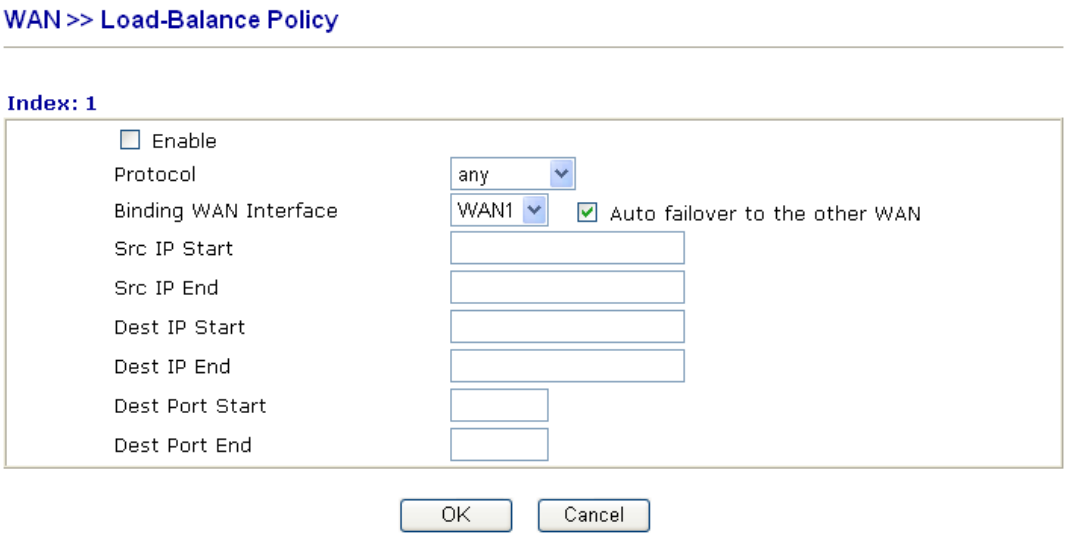
Dest IP End Displays the IP address for the end of the destination IP.

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

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

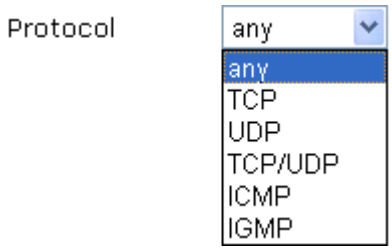
Move UP/Move Down Use **Up** or **Down** link to move the order of the policy.

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



Enable Check this box to enable this policy.

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



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

Src IP Start Type the source IP start for the specified WAN interface.

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

Dest IP Start Type the destination IP start for the specified WAN interface.

Dest IP End Type the destination IP end for the specified WAN interface. If this field is blank, it means that all the destination IPs will be passed through the WAN interface.

Dest Port Start Type the destination port start for the destination IP.

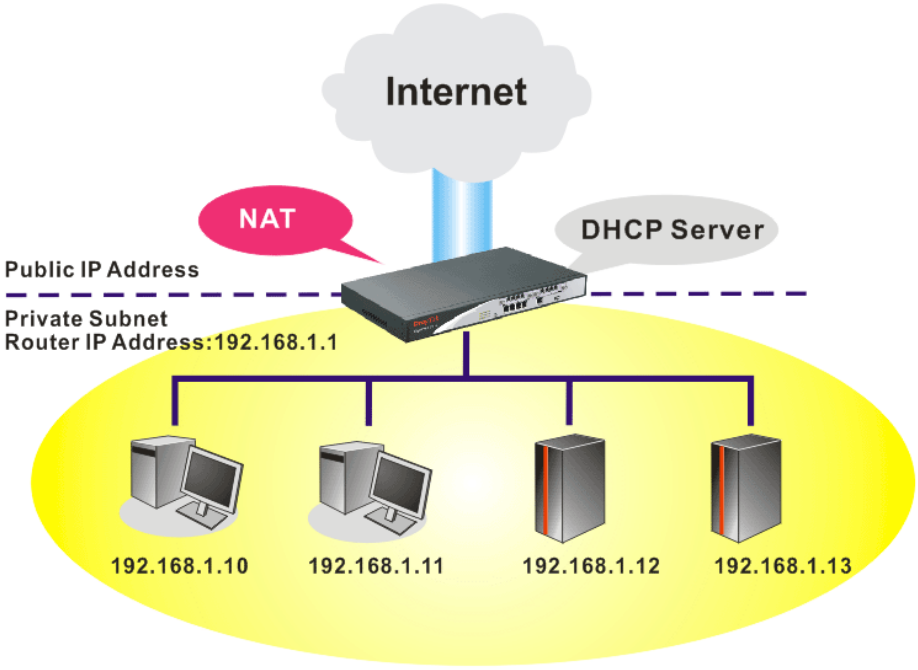
Dest Port End Type the destination port end for the destination IP. If this field is blank, it means that all the destination ports will be passed through the WAN interface.

5.2 LAN

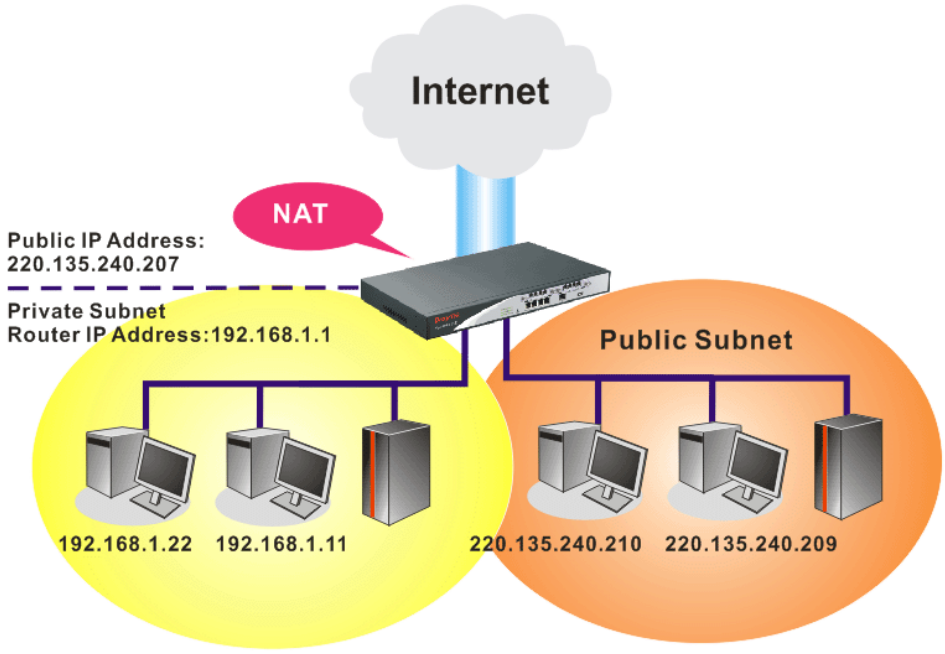
Local Area Network (LAN) is a group of subnets regulated and ruled by router. The design of network structure is related to what type of public IP addresses coming from your ISP.

5.2.1 Basics of LAN

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



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



What is Routing Information Protocol (RIP)

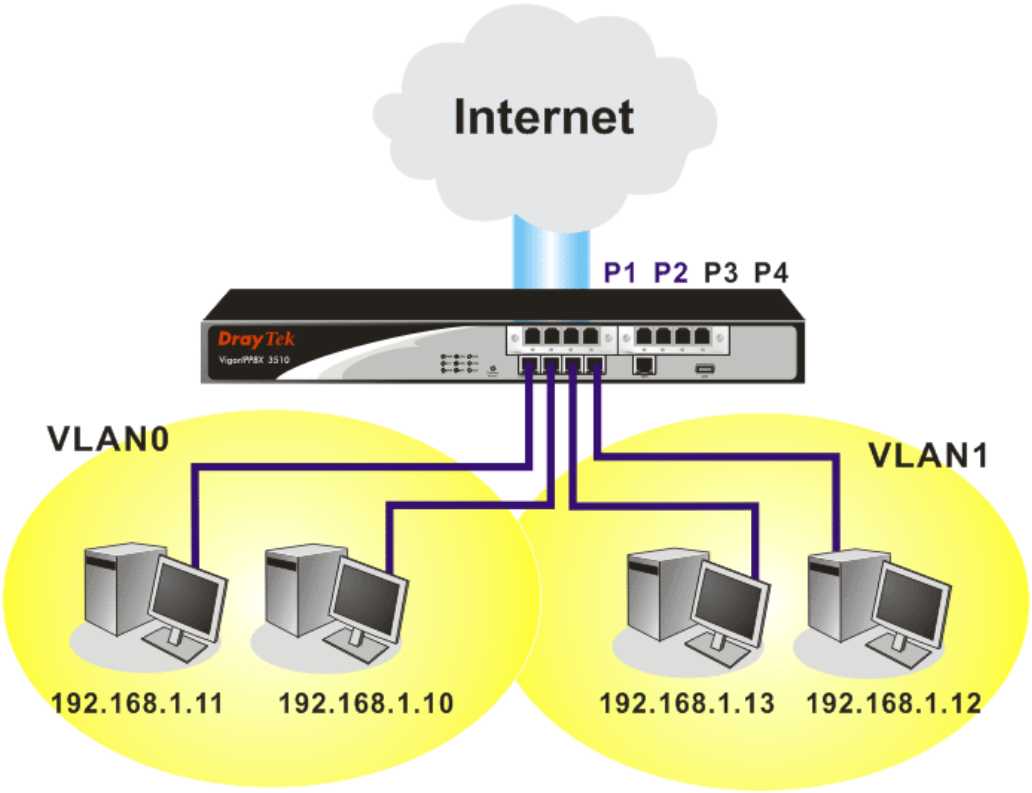
Vigor router will exchange routing information with neighboring routers using the RIP to accomplish IP routing. This allows users to change the information of the router such as IP address and the routers will automatically inform for each other.

What is Static Route

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

What are Virtual LANs

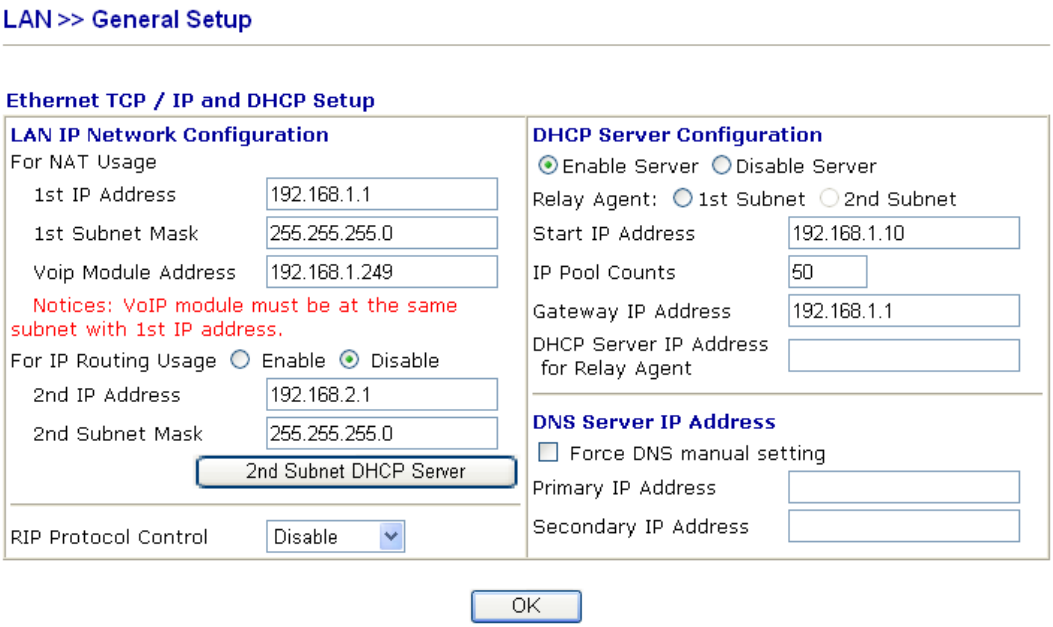
You can group local hosts by physical ports and create up to 4 virtual LANs. To manage the communication between different groups, please set up rules in Virtual LAN (VLAN) function and the rate of each.



5.2.2 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).

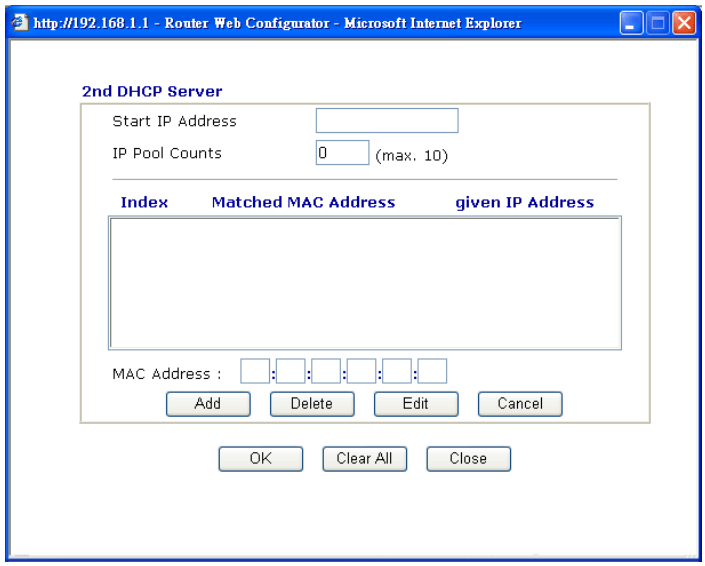
VoIP Module Address Type in the IP address for VoIP connection. (Default: 192.168.1.249)

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

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

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

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



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

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

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

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

1st Subnet - Select the router to change the RIP information of the 1st subnet with neighboring routers.
2nd Subnet - Select the router to change the RIP information of the 2nd subnet with neighboring routers.

DHCP Server Configuration

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

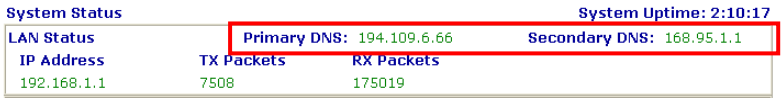
If you want to use another DHCP server in the network other than the Vigor Router's, you can let Relay Agent help you to redirect the DHCP request to the specified location.
Enable Server - Let the router assign IP address to every host in the LAN.
Disable Server – Let you manually assign IP address to every host in the LAN.
Relay Agent – (1st subnet/2nd subnet) Specify which subnet that DHCP server is located the relay agent should redirect the DHCP request to.
Start IP Address - Enter a value of the IP address pool for the DHCP server to start with when issuing IP addresses. If the 1st IP address of your router is 192.168.1.1, the starting IP address must be 192.168.1.2 or greater, but smaller than 192.168.1.254.
IP Pool Counts - Enter the maximum number of PCs that you want the DHCP server to assign IP addresses to. The default is 50 and the maximum is 253.
Gateway IP Address - Enter a value of the gateway IP address for the DHCP server. The value is usually as same as the 1st IP address of the router, which means the router is the default gateway.
DHCP Server IP Address for Relay Agent - Set the IP address of the DHCP server you are going to use so the Relay Agent can help to forward the DHCP request to the DHCP server.

DNS Server Configuration

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

Force DNS manual setting - Force 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:



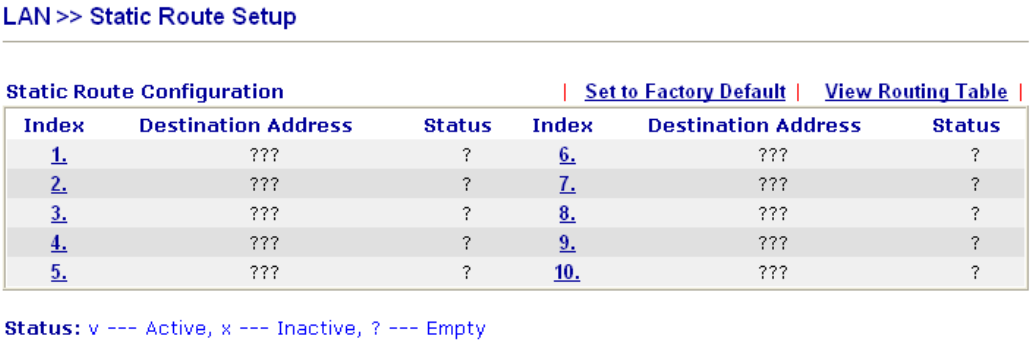
If both the Primary IP and Secondary IP Address fields are left empty, the router will assign its own IP address to local users as a DNS proxy server and maintain a DNS cache.

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. Cable) connection.

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

5.2.3 Static Route

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

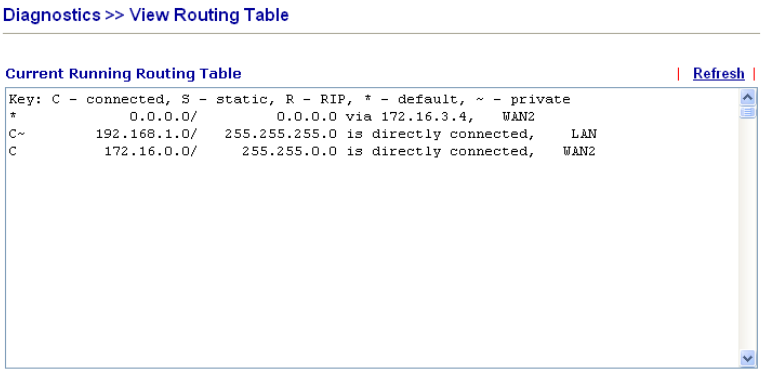


Index The number (1 to 10) under Index allows you to open next page to set up static route.

Destination Address Displays the destination address of the static route.

Status Displays the status of the static route.

Viewing Routing Table Displays the routing table for your reference.



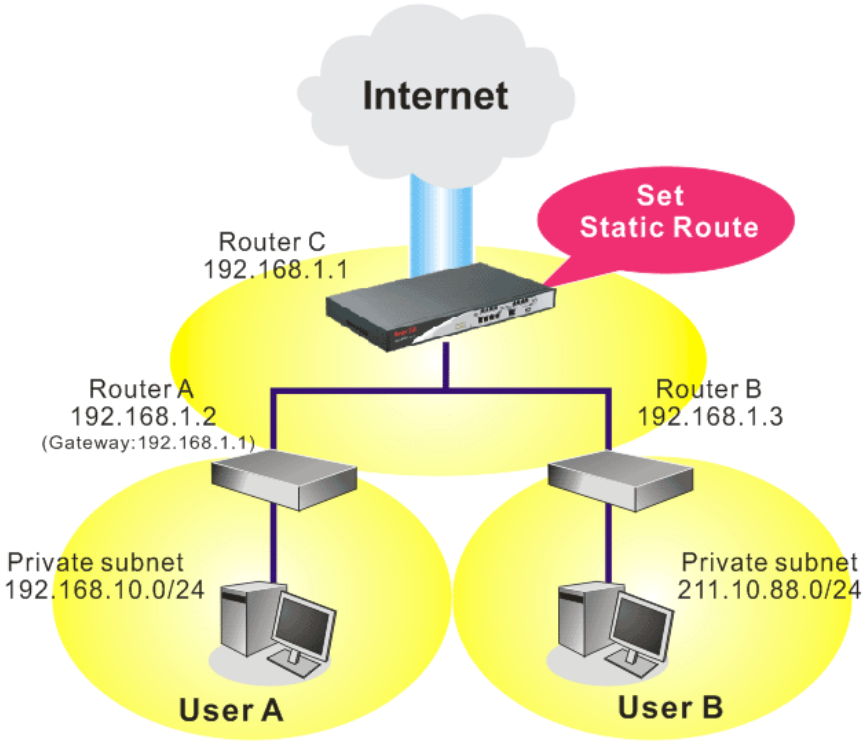
Add Static Routes to Private and Public Networks

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

- use the Main Router to surf the Internet.

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

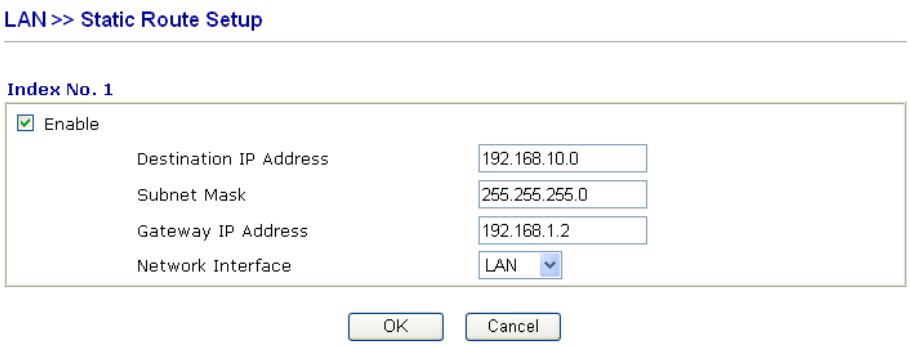
Before setting Static Route, user A cannot talk to user B for Router A can only forward recognized packets to its default gateway Main Router.



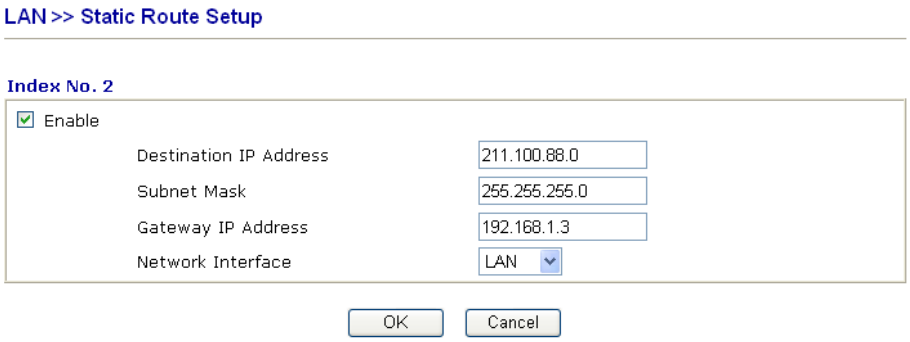
1. Go to **LAN** page and click **General Setup**, select 1st Subnet as the **RIP Protocol Control.** Then click the **OK** button.

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

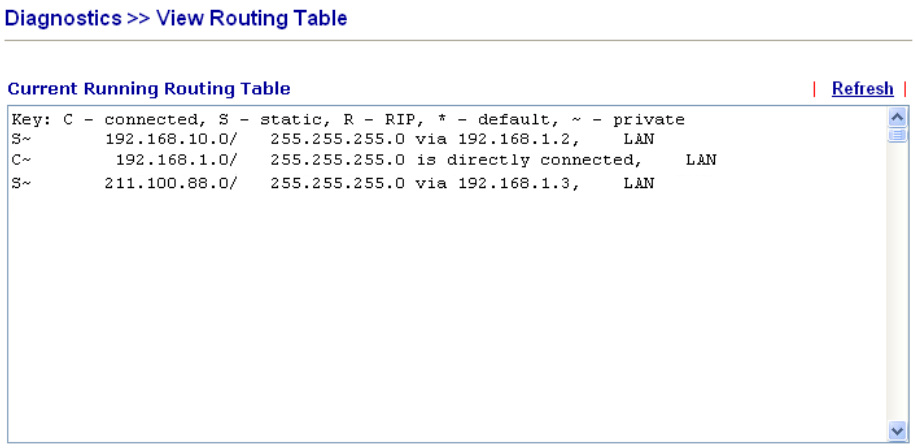
2. Click the **LAN - Static Route** and click on the **Index Number 1.** Check the **Enable** box. Please add a static route as shown below, which regulates all packets destined to 192.168.10.0 will be forwarded to 192.168.1.2. Click **OK**.



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

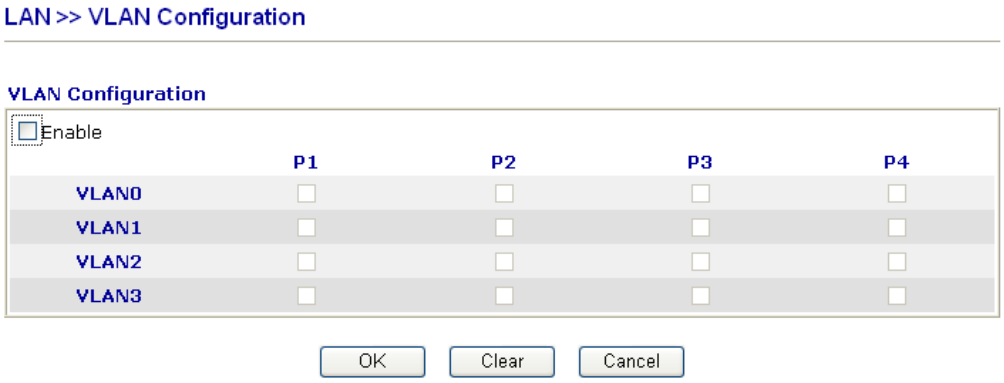


4. Go to **Diagnostics** and choose **Routing Table** to verify current routing table.



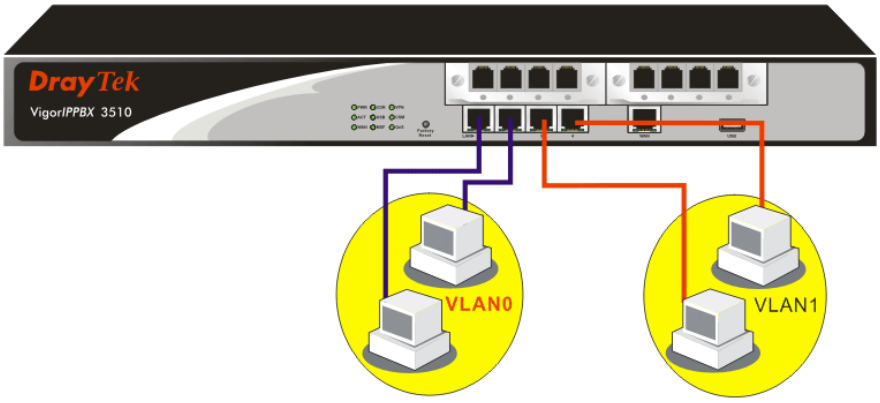
5.2.4 VLAN

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.

LAN >> VLAN Configuration

VLAN Configuration

Enable

	P1	P2	P3	P4
VLAN0	☑	☑	☐	☐
VLAN1	☐	☐	☑	☑
VLAN2	☐	☐	☐	☐
VLAN3	☐	☐	☐	☐

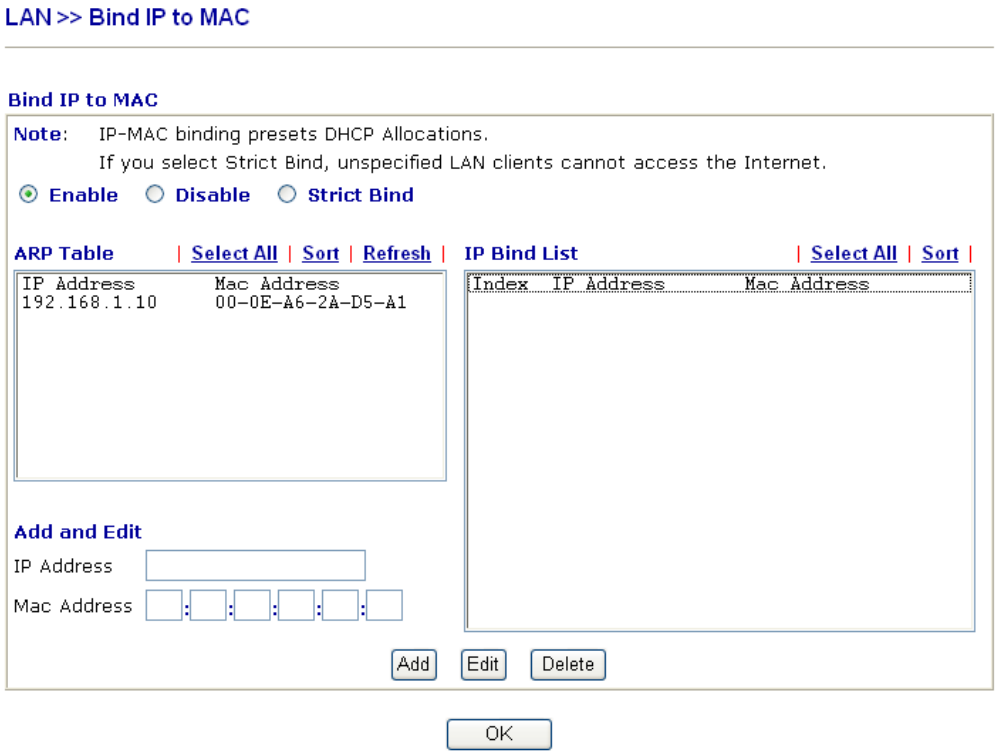
OK Clear Cancel

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

5.2.5 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.

5.3 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.

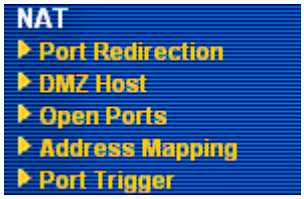
When the outgoing packets destined to some public server on the Internet reach the NAT router, the router will change its source address into the public IP address of the router, select the available public port, and then forward it. At the same time, the router shall list an entry in a table to memorize 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.

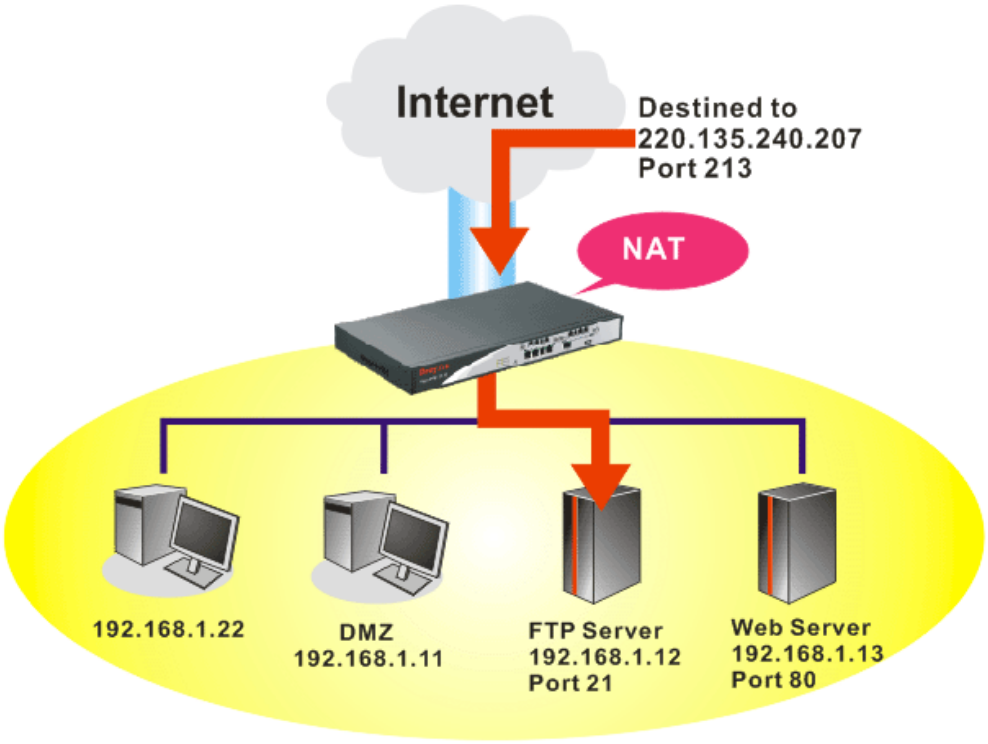
On NAT page, you will see the private IP address defined in RFC-1918. Usually we use the 192.168.1.0/24 subnet for the router. As stated before, the NAT facility can map one or more IP addresses and/or service ports into different specified services. In other words, the NAT function can be achieved by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

Below shows the menu items for NAT.



5.3.1 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.

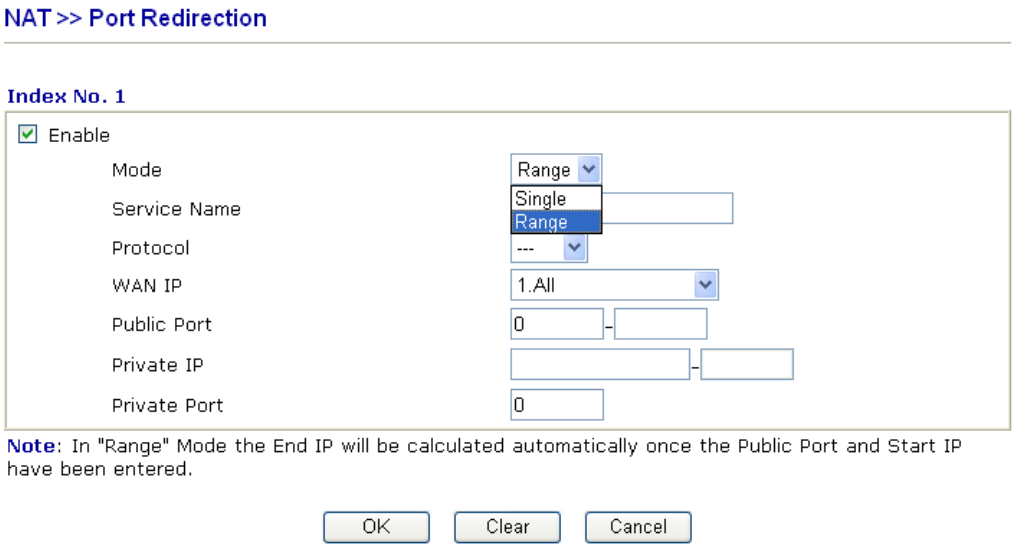
NAT >> Port Redirection

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.

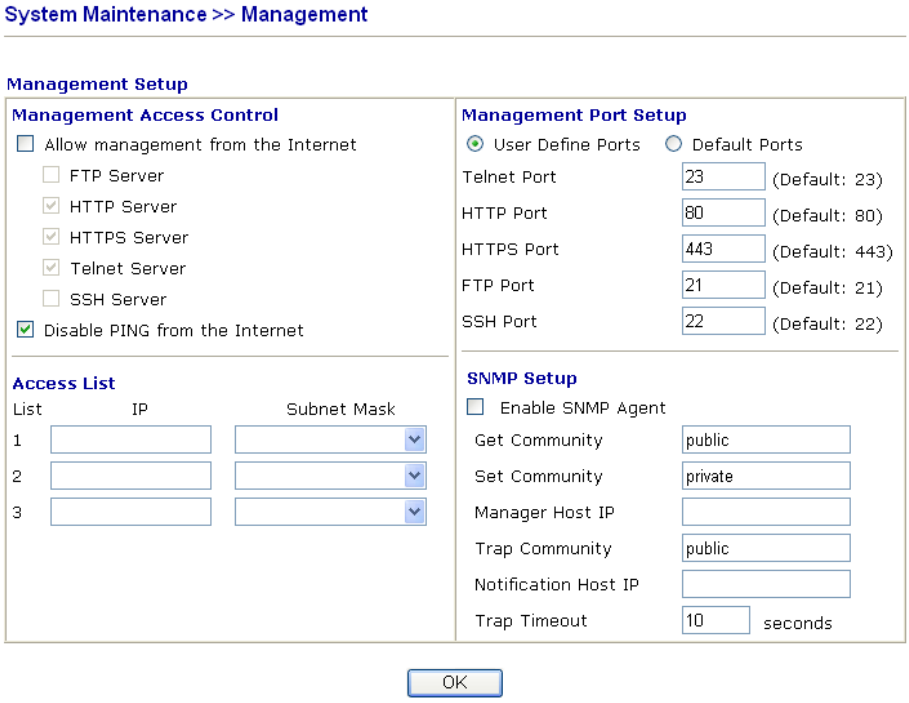


Enable	Check this box to enable such port redirection setting.
Mode	Two options (Single and Range) are provided here for you to choose. To set a range for the specific service, select **Range**. In Range mode, if the public port (start port and end port) and the starting IP of private IP had been entered, 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).
WAN IP	Select the WAN IP used for port redirection. There are eight WAN IP alias that can be selected and used for port redirection. The default setting is **All** which means all the incoming data from any port will be redirected to specified range of IP address and port.
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.

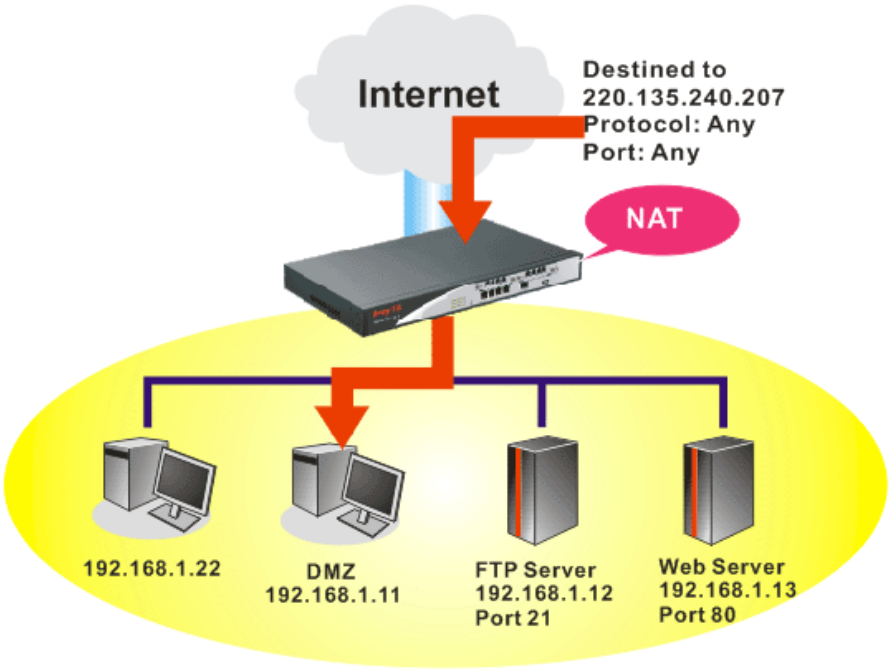
For example, the built-in web configurator in the router is with default port 80, which may conflict with the web server in the local network, http://192.168.1.13:80. Therefore, you need to **change the router's http port to any one other than the default port 80** to avoid

conflict, such as 8080. This can be set in the **System Maintenance >>Management.** 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.



5.3.2 DMZ Host

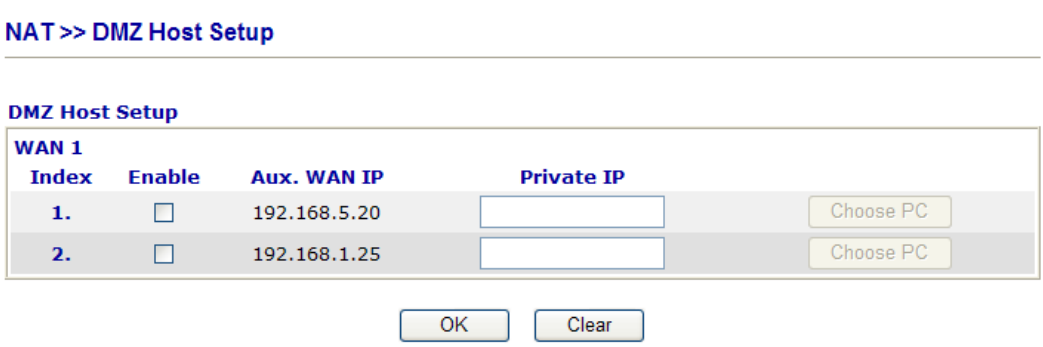
As mentioned above, **Port Redirection** can redirect incoming TCP/UDP or other traffic on particular ports to the specific private IP address/port of host in the LAN. However, other IP protocols, for example Protocols 50 (ESP) and 51 (AH), do not travel on a fixed port. Vigor router provides a facility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

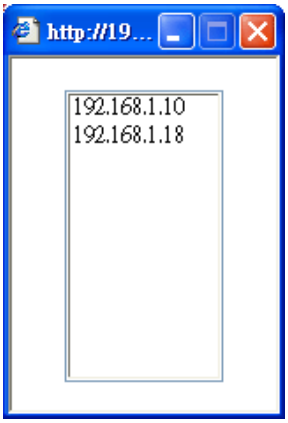
If you previously have set up **WAN Alias** for **PPPoE** or **Static or Dynamic IP** mode**,** you will find them in **Aux. WAN IP** for your selection.



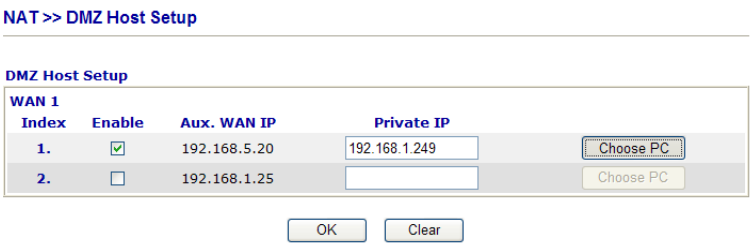
Enable Check to enable the DMZ Host function.

Private IP Enter the private IP address of the DMZ host, or click Choose PC to select one.

Choose PC Click this button and then a window will automatically pop up, as depicted below. The window consists of a list of private IP addresses of all hosts in your LAN network. Select one private IP address in the list to be the DMZ host.



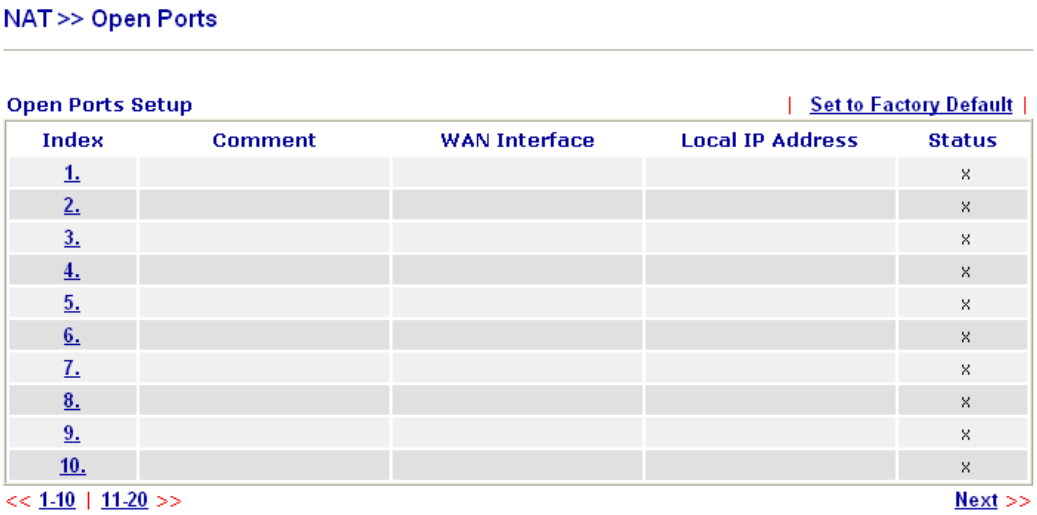
When you have selected one private IP from the above dialog, the IP address will be shown on the following screen. Click **OK** to save the setting.



5.3.3 Open Ports

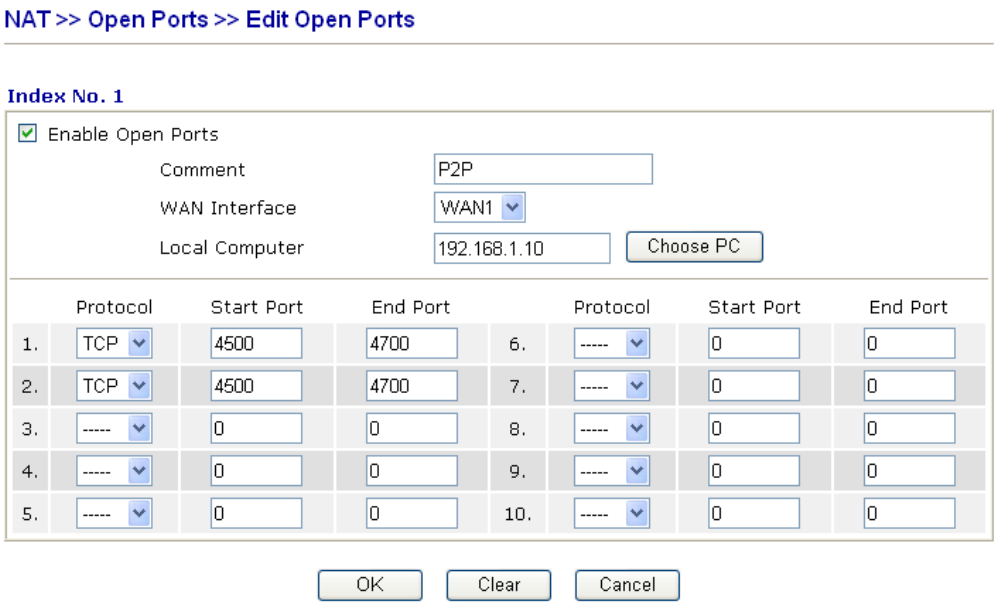
Open Ports allows you to open a range of ports for the traffic of special applications. Common application of Open Ports includes P2P application (e.g., BT, KaZaA, Gnutella, WinMX, eMule and others), Internet Camera etc. Ensure that you keep the application involved up-to-date to avoid falling victim 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.
WAN Interface	Display the WAN interface for the entry.
Local IP Address	Display the private IP address of the local host offering the service.
Status	Display the state for the corresponding entry. X or V is to represent the **Inactive** or **Active** state.

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



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

5.3.4 Address Mapping

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

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

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

NAT >> Address Mapping

Address Mapping Setup | Set to Factory Default |

Index	Protocol	Public IP	Private IP	Mask	Status
1.	ALL	0.0.0.0		/32	x
2.	ALL	0.0.0.0		/32	x
3.	ALL	0.0.0.0		/32	x
4.	ALL	0.0.0.0		/32	x
5.	ALL	0.0.0.0		/32	x
6.	ALL	0.0.0.0		/32	x
7.	ALL	0.0.0.0		/32	x
8.	ALL	0.0.0.0		/32	x
9.	ALL	0.0.0.0		/32	x
10.	ALL	0.0.0.0		/32	x

Protocol Display the protocol used for this address mapping.

Public IP Display the public IP address selected for this entry, e.g., 86.123.123.2.

Private IP Display the private IP set for this address mapping, e.g., 192.168.1.10

Mask Display the subnet mask selected fro this address mapping.

Status Display the status for the entry, enable or disable.

Click the index number link to open the configuration page.

NAT >> Address Mapping

Index No. 1

Enable

Protocol: ALL

WAN Interface: WAN1

WAN IP:

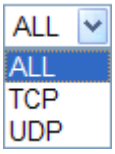
Private IP:

Subnet Mask: /32

OK Clear Cancel

Enable Check to enable this entry.

Protocol Specify the transport layer protocol. It could be **TCP**, **UDP**, or **ALL** for selection.



WAN Interface Specify the WAN interface that will be used for this entry.

WAN IP Select an IP address (the selections provided here are set in **IP Alias List** of **Network >>WAN** interface). Local host can use this IP to connect to Internet.

If you want to choose any on of the Public IP settings, you must specify some IP addresses in the IP Alias List of the Static/DHCP Configuration page first. If you did not type in any IP address in the IP Alias List, the Public IP setting will be empty in this field. When you click **Apply**, a message will appear to inform you.

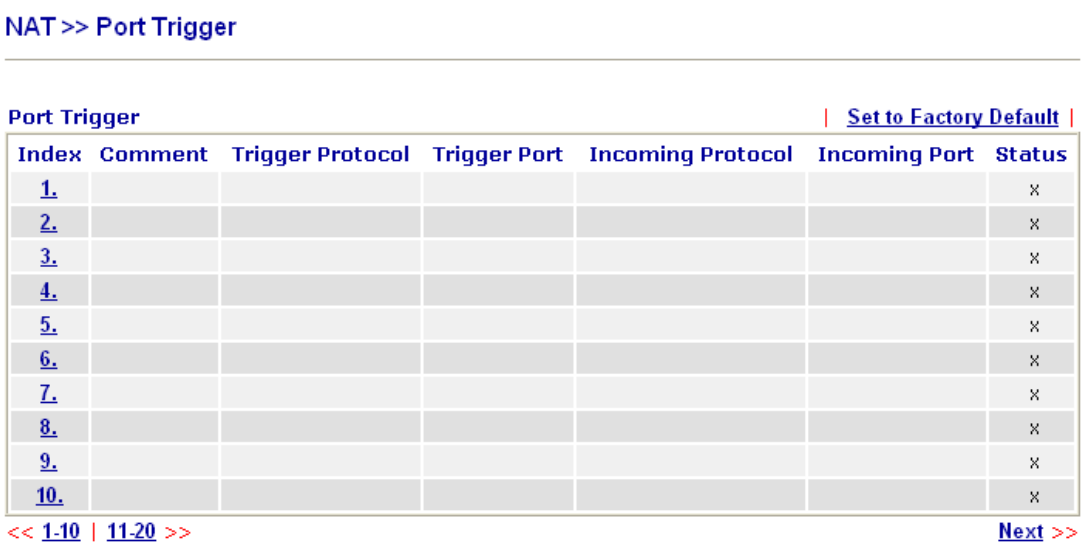
Private IP Assign an IP address (e.g., 192.168.1.10) or a subnet to be compared with the Public IP address for incoming packets.

Subnet Mask Select a value of subnet mask for private IP address.

5.3.5 Port Trigger

Port Trigger is a variation of open ports function; the difference is that the port trigger has the dynamic characteristics. It is more secure comparing to open ports.

In Open Ports setting, once we setup the ports be opened, all traffic can go through these open ports into LAN device; with Port Trigger function, the ports will be opened only when specific application triggers the specific ports, and then the needed ports will be opened automatically.



Comment Display the text which memorizes the application of this rule.

Trigger Protocol Display the protocol of the trigger packets.

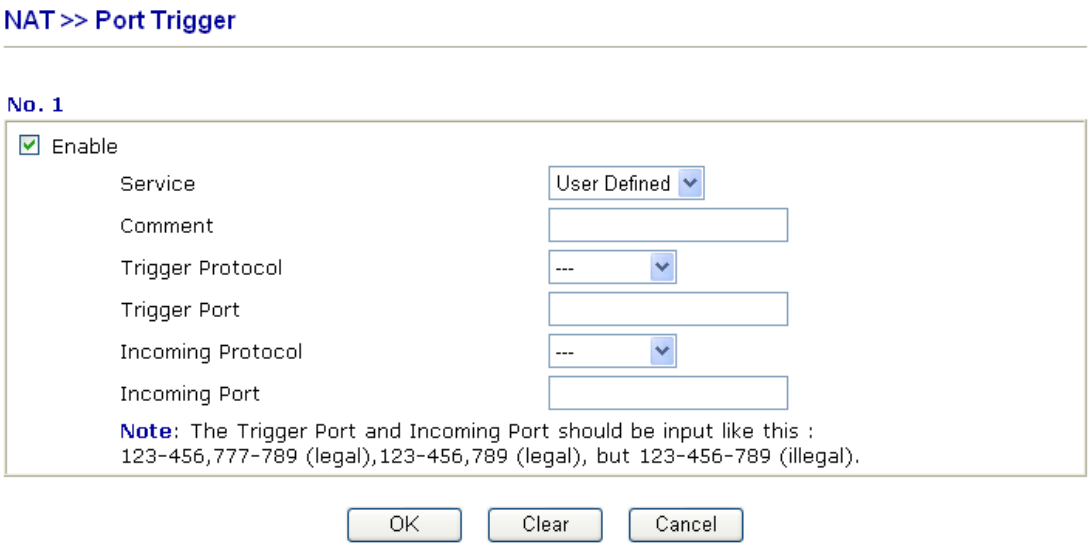
Trigger Port Display the port of the trigger packets.

Incoming Protocol Display the protocol for the incoming data of such trigger profile.

Incoming Port Display the port for the incoming data of such trigger profile.

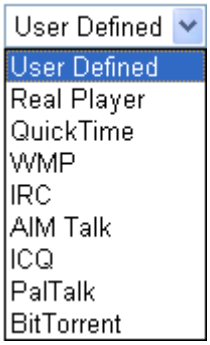
Status Display if the rule is active or de-active.

Click the index number link to open the configuration page.



Enable Check to enable this entry.

Service Choose the **predefined** service to apply for such trigger profile.



Comment Type the text to memorize the application of this rule.

Trigger Protocol Select the protocol (TCP, UDP or TCP/UDP) for such trigger profile.

Trigger Port Type the port or port range for such trigger profile.

Incoming Protocol When the trigger packets received, it is expected the incoming packets will use the selected protocol. Select the protocol (TCP, UDP or TCP/UDP) for the incoming data of such trigger profile.

Incoming Port Type the port or port range for the incoming packets.

5.4 Firewall

5.4.1 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:

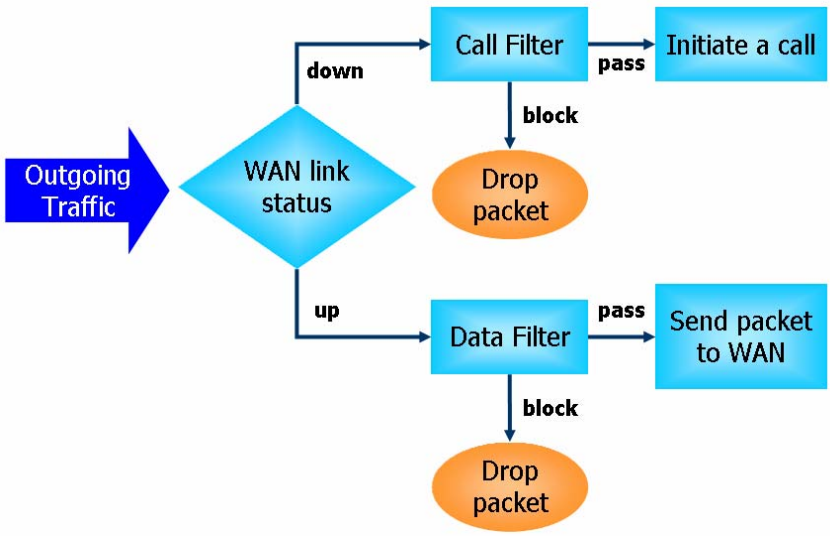
- User-configurable IP filter (Call Filter/ Data Filter).
- Stateful Packet Inspection (SPI): tracks packets and denies unsolicited incoming data
- Selectable Denial of Service (DoS) /Distributed DoS (DDoS) attacks protection

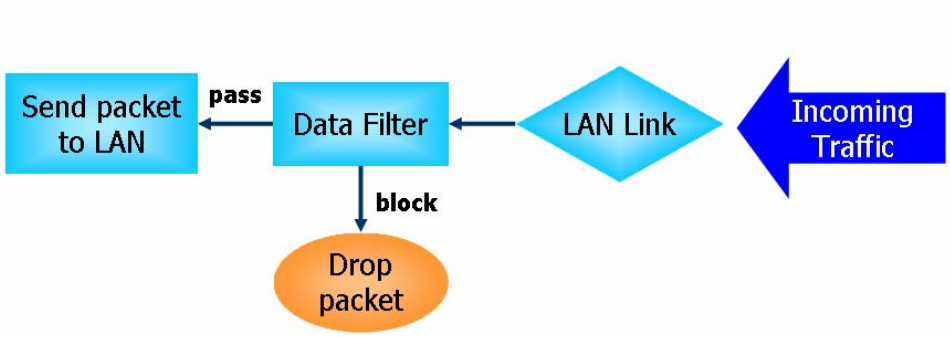
IP Filters

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:

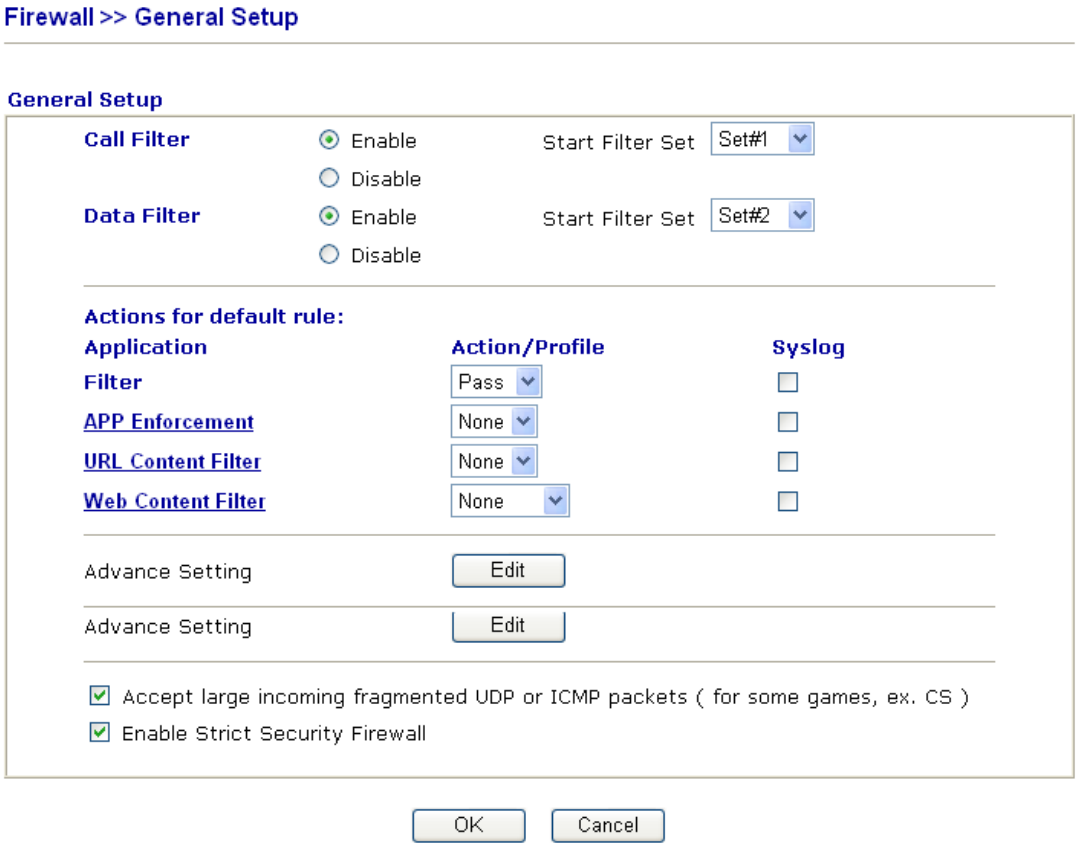
1. SYN flood attack
2. UDP flood attack
3. ICMP flood attack
4. Port Scan attack
5. IP options
6. Land attack
7. Smurf attack
8. Trace route
9. SYN fragment
10. Fraggle attack
11. TCP flag scan
12. Tear drop attack
13. Ping of Death attack
14. ICMP fragment
15. Unknown protocol

Below shows the menu items for Firewall.

5.4.2 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, and **Accept large incoming fragmented UDP or ICMP 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.
Action/Profile	Select **Pass** or **Block** for the packets that do not match with the filter rules.
IM/P2P Filter	Select one of the **APP Enforcement Profile** settings (created in **CSM>> APP Enforcement Profile**) for applying with this router. Please set at least one profile for choosing in **CSM>> APP Enforcement Profile Profile** web page first. For troubleshooting needs, you can specify to record information for **APP Enforcement Profile** by checking the Log box. It will be sent to Syslog server. Please refer to section **Syslog/Mail Alert** for more detailed information.
URL Content Filter	Select one of the **URL Content Filter Profile** settings (created in **CSM>> URL Content Filter Profile**) for applying with this router. Please set at least one profile for choosing in **CSM>> URL Content Filter Profile** web page first. For troubleshooting needs,

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

Web Content Filter

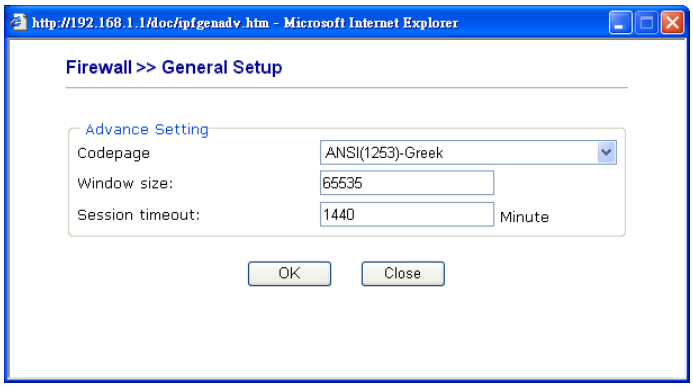
Select one of the **Web Content Filter Profile** settings (created in **CSM>> Web Content Filter Profile**) for applying with this router. Please set at least one profile for anti-virus in **CSM>> Web Content Filter Profile** web page first. For troubleshooting needs, you can specify to record information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

Syslog

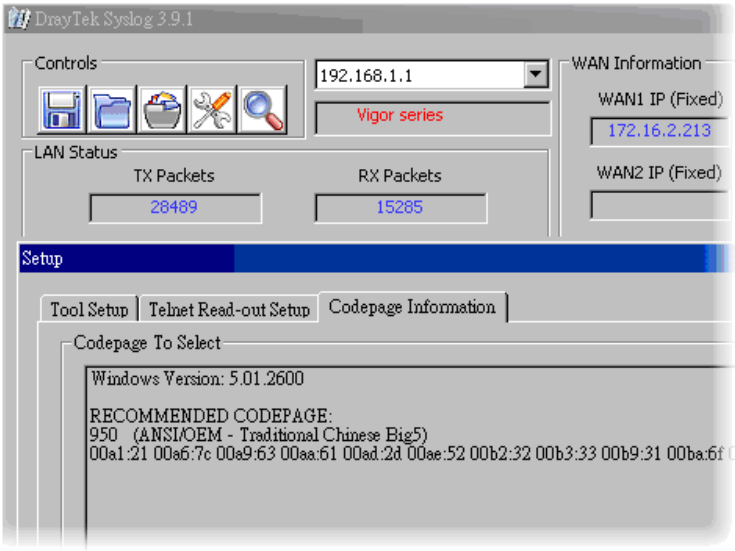
For troubleshooting needs you can specify the filter log and/or CSM log here by checking the box. The log will be displayed on Draytek Syslog window.

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.



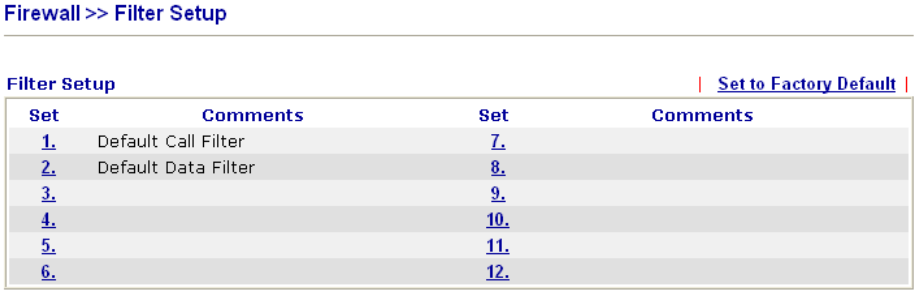
Window size – It determines the size of TCP protocol (0~65535). The more the value is, the better the performance will be. However, if the network is not stable, small value will be proper.

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.

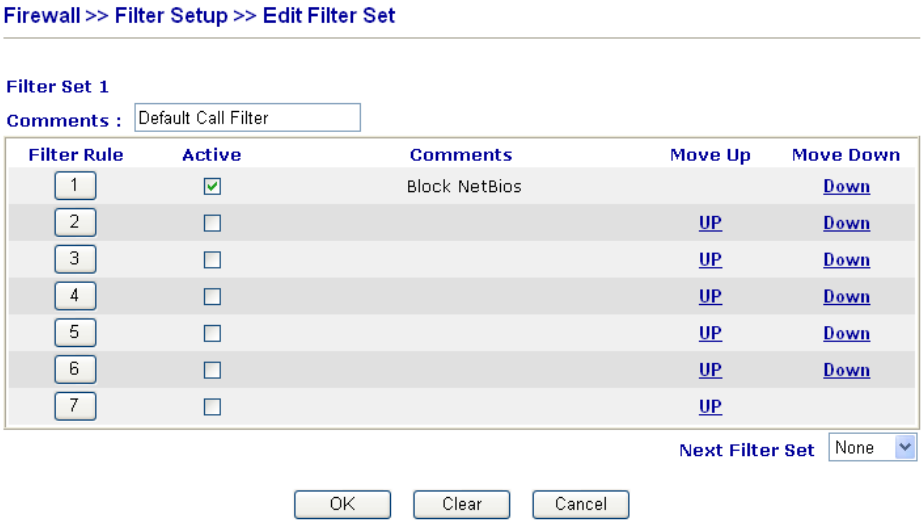
Accept large incoming..	Some on-line games (for example: Half Life) will use lots of fragmented UDP packets to transfer game data. Instinctively as a secure firewall, Vigor router will reject these fragmented packets to prevent attack unless you enable "**Accept large incoming fragmented UDP or ICMP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

5.4.3 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.

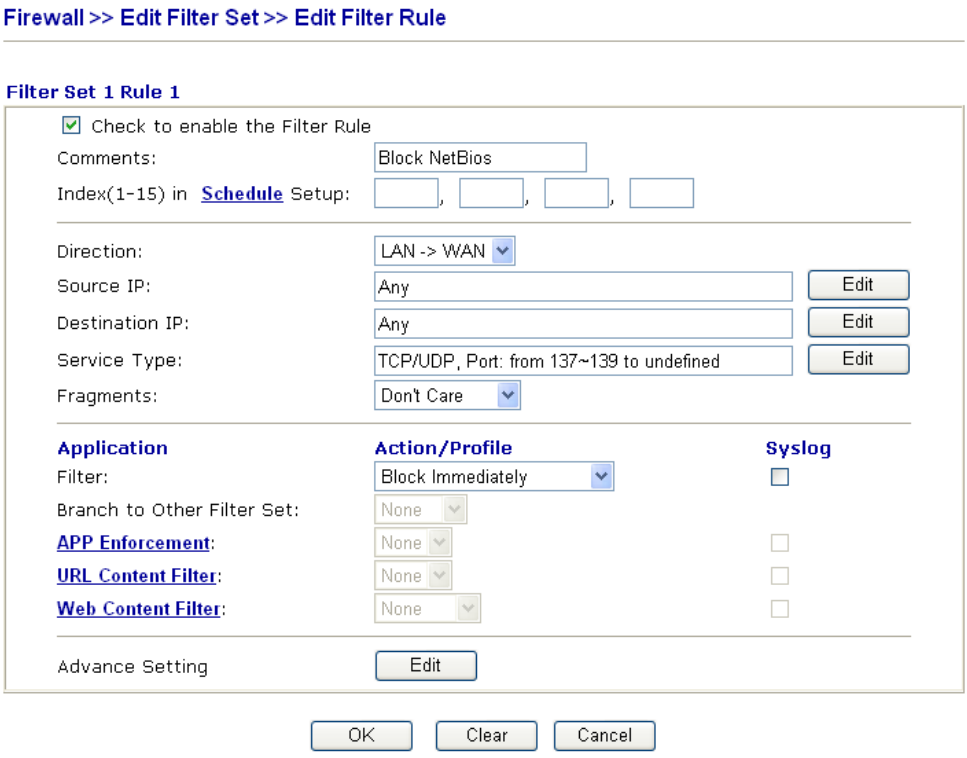
Active Enable or disable the filter rule.

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.



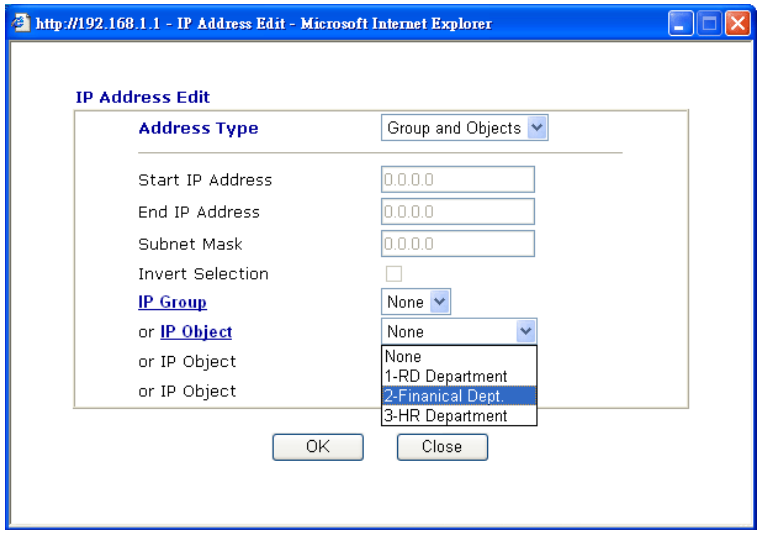
Check to enable the Filter Rule Check this box to enable the filter rule.

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

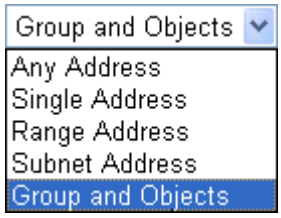
Index(1-15) Set PCs on LAN to work at certain time interval only. You may choose up to 4 schedules out of the 15 schedules pre-defined in **Applications >> Schedule** setup. The default setting of this filed is blank and the function will always work.

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.

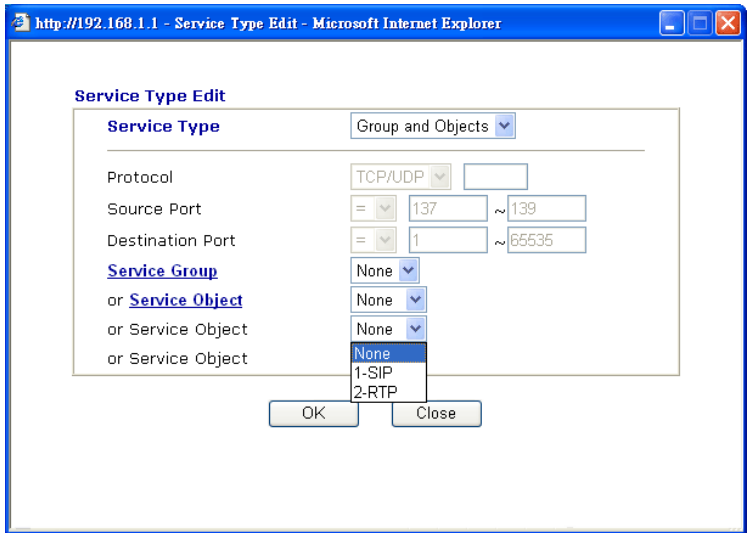


To set the IP address manually, please choose **Any Address/Single Address/Range Address/Subnet Address** as the Address Type and type them in this dialog. In addition, if you want to use the IP range from defined groups or objects, please choose **Group and Objects** as the Address Type.

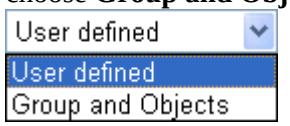


From the **IP Group** drop down list, choose the one that you want to apply. Or use the **IP Object** drop down list to choose the object that you want.

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.

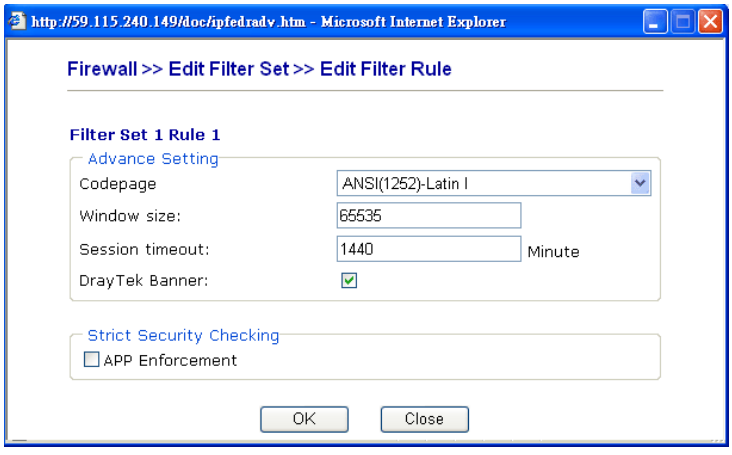
APP Enforcement — Select one of the **APP Enforcement Profile** settings (created in **CSM>> APP Enforcement Profile**) for applying with this router. Please set at least one profile for choosing in **CSM>> APP Enforcement Profile** web page first. For troubleshooting needs, you can specify to record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

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.

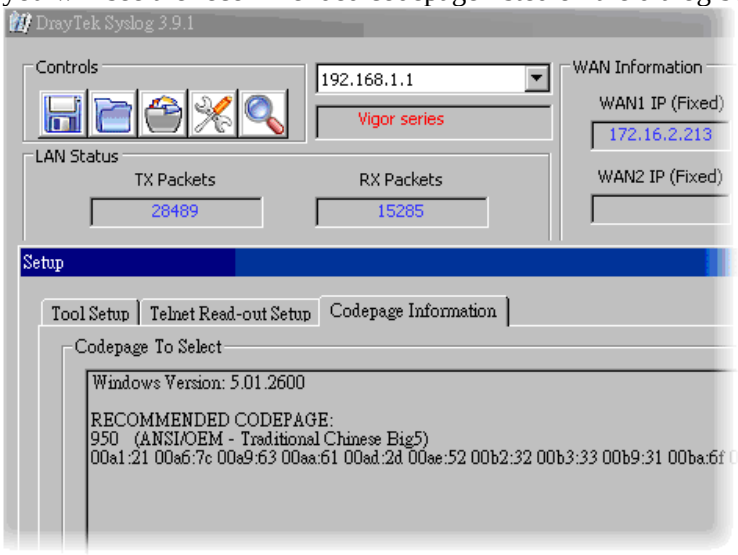
SysLog — For troubleshooting needs you can specify the filter log and/or CSM log here. Check the corresponding box to enable the log function. Then, the filter log and/or CSM log will be shown on Draytek Syslog window.

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

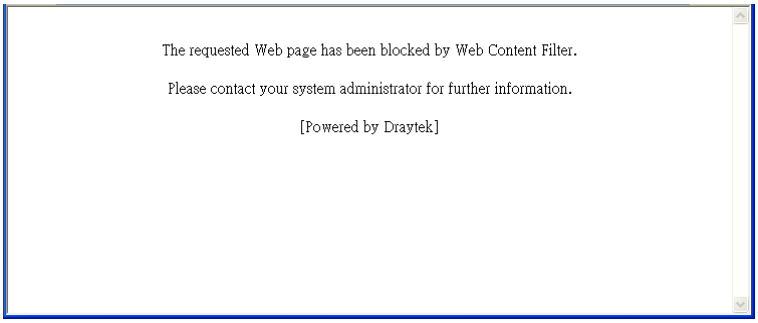
URL and enhance the correctness of URL Content Filter. The default value for this setting is ANSI 1252 Latin I. If you do not choose any codepage, no decoding job of URL will be processed. Please use the drop-down list to choose a codepage.
If you do not have any idea of choosing suitable codepage, please 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.

DrayTek Banner – Please uncheck this box and the following screen will not be shown for the unreachable web page. The default setting is Enabled.



Strict Security Checking - All the packets, while transmitting through Vigor router, will be filtered by firewall settings configured by Vigor router if Strict Security Firewall is enabled. If the firewall system does not have any response (pass or block) for these packets, such as no response coming from Anti-Spam server, then the router's firewall will block the packets directly.

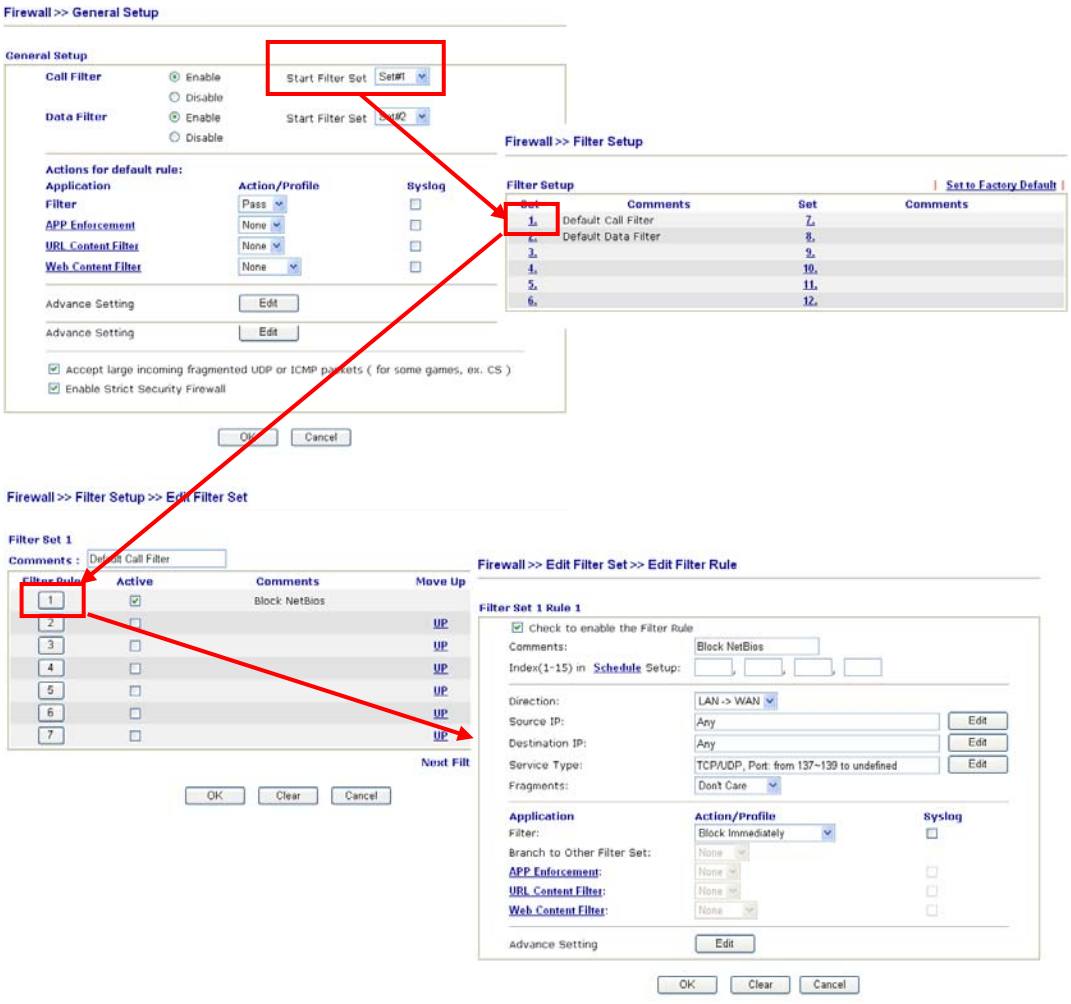
In addition, you can restrict the strict security checking just be done by specified server and conditions such as APP Enforcement. Thus, the packets not only must be filtered by

general rules by Firewall, but also must be filtered by the items selected in Strict Security Checking. Such work can ensure the data security transferring via network.

APP Enforcement – Check this box to execute the critical checking for all the files transferred via IM/P2P.

Example

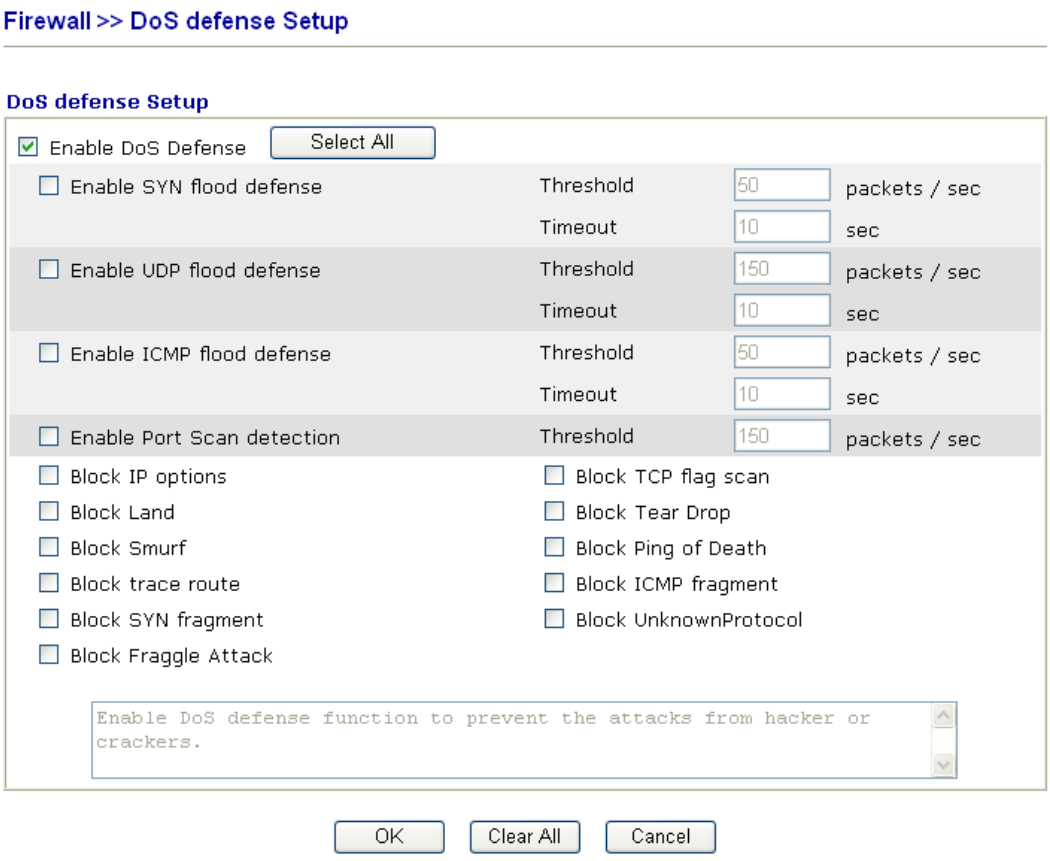
As stated before, all the traffic will be separated and arbitrated using on of two IP filters: call filter or data filter. You may preset 12 call filters and data filters in **Filter Setup** and even link them in a serial manner. Each filter set is composed by 7 filter rules, which can be further defined.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



5.4.4 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. **Select All** - Check this box to select all of the items listed below.
Enable SYN flood defense	Check the box to activate the SYN flood defense function. Once detecting the Threshold of the TCP SYN packets from the Internet has exceeded the defined value, the Vigor router will start to randomly discard the subsequent TCP SYN packets for a period defined in Timeout. The goal for this is prevent the TCP SYN packets' attempt to exhaust the limited-resource of Vigor router. By default, the threshold and timeout values are set to 50 packets per second and 10 seconds, respectively.
Enable UDP flood defense	Check the box to activate the UDP flood defense function. Once detecting the Threshold of the UDP packets from the Internet has exceeded the defined value, the Vigor router will start to randomly discard the subsequent UDP packets for a period defined in Timeout. The default setting for threshold and timeout are 150 packets per second and 10 seconds, respectively.
Enable ICMP flood defense	Check the box to activate the ICMP flood defense function. Similar to the UDP flood defense function, once if the Threshold of ICMP packets from Internet has exceeded the defined value, the router will discard the ICMP echo requests coming from the Internet. The

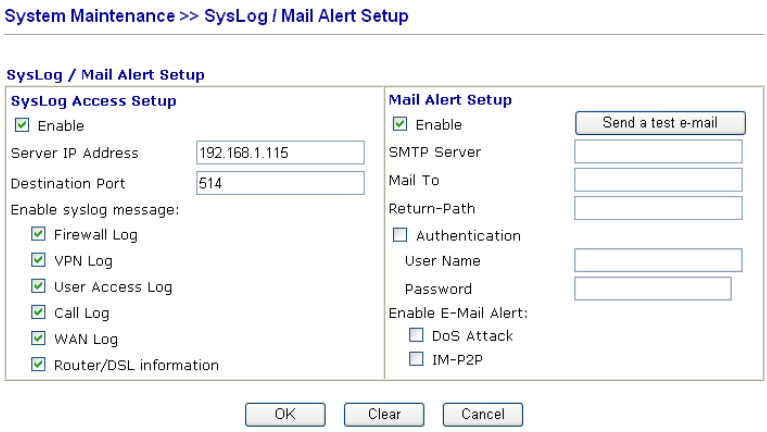
	default setting for threshold and timeout are 50 packets per second and 10 seconds, respectively.
Enable PortScan detection	Port Scan attacks the Vigor router by sending lots of packets to many ports in an attempt to find ignorant services would respond. Check the box to activate the Port Scan detection. Whenever detecting this malicious exploration behavior by monitoring the port-scanning Threshold rate, the Vigor router will send out a warning. By default, the Vigor router sets the threshold as 150 packets per second.
Block IP options	Check the box to activate the Block IP options function. The Vigor router will ignore any IP packets with IP option field in the datagram header. The reason for limitation is IP option appears to be a vulnerability of the security for the LAN because it will carry significant information, such as security, TCC (closed user group) parameters, a series of Internet addresses, routing messages...etc. An eavesdropper outside might learn the details of your private networks.
Block Land	Check the box to enforce the Vigor router to defense the Land attacks. The Land attack combines the SYN attack technology with IP spoofing. A Land attack occurs when an attacker sends spoofed SYN packets with the identical source and destination addresses, as well as the port number to victims.
Block Smurf	Check the box to activate the Block Smurf function. The Vigor router will ignore any broadcasting ICMP echo request.
Block trace router	Check the box to enforce the Vigor router not to forward any trace route packets.
Block SYN fragment	Check the box to activate the Block SYN fragment function. The Vigor router will drop any packets having SYN flag and more fragment bit set.
Block Fraggle Attack	Check the box to activate the Block fraggle Attack function. Any broadcast UDP packets received from the Internet is blocked. Activating the DoS/DDoS defense functionality might block some legal packets. For example, when you activate the fraggle attack defense, all broadcast UDP packets coming from the Internet are blocked. Therefore, the RIP packets from the Internet might be dropped.
Block TCP flag scan	Check the box to activate the Block TCP flag scan function. Any TCP packet with anomaly flag setting is dropped. Those scanning activities include *no flag scan*, *FIN without ACK scan*, *SYN FINscan*, *Xmas scan* and *full Xmas scan*.
Block Tear Drop	Check the box to activate the Block Tear Drop function. Many machines may crash when receiving ICMP datagrams (packets) that exceed the maximum length. To avoid this type of attack, the Vigor router is designed to be capable of discarding any fragmented ICMP packets with a length greater than 1024 octets.
Block Ping of Death	Check the box to activate the Block Ping of Death function. This attack involves the perpetrator sending overlapping packets to the target hosts so that those target hosts will hang once they re-construct the packets. The Vigor routers will block any packets realizing this attacking activity.

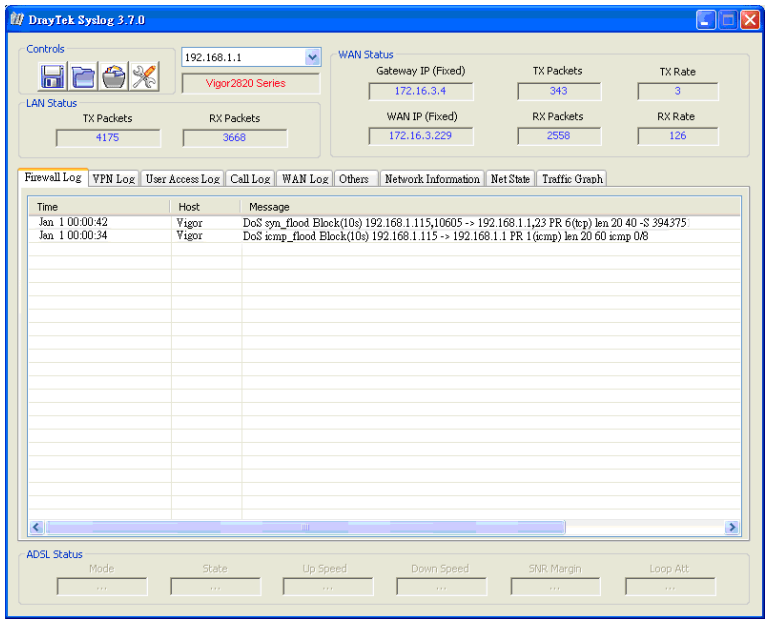
Block ICMP Fragment Check the box to activate the Block ICMP fragment function. Any ICMP packets with more fragment bit set are dropped.

Block 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.

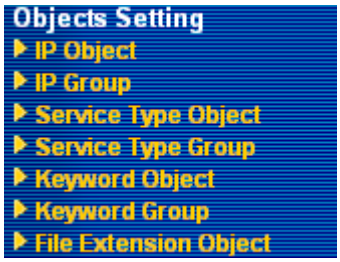
All the warning messages related to **DoS Defense** will be sent to user and user can review it through Syslog daemon. Look for the keyword **DoS** in the message, followed by a name to indicate what kind of attacks is detected.





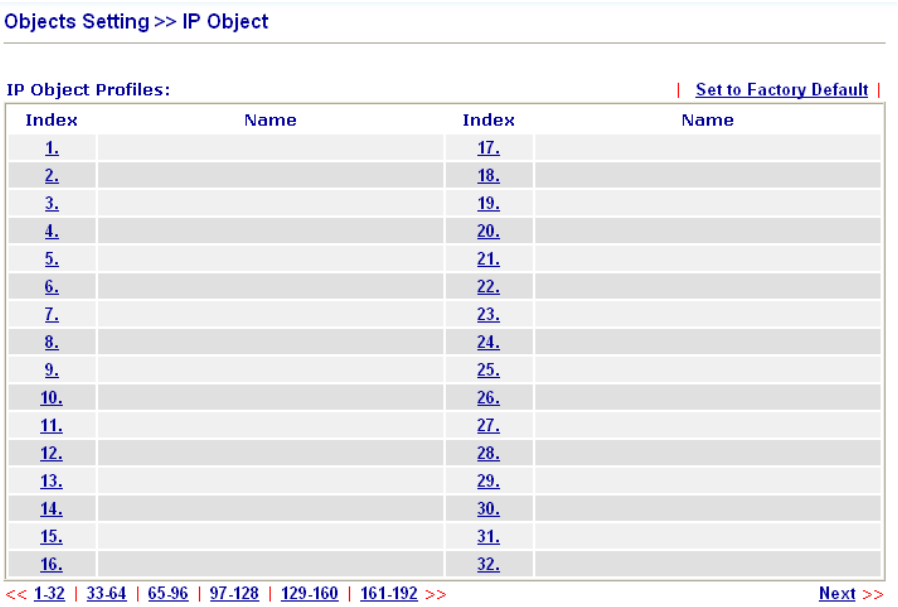
5.5 Objects Settings

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).



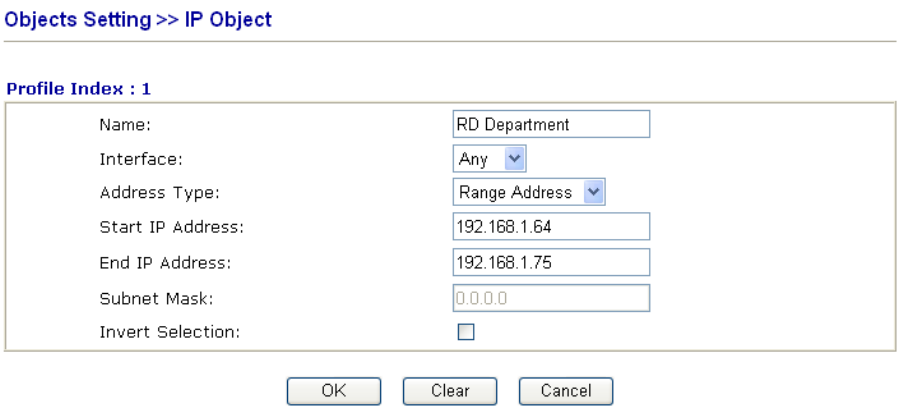
5.5.1 IP Object

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



Set to Factory Default Clear all profiles.

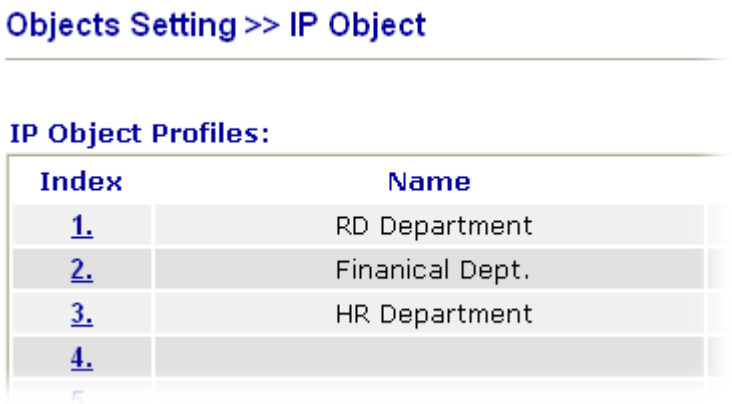
Click the number under Index column for settings in detail.



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

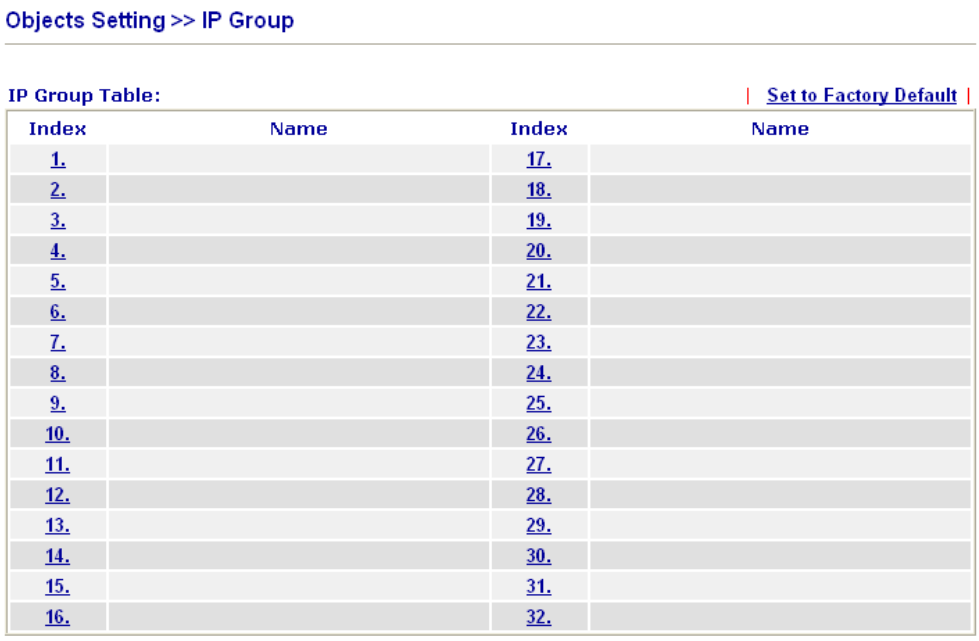
Interface	Choose a proper interface (WAN, LAN or Any). For example, the **Direction** setting in **Edit Filter Rule** will ask you specify IP or IP range for WAN or LAN or any IP address. If you choose LAN as the **Interface** here, and choose LAN as the direction setting in **Edit Filter Rule**, then 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.



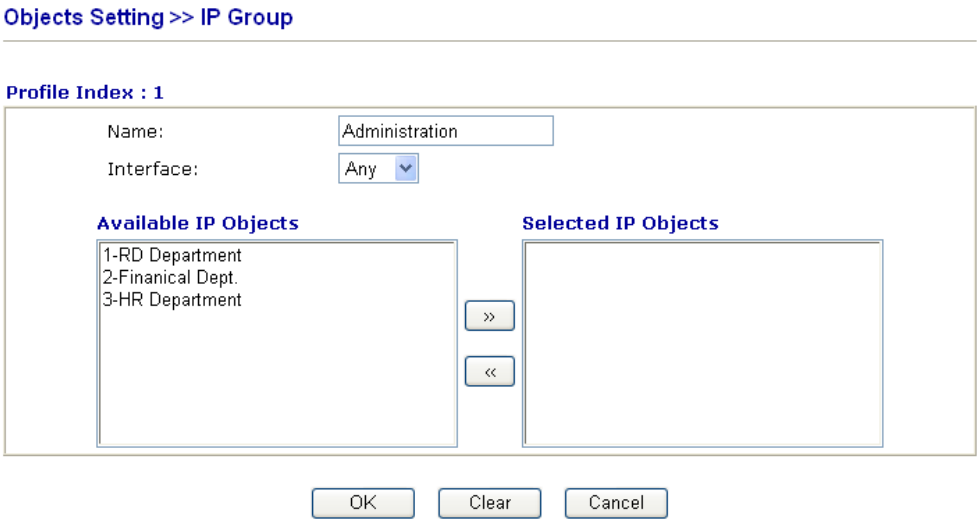
5.5.2 IP Group

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.

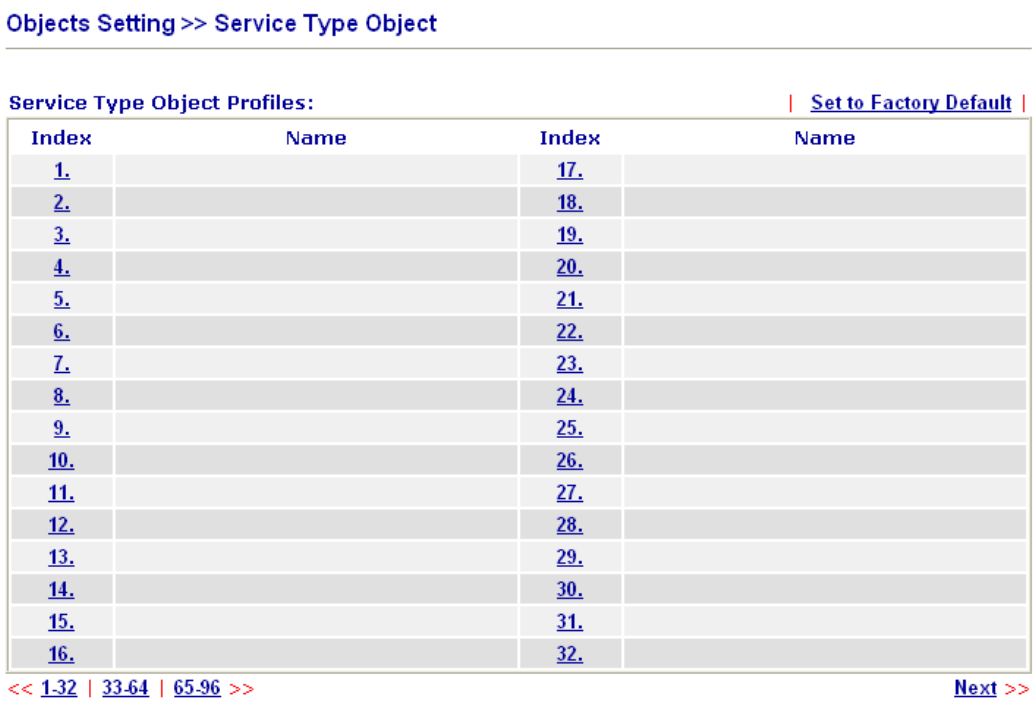
Interface Choose WAN, LAN or Any to display all the available IP objects with the specified interface.

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.

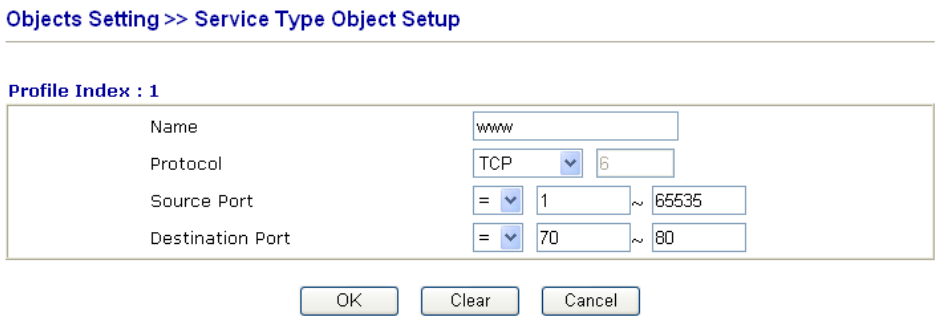
5.5.3 Service Type Object

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



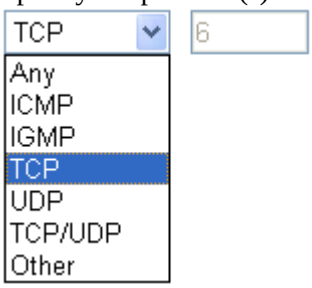
Set to Factory Default Clear all profiles.

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.

Service Type Object Profiles:

Index	Name
1.	SIP
2.	RTP
3.	
4.	

5.5.4 Service Type Group

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

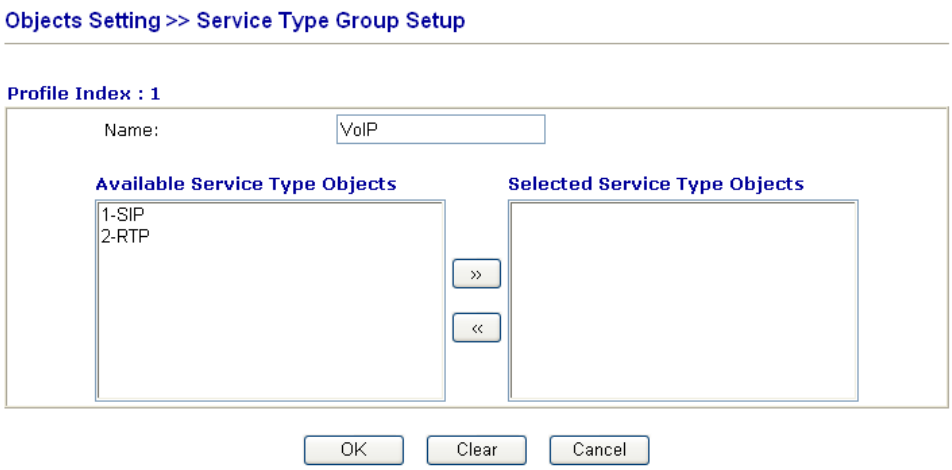
Objects Setting >> Service Type Group

Service Type Group Table: | Set to Factory Default |

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

Set to Factory Default Clear all profiles.

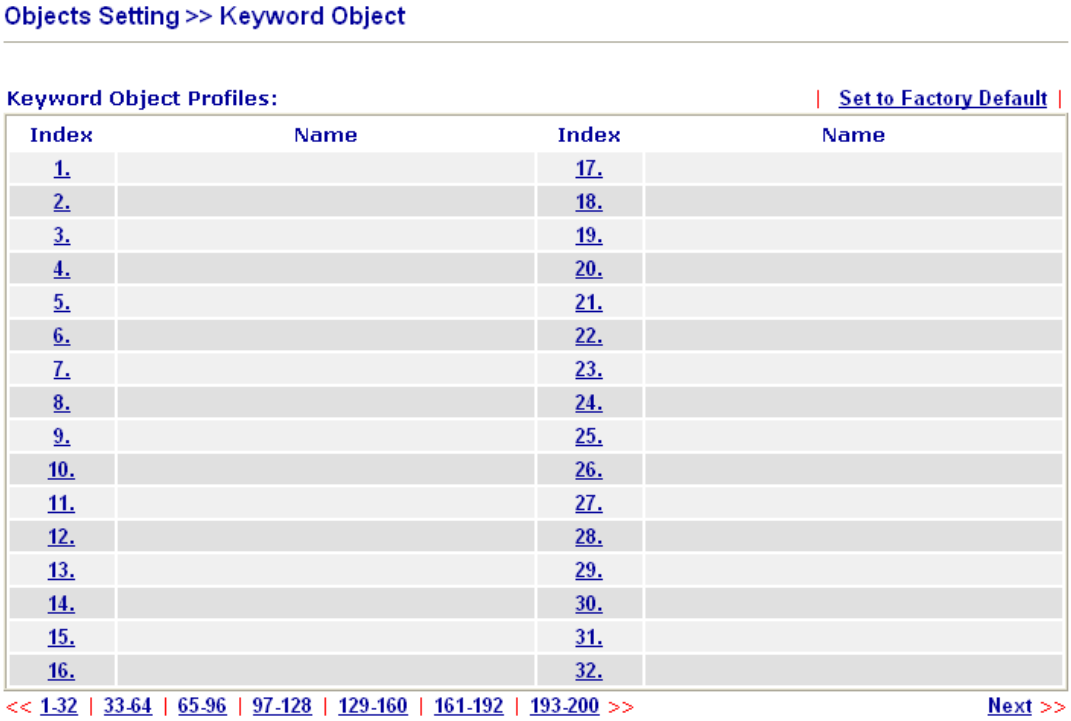
Click the number under Index column for settings in detail.



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.

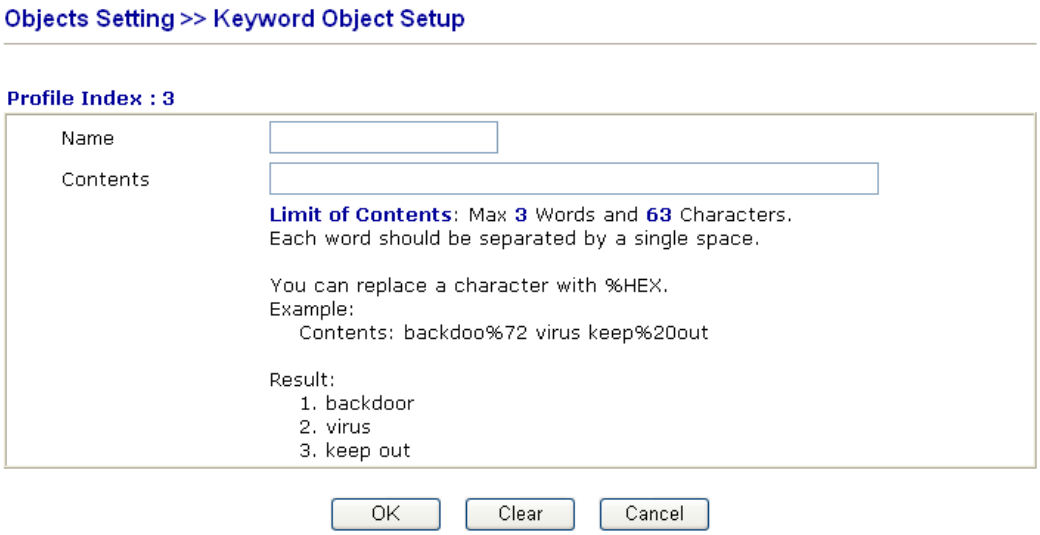
5.5.5 Keyword Object

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.

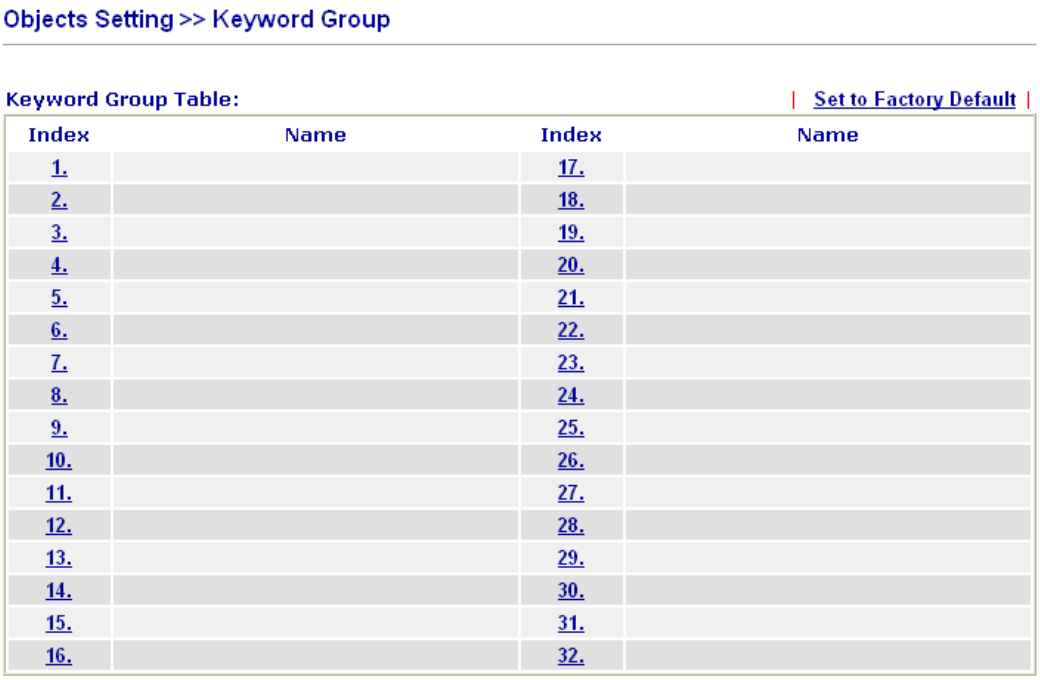
Click the number under Index column for setting in detail.



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.

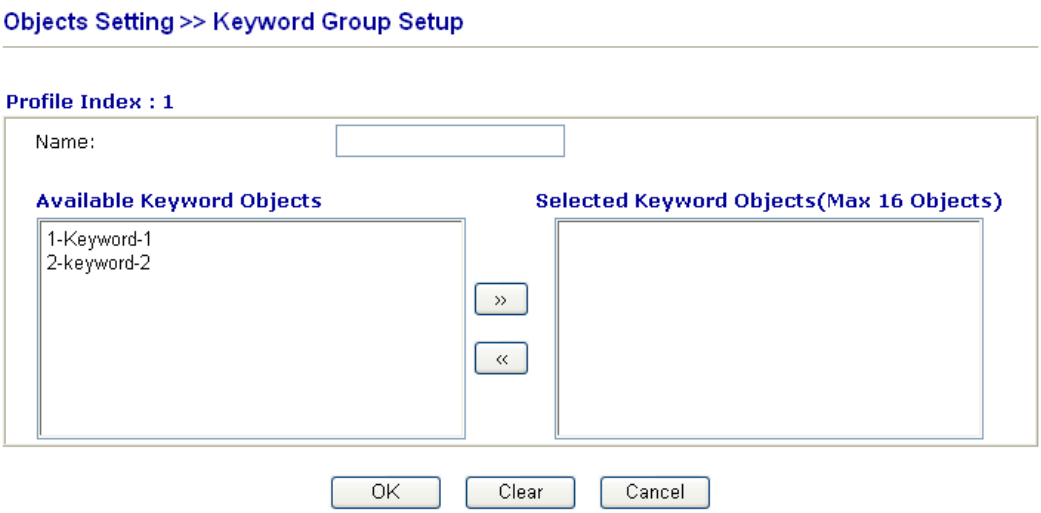
5.5.6 Keyword Group

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.

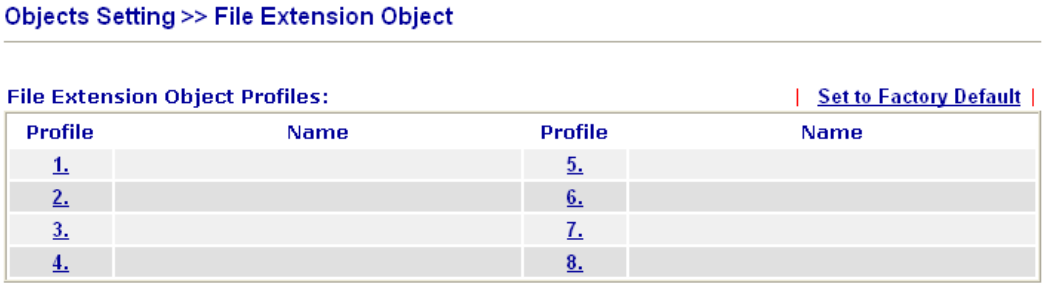


Name	Type a name for this group.
Available Keyword Objects	You can gather keyword objects from Keyword Object page within one keyword group. All the available Keyword objects that you have created will be shown in this box.
Selected Keyword Objects	Click » button to add the selected Keyword objects in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

5.5.7 File Extension Object

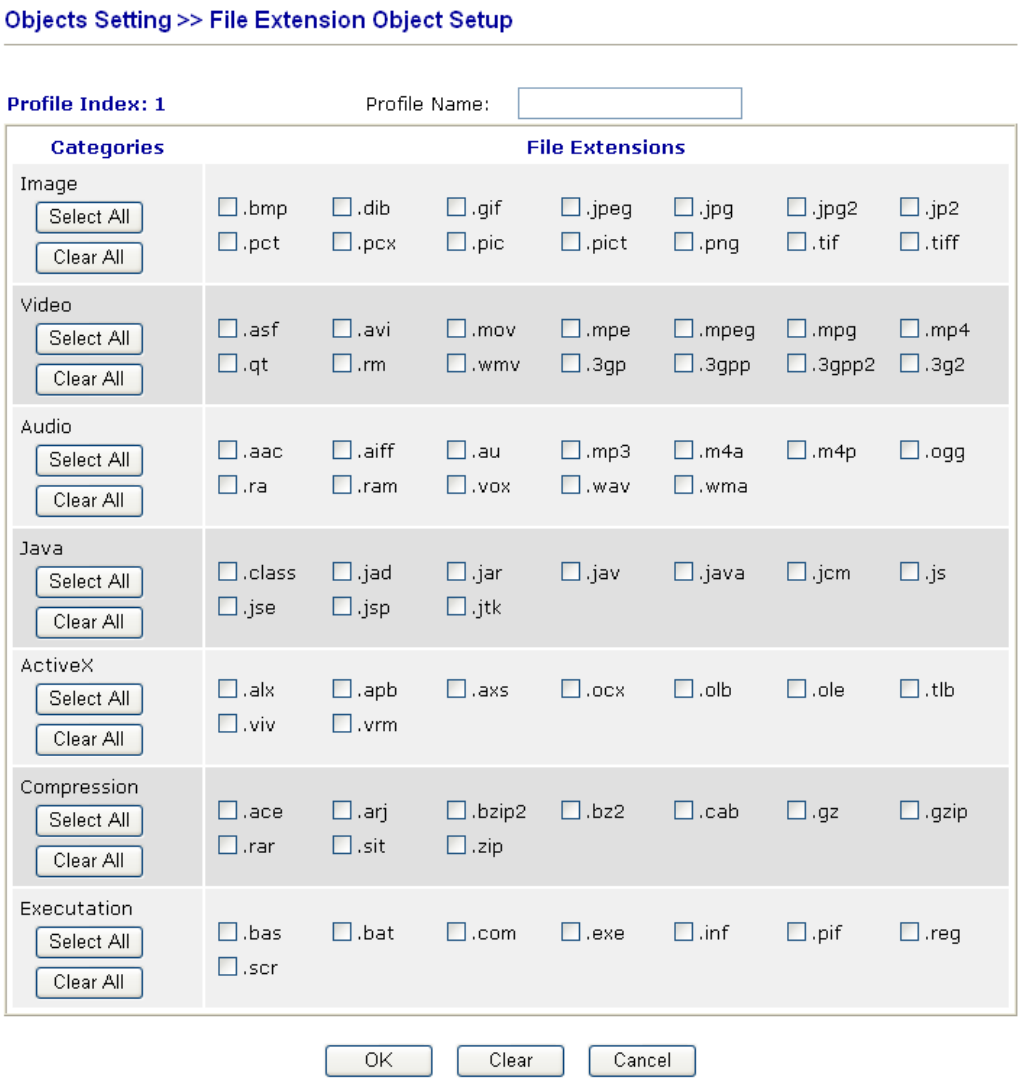
This page allows you to set eight profiles which will be applied in **CSM>>URL Content Filter**. All the files with the extension names specified in these profiles will be processed according to the chosen action.

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.

5.6 CSM

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

IM/P2P Filter

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

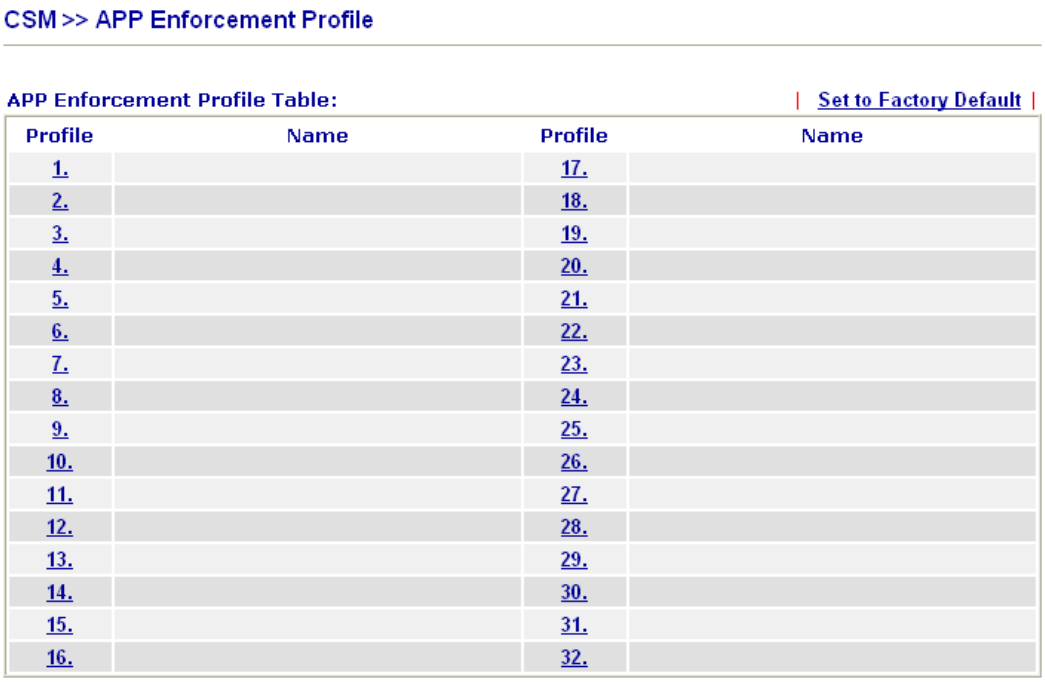
We all know that the content on the Internet just like other types of media may be inappropriate sometimes. As a responsible parent or employer, you should protect those in your trust against the hazards. With Web filtering service of the Vigor router, you can protect your business from common primary 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.

5.6.1 APP Enforcement Profile

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



Set to Factory Default Clear all profiles.

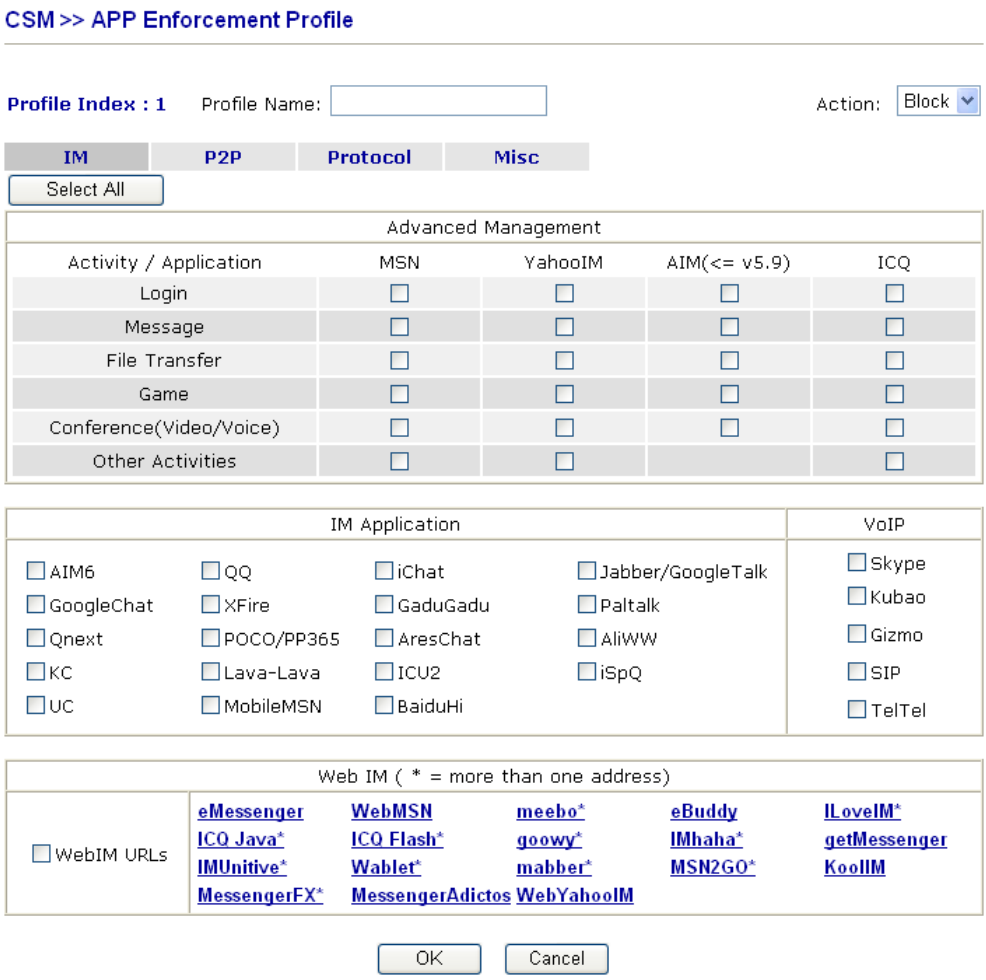
Profile Display the number of the profile which allows you to click to set different policy.

Name Display the name of the APP Enforcement Profile.

Click the number under Index column for settings in detail.

There are four tabs IM, P2P, Protocol and Misc displayed on this page. Each tab will bring out different items that you can choose to disallow people using.

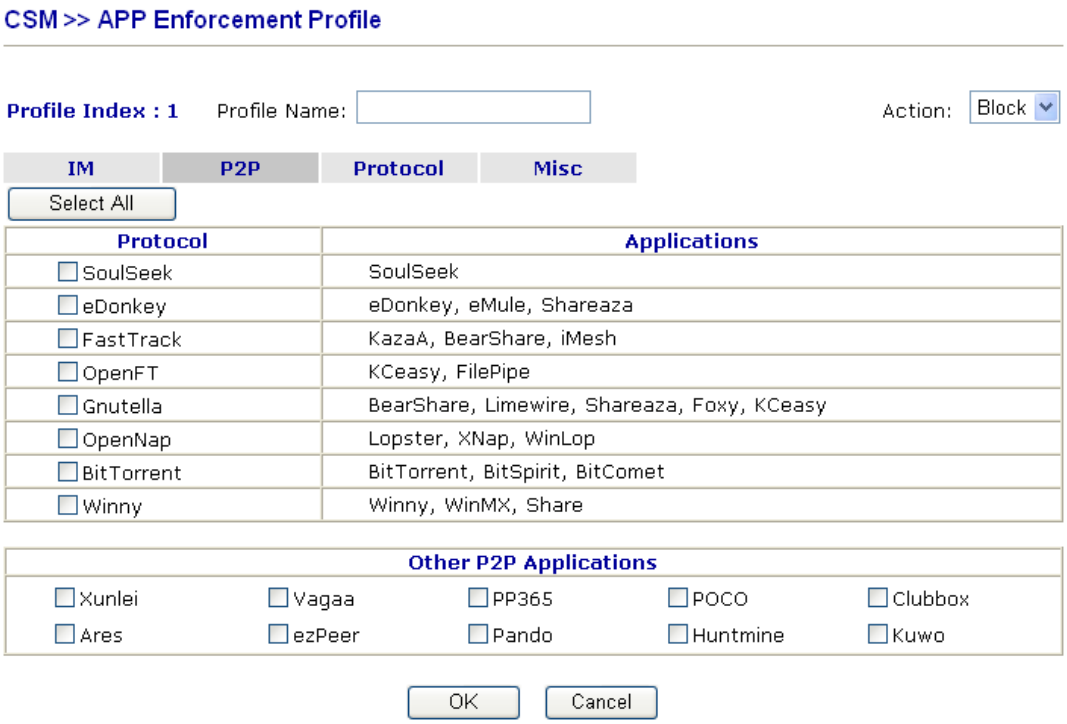
Below shows the items which are categorized under **IM**.



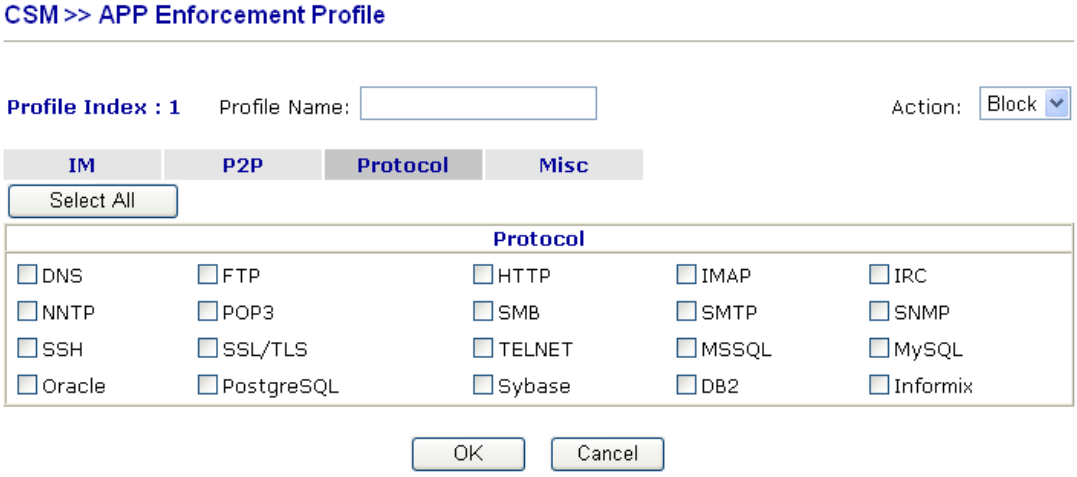
Profile Name	Type a name for the CSM profile.
Action	**Block –** All the items selected in this page will be blocked. Users will not access into related web pages or use the applications. **Pass –** All the items selected in this page will not be blocked. User can access into related web pages or use the applications.
Select All	Click it to choose all of the items in this page.

The profiles configured here can be applied in the **Firewall>>General Setup** and **Firewall>>Filter Setup** pages as the standard for the host(s) to follow.

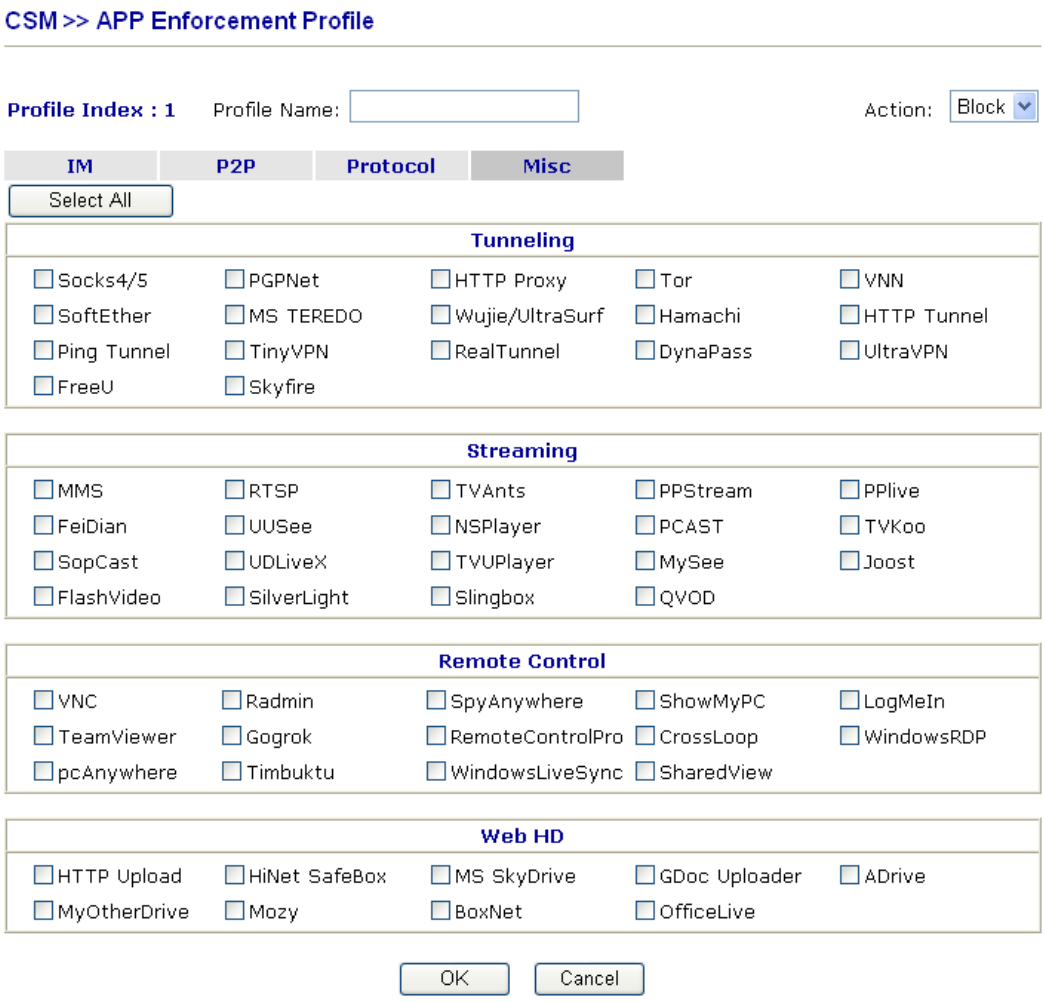
Below shows the items which are categorized under **P2P.**



The items categorized under **Protocol** -----



The items categorized under **Misc** -----



5.6.2 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.

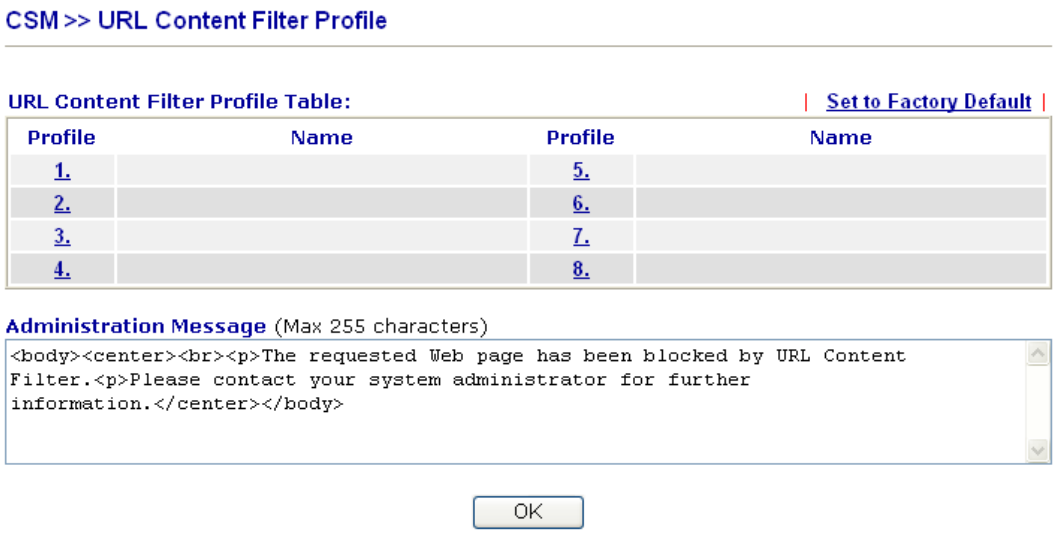
Once a user type in or click on an URL with objectionable keywords, URL keyword blocking facility will decline the HTTP request to that web page thus can limit user's access to the website. You may imagine **URL Content Filter** as a well-trained convenience-store clerk who won't sell adult magazines 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.

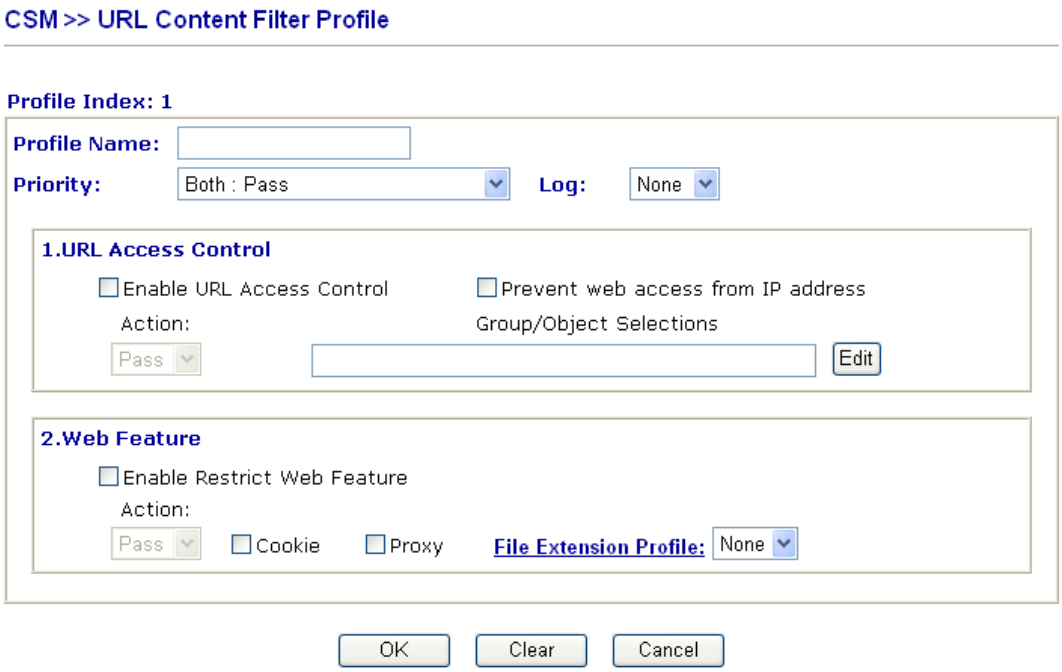
For example, if you add key words such as "sex", Vigor router will limit web access to web sites or web pages such as "www.sex.com", "www.backdoor.net/images/sex/p_386.html". Or you may simply specify the full or partial URL such as "www.sex.com" or "sex.com".

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.

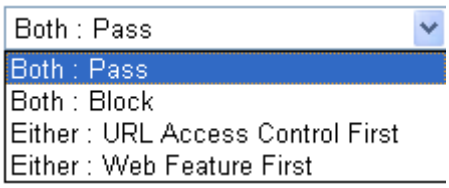


You can set eight profiles as URL content filter. Simply click the index number under Profile to open the following web page.



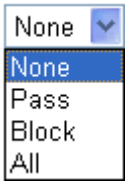
Profile Name Type the name for such profile.

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://202.6.5.2. 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.

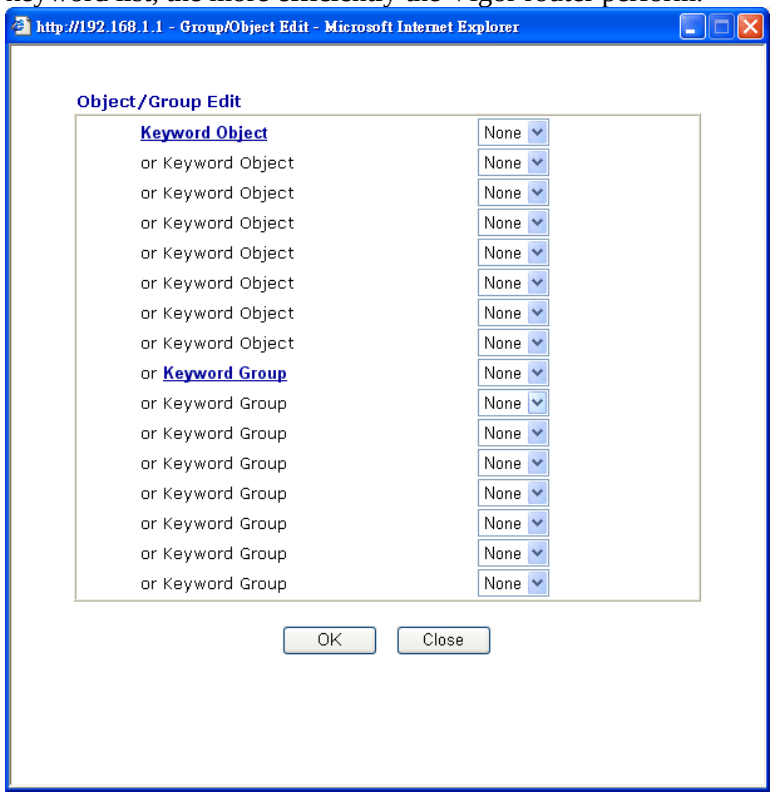
Action – This setting is available only when **Either : URL Access Control First** or **Either : Web Feature First** is selected. ***Pass*** - Allow accessing into the corresponding webpage with the keywords listed on the box below.

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

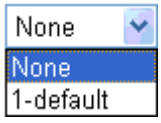
Enable Restrict Web Feature - Check this box to make the keyword being blocked or passed.

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.



5.6.3 Web Content Filter Profile

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

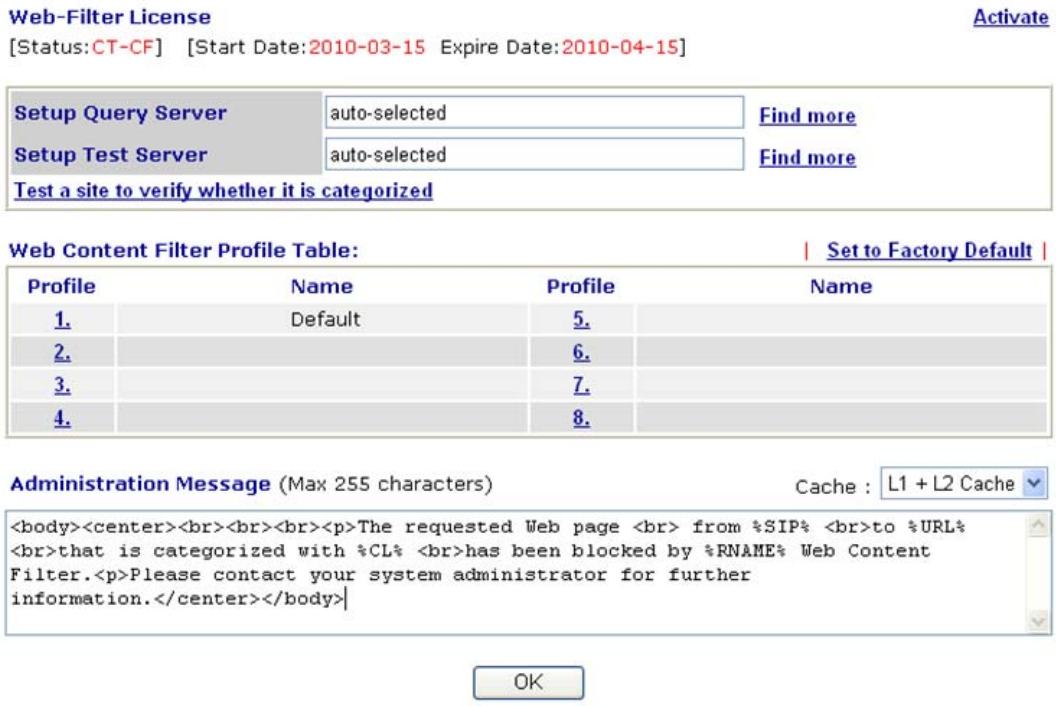
Service Activation Wizard allows you to use trial version or update the license of WCF directly without accessing into the server (***MyVigor***) located on http://myvigor.draytek.com.

However, if you use the **Web Content Filter Profile** page to activate WCF feature, it is necessary for you to access into the server (***MyVigor***) located on http://myvigor.draytek.com. Therefore, you need to register an account on http://myvigor.draytek.com for using corresponding service. Please refer to section **4.8** for more information of creating MyVigor account.

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

WCF adopts the mechanism developed and offered by certain service provider (e.g., DrayTek). No matter activating WCF feature or getting a new license for web content filter, you have to click **Activate** to satisfy your request. Be aware that service provider matching with VigorIPPBX 3510 currently offers a period of time for trial version for users to experiment. If you want to purchase a formal edition, simply contact with the channel partner or your dealer.

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

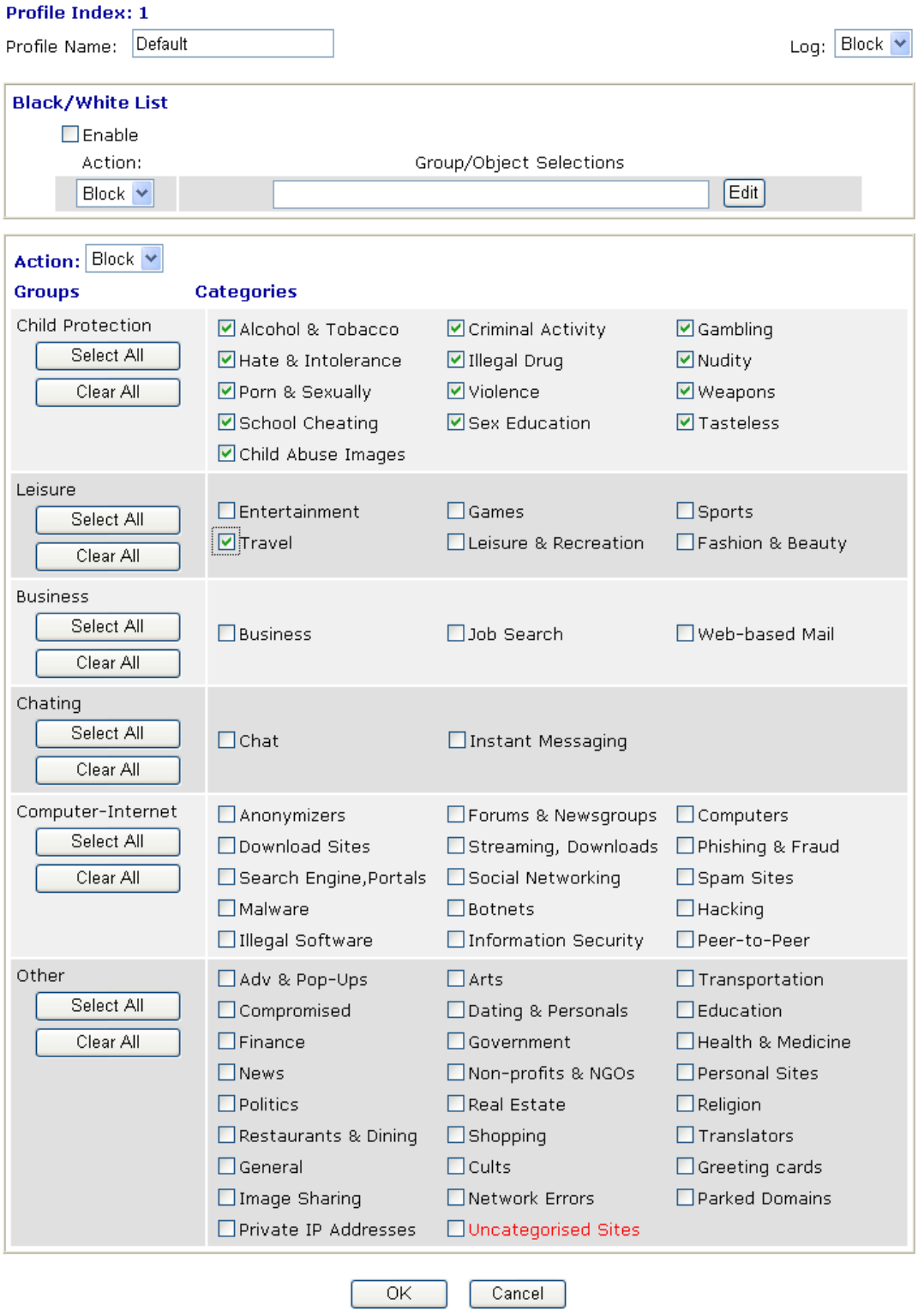


Activate Click it to access into MyVigor for activating WCF service.

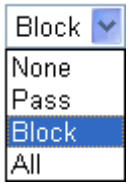
Setup Query Server It is recommend for you to use the default setting, auto-selected. You need to specify a server for categorize searching when you

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

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



Profile Name Type a name for such profile.

Log	**None** – There is no log file will be recorded for this profile. **Pass** – Only the log about Pass will be recorded in Syslog. **Block** – Only the log about Block will be recorded in Syslog. **All** – All the actions (Pass and Block) will be recorded in Syslog. 
White/Black List	**Enable –** Activate white/black list function for such profile. **Group/Object Selections –** Type the characters here as the content of white/black list. **Pass** - **allow** accessing into the corresponding webpage with the characters listed on **Group/Object Selections**. If the web pages do not match with the specified feature set here, they will be processed with the categories listed on the box below. **Block** - **restrict** accessing into the corresponding webpage with the characters listed on **Group/Object Selections**. If the web pages do not match with the specified feature set here, they will be processed with the categories listed on the box below.
Action	**Pass** - allow accessing into the corresponding webpage with the categories listed on the box below. **Block** - restrict accessing into the corresponding webpage with the categories listed on the box below. If the web pages do not match with the specified feature set here, it will be processed with reverse action.

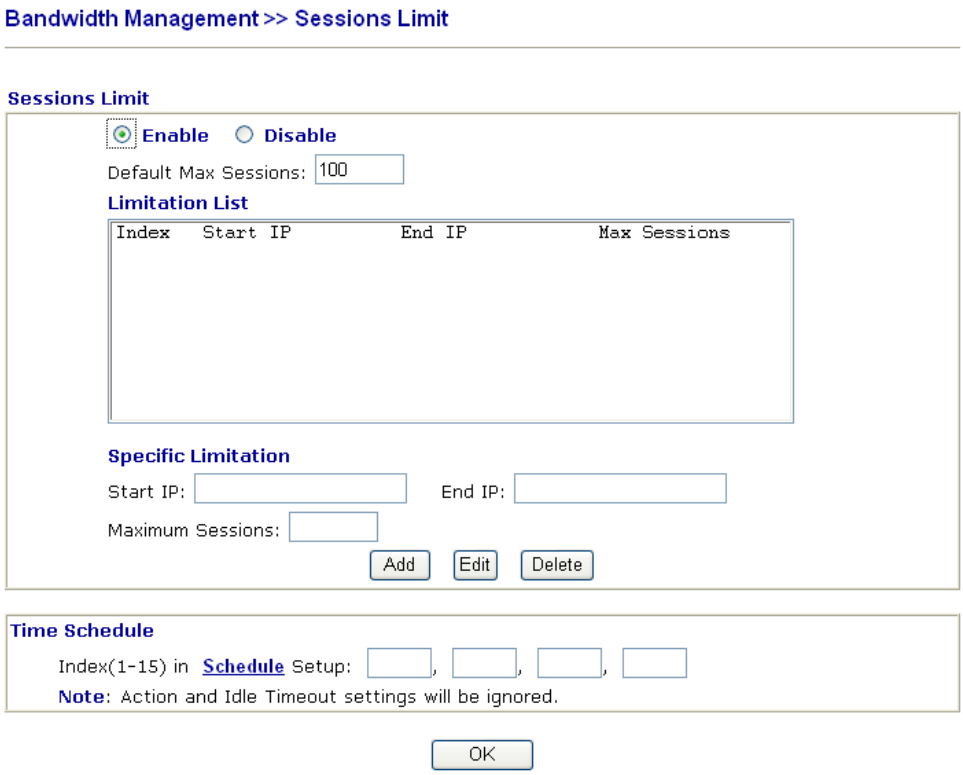
5.7 Bandwidth Management

Below shows the menu items for Bandwidth Management.

5.7.1 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.

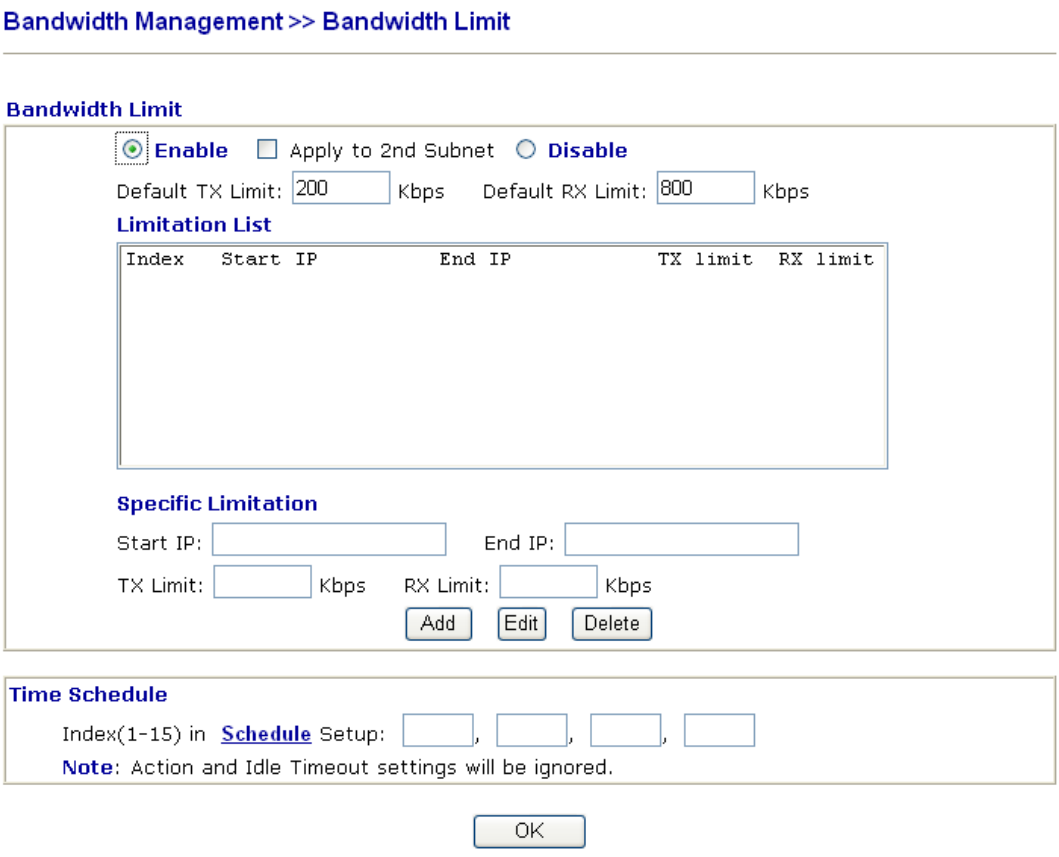
Enable	Click this button to activate the function of limit session.
Disable	Click this button to close the function of limit session.
Default session limit	Defines the default session number used for each computer in LAN.
Limitation List	Displays a list of specific limitations that you set on this web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

5.7.2 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. **Apply to 2nd Subnet** – if bandwidth limit function is enabled, please check this box to apply to second subnet.
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.

5.7.3 Quality of Service

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

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

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

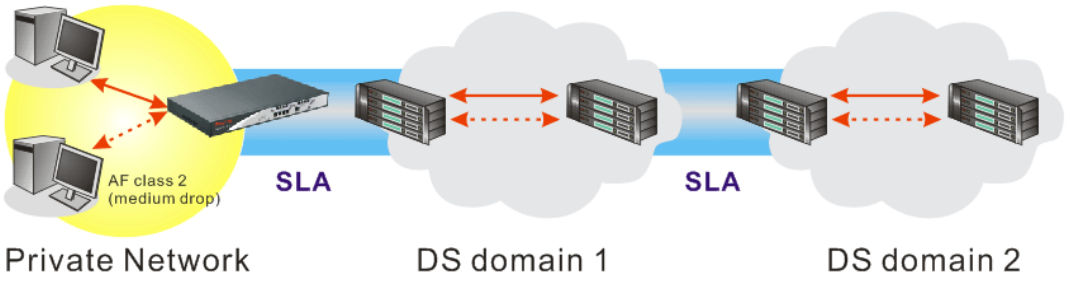
There are two components within Primary configuration of QoS deployment:

- Classification: Identifying low-latency or crucial applications and marking them for high-priority service level enforcement throughout the network.
- Scheduling: Based on classification of service level to assign packets to queues and associated service types

The basic QoS implementation in Vigor routers is to classify and schedule packets based on the service type information in the IP header. For instance, to ensure the connection with the headquarter, a teleworker may enforce an index of QoS Control to reserve bandwidth for HTTPS connection while using lots of application at the same time.

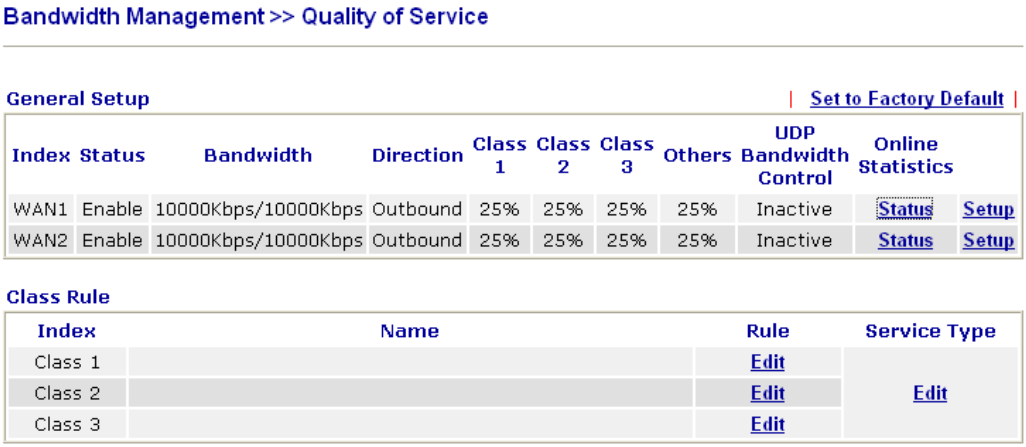
One more larger-scale implementation of QoS network is to apply DSCP (Differentiated Service Code Point) and IP Precedence disciplines at Layer 3. Compared with legacy IP Precedence that uses Type of Service (ToS) field in the IP header to define 8 service classes, DSCP is a successor creating 64 classes possible with backward IP Precedence compatibility. In a QoS-enabled network, or Differentiated Service (DiffServ or DS) framework, a DS domain owner should sign a Service License Agreement (SLA) with other DS domain owners to define the service level provided toward traffic from different domains. Then each DS node in these domains will perform the priority treatment. This is called per-hop-behavior (PHB). The definition of PHB includes Expedited Forwarding (EF), Assured Forwarding (AF), and Best Effort (BE). AF defines the four classes of delivery (or forwarding) classes and three levels of drop precedence in each class.

Vigor routers as edge routers of DS domain shall check the marked DSCP value in the IP header of bypassing traffic, thus to allocate certain amount of resource execute appropriate policing, classification or scheduling. The core routers in the backbone will do the same checking before executing treatments in order to ensure service-level consistency throughout the whole QoS-enabled network.



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

In the **Bandwidth Management** menu, click **Quality of Service** to open the web page.

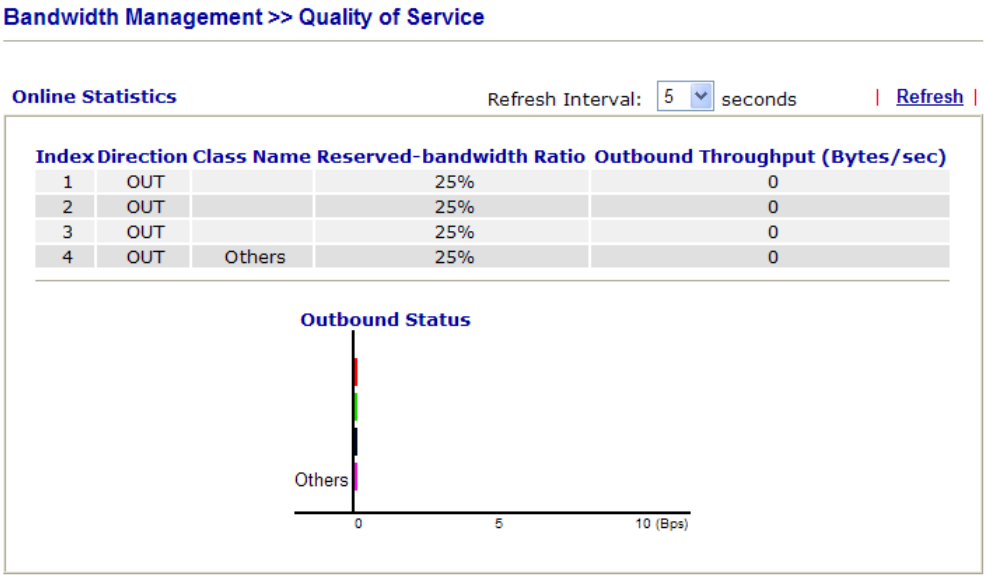


This page displays the QoS settings result of the WAN interface. Click the **Setup** link to access into next page for the general setup of WAN (1/2) interface. As to class rule, simply click the **Edit** link to access into next for configuration.

You can configure general setup for the WAN interface, edit the Class Rule, and edit the Service Type for the Class Rule for your request.

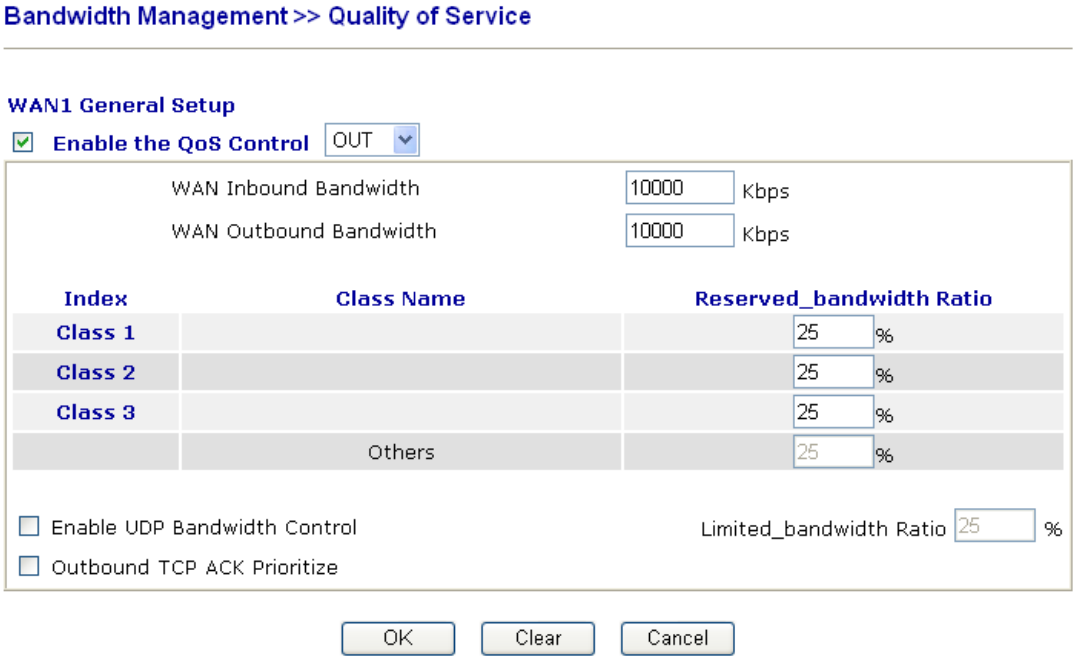
Online Statistics

Display an online statistics for quality of service for your reference. Click the **Status** link under **Online Statistics** to show the following screen.



General Setup for WAN Interface

When you click **Setup**, you can configure the bandwidth ratio for QoS of the WAN interface. There are four queues allowed for QoS control. The first three (Class 1 to Class 3) class rules can be adjusted for your necessity. Yet, the last one is reserved for the packets which are not suitable for the user-defined class rules.



Enable the QoS Control The factory default for this setting is checked.
Please also define which traffic the QoS Control settings will apply to.
IN- apply to incoming traffic only.
OUT-apply to outgoing traffic only.

BOTH- apply to both incoming and outgoing traffic.
Check this box and click **OK**, then click **Setup** link again. You will see the **Online Statistics** link appearing on this page.

WAN Inbound Bandwidth It allows you to set the connecting rate of data input for WAN. For example, if the connection supports 1M of downstream and 256K upstream, please set 10000kbps for this box. The default value is 10000kbps.

WAN Outbound Bandwidth It allows you to set the connecting rate of data output for WAN. For example, if the connection supports 1M of downstream and 256K upstream, please set 256kbps for this box. The default value is 10000kbps.

Note: The rate of outbound/inbound must be smaller than the real bandwidth to ensure correct calculation of QoS. It is suggested to set the bandwidth value for inbound/outbound as 80% - 85% of physical network speed provided by ISP to maximize the QoS performance.

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

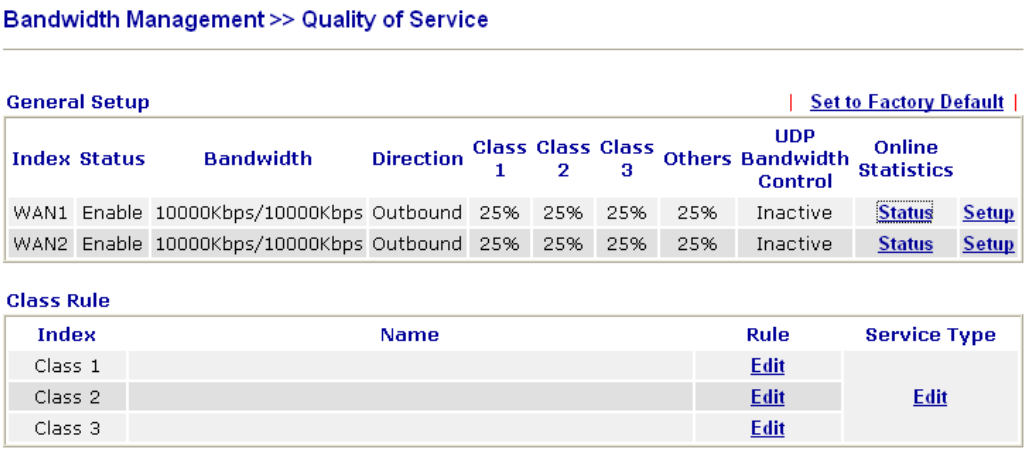
Enable UDP Bandwidth Control Check this and set the limited bandwidth ratio on the right field. This is a protection of TCP application traffic since UDP application traffic such as streaming video will exhaust lots of bandwidth.

Outbound TCP ACK Prioritize For the download speed might be impacted by the uploading TCP ACK, you can check this box to push ACK of upload faster to speed the network traffic.

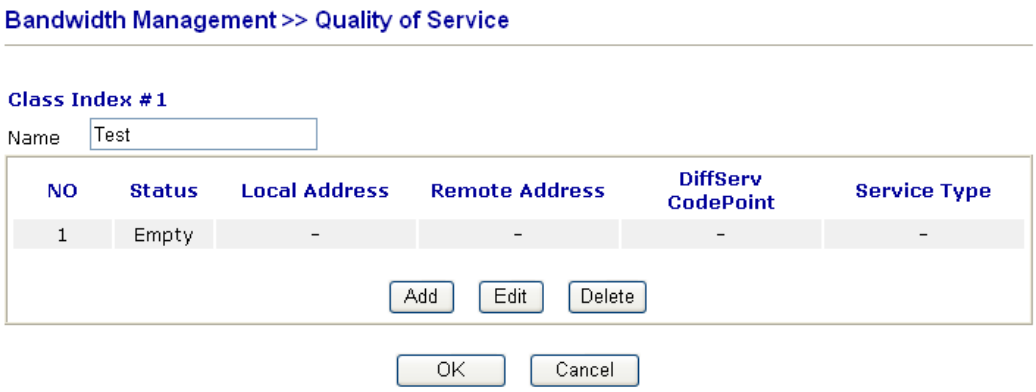
Limited_bandwidth Ratio The ratio typed here is reserved for limited bandwidth of UDP application.

Edit the Class Rule for QoS

The first three (Class 1 to Class 3) class rules can be adjusted for your necessity. To add, edit or delete the class rule, please click the **Edit** link of that one.



After you click the **Edit** link, you will see the following page. Now you can define the name for that Class. In this case, “Test” is used as the name of Class Index #1.



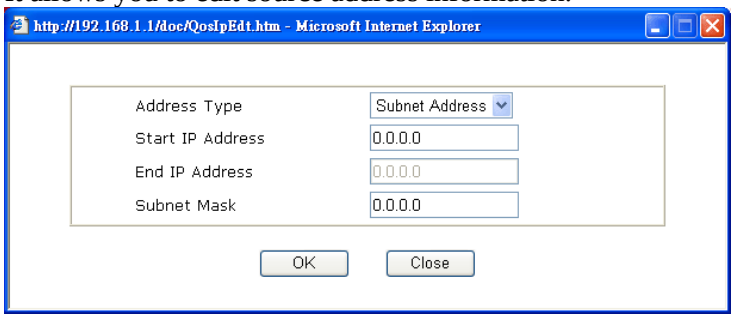
For adding a new rule, click **Add** to open the following page.

ACT — Check this box to invoke these settings.

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

Remote Address — Click the **Edit** button to set the remote IP address (on LAN/WAN) for the rule.

Edit — It allows you to edit source address information.



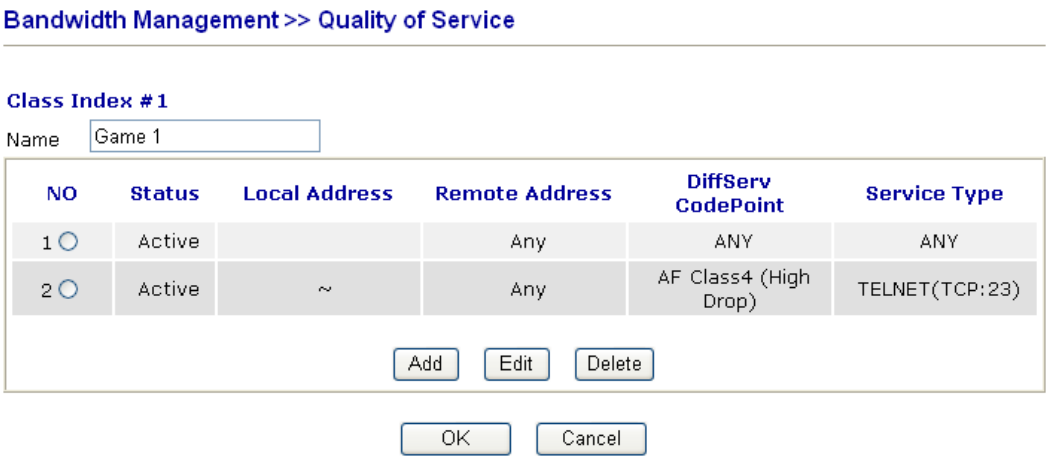
Address Type – Determine the address type for the source address.
For **Single Address**, you have to fill in Start IP address.
For **Range Address**, you have to fill in Start IP address and End IP address.
For **Subnet Address**, you have to fill in Start IP address and Subnet Mask.

DiffServ CodePoint — All the packets of data will be divided with different levels and will be processed according to the level type by the

system. Please assign one of the levels of the data for processing with QoS control.

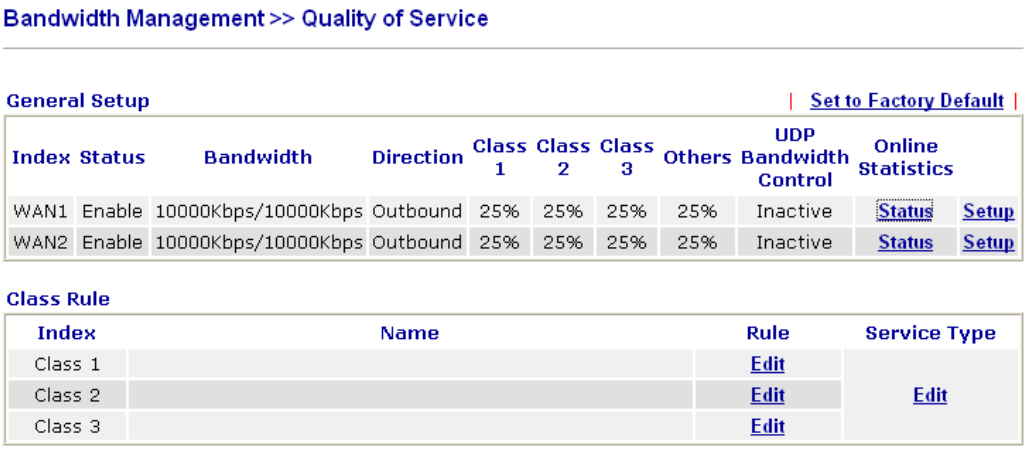
Service Type — It determines the service type of the data for processing with QoS control. It can also be edited. You can choose the predefined service type from the Service Type drop down list. Those types are predefined in factory. Simply choose the one that you want for using by current QoS.

By the way, you can set up to 20 rules for one Class. If you want to edit an existed rule, please select the radio button of that one and click **Edit** to open the rule edit page for modification.

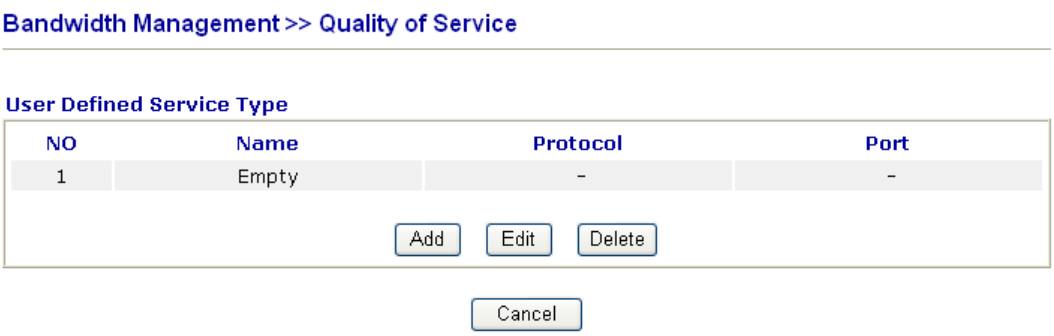


Edit the Service Type for Class Rule

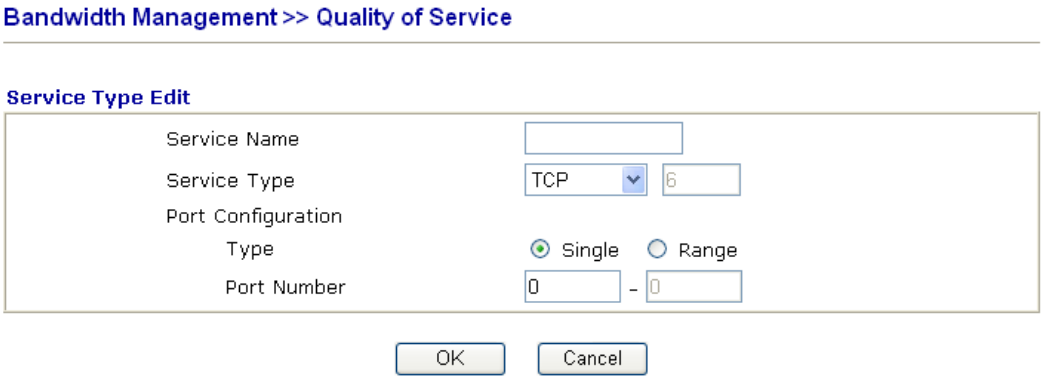
To add a new service type, edit or delete an existed service type, please click the **Edit** link under **Service Type** field.



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



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

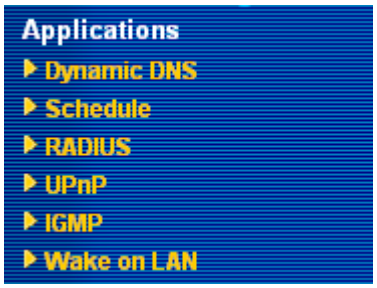


Service Name	Type in a new service for your request.
Service Type	Choose the type (TCP, UDP or TCP/UDP) for the new service.
Port Configuration	Click **Single** or **Range** as the **Type**. If you select Range, you have to type in the starting port number and the end porting number on the boxes below. **Port Number** – Type in the starting port number and the end porting number here if you choose Range as the type.

By the way, you can set up to 40 service types. If you want to edit/delete an existed service type, please select the radio button of that one and click **Edit/Delete** for modification.

5.8 Applications

Below shows the menu items for Applications.



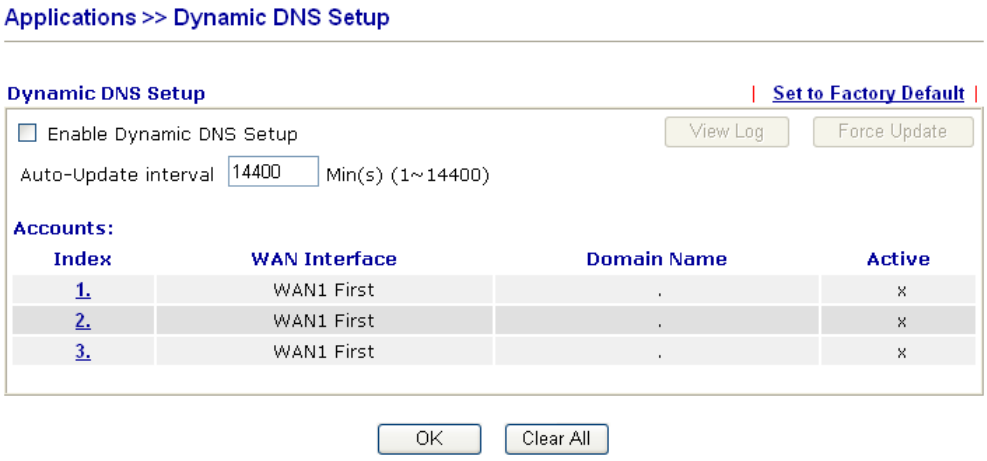
5.8.1 Dynamic DNS

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

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

Enable the Function and Add a Dynamic DNS Account

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



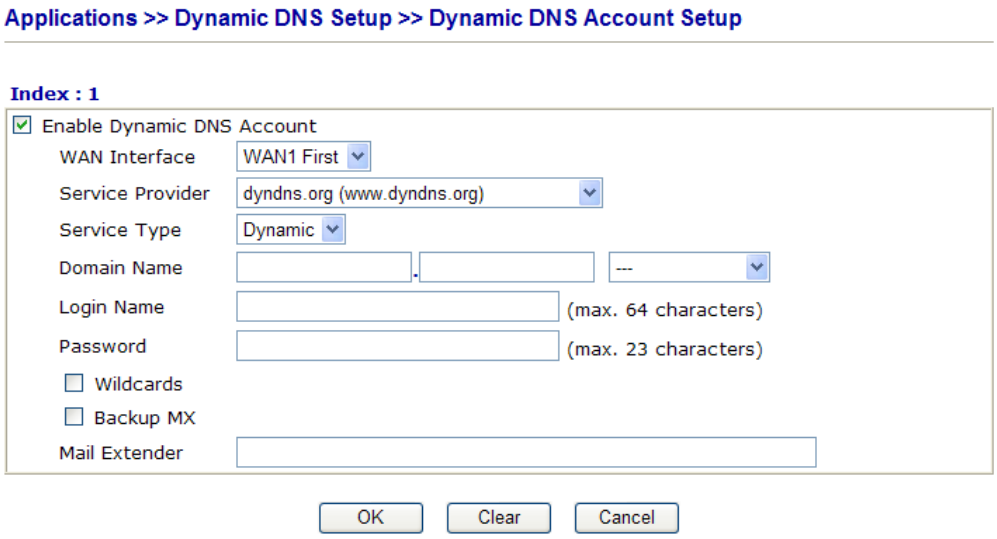
Set to Factory Default Clear all profiles and recover to factory settings.

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

Auto-Update interval Set the time for the router to perform auto update for DDNS service.

Index	Click the number below Index to access into the setting page of DDNS setup to set account(s).
WAN Interface	Display current WAN interface used for accessing Internet.
Domain Name	Display the domain name that you set on the setting page of DDNS setup.
Active	Display if this account is active or inactive.
View Log	Display DDNS log status.
Force Update	Force the router updates its information to DDNS server.

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



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.

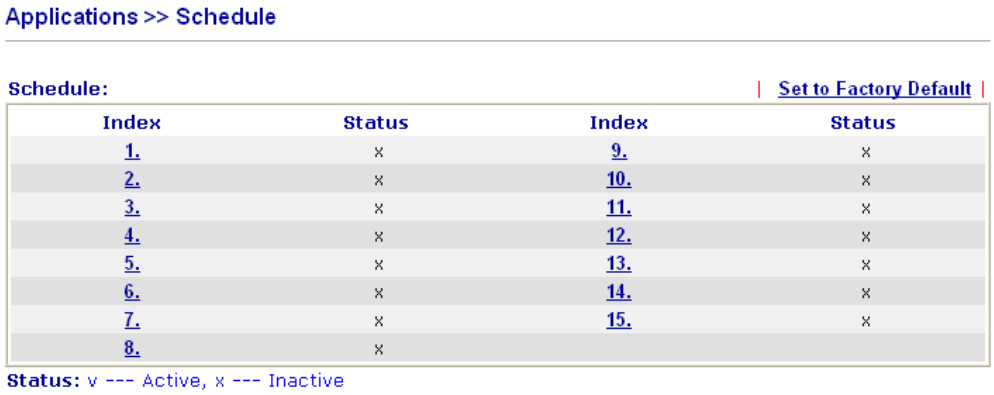
4. Click **OK** button to activate the settings. You will see your setting has been saved.

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

5.8.2 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.

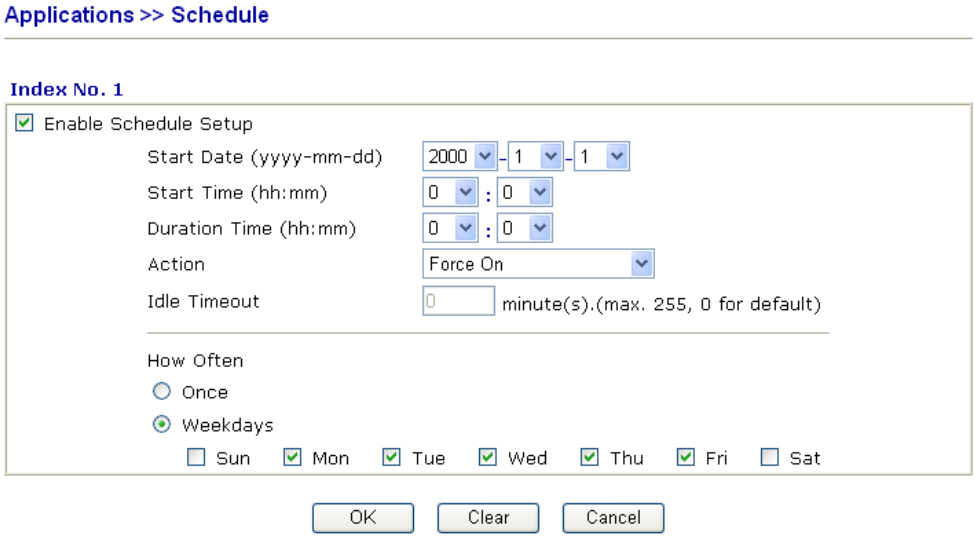
You have to set your time before set schedule. In **System Maintenance>> Time and Date** menu, press **Inquire Time** button to set the Vigor router's clock to current time of your PC. The clock will reset once if you power down or reset the router. There is another way to set up time. You can inquiry 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)

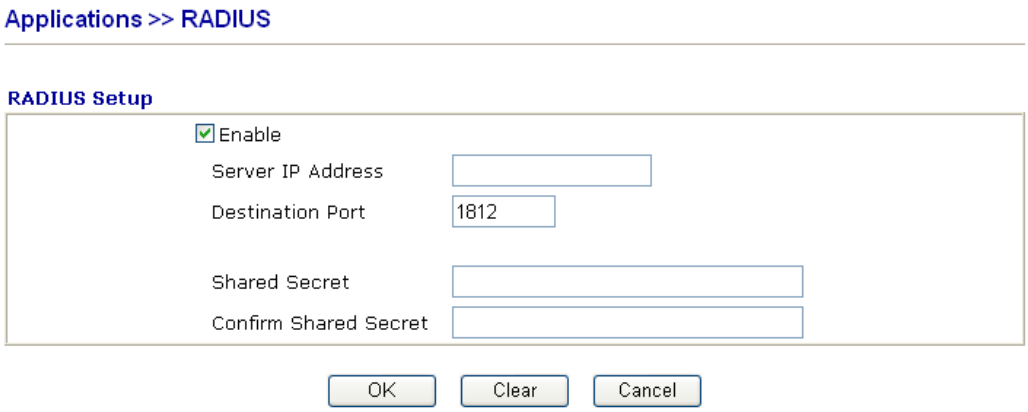
Mon - Sun **9:00 am** **to** **6:00 pm**

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.

5.8.3 RADIUS

Remote Authentication Dial-In User Service (RADIUS) is a security authentication client/server protocol that supports authentication, authorization and accounting, which is widely used by Internet service providers. It is the most common method of authenticating and authorizing dial-up and tunneled network users.

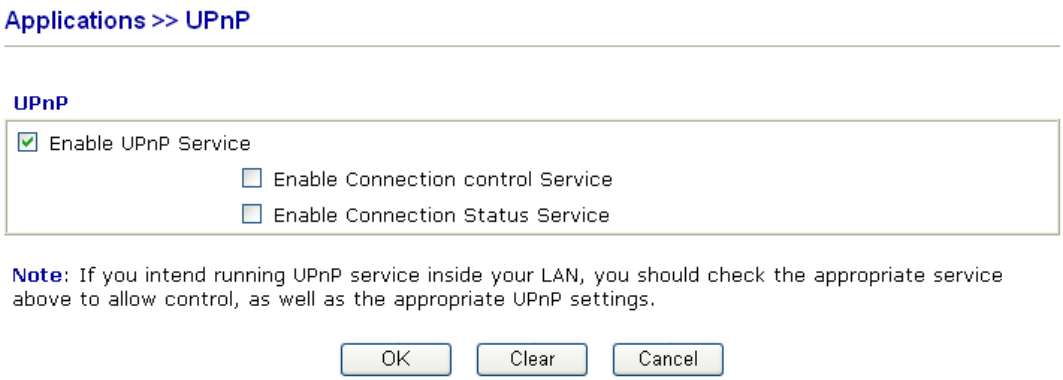
The built-in RADIUS client feature enables the router to assist the remote dial-in user and the RADIUS server in performing mutual authentication. It enables centralized remote access authentication for network management.



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

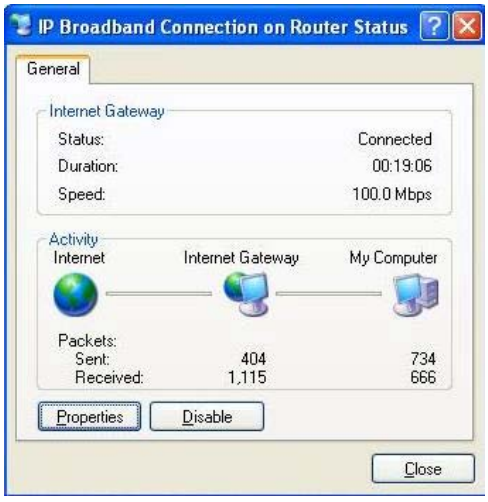
5.8.4 UPnP

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

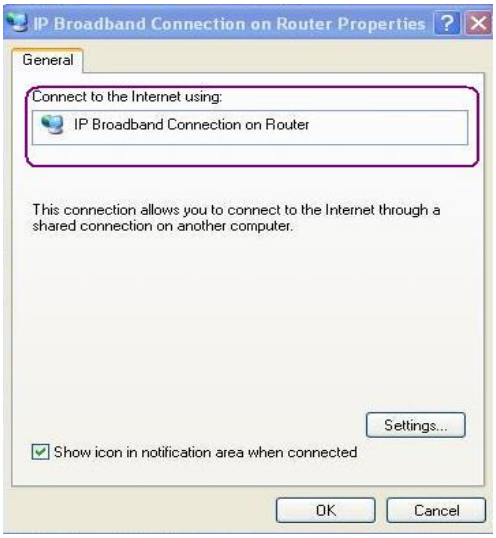


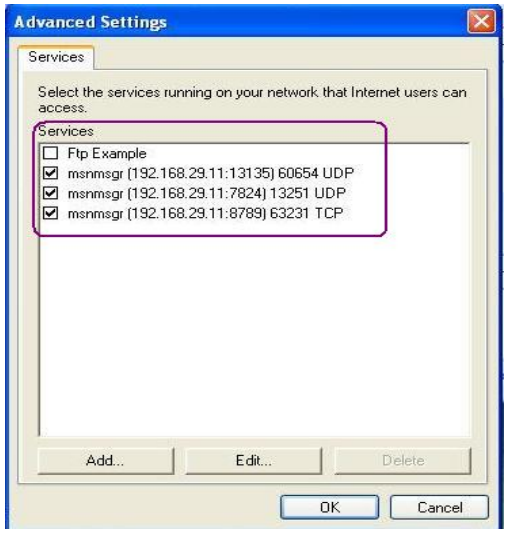
Enable UPNP Service Accordingly, you can enable either the **Connection Control Service** or **Connection Status Service**.

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

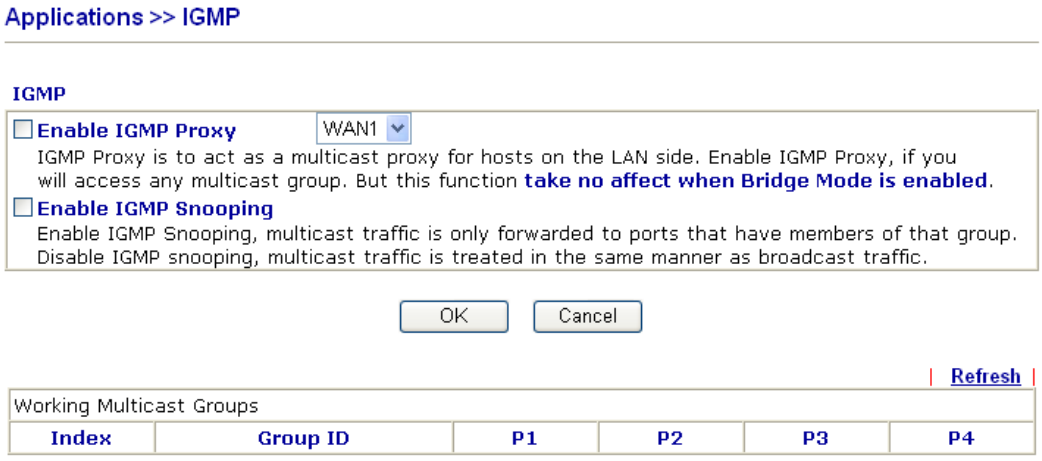
Activating the UPnP function on your network may incur some security threats. You should consider carefully these risks before activating the UPnP function.

- 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.

5.8.5 IGMP

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



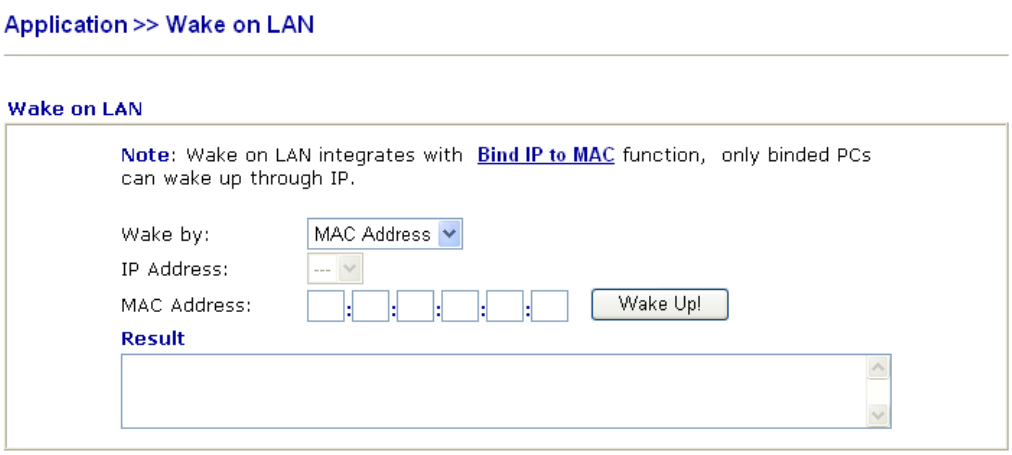
Enable IGMP Proxy	Check this box to enable this function. The application of multicast will be executed through the selected WAN port. In addition, such function is available in NAT mode.
Enable IGMP Snooping	Check this box to enable this function. The application of multicast will be executed for the clients in LAN.
Group ID	This field displays the ID port for the multicast group. The available range for IGMP starts from 224.0.0.0 to 239.255.255.254.
P1 to P4	It indicates the LAN port used for the multicast group.
Refresh	Click this link to renew the working multicast group status.

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

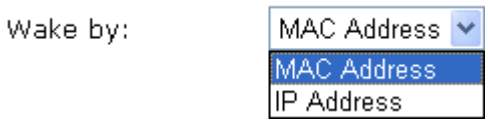
5.8.6 Wake on LAN

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

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



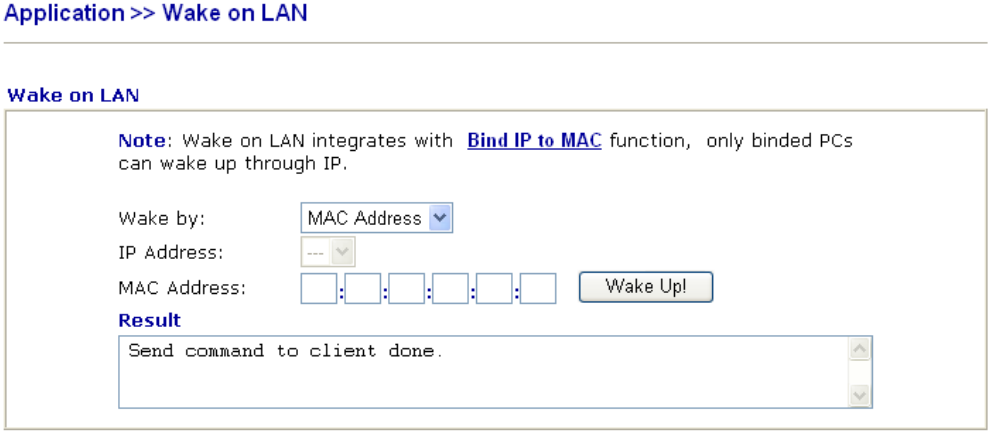
Wake by Two types provide for you to wake up the binded IP. If you choose Wake by MAC Address, you have to type the correct MAC address of the host in MAC Address boxes. If you choose Wake by IP Address, you have to choose the correct IP address.



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.

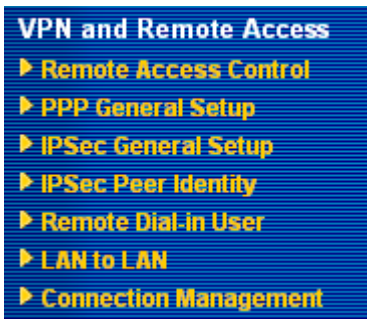
Wake Up Click this button to wake up the selected IP. See the following figure. The result will be shown on the box.



5.9 VPN and Remote Access

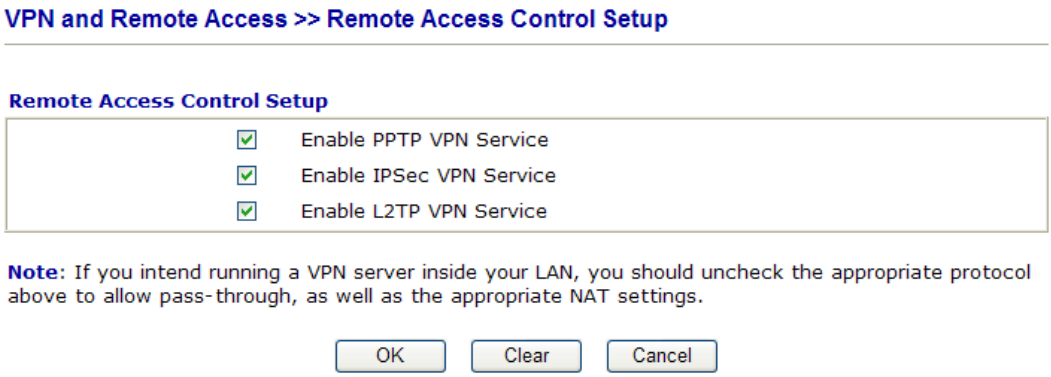
A Virtual Private Network (VPN) is the extension of a private network that encompasses links across shared or public networks like the Internet. In short, by VPN technology, you can send data between two computers across a shared or public network in a manner that emulates the properties of a point-to-point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

Below shows the menu items for VPN and Remote Access.



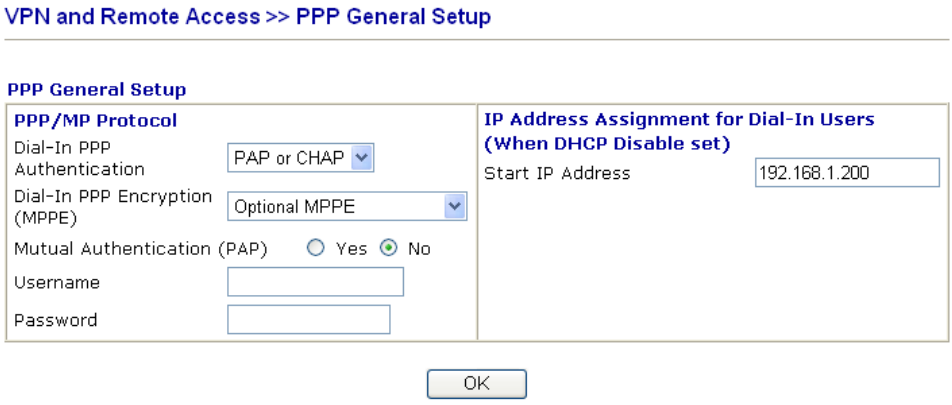
5.9.1 Remote Access Control

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



5.9.2 PPP General Setup

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



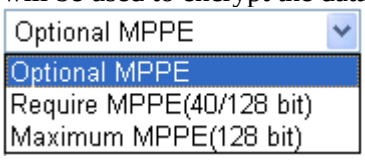
Dial-In PPP Authentication

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

PAP or CHAP - Selecting this option means the router will attempt to authenticate dial-in users with the CHAP protocol first. If the dial-in user does not support this protocol, it will fall back to use the PAP protocol for authentication.

Dial-In PPP Encryption (MPPE Optional MPPE

This option represents that the MPPE encryption method will be optionally employed in the router for the remote dial-in user. If the remote dial-in user does not support the MPPE encryption algorithm, the router will transmit “no MPPE encrypted packets”. Otherwise, the MPPE encryption scheme will be used to encrypt the data.



Require MPPE (40/128bits) - Selecting this option will force the router to encrypt packets by using the MPPE encryption algorithm. In addition, the remote dial-in user will use 40-bit to perform encryption prior to using 128-bit for encryption. In other words, if 128-bit MPPE encryption method is not available, then 40-bit encryption scheme will be applied to encrypt the data.

Maximum MPPE - This option indicates that the router will use the MPPE encryption scheme with maximum bits (128-bit) to encrypt the data.

Mutual Authentication (PAP)

The Mutual Authentication function is mainly used to communicate with other routers or clients who need bi-directional authentication in order to provide stronger security, for example, Cisco routers. So you should enable this function when your peer router requires mutual authentication. You should further specify the **User Name** and **Password** of the mutual authentication peer.

Start IP Address Enter a start IP address for the dial-in PPP connection. You should choose an IP address from the local private network. For example, if the local private network is 192.168.1.0/255.255.255.0, you could choose 192.168.1.200 as the Start IP Address. But, you have to notice that the first two IP addresses of 192.168.1.200 and 192.168.1.201 are reserved for ISDN remote dial-in user.

5.9.3 IPSec General Setup

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

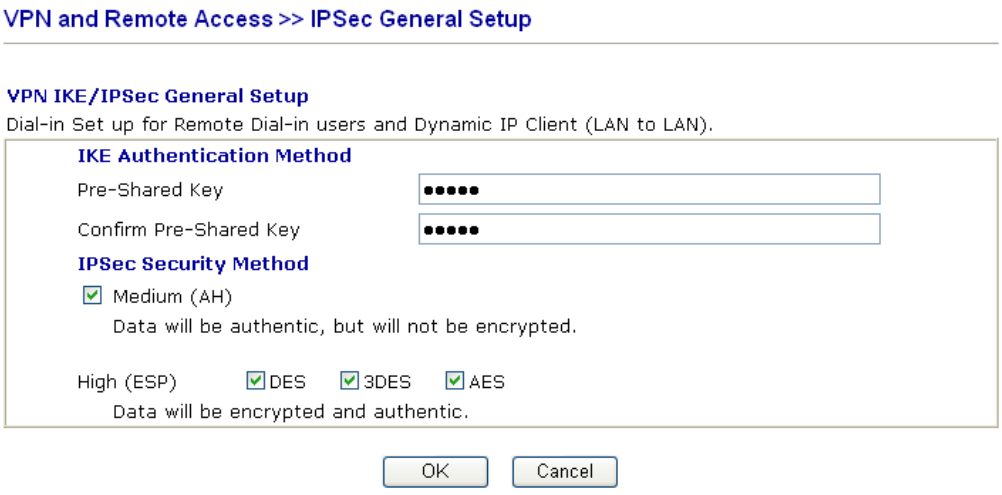
There are two phases of IPSec.

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

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

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

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



IKE Authentication Method This usually applies to those are remote dial-in user or node (LAN-to-LAN) which uses dynamic IP address and IPSec-related VPN connections such as L2TP over IPSec

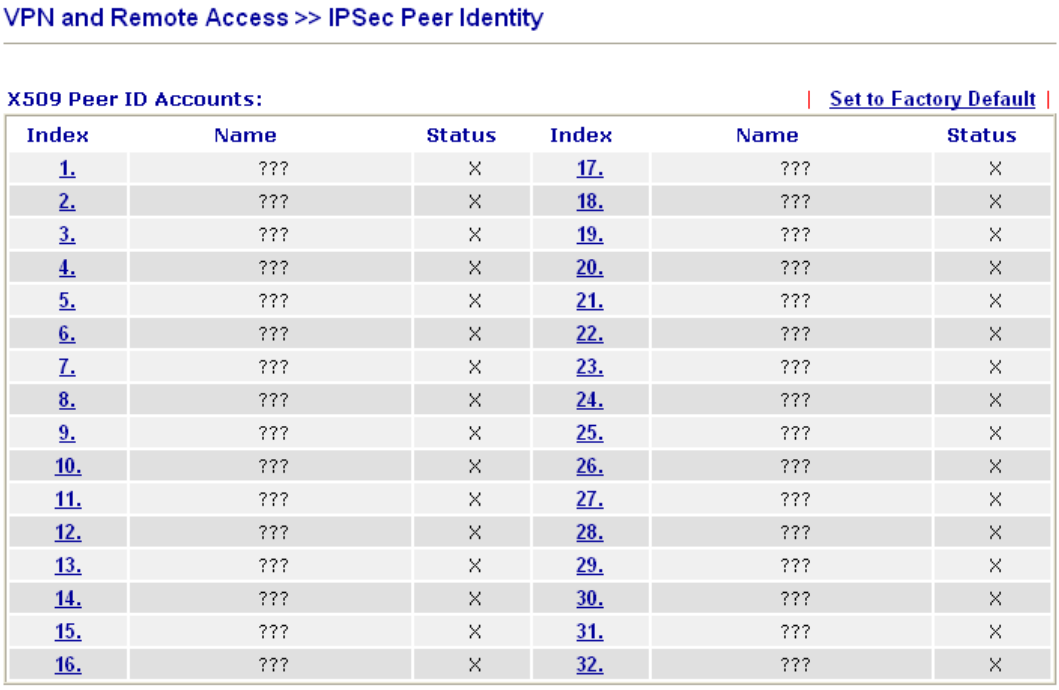
and IPSec tunnel.
Pre-Shared Key -Currently only support Pre-Shared Key authentication.
Pre-Shared Key- Specify a key for IKE authentication
Confirm Pre-Shared Key- Retype the characters to confirm the pre-shared key.

IPSec Security Method

Medium - Authentication Header (AH) means data will be authenticated, but not be encrypted. By default, this option is active.
High - Encapsulating Security Payload (ESP) means payload (data) will be encrypted and authenticated. You may select encryption algorithm from Data Encryption Standard (DES), Triple DES (3DES), and AES.

5.9.4 IPSec Peer Identity

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

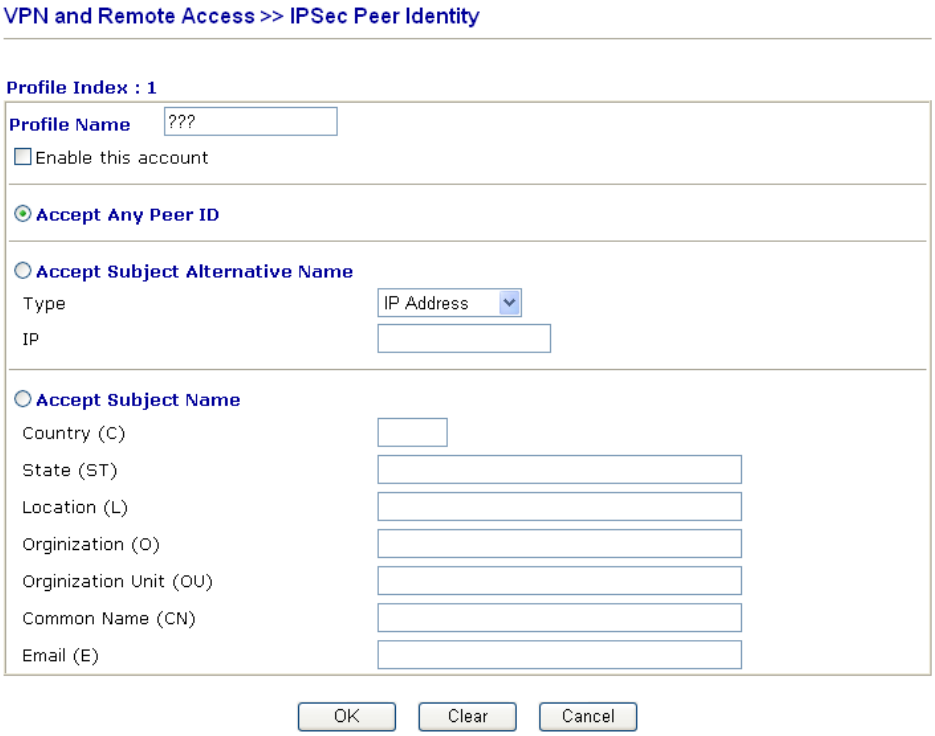


Set to Factory Default Click it to clear all indexes.

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

Name Display the profile name of that index.

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.

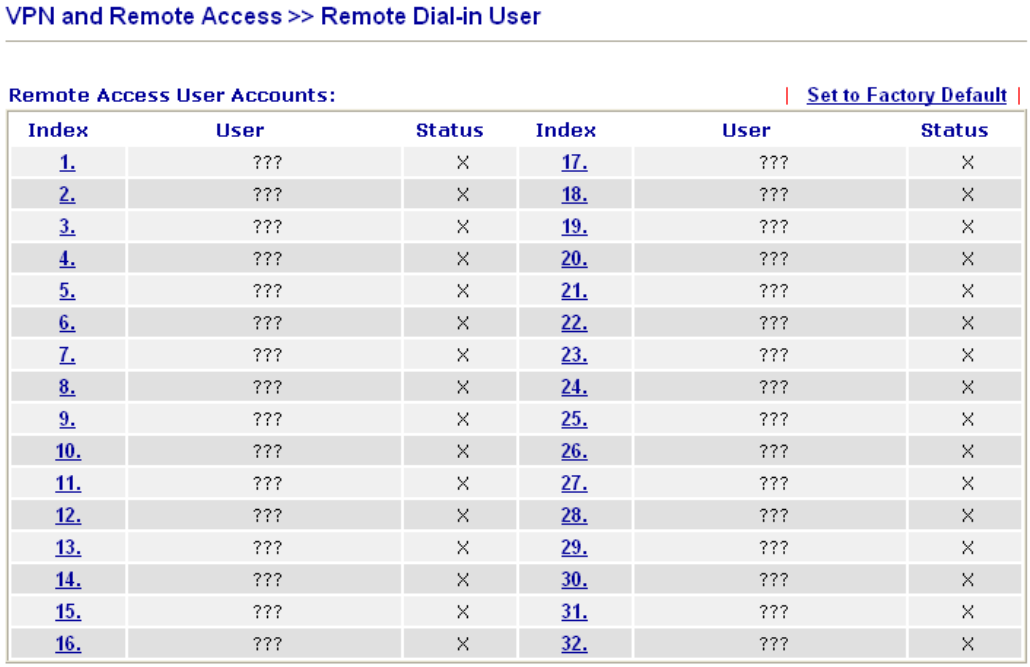


Profile Name	Type in a name in this file.
Accept Any Peer ID	Click to accept any peer regardless of its identity.
Accept Subject Alternative Name	Click to check one specific field of digital signature to accept the peer with matching value. The field can be **IP Address, Domain,** or **E-mail Address**. 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)**.

5.9.5 Remote Dial-in User

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

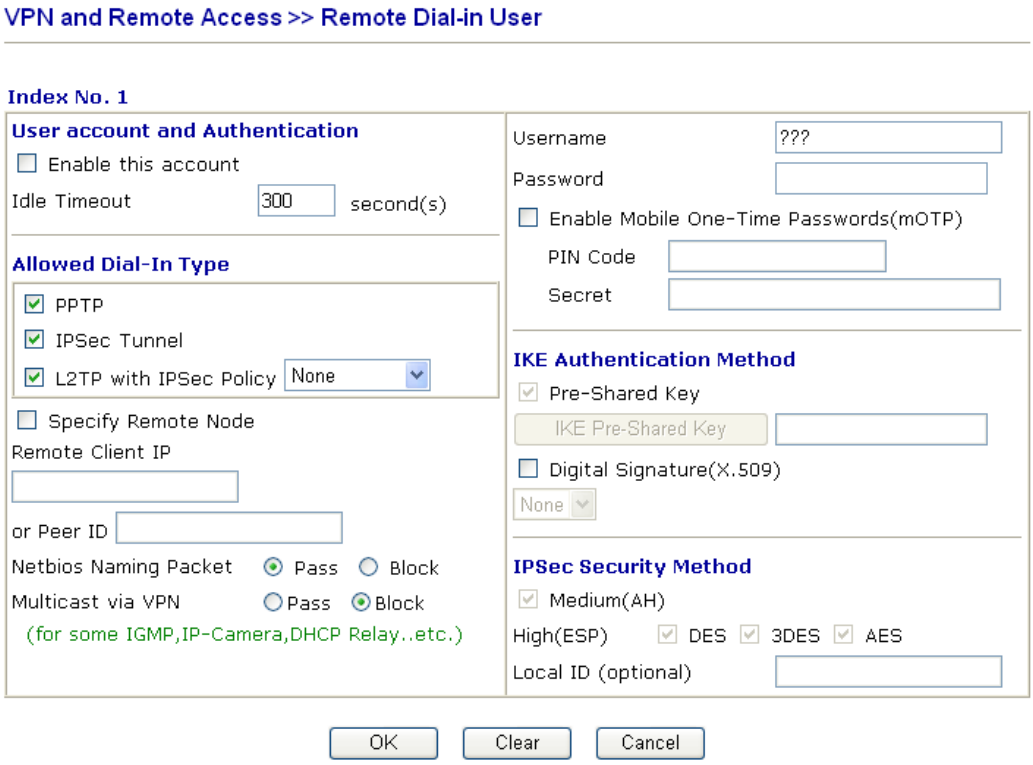
The router provides **32** access accounts for dial-in users. Besides, you can extend the user accounts to the RADIUS server through the built-in RADIUS client function. The following figure shows the summary table.



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

Set to Factory Default	Click to clear all indexes.
Index	Click the number below Index to access into the setting page of Remote Dial-in User.
User	Display the username for the specific dial-in user of the LAN-to-LAN profile. The symbol **???** represents that the profile is empty.
Status	Display the access state of the specific dial-in user. The symbol V and X represent the specific dial-in user to be active and inactive, respectively.

Click each index to edit one remote user profile. **Each Dial-In Type requires you to fill the different corresponding fields on the right.** If the fields gray out, it means you may leave it untouched. The following explanation will guide you to fill all the necessary fields.



User account and Authentication

Enable this account - Check the box to enable this function.

Idle Timeout- If the dial-in user is idle over the limitation of the timer, the router will drop this connection. By default, the Idle Timeout is set to 300 seconds.

Allowed Dial-In Type

PPTP - Allow the remote dial-in user to make a PPTP VPN connection through the Internet. You should set the User Name and Password of remote dial-in user below.

IPSec Tunnel - Allow the remote dial-in user to make an IPSec VPN connection through Internet.

L2TP with IPSec Policy - Allow the remote dial-in user to make a L2TP VPN connection through the Internet. You can select to use L2TP alone or with IPSec. Select from below:

None - Do not apply the IPSec policy. Accordingly, the VPN connection employed the L2TP without IPSec policy can be viewed as one pure L2TP connection.

Nice to Have - Apply the IPSec policy first, if it is applicable during negotiation. Otherwise, the dial-in VPN connection becomes one pure L2TP connection.

Must -Specify the IPSec policy to be definitely applied on the L2TP connection.

Specify Remote Node

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

Uncheck the checkbox-This means the connection type you select above will apply the authentication methods and security methods in the **general settings**.

Netbios Naming Packet -

Pass : Click it to have an inquiry for data transmission between the hosts located on both sides of VPN Tunnel while connecting.

Block : When there is conflict occurred between the hosts on both sides of VPN Tunnel in connecting, such function can block data transmission of Netbios Naming Packet inside the tunnel.

Multicast via VPN - Some programs might send multicast packets via VPN connection.

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

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

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.

Enable Mobile One-Time Passwords (mOTP) - Check this box to make the authentication with mOTP function.

PIN Code – Type the code for authentication (e.g, 1234).

Secret – Use the 32 digit-secret number generated by mOTP in the mobile phone (e.g., e759bb6f0e94c7ab4fe6).

IKE Authentication Method

This group of fields is applicable for IPSec Tunnels and L2TP with IPSec Policy when you specify the IP address of the remote node. The only exception is Digital Signature (X.509) can be set when you select IPSec tunnel either with or without specify the IP address of the remote node.

Pre-Shared Key - Check the box of Pre-Shared Key to invoke this function and type in the required characters (1-63) as the pre-shared key.

Digital Signature (X.509) – Check the box of Digital Signature to invoke this function and Select one predefined Profiles set in the **VPN and Remote Access >>IPSec Peer Identity.**

IPSec Security Method

This group of fields is a must for IPSec Tunnels and L2TP with IPSec Policy when you specify the remote node. Check the Medium, DES, 3DES or AES box as the security method. **Medium-Authentication Header (AH)** means data will be authenticated, but not be encrypted. By default, this option is invoked. You can uncheck it to disable it.

High-Encapsulating Security Payload (ESP) means payload (data) will be encrypted and authenticated. You may select encryption algorithm from Data Encryption Standard (DES), Triple DES (3DES), and AES.

Local ID - Specify a local ID to be used for Dial-in setting in the LAN-to-LAN Profile setup. This item is optional and can

be used only in IKE aggressive mode.

5.9.6 LAN to LAN

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

The router supports up to **32** profiles simultaneously. The following figure shows the summary table.

VPN and Remote Access >> LAN to LAN

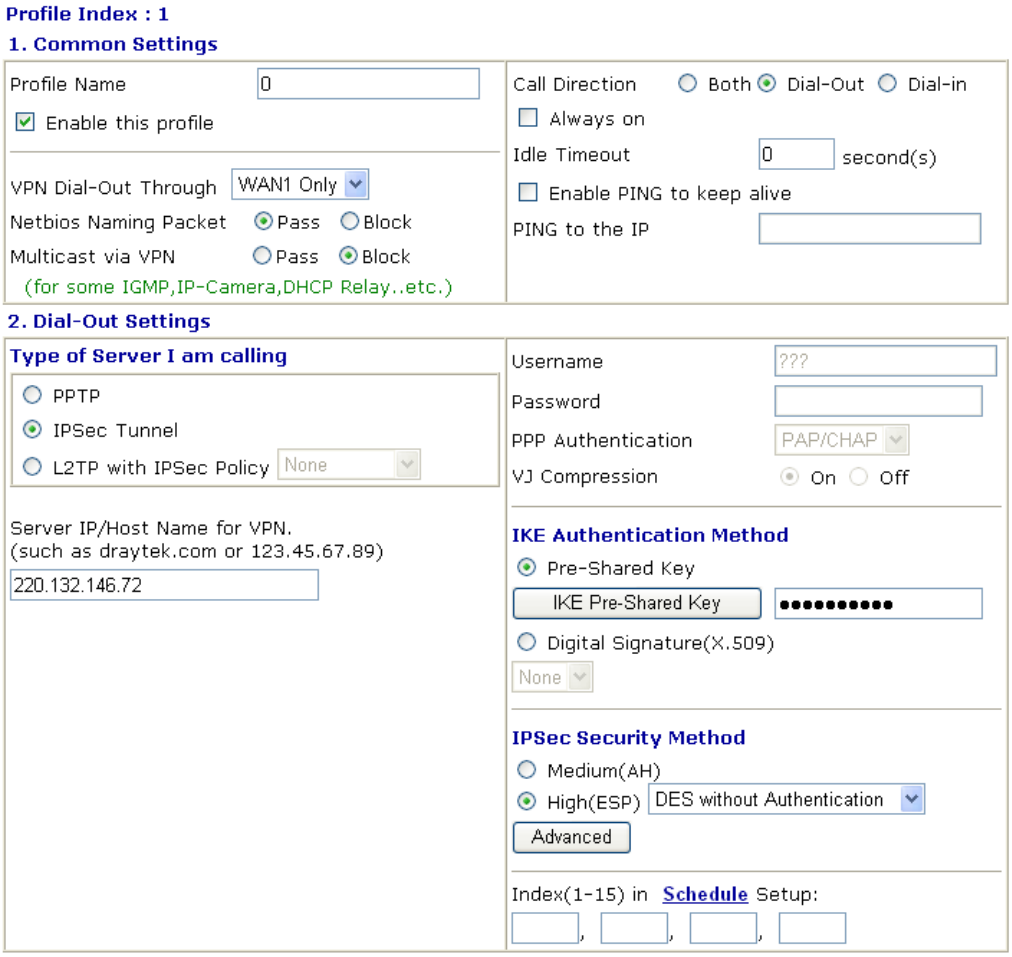
LAN-to-LAN Profiles: | Set to Factory Default |

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

Set to Factory Default	Click to clear all indexes.
Name	Indicate the name of the LAN-to-LAN profile. The symbol **???** represents that the profile is empty.
Status	Indicate the status of individual profiles. The symbol V and X represent the profile to be active and inactive, respectively.

Click each index to edit each profile and you will get the following page. Each LAN-to-LAN profile includes 4 subgroups. If the fields gray out, it means you may leave it untouched. The following explanations will guide you to fill all the necessary fields.

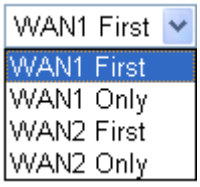
For the web page is too long, we divide the page into several sections for explanation.



Profile Name Specify a name for the profile of the LAN-to-LAN connection.

Enable this profile Check here to activate this profile.

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

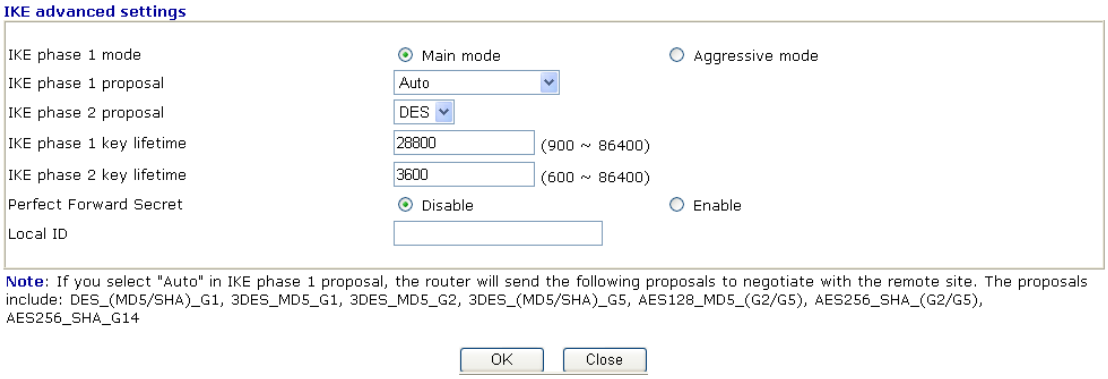


WAN1 First - While connecting, the router will use WAN1 as the first channel for VPN connection. If WAN1 fails, the router will use another WAN interface instead.
WAN1 Only - While connecting, the router will use WAN1 as the only channel for VPN connection.
WAN2 First - While connecting, the router will use WAN2 as the first channel for VPN connection. If WAN2 fails, the router will use another WAN interface instead.
WAN2 Only - While connecting, the router will use WAN2 as the only channel for VPN connection.

Netbios Naming Packet **Pass** – click it to have an inquiry for data transmission between the hosts located on both sides of VPN Tunnel while connecting.

	Block – When there is conflict occurred between the hosts on both sides of VPN Tunnel in connecting, such function can block data transmission of Netbios Naming Packet inside the tunnel.
Multicast via VPN	Some programs might send multicast packets via VPN connection. **Pass** – Click this button to let multicast packets pass through the router. **Block** – This is default setting. Click this button to let multicast packets be blocked by the router.
Call Direction	Specify the allowed call direction of this LAN-to-LAN profile. **Both**:-initiator/responder **Dial-Out**- initiator only **Dial-In-** responder only.
Always On or Idle Timeout	**Always On**-Check to enable router always keep VPN connection. **Idle Timeout:** The default value is 300 seconds. If the connection has been idled over the value, the router will drop the connection.
Enable PING to keep alive	This function is to help the router to determine the status of IPSec VPN connection, especially useful in the case of abnormal VPN IPSec tunnel disruption. For details, please refer to the note below. Check to enable the transmission of PING packets to a specified IP address.
PING to the IP	Enter the IP address of the remote host that located at the other-end of the VPN tunnel.
	Enable PING to Keep Alive is used to handle abnormal IPSec VPN connection disruption. It will help to provide the state of a VPN connection for router's judgment of redial. Normally, if any one of VPN peers wants to disconnect the connection, it should follow a serial of packet exchange procedure to inform each other. However, if the remote peer disconnect without notice, Vigor router will by no where to know this situation. To resolve this dilemma, by continuously sending PING packets to the remote host, the Vigor router can know the true existence of this VPN connection and react accordingly. This is independent of DPD (dead peer detection).
PPTP	Build a PPTP VPN connection to the server through the Internet. You should set the identity like User Name and Password below for the authentication of remote server.
IPSec Tunnel	Build an IPSec VPN connection to the server through Internet.
L2TP with IPSec Policy	Build a L2TP VPN connection through the Internet. You can select to use L2TP alone or with IPSec. Select from below: **None:** Do not apply the IPSec policy. Accordingly, the VPN connection employed the L2TP without IPSec policy can be

	viewed as one pure L2TP connection. **Nice to Have:** Apply the IPSec policy first, if it is applicable during negotiation. Otherwise, the dial-out VPN connection becomes one pure L2TP connection. **Must:** Specify the IPSec policy to be definitely applied on the L2TP connection.
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 ISDN, PPTP or L2TP with or without IPSec policy above. PAP/CHAP is the most common selection due to wild compatibility.
VJ compression	This field is applicable when you select 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.

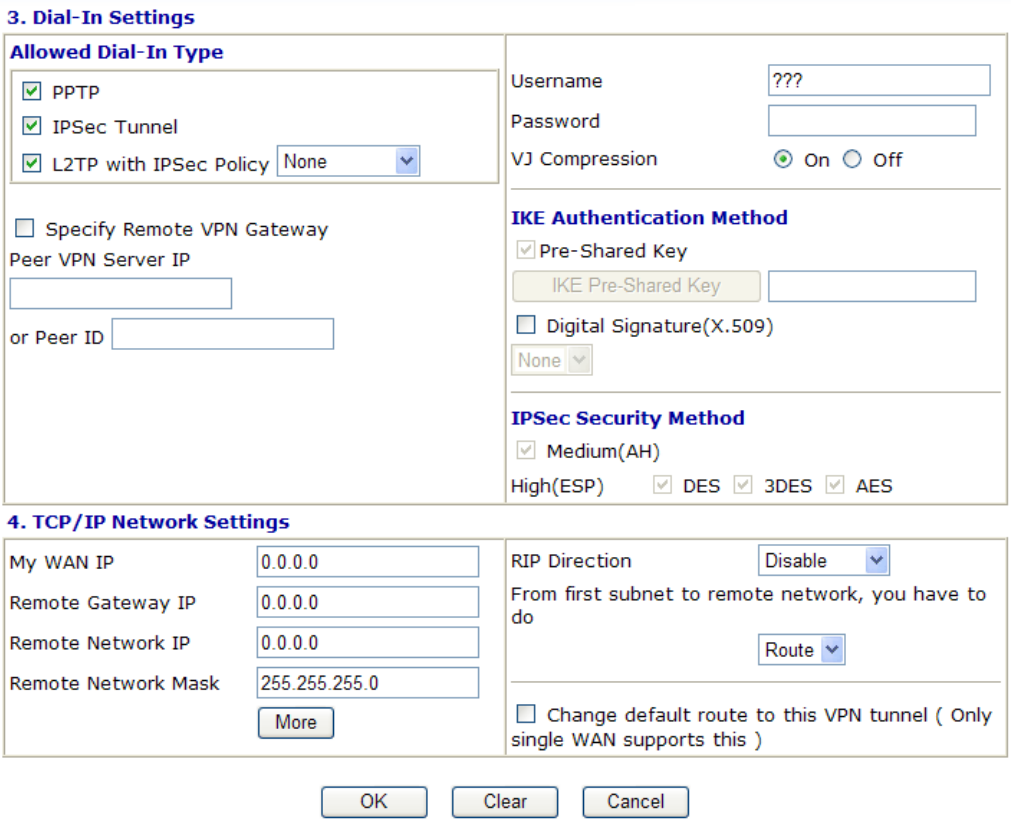
IKE phase 1 key lifetime-For security reason, the lifetime of key should be defined. The default value is 28800 seconds. You may specify a value in between 900 and 86400 seconds.

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.

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.



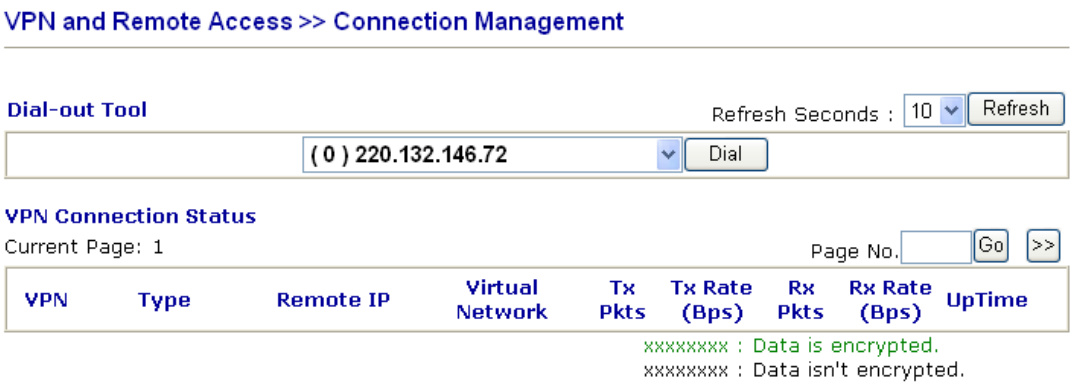
Allowed Dial-In Type	Determine the dial-in connection with different types.
PPTP	Allow the remote dial-in user to make a PPTP VPN connection through the Internet. You should set the User Name and Password of remote dial-in user below.
IPSec Tunnel	Allow the remote dial-in user to trigger an IPSec VPN connection through Internet.
L2TP	Allow the remote dial-in user to make a L2TP VPN connection through the Internet. You can select to use L2TP alone or with IPSec. Select from below: **None -** Do not apply the IPSec policy. Accordingly, the VPN connection employed the L2TP without IPSec policy can be viewed as one pure L2TP connection. **Nice to Have** - Apply the IPSec policy first, if it is applicable during negotiation. Otherwise, the dial-in VPN connection becomes one pure L2TP connection. **Must -** Specify the IPSec policy to be definitely applied on the L2TP connection.
Specify CLID or Remote VPN Gateway	You can specify the IP address of the remote dial-in user or peer ID (should be the same with the ID setting in dial-in type) by checking the box. Enter Peer ISDN number if you select ISDN above. Also, you should further specify the corresponding security methods on the right side. If you uncheck the checkbox**,** the connection type you select above will apply the authentication methods and security methods in the general settings.
User Name	This field is applicable when you select 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.
VJ Compression	VJ Compression is used for TCP/IP protocol header compression. This field is applicable when you select PPTP or L2TP with or without IPSec policy above.
IKE Authentication Method	This group of fields is applicable for IPSec Tunnels and L2TP with IPSec Policy when you specify the IP address of the remote node. The only exception is Digital Signature (X.509) can be set when you select IPSec tunnel either with or without specify the IP address of the remote node. **Pre-Shared Key -** Check the box of Pre-Shared Key to invoke this function and type in the required characters (1-63) as the pre-shared key. **Digital Signature (X.509) –**Check the box of Digital Signature to invoke this function and select one predefined Profiles set in the **VPN and Remote Access >>IPSec Peer Identity**.
IPSec Security Method	This group of fields is a must for IPSec Tunnels and L2TP with IPSec Policy when you specify the remote node. **Medium-** Authentication Header (AH) means data will be authenticated, but not be encrypted. By default, this option is active. **High-** Encapsulating Security Payload (ESP) means payload (data) will be encrypted and authenticated. You may select encryption algorithm from Data Encryption Standard (DES), Triple DES (3DES), and AES.
My WAN IP	This field is only applicable when you select ISDN, PPTP or L2TP with or without IPSec policy above. The default value is 0.0.0.0, which means the Vigor router will get a PPP IP address from the remote router during the IPCP negotiation phase. If the PPP IP address is fixed by remote side, specify the fixed IP address here. Do not change the default value if you do not select ISDN, PPTP or L2TP.
Remote Gateway IP	This field is only applicable when you select ISDN, PPTP or L2TP with or without IPSec policy above. The default value is 0.0.0.0, which means the Vigor router will get a remote Gateway PPP IP address from the remote router during the IPCP negotiation phase. If the PPP IP address is fixed by remote side, specify the fixed IP address here. Do not change the default value if you do not select ISDN, PPTP or L2TP.
Remote Network IP/ Remote Network Mask	Add a static route to direct all traffic destined to this Remote Network IP Address/Remote Network Mask through the VPN connection. For IPSec, this is the destination clients IDs of phase 2 quick mode.
More	Add a static route to direct all traffic destined to more Remote Network IP Addresses/ Remote Network Mask through the VPN connection. This is usually used when you find there are several subnets behind the remote VPN router.
RIP Direction	The option specifies the direction of RIP (Routing Information Protocol) packets. You can enable/disable one of direction

	here. Herein, we provide four options: TX/RX Both, TX Only, RX Only, and Disable.
From first subnet to remote network, you have to do	If the remote network only allows you to dial in with single IP, please choose **NAT**, otherwise choose **Route**.
Change default route to this VPN tunnel	Check this box to change the default route with this VPN tunnel. Be aware that this setting is available only for WAN interface is enabled.

5.9.7 Connection Management

You can find the summary table of all VPN connections. You may disconnect any VPN connection by clicking **Drop** button. You may also aggressively Dial-out by using Dial-out Tool and clicking **Dial** button.



Dial	Click this button to execute dial out function.
Refresh Seconds	Choose the time for refresh the dial information among 5, 10, and 30.
Refresh	Click this button to refresh the whole connection status.

5.10 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.

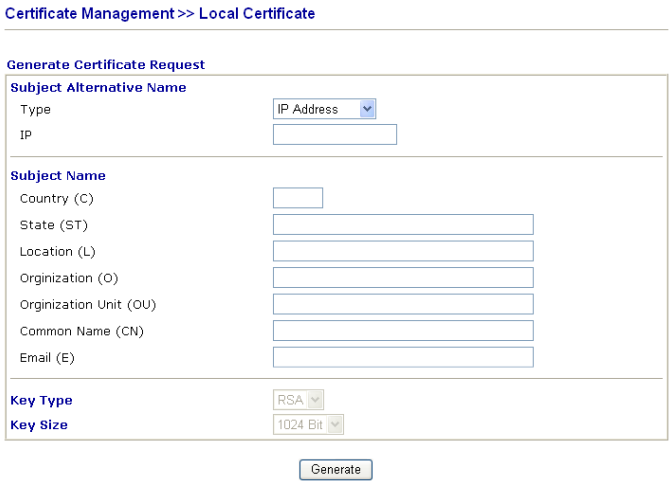
Any entity wants to utilize digital certificates should first request a certificate issued by a CA server. It should also retrieve certificates of other trusted CA servers so it can authenticate the peer with certificates issued by those trusted CA servers.

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.

5.10.1 Local Certificate

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



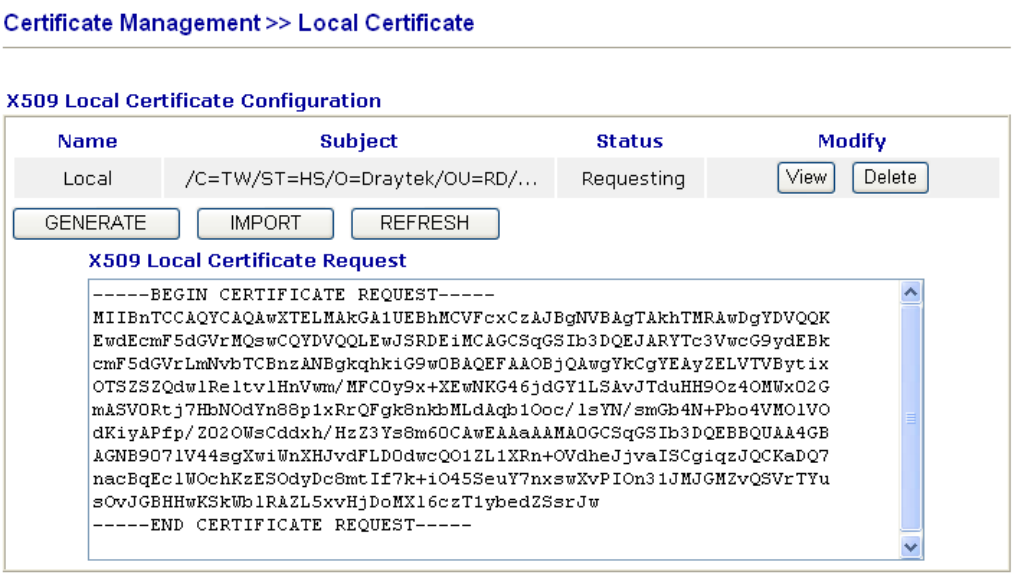
Type in all the information that the window request. Then click **Generate** again.

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

Refresh Click this button to refresh the information listed below.

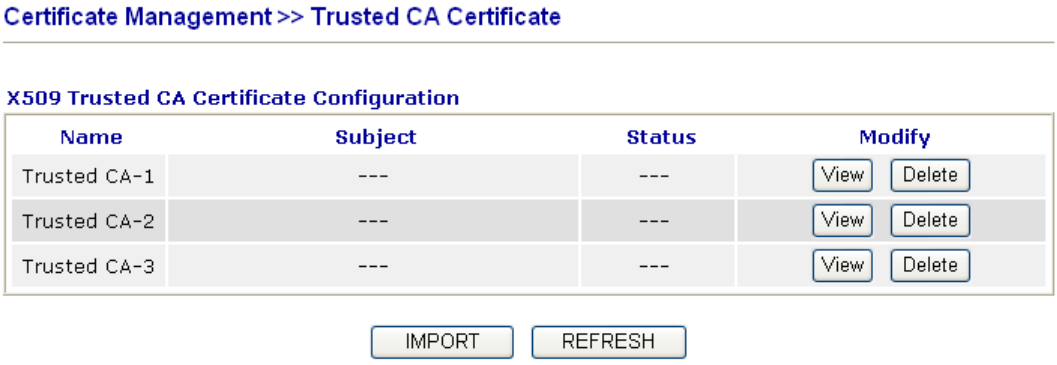
View Click this button to view the detailed settings for certificate request.

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

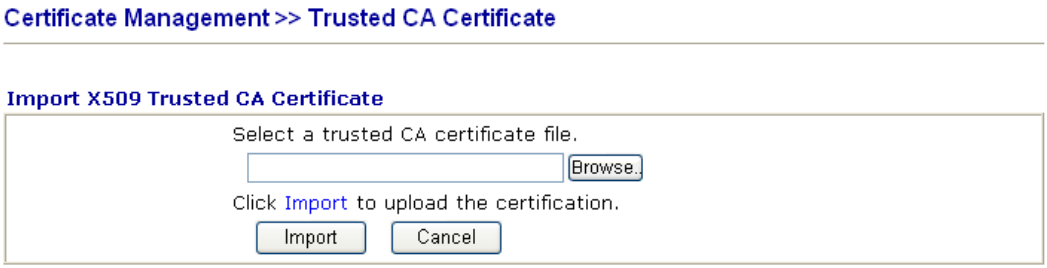


5.10.2 Trusted CA Certificate

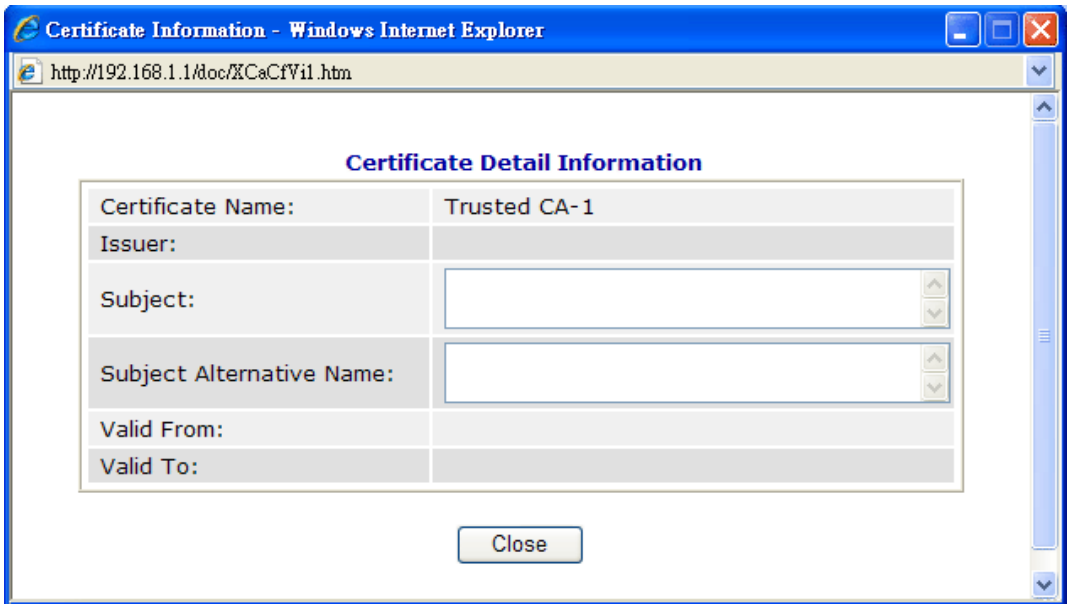
Trusted CA certificate lists three sets of trusted CA certificate.



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.



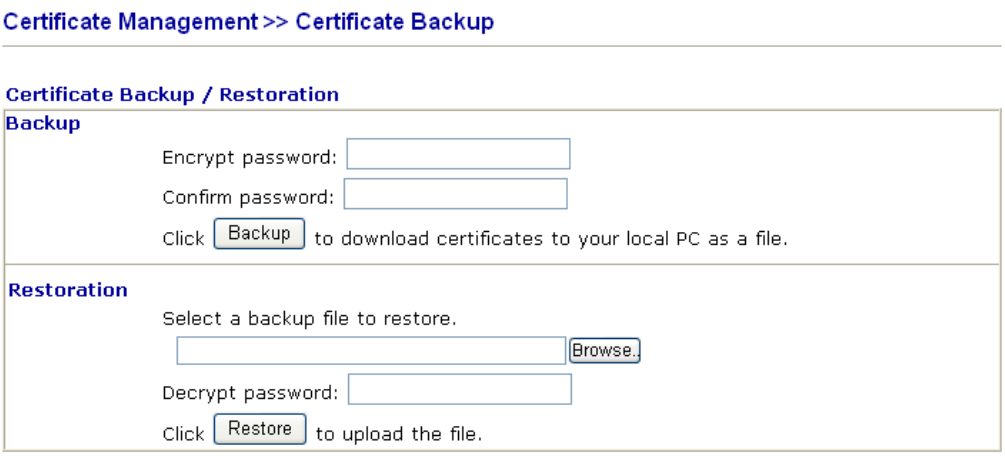
For viewing each trusted CA certificate, click **View** to open the certificate detail information window. If you want to delete a CA certificate, choose the one and click **Delete** to remove all the certificate information.



5.10.3 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 **Confirm password**.

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



5.11 IP PBX

IP PBX（***IP -Private Branch eXchange***）is a private telephone network used within an enterprise. Users of the PBX can share a certain number of outside lines for making telephone calls external to the PBX.

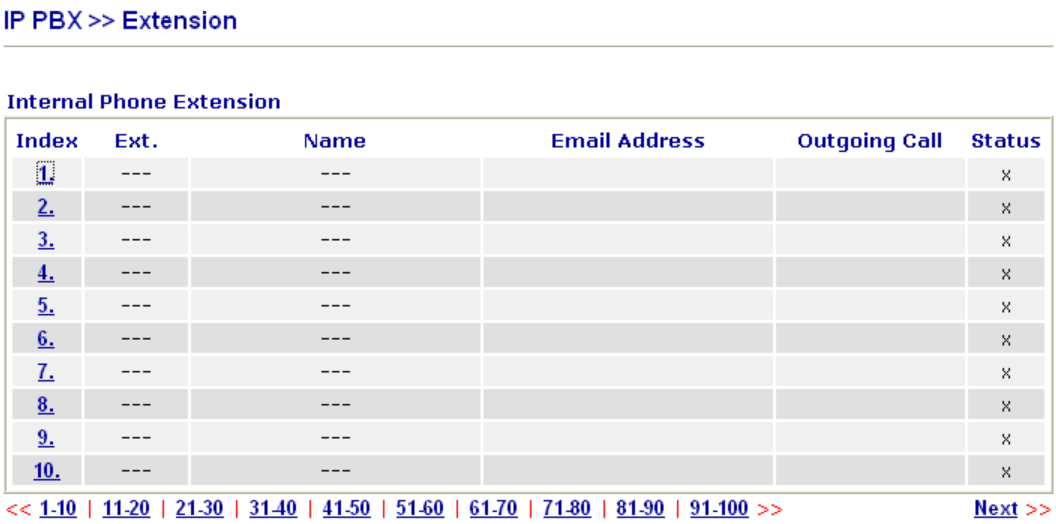
IP PBX integrates the benefits of VoIP/PSTN/ISDN and transfers the message from IP phone into the data that can be accepted by traditional PBX through IP network. It is a new platform that enterprises can use data network to deliver voice. Additionally, to move the IP phone set(s), users just need to plug into another network connector. Such thing simplifies the procedure of moving, increasing, changing and deleting phone settings; also it can join with other system such as CALL center to be a multi-functional communication platform. Moreover, it can save large cost in communication for the enterprise.

This menu can assist users to configure most of settings in IP PBX.

Below shows menu items for IP PBX:

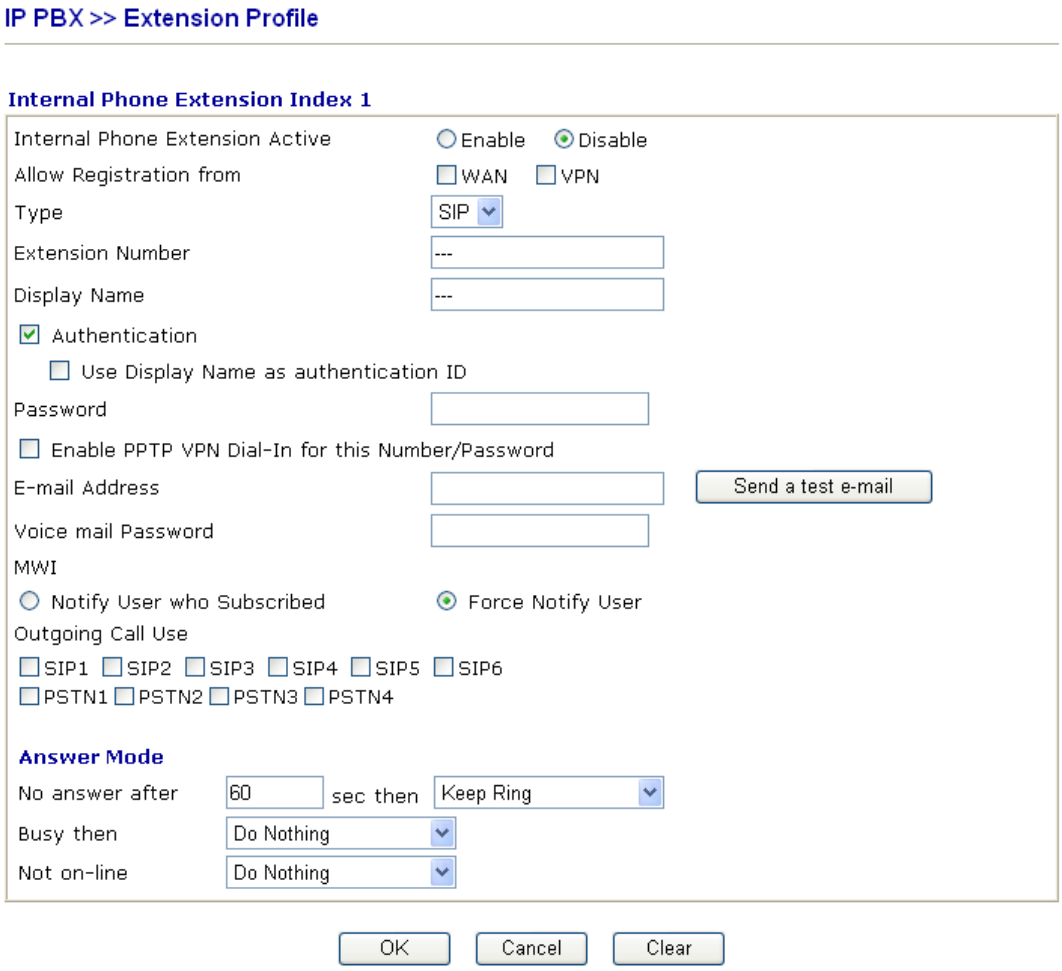
5.11.1 Extension

The system allows you to set **100** extension numbers. Please open **IP PBX>>Extension** to get the following pages.

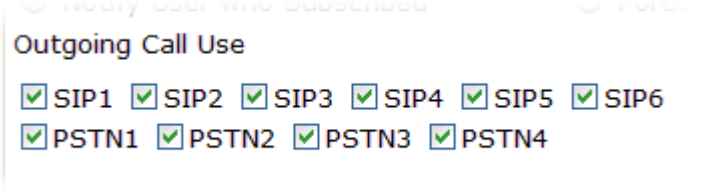
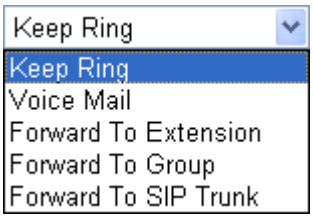
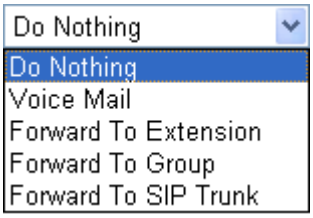


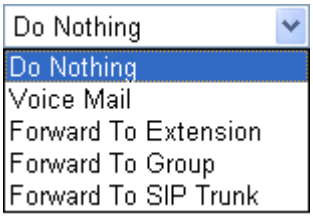
There are 100 groups of extension numbers that you can configure. Please click any number under Index to set detailed configuration.

Note: The items listed under Outgoing Call will be changed according to the module(s) inserted into the device.



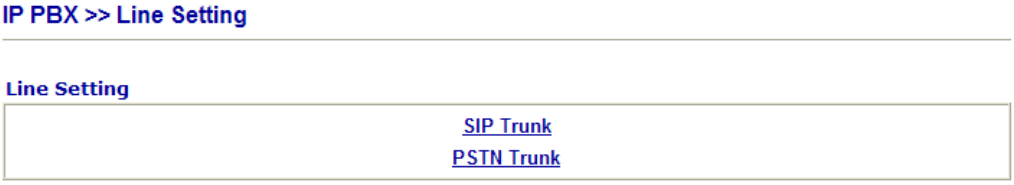
Internal Phone Extension Active	Click **Enable** to invoke such profile.
Allow Registration from	Check **WAN** or **VPN** as the interface for registration of the extension. To get secure communication, choose **VPN** will be better.
Extension Number	Type the number of extension for such index.
User Name	Type a name for the IP PBX to execute authentication. When an IP phone connects to network, IP PBX will use such name for authentication.
Display Name	Used to memorize who uses this extension.
Authentication	Check this box to make the IP PBX executing authentication while the number is dialed.
Password	Type a number for the IP PBX to execute authentication. When an IP phone connects to network, IP PBX will use such password for authentication.
Enable PPTP VPN Dial-In for this Number /Password	Check this box to enable remote user can use this account setting as PPTP remote dial-in authentication account.
E-mail Address	Type an e-mail address to receive media (voice) file sent by incoming calls. **Send a test e-mail**: Click this button to send a test e-mail to

	the mail box you typed here.
Voice Mail Password	Type a password here. When the user wants to listen the voice mail, he/she muse use such password to open it.
MWI (Message Waiting Indicator)	There are two types of MWI for users to choose. Please click the one according to the real application. **Notify User who Subscribed** - The user needs to send out SUBSCRIBE message first. When IPPBX detects new voice message from some extension number or the condition of the voice message is changed, it will transfer "NOTIFY" message to the users within the valid time subscribed. **Force Notify User**- The user does not send out SUBSCRIBE message. The IPPBX will deliver "NOTIFY" message to the users if there is a new message or the user registers on IPPBX again.
Outgoing Call Use	There are several outside lines (SIP accounts) for you to specify for such extension. Please check the one(s) you want. The available boxes listed here will be changed according to the **FXS/FXO** module inserted to VigorIPPBX 3510. 
Answer Mode	Specify the way to process incoming phone calls. **No answer after** ….. – When the incoming phone call is not picked up, it will be processed by keeping, forwarding to certain extension or group or SIP Trunk. Please specify the waiting time and determine the way you want to process.  **Busy then** – When this extension number is busy, you can forward the incoming phone call to other extension number or group or SIP Trunk.  **Not on-line** – When this extension number is not online, you can forward the incoming phone call to other extension number or group or SIP Trunk.



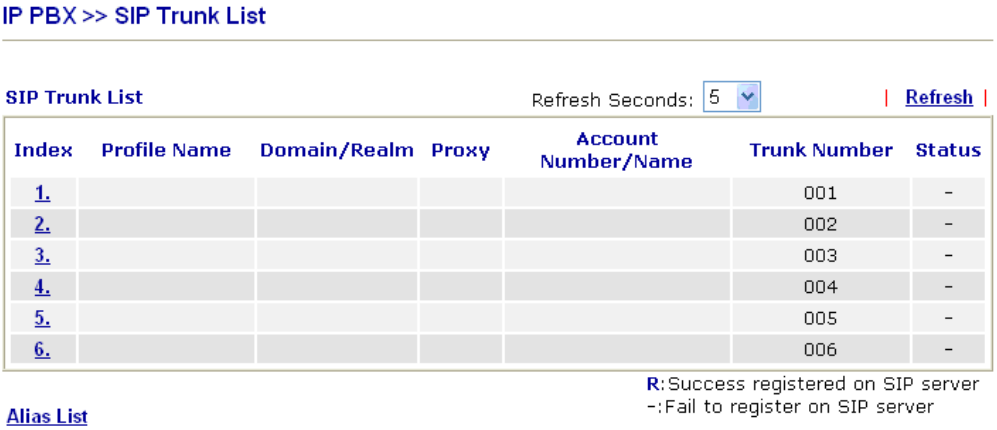
5.11.2 Line Setting

There are six SIP outside lines and one ISDN line provided by this IP PBX device. Users can set them respectively from SIP Trunk and PSTN Trunk.



5.11.2.1 SIP Trunk

This page allows you to set profiles for six SIP outside lines at one time.



Profile Name Display the name for such main account.

Domain/Realm Display domain name or IP address of the SIP **Registrar** server.

Proxy Display the domain name or IP address of SIP **proxy** server.

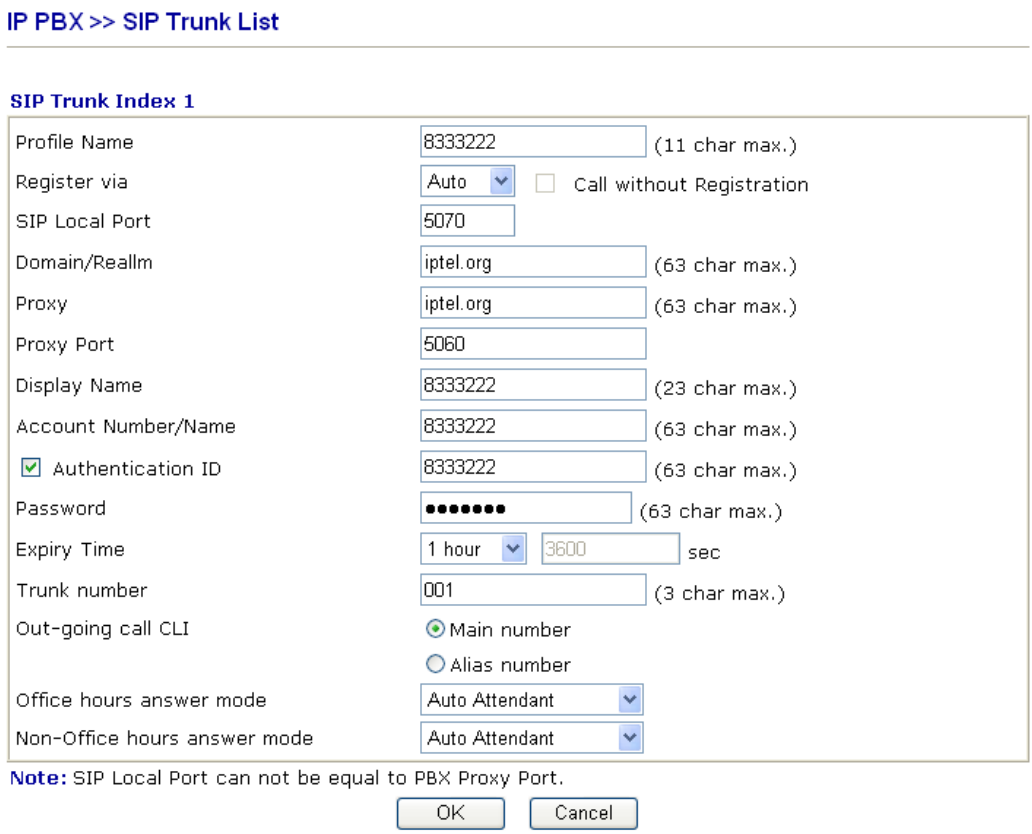
Account Number/Name Display the account name of SIP Address.

Trunk Number Display the short number for such account.

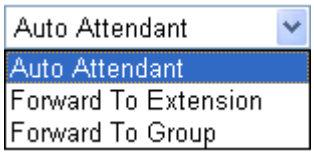
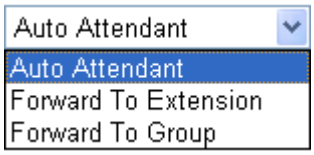
Status Display current status for the account (successful registration or failed registration).

Alias List Allows you to set sub accounts for the main accounts in SIP Trunk.

Please click any number under Index to set detailed configuration.

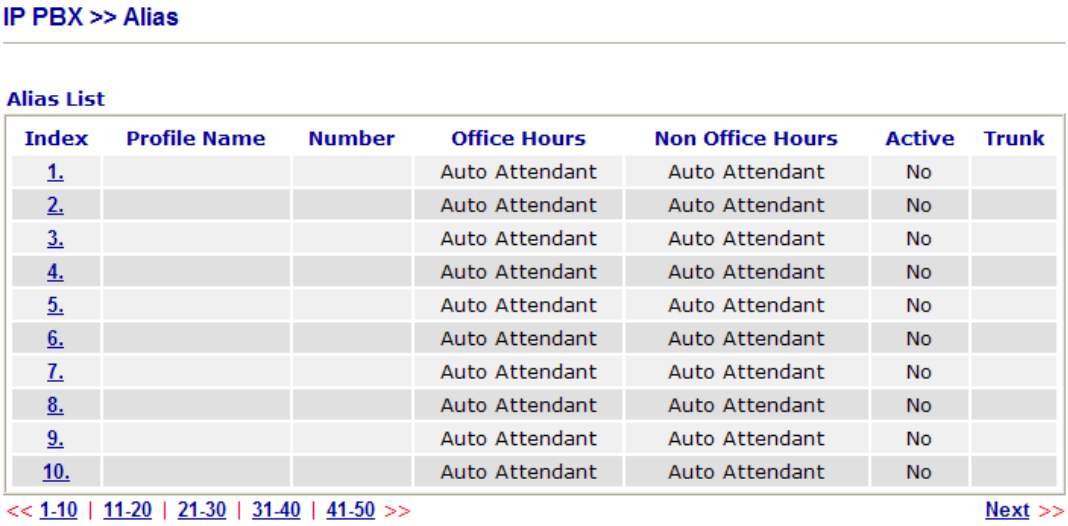


Profile Name	Assign a name for this profile for identifying. You can type similar name with the domain. For example, if the domain name is *draytel.org*, then you might set *draytel-1* in this field.
Register via	If you want to make VoIP call without register personal information, please choose **None** and check the box to achieve the goal. Some SIP server allows user to use VoIP function without registering. Choosing **Auto** is recommended.
SIP Local Port	Set the port number for sending/receiving SIP message for building a session. The default value is **5070.**
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**)
Proxy Port	Set port number for the proxy server.
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	It is 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.
Trunk Number	There are two ways to dial outside lines for an extension number. First, dial a short number and wait for a while. When dial tone appears, please dial the real outside line number. Second, dial a short number and then the real outside line number without waiting for dial tone. The short number is defined here as Trunk Number.
Out-going call CLI	Determine which phone number will be shown to the remote end. **Main number** – Choose this item to display the SIP trunk number. **Alias number** – Choose this item to display the alias phone number, that is, the sub account.
Office hours answer mode	Set the answering mode for such outside line in office time. You can specify it with Auto Attendant (AA), or forward it to any Extension or Group directly. 
Non-office hours answer mode	Set the answering mode for such outside line in non-office time. You can specify it with Auto Attendant (AA), or forward it to any Extension or Group directly. 

Alias List

Click the **Alias List** link to access into the configuration page as shown below.



Profile Name Display the alias name for such sub account.

Number Display the phone number of such account.

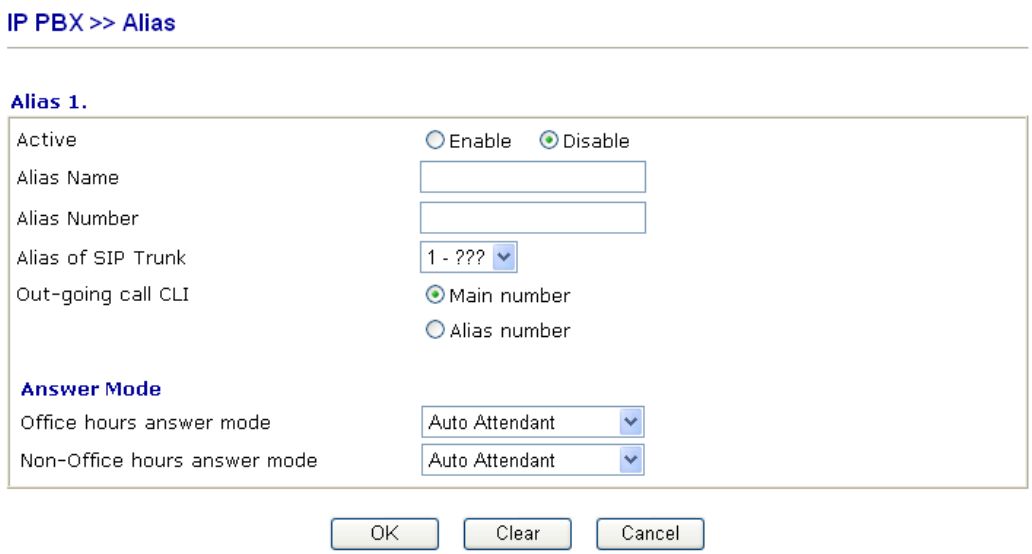
Office Hours Display the selected answer mode for office hours.

Non Office Hours Display the selected answer mode for non office hours.

Active Display current activation status for such account, enabled or disabled.

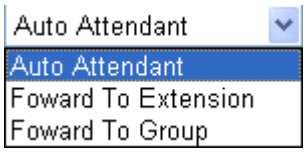
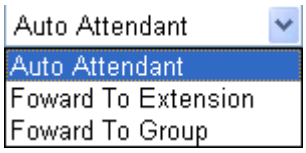
Trunk Display the SIP Trunk for such sub account attached.

You can set 50 profiles as alias for SIP Trunk list. Click the number under Index to set detailed configuration.



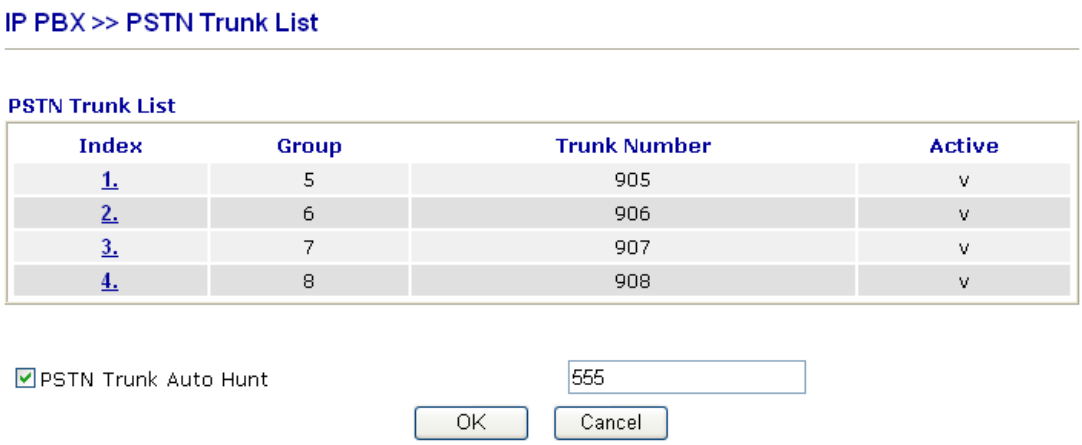
Active Click **Enable** to activate this entry. Or, click **Disable** to inactive this entry.

Alias Type a name for such account.

Alias Number	Type a number for such account.
Alias of SIP Trunk	Choose one of the items listed in SIP Trunk List for this alias profile.
Out-going call CLI	Determine which phone number will be shown to the remote end. **Main number** –Choose this item to display the number which set in corresponding SIP TRUNK. **Alias number** – Choose this item to display the alias number.
Office hours answer mode	Set the answering mode for such outside line in office time. You can specify it with Auto Attendant (AA), or forward it to any Extension or Group directly. 
Non-office hours answer mode	Set the answering mode for such outside line in non-office time. You can specify it with Auto Attendant (AA), or forward it to any Extension or Group directly. 

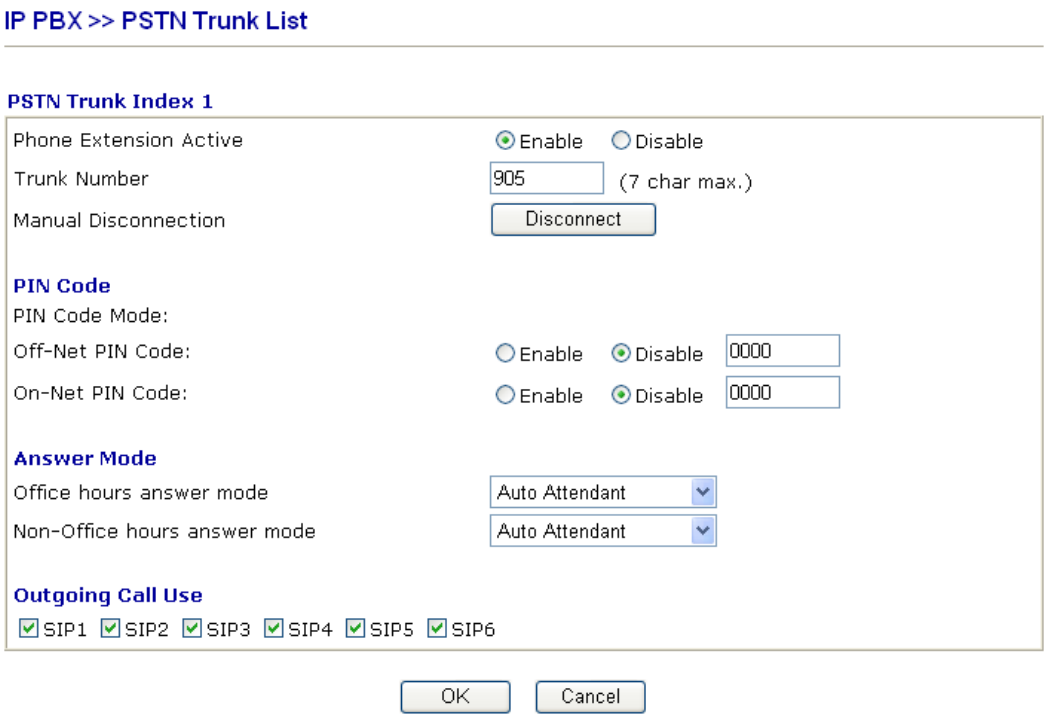
5.11.2.2 PSTN Trunk

This page allows you to set profiles for PSTN outside lines at one time.



Index	Display the number that you can click to edit the trunk profile.
Group	Display the name of each entry.
Trunk Number	Display the default trunk number of each entry.
Active	V – means current trunk number is available.
PSTN Trunk Auto Hunt	Display the default value.

Please click any number under Index to set detailed configuration.



Phone Extension Active — Click **Enable** to invoke this setting.

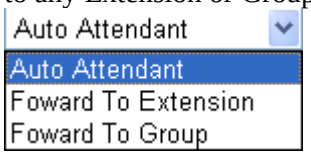
Trunk Number — The default setting is 905. Please modify it to meet the request for your PSTN environment.

Manual Disconnection — To disconnect the PSTN trunk, simply click the **Disconnect** button. The PSTN phone call will be disconnected immediately.

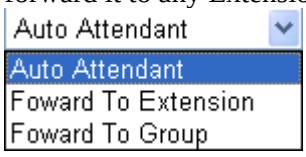
PIN Code Mode — **Off-Net PIN Code ID** - Click **Enable** to invoke this setting. Type the PIN code number to make off-net call to PSTN trunk.

On-Net PIN Code ID - Click **Enable** to invoke this setting. Type the PIN code number to make on-net call to PSTN trunk.

Office hours answer mode — Set the answering mode for such outside line in office time. You can specify it with Auto Attendant (AA), or forward it to any Extension or Group directly.



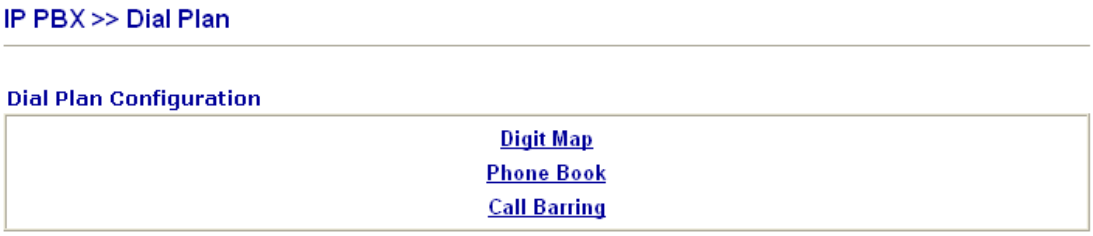
Non-office hours answer mode — Set the answering mode for such outside line in non-office time. You can specify it with Auto Attendant (AA), or forward it to any Extension or Group directly.



Outgoing Call Use — There are several outside lines (SIP accounts) for you to specify for such extension. Please check the one(s) you want.

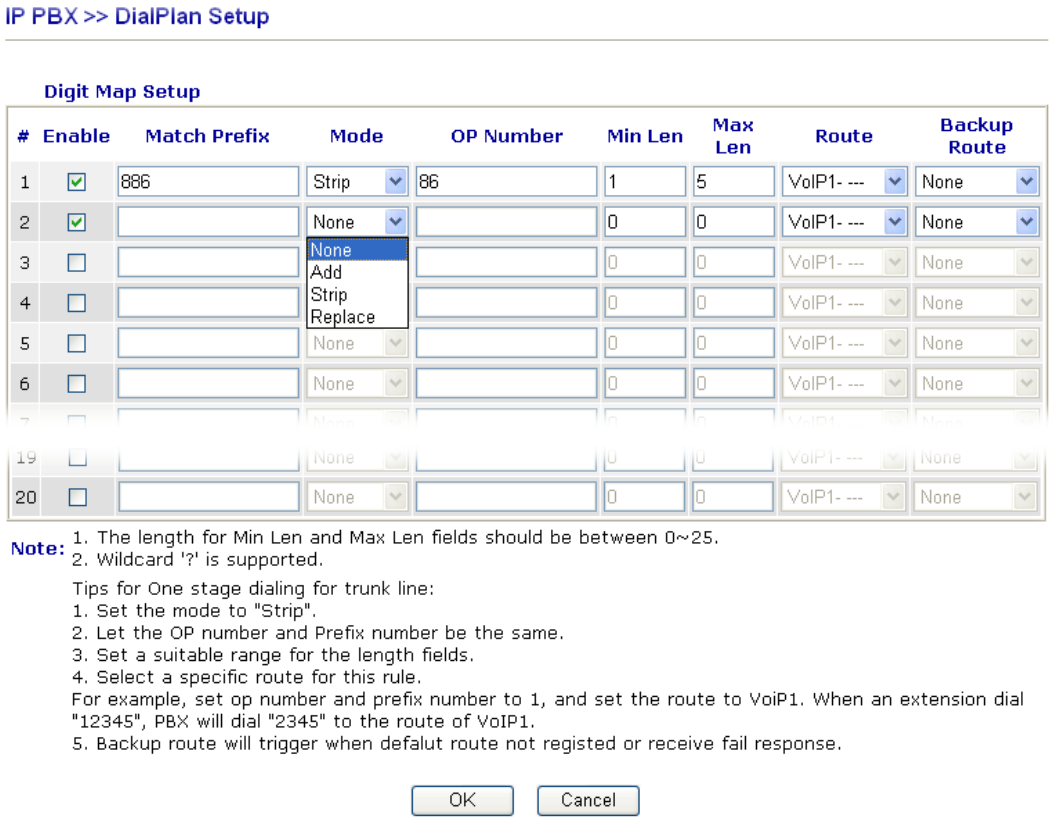
The available boxes listed here will be changed according to the FXS/FXO module inserted to VigorIPPBX 3510.

5.11.3 Dial Plan



5.11.3.1 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.



Note: 1. The length for Min Len and Max Len fields should be between 0~25.
2. Wildcard '?' is supported.

Tips for One stage dialing for trunk line:
1. Set the mode to "Strip".
2. Let the OP number and Prefix number be the same.
3. Set a suitable range for the length fields.
4. Select a specific route for this rule.

For example, set op number and prefix number to 1, and set the route to VoIP1. When an extension dial "12345", PBX will dial "2345" to the route of VoIP1.

5. Backup route will trigger when defalut route not registed or receive fail response.

OK Cancel

Enable Check this box to invoke this setting.

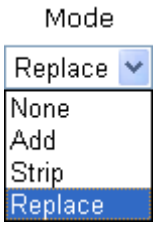
Match Prefix It is used to match with the number you dialed and can be modified with the **OP Number** by the mode (add, strip or replace).

Mode **None** - No action.

Add - When you choose this mode, the OP number will be added before the prefix number for calling out through the specific route.

Strip - When you choose this mode, partial or the whole prefix number will be deleted according to the OP number. 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.

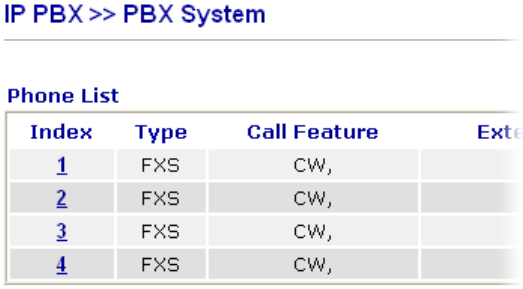


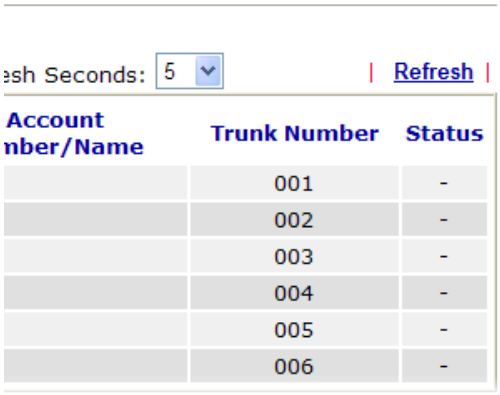
OP Number — The front number you type here is the first part of the account number that you want to execute special function (according to the chosen mode) by using the prefix number.

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.

Route — Choose the one that you want to enable the match prefix settings from the saved SIP accounts. Please set up one SIP account first to make this route available. This item will be changed according to the port settings configured in **IP PBX>>PBX System>>Phone Settings** and **IP PBX>>Line Settings>>SIP Trunk**.

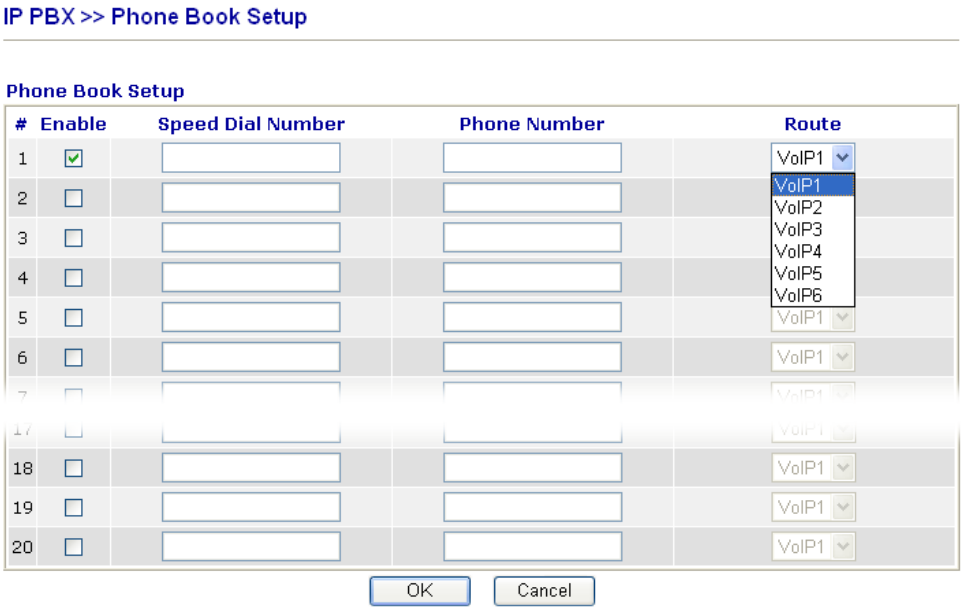




Backup Route It will be triggered when the original route is not registered or receives failed response.

5.11.3.2 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 Number**. There are total 20 index entries in the phonebook for you to store all your friends and family members’ phone numbers.



Enable Check the box to enable the entry.

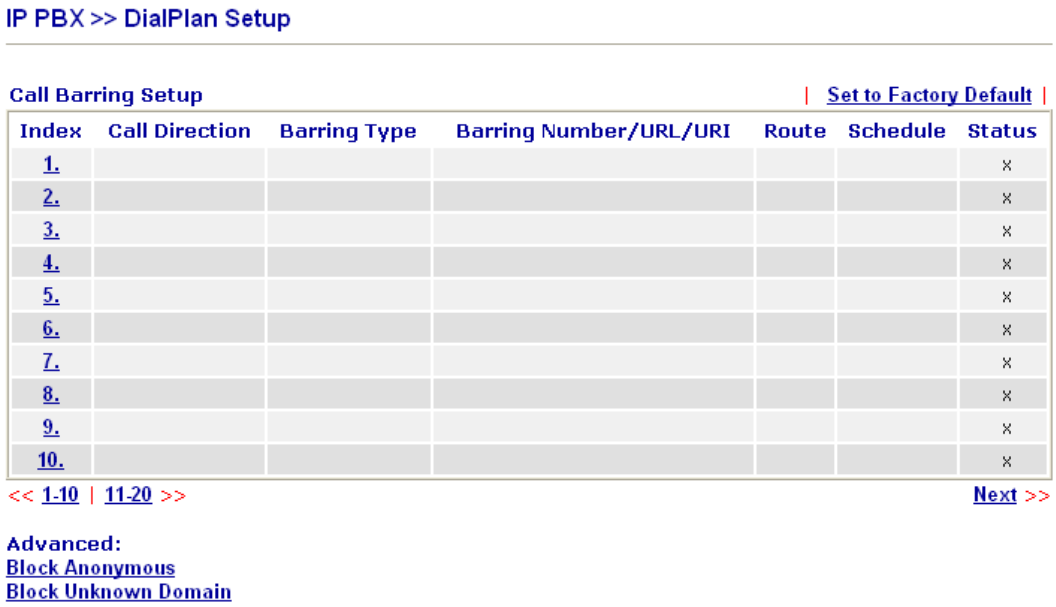
Speed Dial Number Type the digit number (maximum 6) in this field which can dial to the client with the phone number specified later.

Phone Number Type the complete phone number (maximum 19) for the client that you want to dial out.

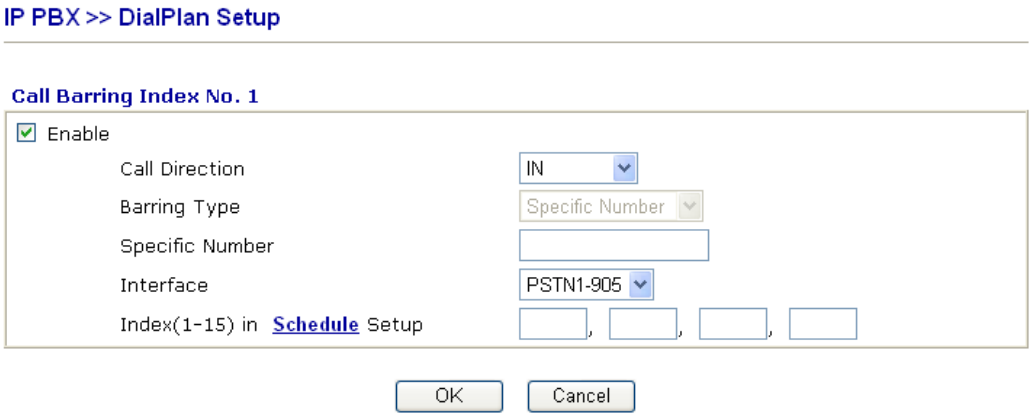
Route Choose the interface (from VoIP 1 to VoIP 6) for the phone call to dial out.

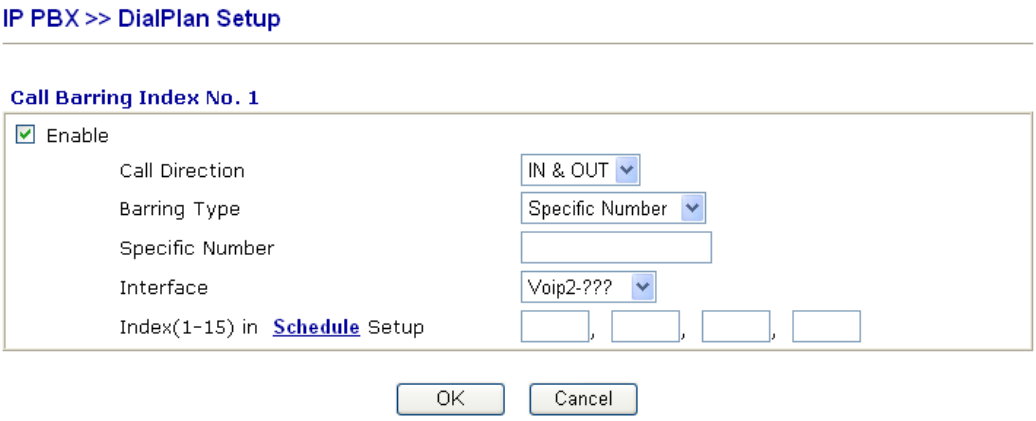
5.11.3.3 Call Barring

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.

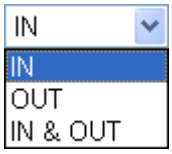




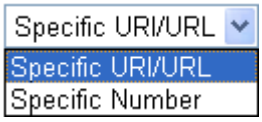
Enable Click this to enable this entry.

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

outgoing calls.



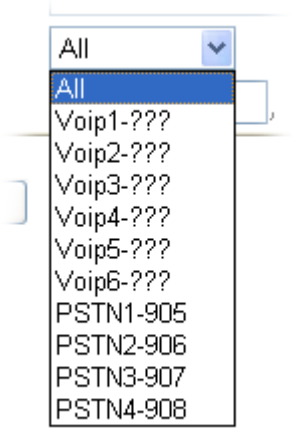
Barring Type Determine the type of the VoIP phone call, URI/URL or number. It will bring out different setting options.



It will be invalid if you choose PSTN-XX as the interface.

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

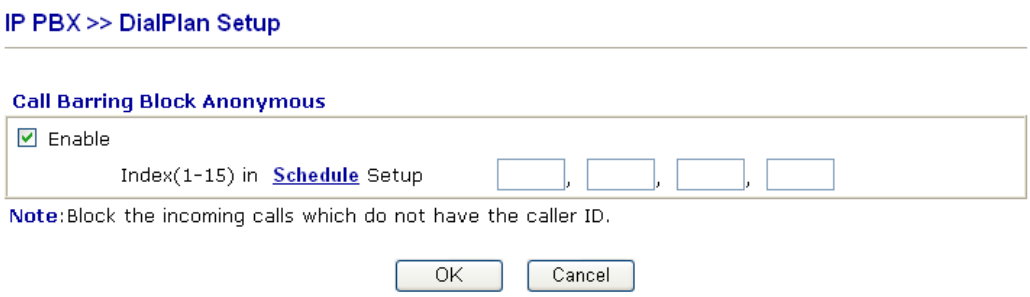
Interface "All" means all the phone calls will be blocked with such mechanism. Or you can specify certain port (set in **IP PBX>>Line Setting>> SIP Trunk**) to be blocked by choosing from the drop down list.



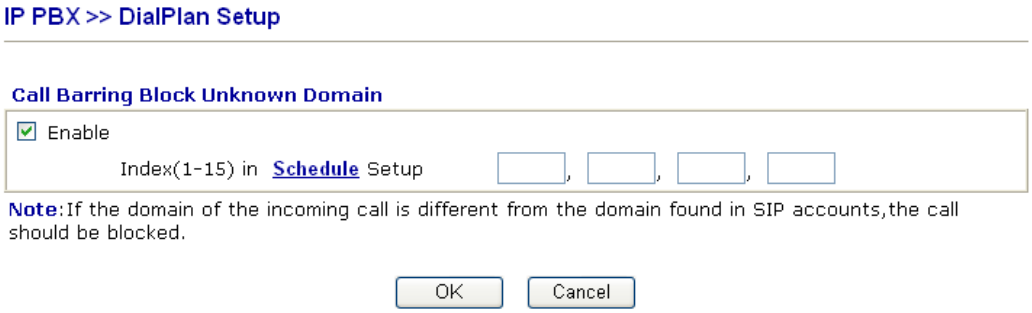
Index (1-15) in Schedule Enter the index of schedule profiles to control the call barring according to the preconfigured schedules. Refer to section **Application >>Schedule** for detailed configuration.

Additionally, you can set advanced settings for call barring such as **Block Anonymous** or **Block Unknown Domain**. 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 specified in the following window. Such controlling also can be done based on preconfigured schedules.



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

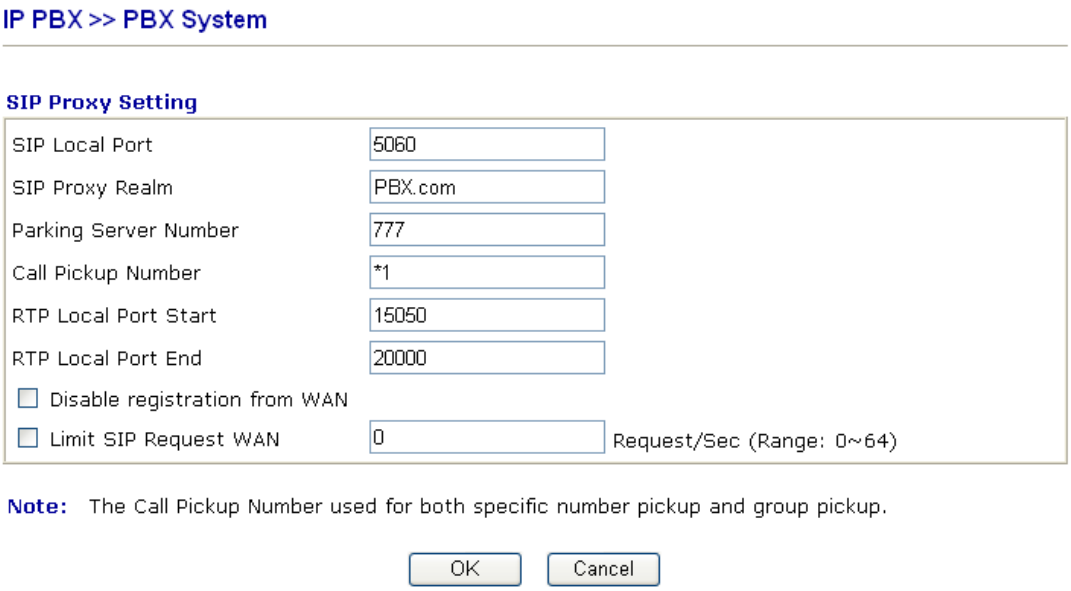


5.11.4 PBX System

This page allows you to set relational (advanced) settings for IP PBX device.

5.11.4.1 SIP Proxy Setting

To make the IP phone to be registered in IP PBX device successfully, it is necessary for the users to configure settings in this page.



SIP Local Port Set a port number as SIP local port. The default setting is 5060.

SIP Proxy Realm Type SIP service domain name. In full SIP URI, such is the part after @ symbol.

Parking Server Number This number is used to communicate with the parking server and invoke the parking function. The default setting number is “777”.

1. When you receive a phone call and need to go to the remote end to talk with the same caller, you have to hold the phone call and transfer the call to this number from VoIP phone set.
2. The parking sever will give you another voice number (e.g., your parking number is XXXX).

   Please remember it and hang up the phone set.
3. Next, use another phone set in remote end to communicate with that caller again by dialing the voice number (XXXX).

Call Pickup Number Press the number specified here to pickup a call which is ringing on another extension. For specific extension pickup, press 'pickup number' + 'extension number' + #; for group pickup, just press 'pickup number' + #.

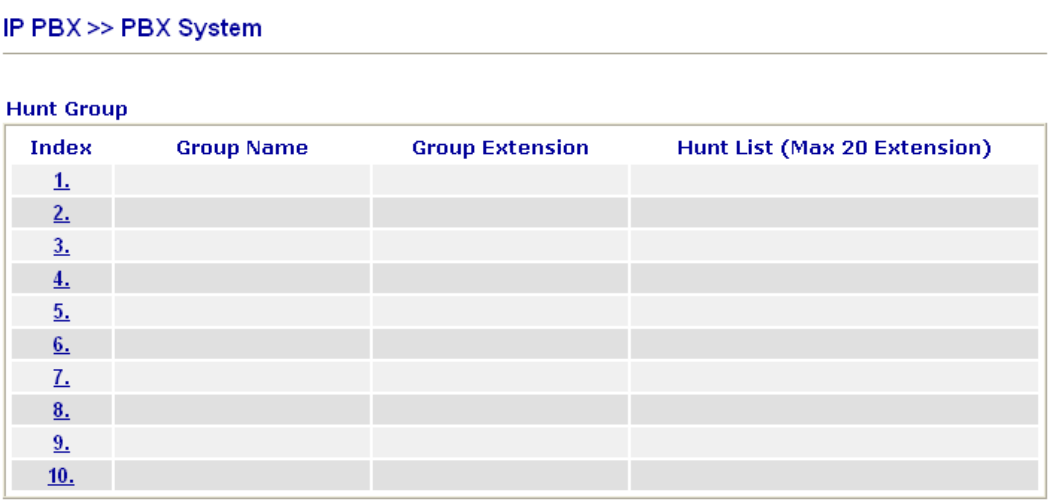
For example, pickup number is *1 and 101 ~ 105 are set in the same hunt group. When an incoming call rings extension 101; the extension 102~105 can just dial ***1#** to pickup the call. However, if the extension 106 wants to pickup that call, it needs to dial ***1101#**.

RTP Local Port Start/ If your VoIP service provider gave you such information,

RTP Local Port End	please type the port number for RTP traffic. Otherwise, keep the default setting. For one port number used, type the same port number in RTP Local Port Start and RTP Local Port End fields. To set a range for port numbers type different port numbers in RTP Local Port Start and RTP Local Port End fields.
Disable registration from WAN	Check this box to disable the SIP account registration from WAN side. It can prevent unauthorized users to use your system. If this option is selected, you can still enable certain extensions to register from **WAN/VPN** on individual extension profile page.
Limit SIP Request WAN	Choose this item to restrict number of request per second from WAN side.

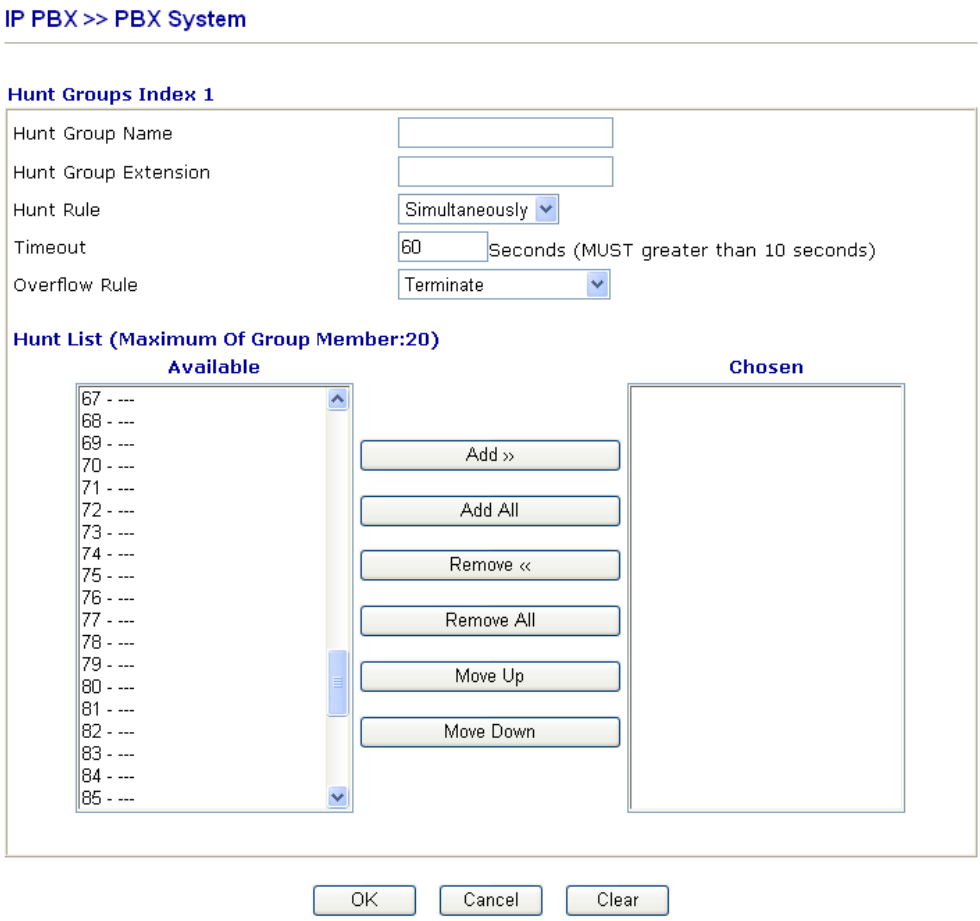
5.11.4.2 Hunt Group

This page allows you to make several extension numbers under certain group. Thus, when a phone call incomes, all the extension numbers under such group will ring.

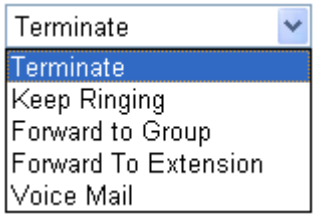


Index	You can set 10 groups for using in different conditions. Simply click the number under Index to specify detailed information.
Group Name	Display the name of such group.
Group Extension	Display the extension number of such group.
Hunt List	Display the members inside the group.

Click any index number to display the hunt group setup page.



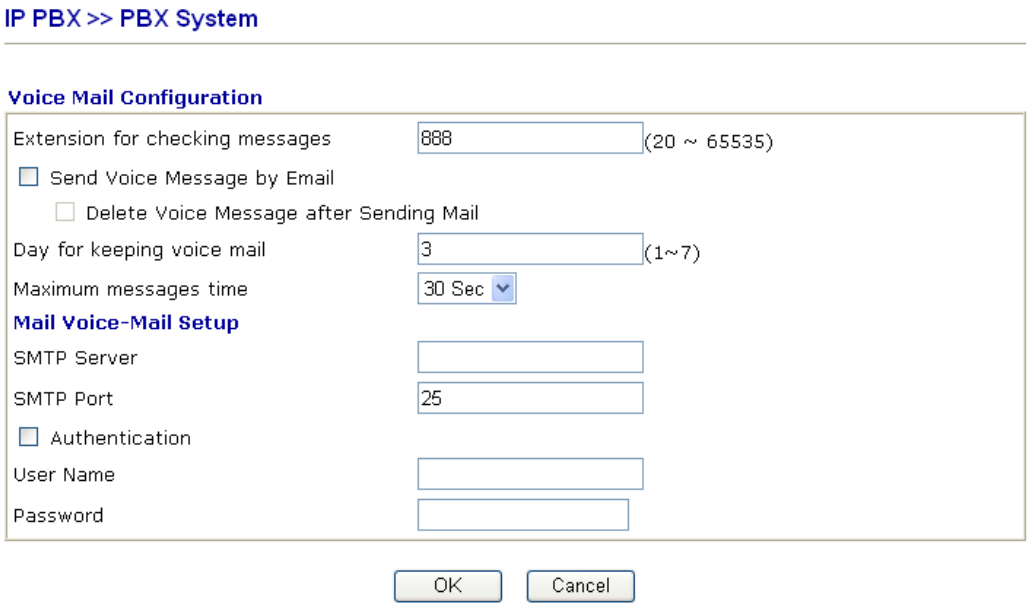
Hunt Group Name	Type suitable name for such group.
Hunt Group Extension	Type extension number for such group.
Hunt Rule	Use the drop down menu to choose rule for such group. **Simultaneously** – Choose such rule can make all the phones in the groups ring while receiving incoming calls. **Sequentially** - Choose such rule can make all the phones in the groups ring one by one while receiving incoming calls.
Timeout	Set the timeout for such group. The default setting is 60 seconds. After timeout, the system will execute overflow rule selected below.
Overflow Rule	When the hunt group does not have any response to an incoming call, the call will be processed with the way chosen here such as being terminated, keeping ringing, forwarding to certain group, forwarding to certain extension or leaving voice mail and so one. If you choose Forward to Group or Forward to Extension, a drop down box will appear for you to choose the extension / group to transfer to.



Add>>	Click this button to move the selected item in Available area to Chosen area.
Add All	Click this button to move all of the items in Available area to Chosen area.
Remove<<	Click this button to move the selected item in Chosen area to Available area.
Remove All	Click this button to clear all of the selections in Chosen area.
Move Up	Click this button to move the selected item to the upper place.
Move Down	Click this button to move the selected item to the lower place.

5.11.4.3 Voice Mail Configuration

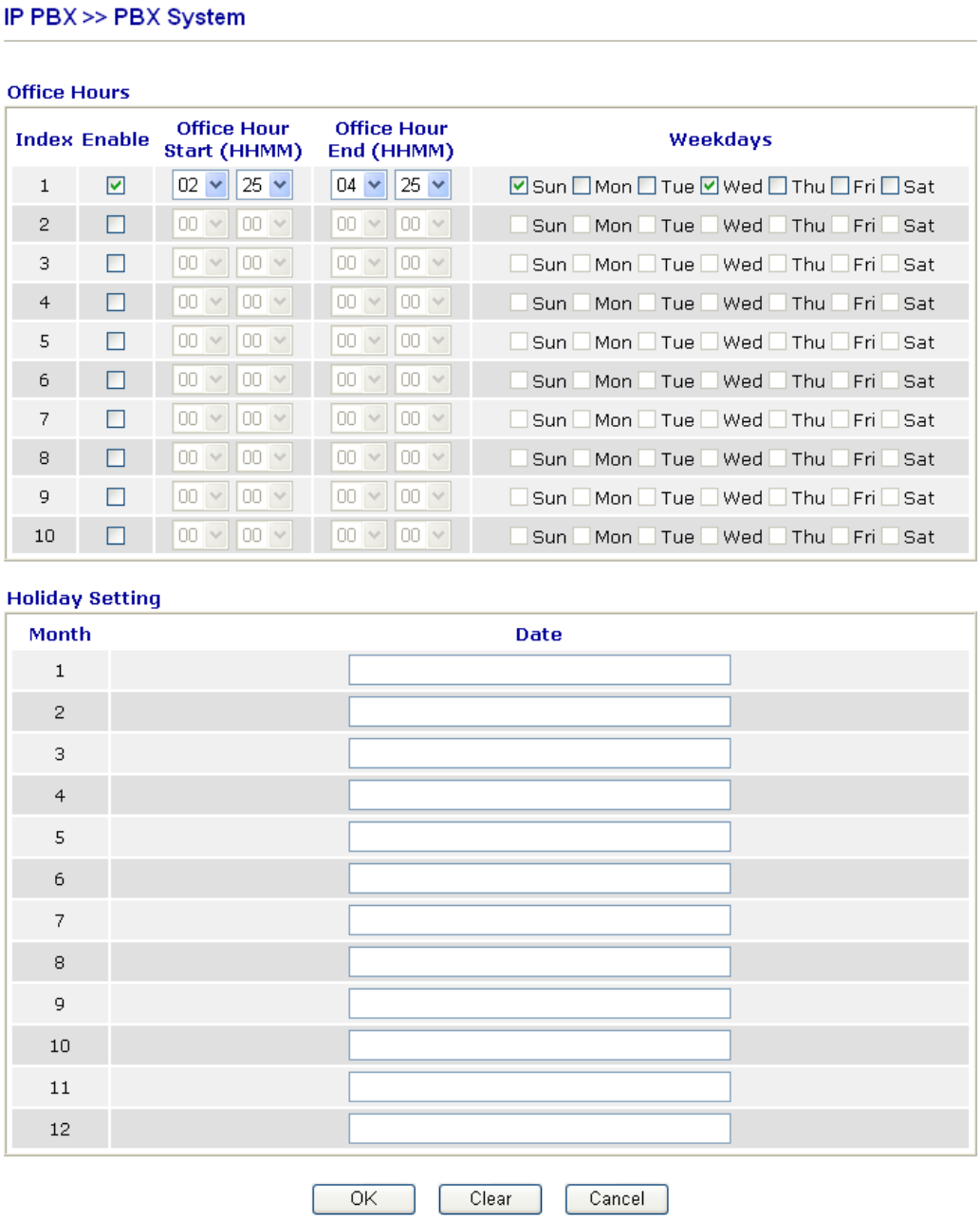
This page allows users to set actions for voices mails.



Extension for checking messages	The number specified here is used for the user to listen personal voice mail from IP PBX device.
Send Voice Message by Email	IP PBX can send the voice mail to the specified e-mail address for the incoming call if you check this box. **Delete Voice Message after Sending Mail** - IP PBX can send the voice mail to the specified e-mail address for the incoming call directly and delete the temporary file in IP PBX if you check this box.
Days for keeping voice mail	Type the days for keeping each voice mail.
Maximum message time	Type the recording length for each voice mail.
SMTP Server	Type IP address or domain name for the server specified for receiving voice messages.
SMTP Port	Type the port number for the server. The default value is 25.
Authentication	Check this box to authenticate the mail server.
User Name	Type a name for IP PBX to authenticate the mail server automatically while connecting.
Password	Type a password for IP PBX to authenticate the mail server automatically while connecting.

5.11.4.4 Office Hours

You can set ten groups of office hours including starting point, ending point on duty day(s).



Office Hour Start — Use the drop down menu to choose the time as the starting point.

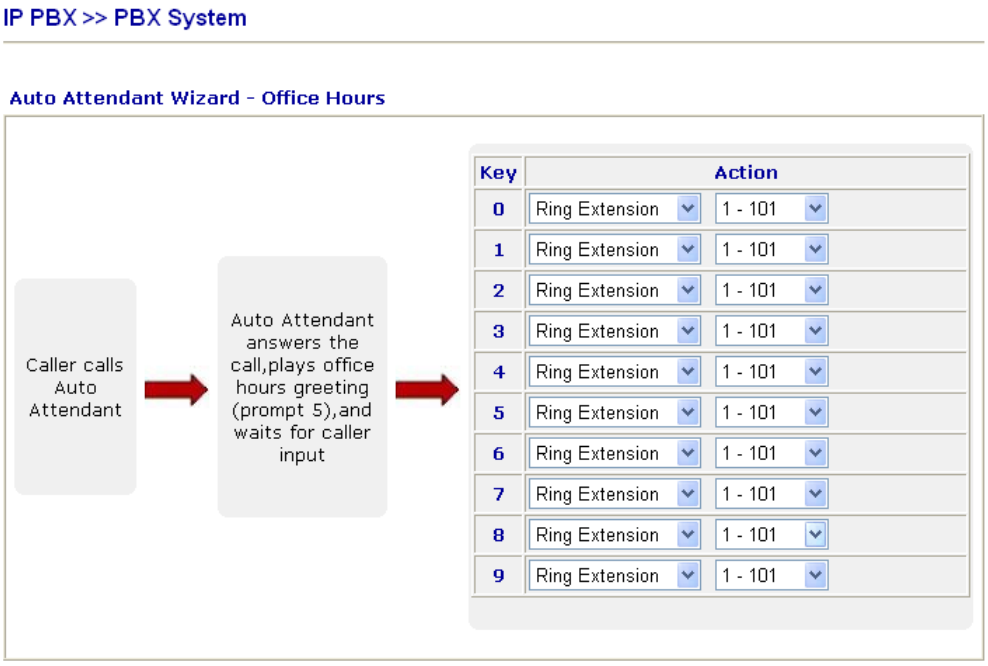
Office Hour End — Use the drop down menu to choose the time as the ending point.

Weekdays — Check the day(s) to apply the office hour for that index.

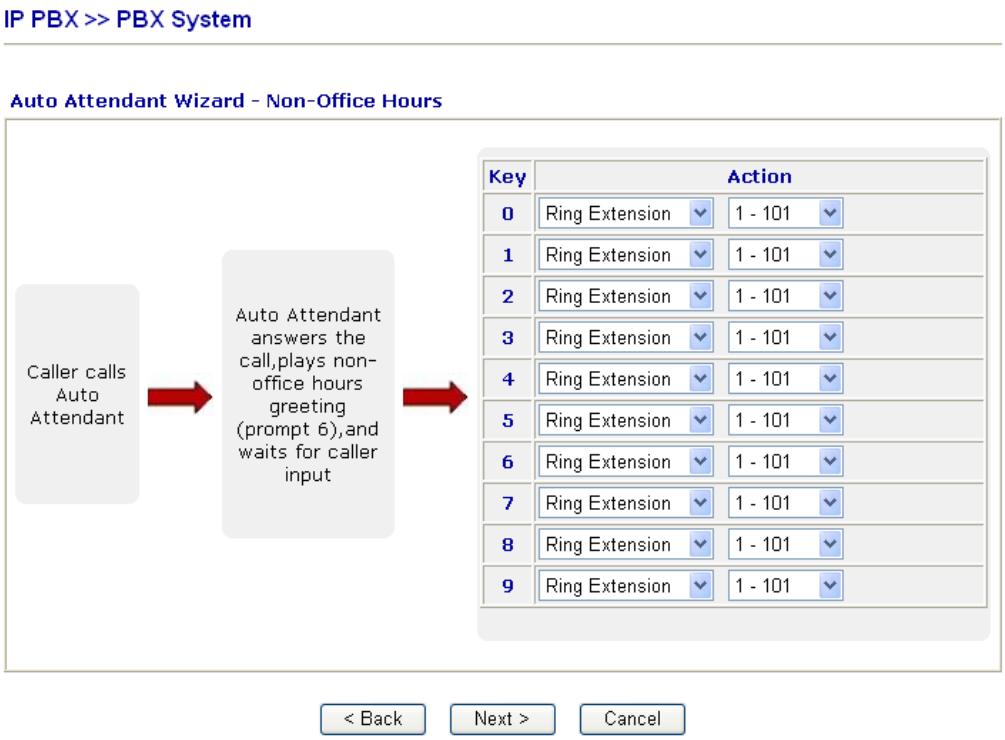
Date — Specify date(s) for applying the office hour settings in holiday, for example, type 2,4 6 & 7 in the field of Date for Month 1. It means January 2,4,6 & 7 will apply the office hour settings configured in this page.

5.11.4.5 Auto Attendant Wizard

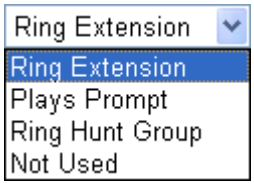
The first page is configured for phone calls in office hours.



Click **Next**. The second page is configured for phone calls in non-office hours.



Key 0-9	Key 0 – 9 can be set with different actions.
Action	Drop down menu contains Ring Extension /Plays Prompt/Ring Hunt Group/Not Used.



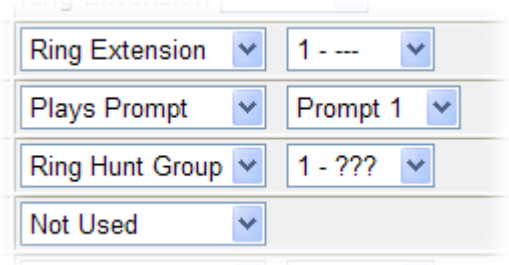
Ring Extension - Only the extension number selected here will ring.

Plays Prompt - Audio file will be played automatically.

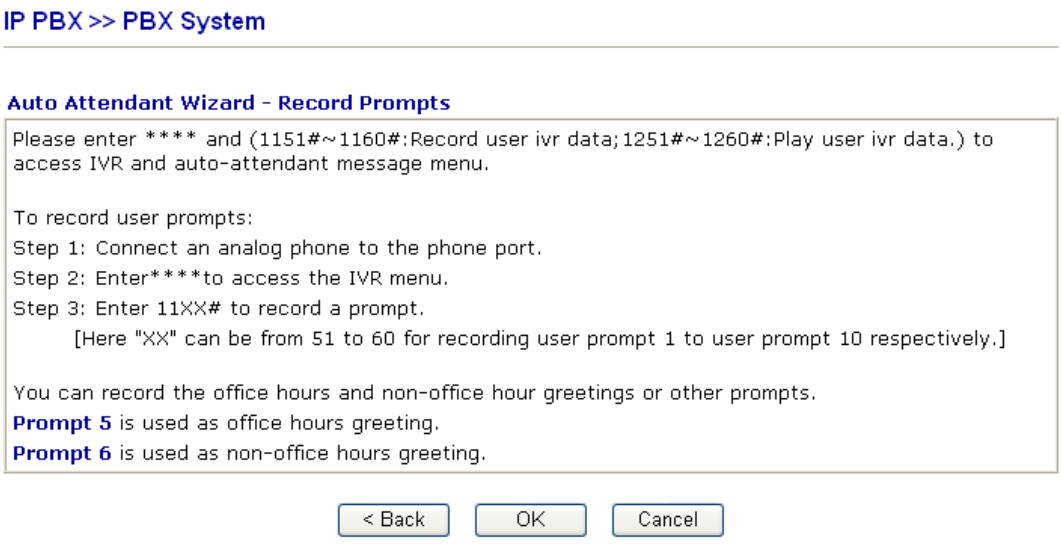
Ring Hunt Group – Only the extension number within the Hunt Group will ring.

Not Used – Nothing will be done for the key.

Drop down menu 2 contains extension name (ex. Tom, Mike)] or prompt [Prompt 1~ Prompt 10, audio files] or Hunt Group Name [(ex. Sales, RD2)]. It will be changed according to drop down menu 1.

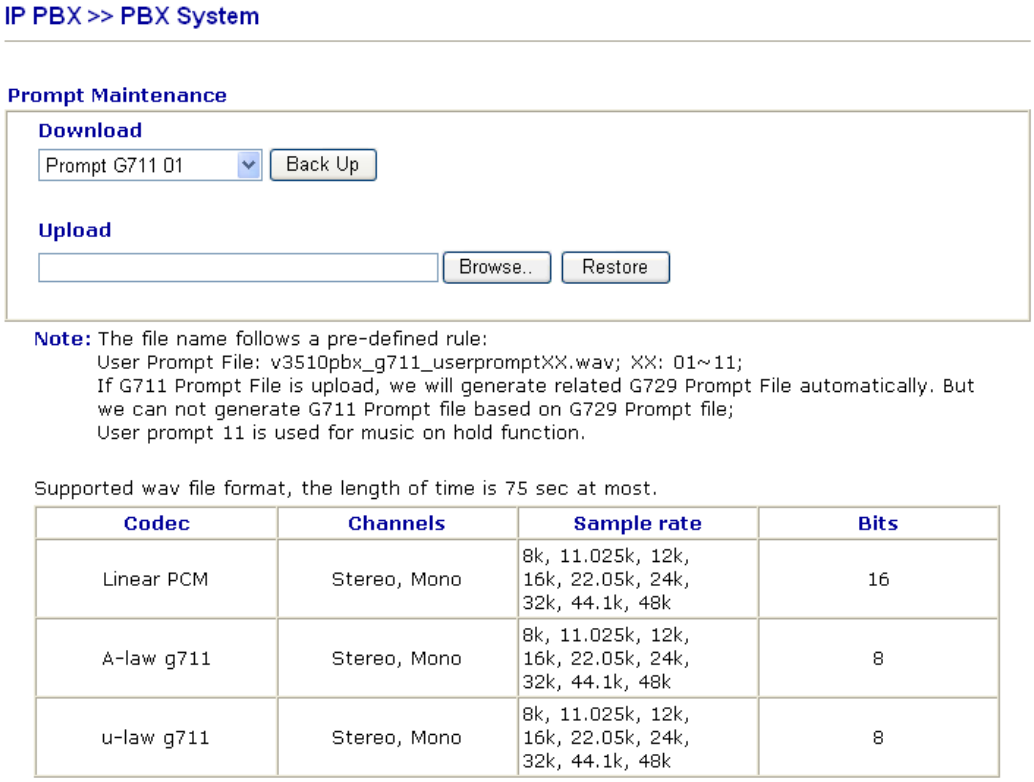


Finally, the following window will appear.



5.11.4.6 Prompt Maintenance

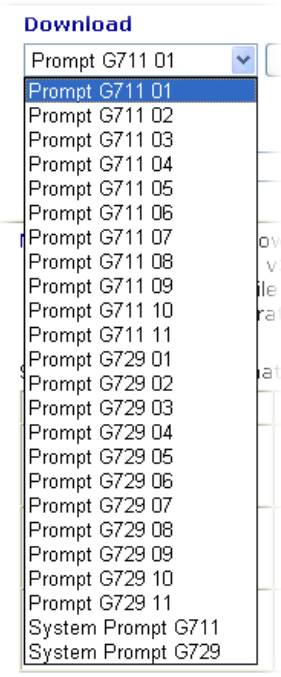
The IP PBX system provides several audio files for users to choose for playing. Moreover, users can upload other audio files from USB storage or hard disk or others to make the IP PBX system playing. Users can record audio files and upload to router or download to PC. However, the file format of the audio file must follow the rule stated on the web page. Users can record the audio files through a phone set connected to the router or use audio record program on PC.



Codec	Channels	Sample rate	Bits
Linear PCM	Stereo, Mono	8k, 11.025k, 12k, 16k, 22.05k, 24k, 32k, 44.1k, 48k	16
A-law g711	Stereo, Mono	8k, 11.025k, 12k, 16k, 22.05k, 24k, 32k, 44.1k, 48k	8
u-law g711	Stereo, Mono	8k, 11.025k, 12k, 16k, 22.05k, 24k, 32k, 44.1k, 48k	8

Download

The audio file can be saved with IVR file format or WAV file format. In general, it will be saved in the router's memory after you record it. To back up the audio file(s) (saved in FLASH of the router) to your computer, please choose the one you want from the drop-down menu and click **Back Up**.



Prompt 1 to prompt 10 will be used for user-defined audio files (file format must be .WAV). System Prompt file is provided by router firmware.

Upload System Prompt file is provided by router firmware. To use such audio file, you have to upload it to flash memory of the router after finishing firmware update.
Click this **Browse** button to browse and choose other audio files.

Restore Click this button to save the file to the router. Next time, the audio file will be played in IP PBX system.

Upload prompts to your router

You can modify and customize the default system prompt by using the following steps.

Please follow the steps below to upload System Prompt to your router:

1. Please use *DOS-BOX FTP client* (Windows built-in FTP client utility) to login VigorIPPBX FTP server.
2. Press Enter to pass authentication.
3. Type **put v3510_sysprompt.ivr**.
4. Wait for a while. The message of **226 System prompts file has been uploaded successfully** will appear
5. Type **put v3510_g729_sysprompt.ivr**.
6. Wait for a while. The message of **226 System prompts G7.729 file has been uploaded successfully** will appear
7. Type **quit** to close FTP client. **221 Goodbye! Router will be reboot now** will appear and the router will reboot.

Please follow the steps below to upload G.729 user Prompts to your router:

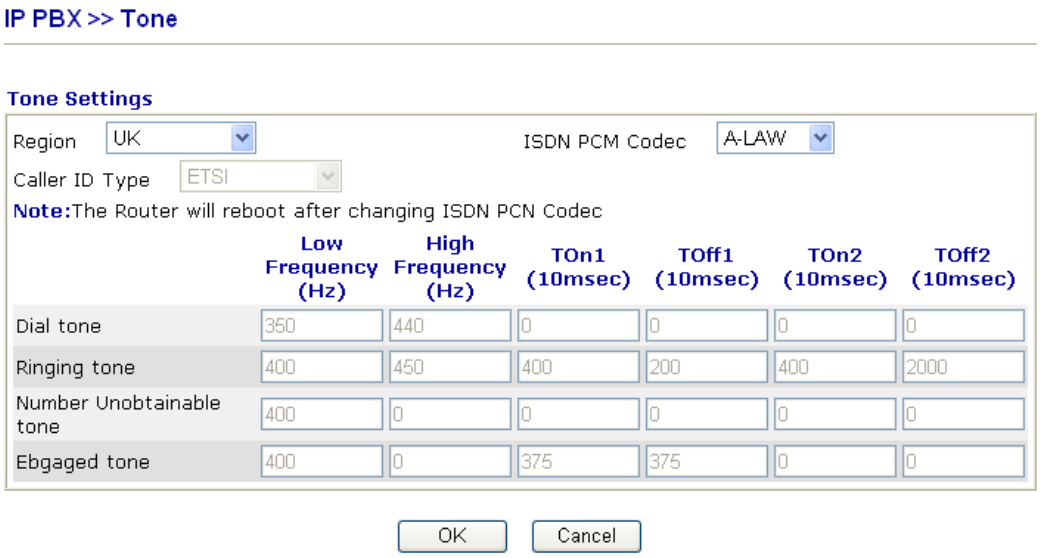
1. Please use *DOS-BOX FTP client* (Windows built-in FTP client utility) to login VigorIPPBX FTP server.
2. Press Enter to pass authentication.
3. Type **put v3510_g729_userprompt.ivr**.
4. Wait for a while. The message of **226 user prompts G.729 file has been uploaded successfully** will appear.
5. Type **quit** to close FTP client. **221 Goodbye! Router will be reboot now** will appear and the router will reboot.

Please follow the steps below to download G.729 user Prompts to your computer:

1. Please use *DOS-BOX FTP client* (Windows built-in FTP client utility) to login VigorIPPBX FTP server.
2. Press Enter to pass authentication.
3. Type **get v3510_g729_userprompt.ivr**.
4. Wait for a while. The message of **226 File sent OK** will appear.
5. Type **quit** to close FTP client.

5.11.4.7 Tone Setting

Tone setting is provided for fitting the telecommunication custom for the local area of the router installed. Wrong tone setting 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.

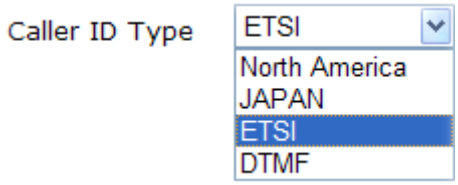


Region Select the proper region which you are located. The common settings of **Caller ID Type**, **Dial tone**, **Ringing tone**, **Busy tone** and **Congestion tone** will be shown automatically on the page. If you cannot find out a suitable one, please choose **User Defined** and fill out the corresponding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

ISDN PCM Code Used to change to A-law or u-law for ISDN network.

Caller ID Type It is available only when **User Defined** is selected in the field of **Region**. Select the caller ID type for setting Dial tone, Ringing tone, Busy tone and Congestion tone respectively.



5.11.4.8 Phone Setting

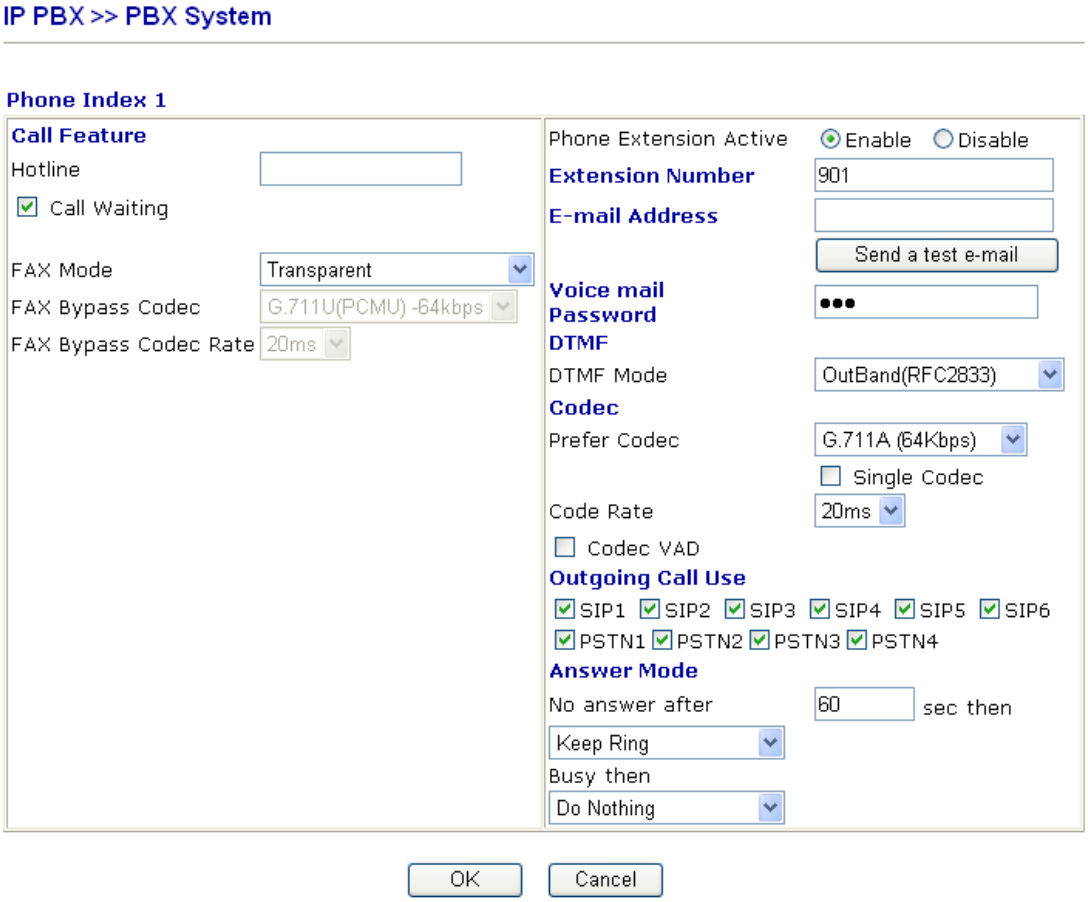
This page allows user to set phone settings for FXS module.

IP PBX >> PBX System

Phone List

Index	Type	Call Feature	Extension Number	DTMF Relay	Codec
1	FXS	CW,	901	OutBand	G.729A/B
2	FXS	CW,	902	OutBand	G.729A/B
3	FXS	CW,	903	OutBand	G.729A/B
4	FXS	CW,	904	OutBand	G.729A/B

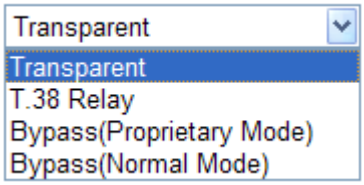
Click any index number link to open the following page for configuration.



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.

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.

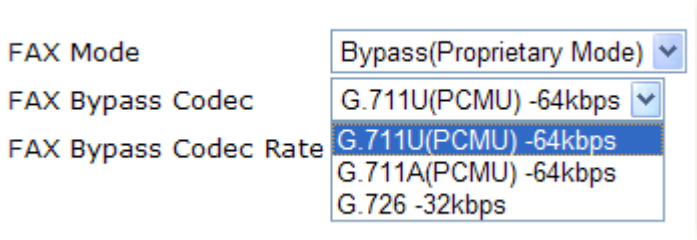
FAX Mode The FAX function mode. There are several options:



Transparent: FAX will be transmitted via voice channel; no fax relay and no Codec change will be involved.
T.38 Relay: Using T.38 Fax Relay. This is the default value.
Bypass: Once FAX is detected, the Codec will automatically switch to a high bit rate type (G.711a/u or G.726) to make sure FAX can transmit successfully.
If this option is selected, the Vigor router will apply these two following settings (FAX Bypass Codec and FAX Bypass Codec Rate).

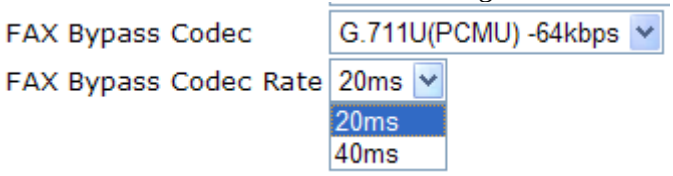
FAX Bypass Codec

Select one option to be applied if FAX mode is configured as **Bypass** mode.



FAX Bypass Code Rate

Select one option (20 or 40) to be applied if FAX mode is configured as **Bypass** mode. The stability for the faxing result of documents with codec rate 20ms is higher than 40ms.



Phone Extension Active

Click **Enable** to invoke this function. If you do not check this box, the extension number set here will not work.

Extension Number

Type the number of extension for such index.
The default number is 901.

E-mail Address

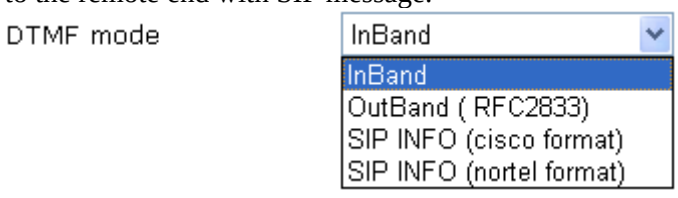
Voice mail can be sent to the specified e-mail address for the user to check and listen.
Send a test e-mail –Make a simple test for the e-mail address specified in this page. Please assign the mail address first and click this button to execute a test for verify the mail address is available or not.

Voice mail Password

Type a password here. When the user wants to listen the voice mail, he/she muse use such password to open it.

DTMF

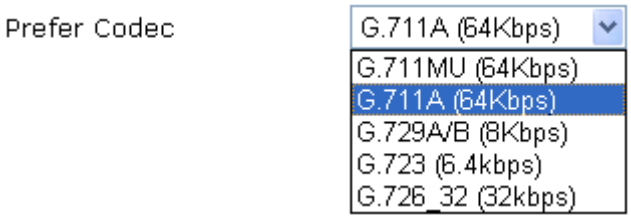
DTMF Mode – There are four DTMF modes for you to choose.
InBand **-** Choose this one then the Vigor will send the DTMF tone as audio directly when you press the keypad on the phone
OutBand **-** Choose this one then the Vigor will capture the keypad number you pressed and transform it to digital form 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.



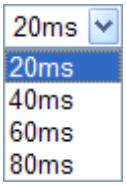
Codec

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.



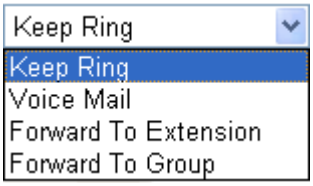
Single Codec – If the box is checked, only the selected Codec will be applied.
Code Rate – The amount of data contained in a single packet. The default value is 20 ms, which means the data packet will contain 20 ms voice information.



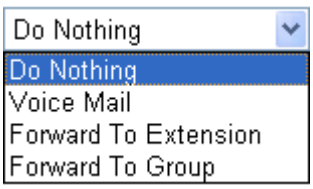
Codec VAD – This function can detect if the voice on both sides is active or not. If not, the router will do something to save the bandwidth for other using. Check it to invoke this function.

Outgoing Call Use – There are several outside lines (SIP accounts) for you to specify for such extension. Please check the one(s) you want. The available boxes listed here will be changed according to the FXS/FXO module inserted to VigorIPPBX 3510.

Answer Mode – Specify the way to process incoming phone calls.
No answer after ….. – When the incoming phone call is not picked up, it will be processed by keeping, forwarding to certain extension. Please specify the waiting time and determine the way you want to process.

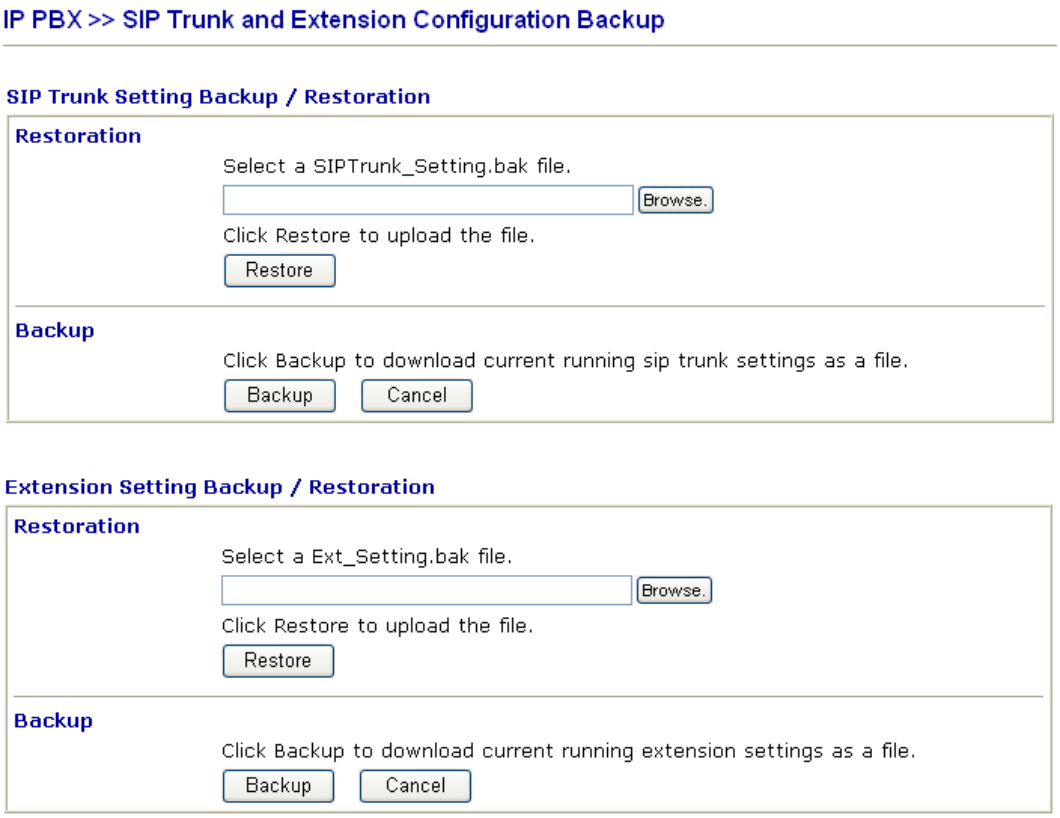


Busy then – When this extension number is busy, you can forward the incoming phone call to other extension number.



5.12.4.9 SIP Trunk and Extension Configuration Backup

This page allows you to backup or restore SIP Trunk and Extension Configuration to the host and restore them to the router if required.



Backup the Configuration for SIP Trunk or Extension Settings

Follow the steps below to backup your configuration.

1. Click **Backup** button. A dialog appears for you to confirm the settings backup. Click **Save** button to open another dialog for saving configuration as a file.
2. In **Save As** dialog, the default filename is **v3510pbx_SIPTrunk_Setting_2010XXXX** (for SIP Trunk) or **v3510pbx_Ext_Setting_2010XXX** (for extension settings). You could give it another name by yourself.
3. Click **Save** button, the configuration will download automatically to your computer as a file named **v3510pbx_SIPTrunk_Setting_2010XXXX** (for SIP Trunk) or **v3510pbx_Ext_Setting_2010XXX** (for extension settings).

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

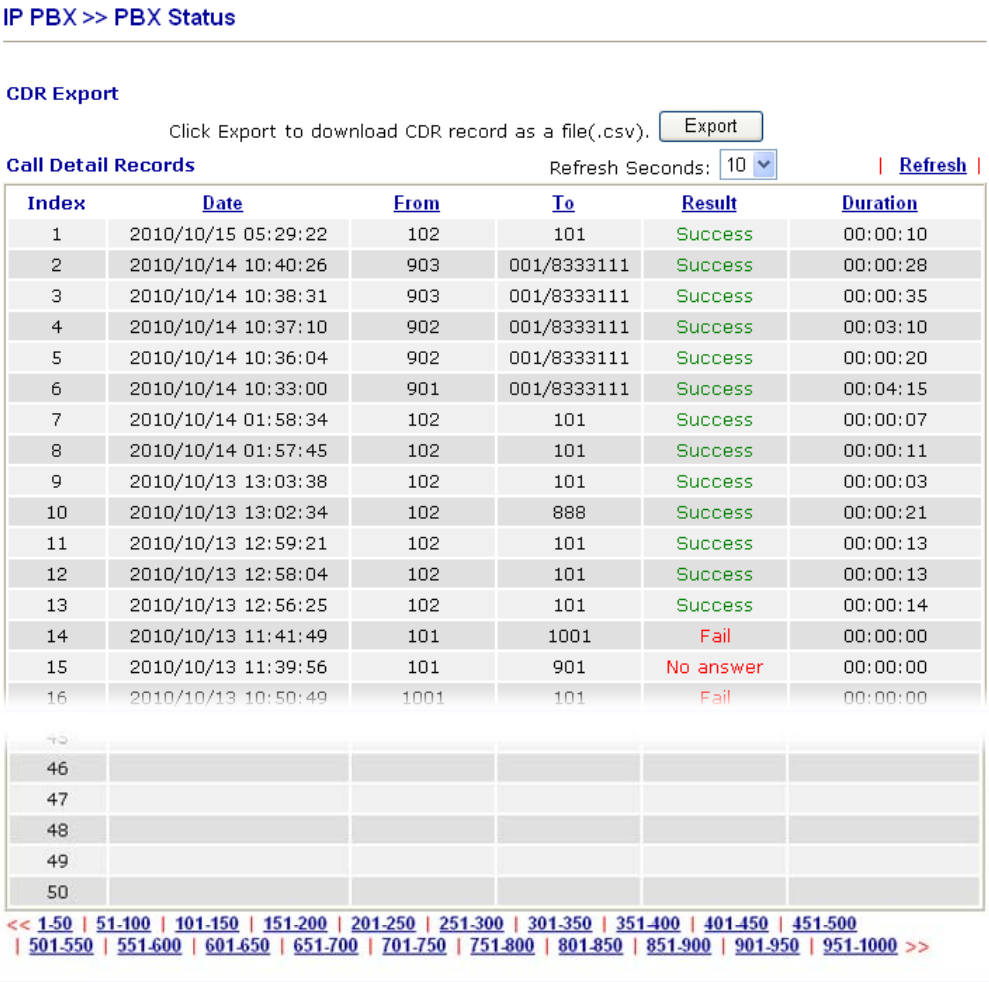
Restore Configuration

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

5.11.5 PBX Status

5.11.5.1 Call Detail Records

This page displays call records of IP PBX such as failed call, successful call, no-answer call, date of the call and the duration of each call, and so on. Each page will display 50 records.

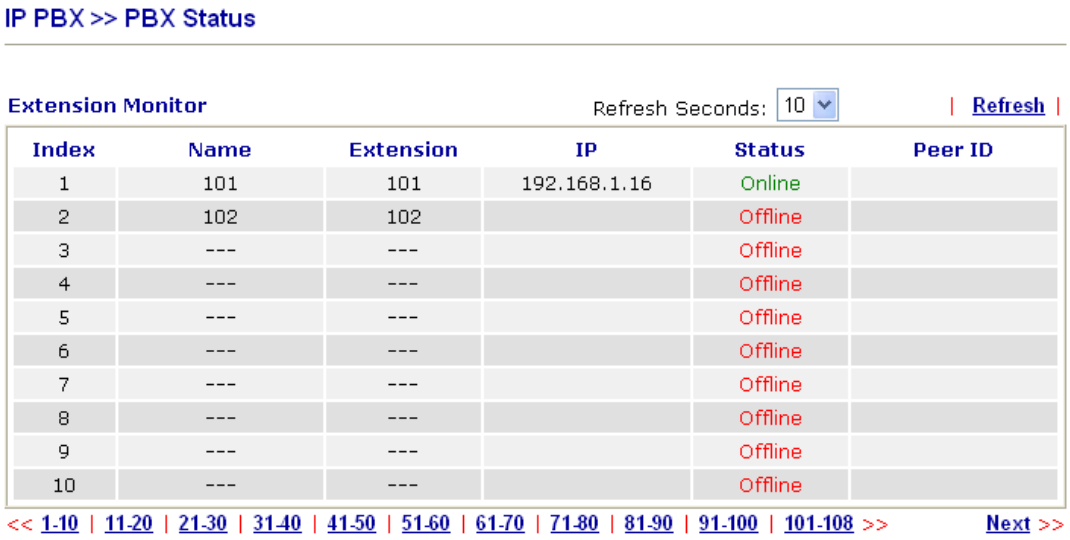


CDR Export Click the **Export** button to export the call detail records as a file.

Refresh Click it to reload the page.

5.11.5.2 Extension Monitor

This page displays owner's name, IP address, status and peer ID for each extension number.



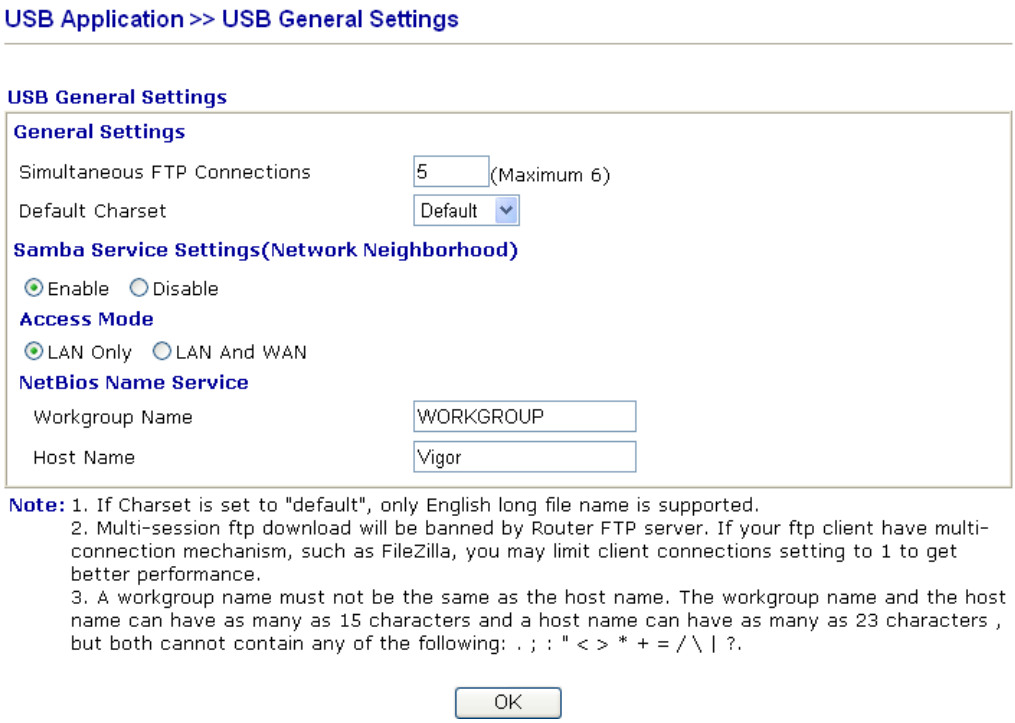
Refresh Click it to reload the page.

5.12 USB Application

USB storage disk connected on Vigor router can be regarded as a server. By way of Vigor router, clients on LAN can access, write and read data stored in USB storage disk with different applications. After setting the configuration in **USB Application**, you can type the IP address of the Vigor router and username/password created in **USB Application>>USB User Management** on the client software. Then, the client can use the FTP site (USB storage disk) or share the Samba service through Vigor router.

5.12.1 USB General Settings

This page will determine the number of concurrent FTP connection, default charset for FTP server and enable Samba service. At present, the Vigor router can support USB storage disk with formats of FAT16 and FAT32 only. Therefore, before connecting the USB diskette into the Vigor router, please make sure the memory format for the USB storage disk is FAT16 or FAT32. It is recommended for you to use FAT32 for viewing the filename completely (FAT16 cannot support long filename).



General Settings

Simultaneous FTP Connection - This field is used to specify the quantity of the FTP sessions. The router allows up to 6 FTP sessions connecting to USB storage disk at one time.

Default Charset - At present, Vigor router supports three types of character sets: default, GB2312 and BIG5.

Default Charset is for English based file name. For Simplified Chinese file/directory names, please choose GB2312; for Traditional Chinese file/directory names, choose BIG5.

Samba Service Settings

Click **Enable** to invoke samba service via the router.

Access Mode

LAN Only – Users coming from internet cannot connect to the samba server of the router.

LAN And WAN - Both LAN and WAN users can access samba server of the router.

NetBios Name Service

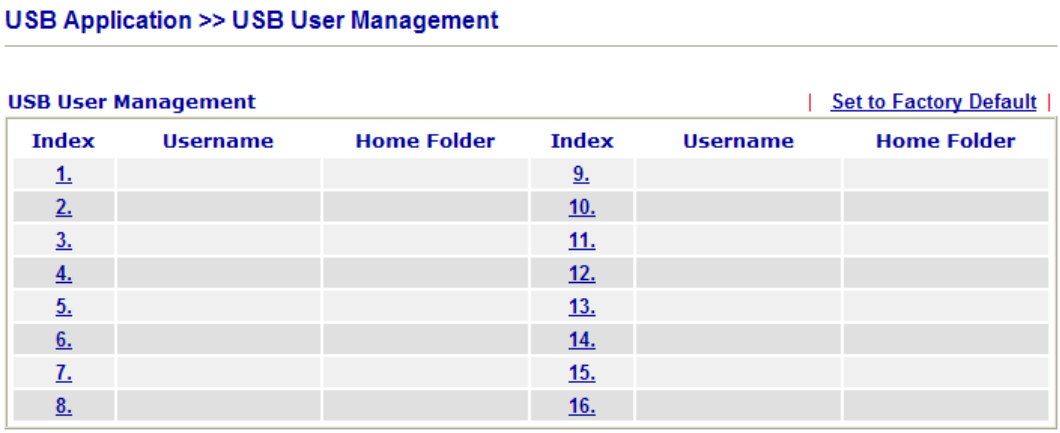
For the NetBios service of USB diskette, you have to specify a workgroup name and a host name. A workgroup name must not be the same as the host name. The workgroup name can have as many as 15 characters and the host name can have as many as 23 characters. Both them cannot contain any of the following--- ; : " < > * + = \ | ?.

Workgroup Name – Type a name for the workgroup.

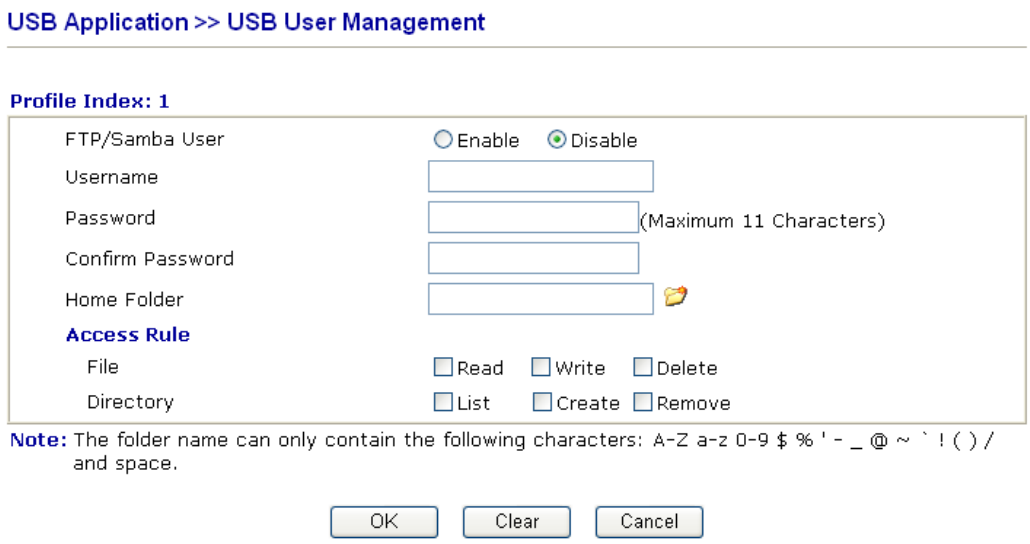
Host Name – Type the host name for the router.

5.12.2 USB User Management

This page allows you to set profiles for FTP/Samba users. Any user who wants to access into the USB storage disk must type the same username and password configured in this page. Before adding or modifying settings in this page, please insert a USB storage disk first. Otherwise, an error message will appear to warn you.



Click index number to access into configuration page.



FTP/Samba User

Enable – Click this button to activate this profile (account) for FTP service or Samba User service. Later, the user can use the username specified in this page to login into FTP server.

Disable – Click this button to disable such profile.

Username

Type the username for FTP/Samba users for accessing into FTP server (USB storage disk). Be aware that users cannot access into USB storage disk in anonymity. Later, you can open FTP client software and type the username specified here for accessing into USB storage diskette.

Note: "Admin" could not be typed here as username, for the word is specified for accessing into web pages of Vigor router only. Also, it is reserved for FTP firmware upgrade usage.

Note: FTP Passive mode is not supported by Vigor Router.

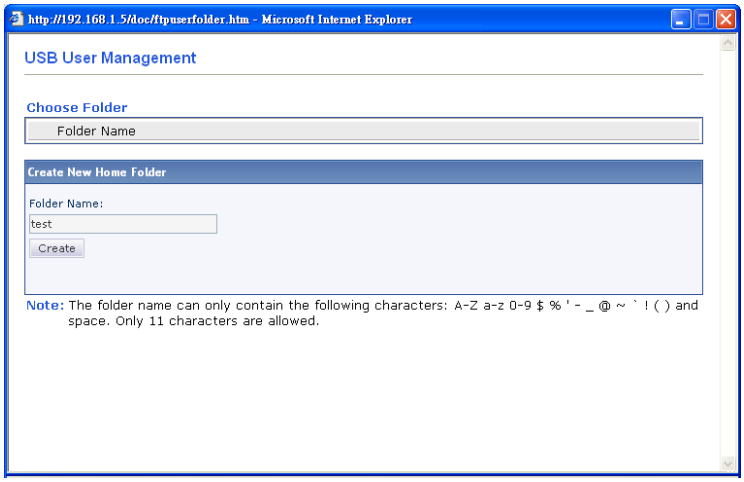
Please disable the mode on the FTP client.

Password Type the password for FTP/Samba users for accessing FTP server. Later, you can open FTP client software and type the password specified here for accessing into USB storage disk.

Confirm Password Type the password again to make confirmation.

Home Folder It determines the folder for the client to access into.
The user can enter a directory name in this field. Then, after clicking **OK**, the router will create the specific/new folder in the USB storage disk. In addition, if the user types "/" here, he/she can access into all of the disk folders and files in USB storage disk.
Note: When write protect status for the USB storage disk is **ON**, you cannot type any new folder name in this field. Only "/" can be used in such case.

You can click to open the following dialog to add any new folder which can be specified as the Home Folder.



Access Rule It determines the authority for such profile. Any user, who uses such profile for accessing into USB storage disk, must follow the rule specified here.

File – Check the items (Read, Write and Delete) for such profile.

Directory –Check the items (List, Create and Remove) for such profile.

Before you click **OK**, you have to insert a USB storage disk into the USB interface of the Vigor router. Otherwise, you cannot save the configuration.

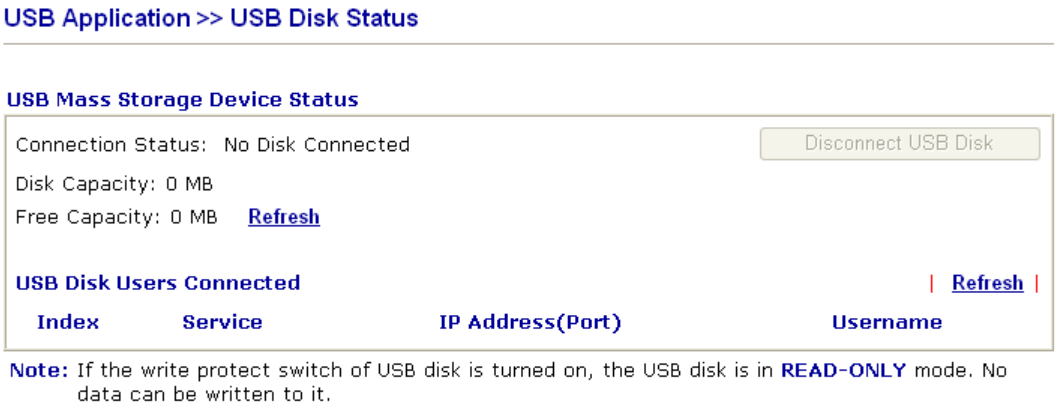
5.12.3 File Explorer

File Explorer offers an easy way for users to review and manage the content of USB storage disk connected on Vigor router.

Refresh	Click this icon to refresh files list.
Back	Click this icon to return to the upper directory.
Create	Click this icon to add a new folder.
Current Path	Display current folder.
Upload	Click this button to upload the selected file to the USB storage disk. The uploaded file in the USB storage disk can be shared for other user through FTP.

5.12.4 USB Disk Status

This page is to monitor the status for the users who accessing into FTP or Samba server (USB storage disk) via the Vigor router. If you want to remove the diskette from USB port in router, please click **Disconnect USB Disk** first. And then, remove the USB storage disk later.

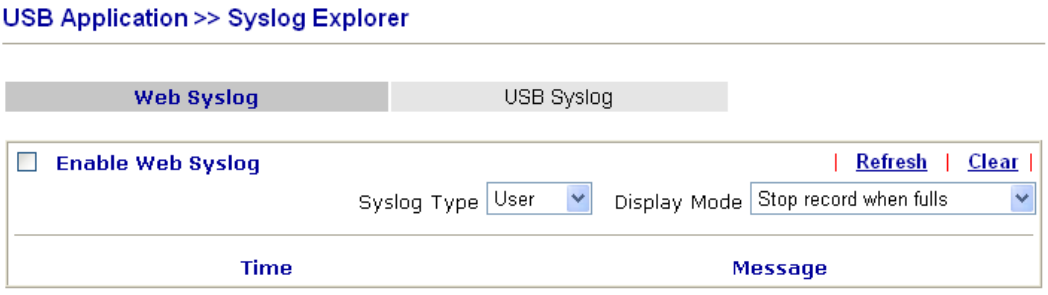


Connection Status	If there is no USB storage disk connected to Vigor router, "**No Disk Connected**" will be shown here.
Disk Capacity	It displays the total capacity of the USB storage disk.
Free Capacity	It displays the free space of the USB storage disk. Click **Refresh** at any time to get new status for free capacity.
Index	It displays the number of the client which connecting to FTP server.
Service	It displays the server (FTP or SMB) that the client wants to connect.
IP Address (Port)	It displays the IP address of the user's host which connecting to the FTP server.
Username	It displays the username that user uses to login to the FTP server.

When you insert USB storage disk into the Vigor router, the system will start to find out such device within several seconds.

5.12.5 Syslog Explorer

Such page provides real-time syslog and displays the information on the screen.

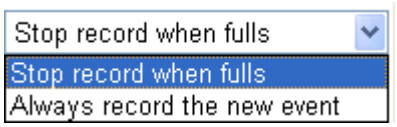


For Web Syslog

Enable Web Syslog Check this box to enable the function of Web Syslog.

Syslog Type Use the drop down list to specify a type of Syslog to be displayed.

Display Mode There are two modes for you to choose.



Stop record when fulls – when the capacity of syslog is full, the system will stop recording.

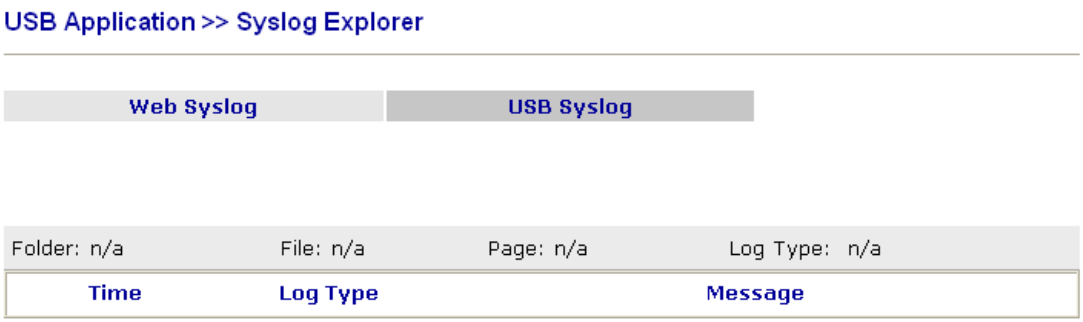
Always record the new event – only the newest events will be recorded by the system.

Time Display the time of the event occurred.

Message Display the information for each event.

For USB Syslog

This page displays the syslog recorded on the USB storage disk.



Time Display the time of the event occurred.

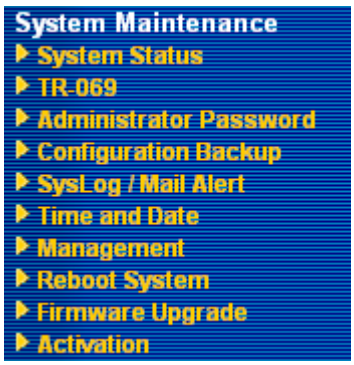
Log Type Display the type of the record.

Message Display the information for each event.

5.13 System Maintenance

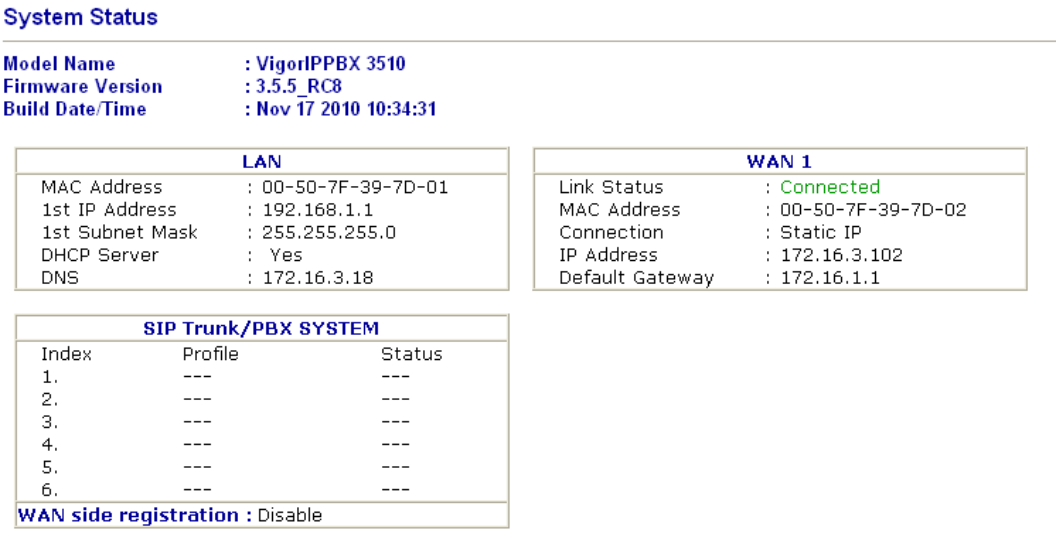
For the system setup, there are several items that you have to know the way of configuration: Status, Administrator Password, Configuration Backup, Syslog, Time setup, Reboot System, Firmware Upgrade.

Below shows the menu items for System Maintenance.



5.13.1 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.

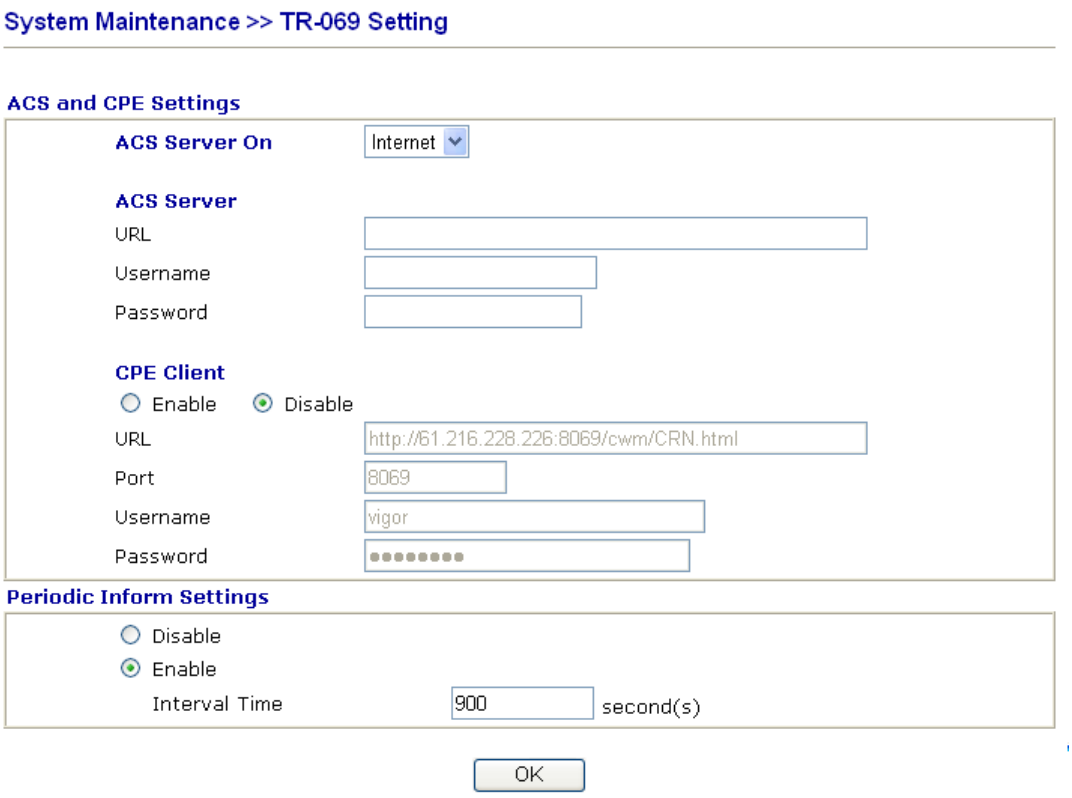


Model Name	Display the model name of the router.
Firmware Version	Display the firmware version of the router.
Build Date/Time	Display the date and time of the current firmware build.
LAN-------	
MAC Address	Display the MAC address of the LAN Interface.
1st IP Address	Display the IP address of the LAN 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.
SIP Trunk/PBX System-------	
Index/Profile/Status	Display current status for SIP profiles.

5.13.2 TR-069

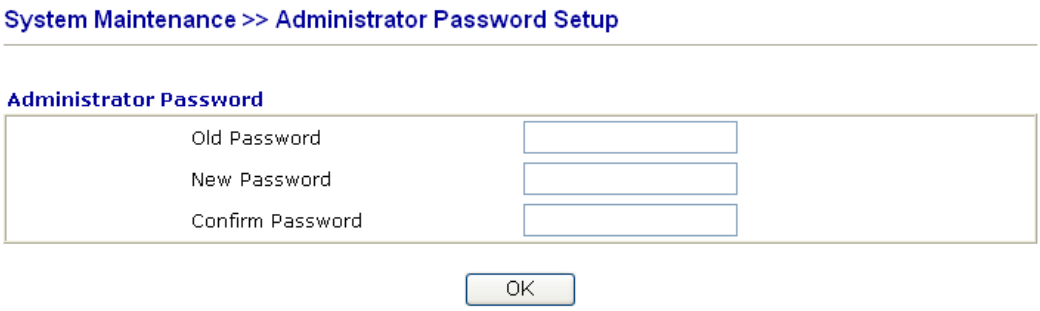
This device supports TR-069 standard. It is very convenient for an administrator to manage a TR-069 device through an Auto Configuration Server, e.g., VigorACS.



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	Such information is useful for Auto Configuration Server. **Enable/Disable** – Allow/Deny the CPE Client to connect with Auto Configuration Server. **Port** – Sometimes, port conflict might be occurred. To solve such problem, you might change port number for CPE.
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.

5.13.3 Administrator Password

This page allows you to set new password.

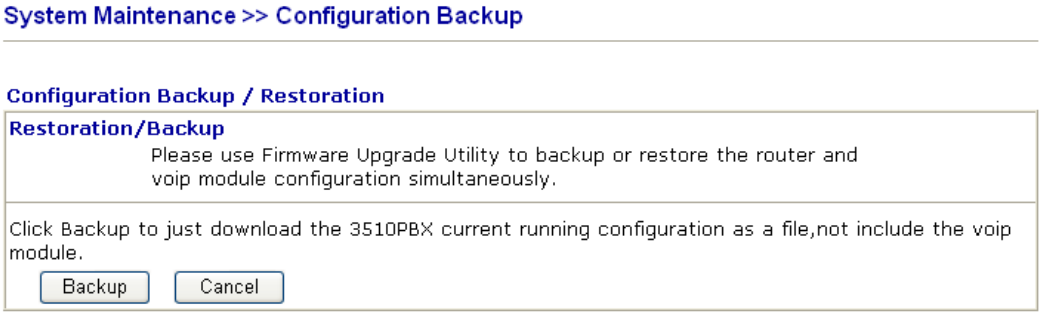


Old Password	Type in the old password. The factory default setting for password is blank.
New Password	Type in new password in this filed.
Confirm Password	Type in the new password again.

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

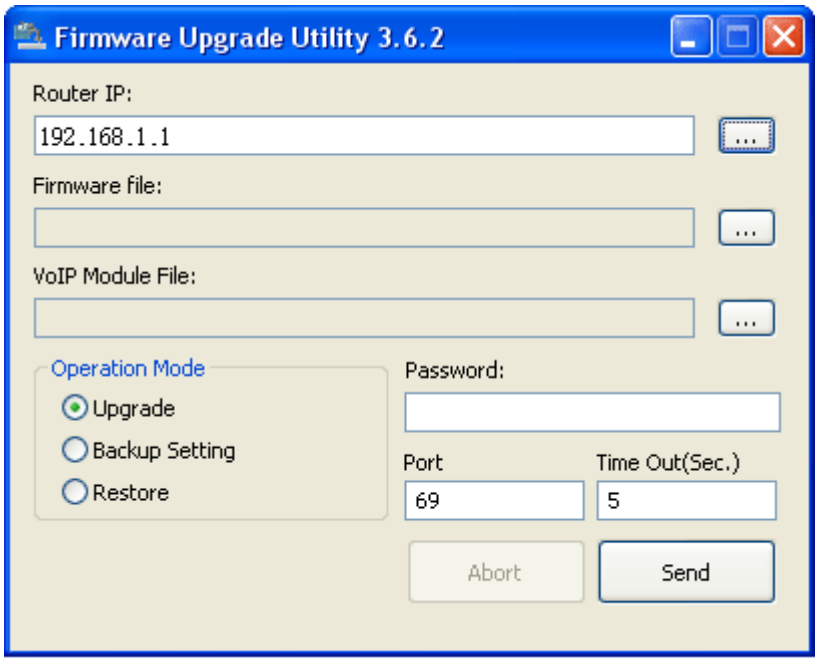
5.13.4 Configuration Backup

This page allows you to backup current configuration as a file.



To backup or restore the configuration of the router, please download the Firmware Upgrade Utility from DrayTek website first.

Run the firmware upgrade utility. You will see a dialog as the following figure.

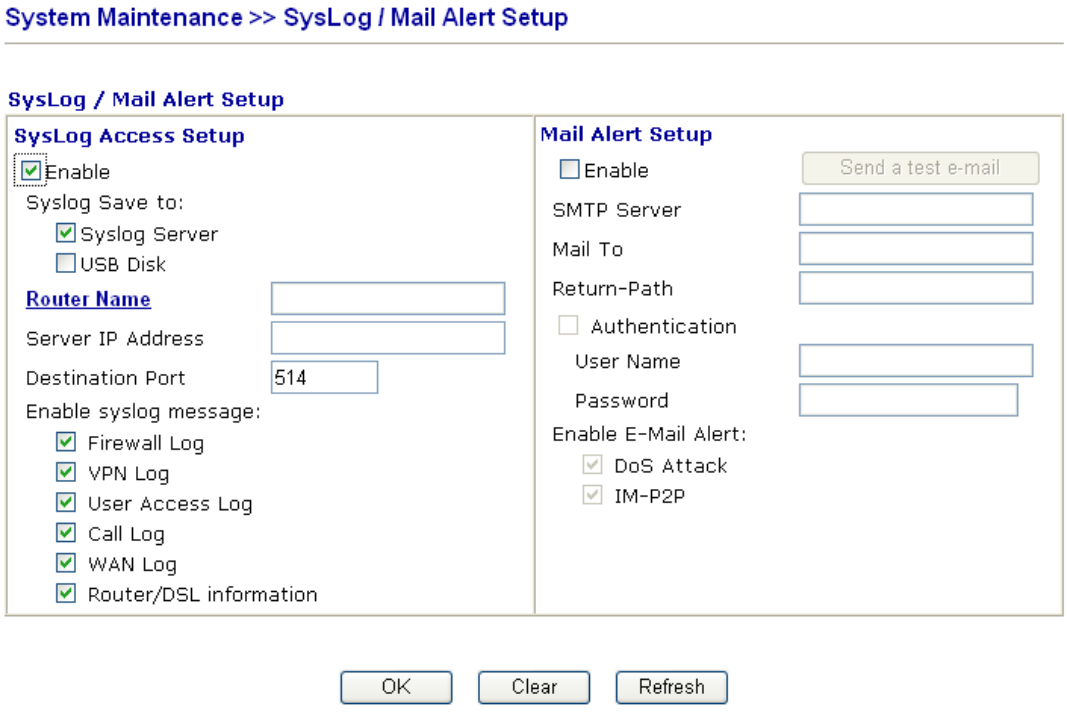


Click the browse button to get the IP address of VigorIPPBX 3510. Then you can specify which operation (Upgrade, Backup Setting, or Restore) you want to perform for the router.

Finally click the bottom right button (e.g., **Send** in the above figure) to perform the operation.

5.13.5 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 Check **Enable** to activate function of syslog.

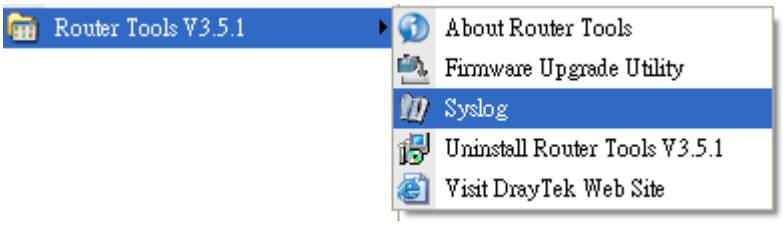
Syslog Save to Check **Syslog Server** to save the log to Syslog directly.

	Check **USB Disk** to save the log to the attached USB diskette.
Syslog Server	Check it to make the syslog saved to the specified server.
USB Disk	Check it to make the syslog saved to the attached USB disk.
Router Name	Click the link to get the router name configured in **System Maintenance>>Management**.
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 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.

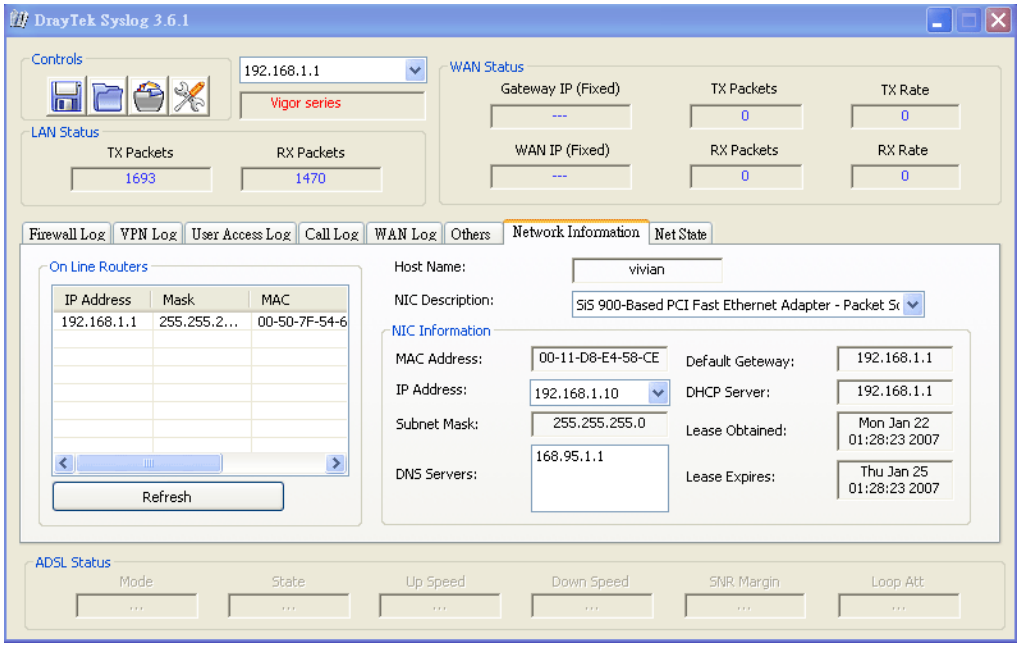
Click **OK** to save these settings.

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.

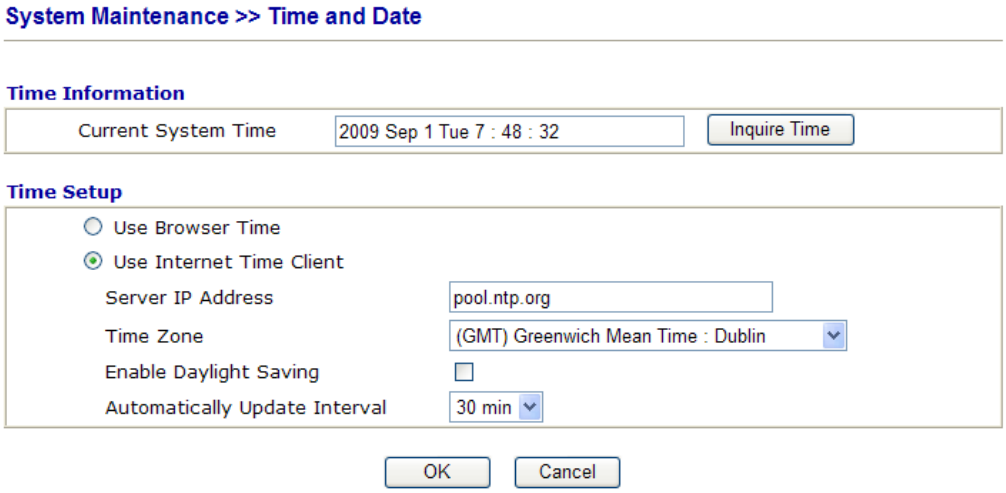


3. From the Syslog screen, select the router you want to monitor. Be reminded that in **Network Information**, select the network adapter used to connect to the router. Otherwise, you won't succeed in retrieving information from the router.



5.13.6 Time and Date

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

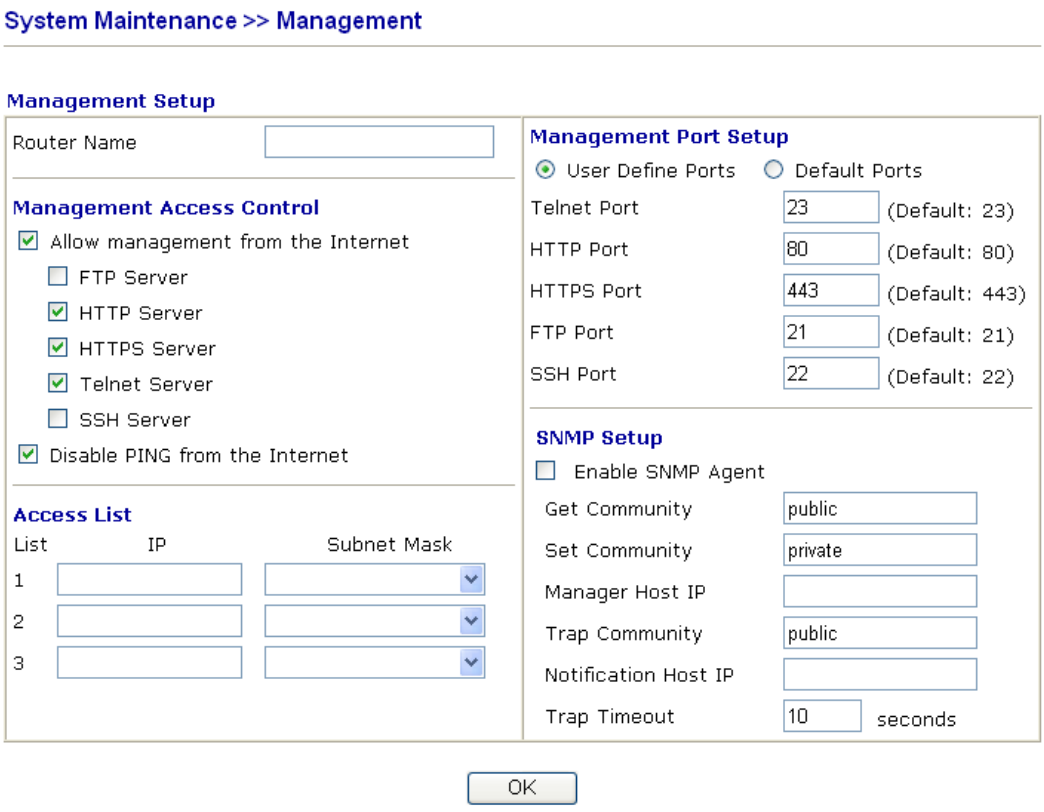


Current System Time	Click **Inquire Time** to get the current time.
Use Browser Time	Select this option to use the browser time from the remote administrator PC host as router's system time.
Use Internet Time	Select to inquire time information from Time Server on the Internet using assigned protocol.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

Click **OK** to save these settings.

5.13.7 Management

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

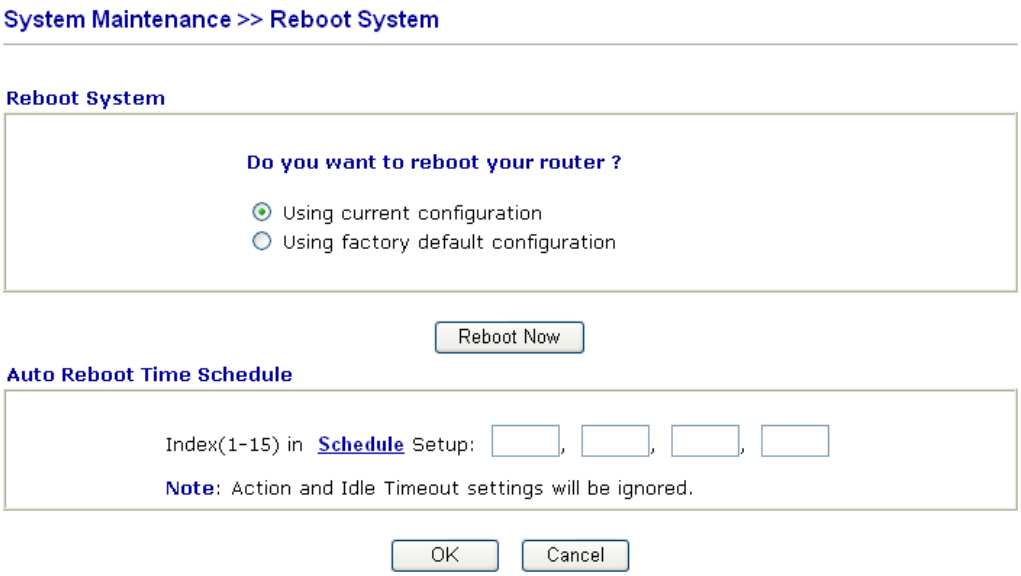


Router Name	Type in the router name provided by ISP.
Allow management from the Internet	Enable the checkbox to allow system administrators to login from the Internet. There are several servers provided by the system to allow you managing the router from Internet. Check the box(es) to specify.
Disable 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.

5.13.8 Reboot System

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



Index (1-15) in Schedule Setup - You can type in four sets of time schedule for performing system reboot. 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.

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

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

5.13.9 Firmware Upgrade

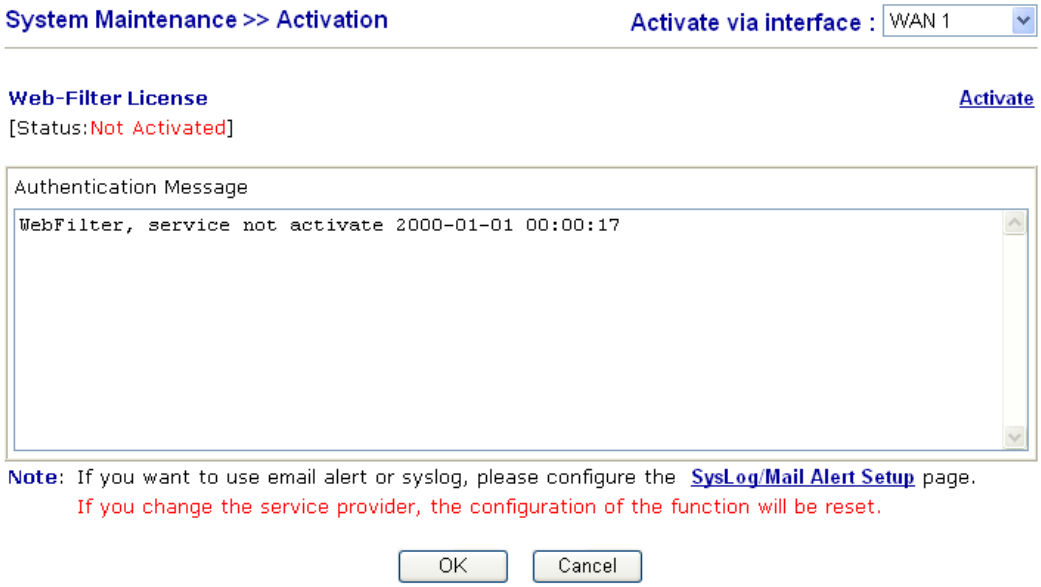
For the detailed information about firmware update, please refer to **4.5 Upgrade Firmware for VigorIPPBX 3510** for detailed operation.

5.13.10 Activation

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

After you have finished the setting profiles for WCF (refer to the section of **Web Content Filter Profile**), it is the time to activate the mechanism for your computer.

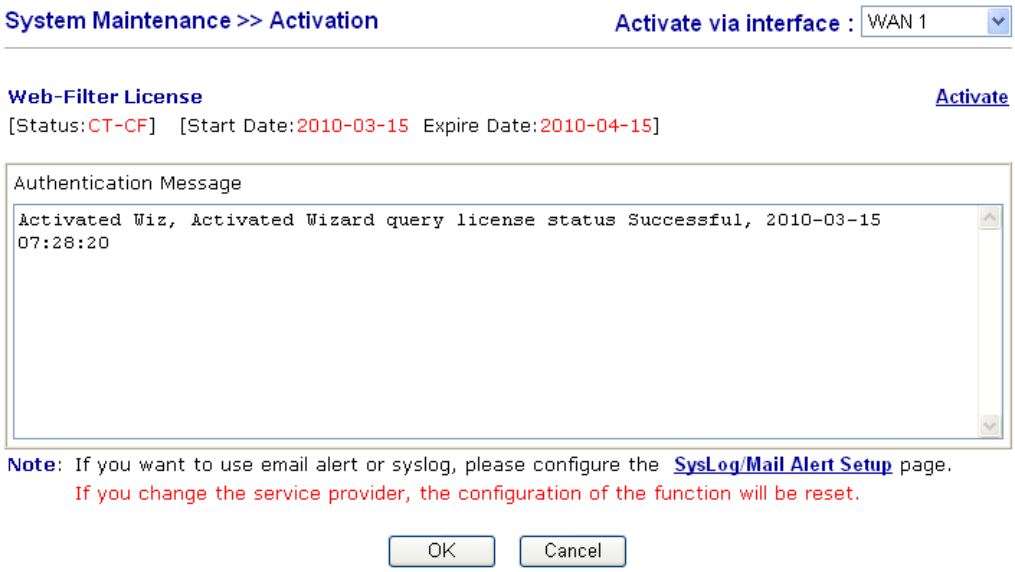
Click **System Maintenance>>Activation** to open the following page for accessing http://myvigor.draytek.com.



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

Activate	The **Activate** link brings you accessing into www.vigorpro.com to finish the activation of the account and the router.
Authentication Message	As for authentication information of **web filter**, the process of authenticating will be displayed on this field for your reference.

Below shows the successful activation of Web Content Filter:

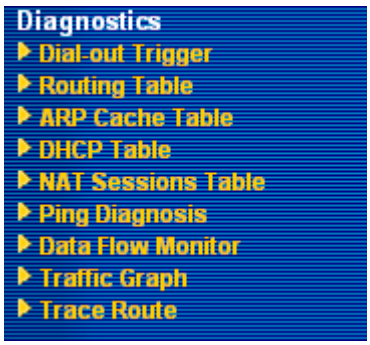


Activate via interface	Use the drop down menu to choose the interface for accessing the server.
Status	Display the mechanism (represented with code number, e.g., CT-CF) adopted by such router.
Start Date	Display the starting date of WCF license activated successfully.
Expire Date	Display the ending date of WCF license activated successfully.
Activate	Click this link to access into http://myvigor.draytek.com for activating WCF function.

5.14 Diagnostics

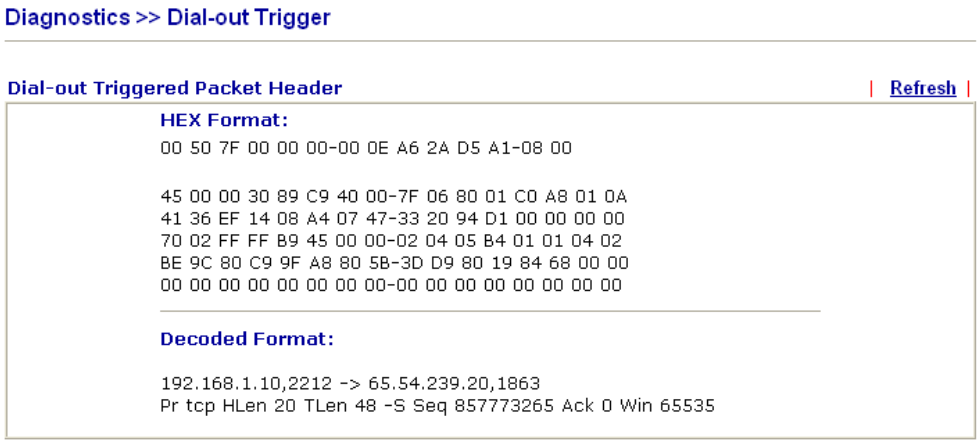
Diagnostic Tools provide a useful way to **view** or **diagnose** the status of your Vigor router.

Below shows the menu items for Diagnostics.



5.14.1 Dial-out Trigger

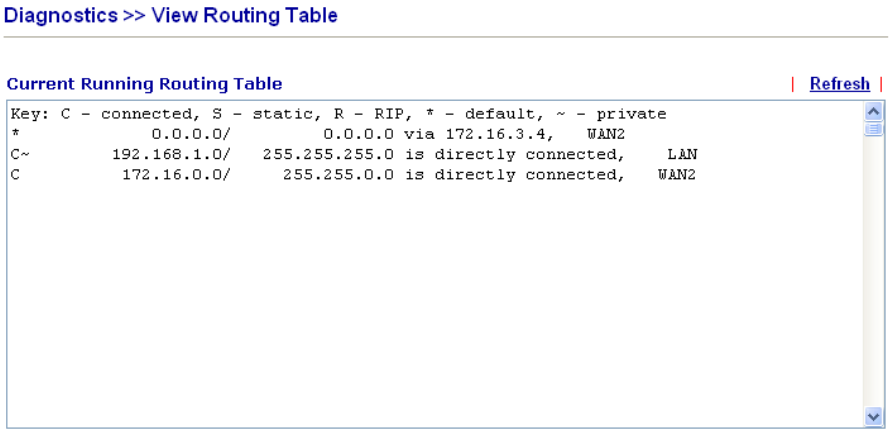
Click **Diagnostics** and click **Dial-out Trigger** to open the web page. The internet connection (e.g., ISDN, PPPoE, PPPoA, etc) is triggered by a package sending from the source IP address.



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.

5.14.2 Routing Table

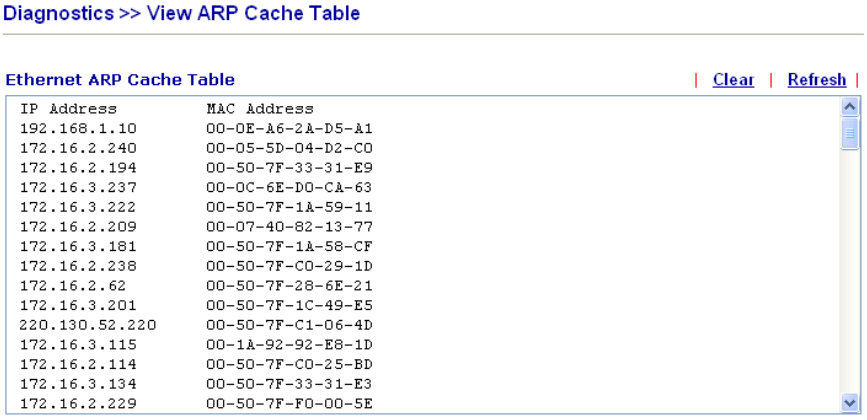
Click **Diagnostics** and click **Routing Table** to open the web page.



Refresh Click it to reload the page.

5.14.3 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.



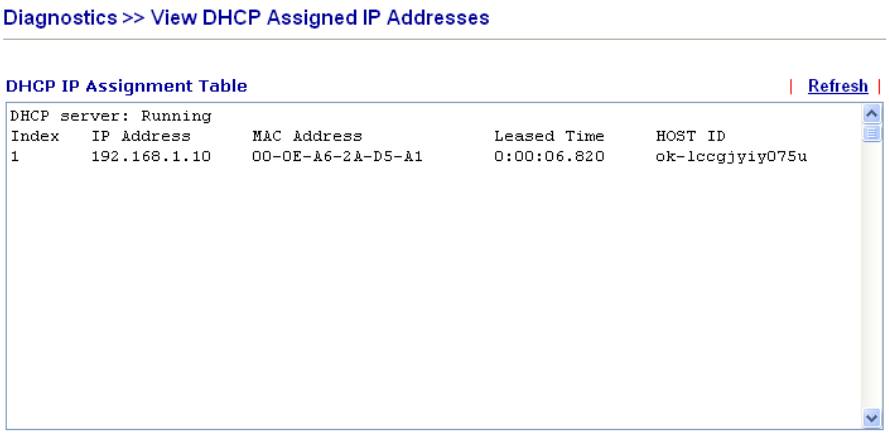
Refresh Click it to reload the page.

Clear Click it to clear the whole table.

5.14.4 DHCP Table

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

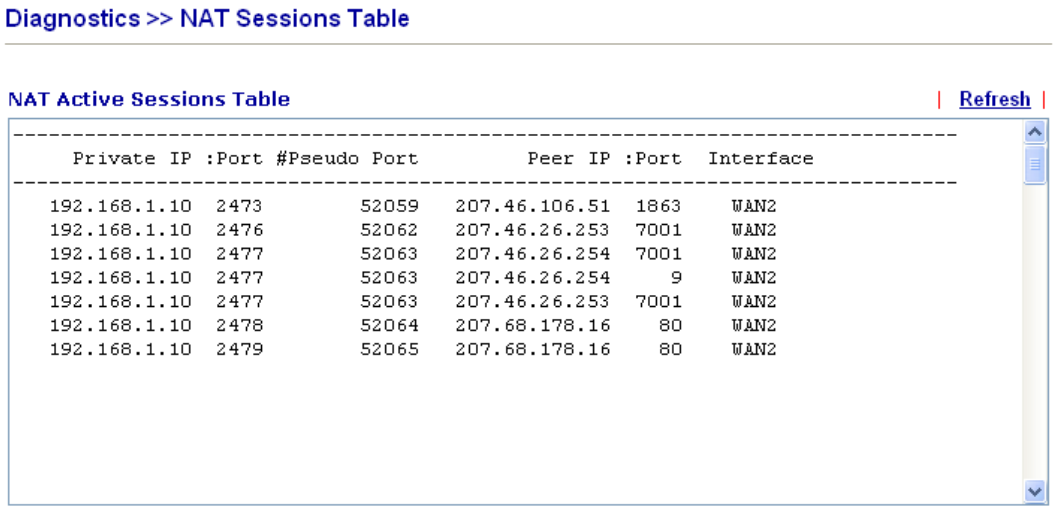
Click **Diagnostics** and click **DHCP Table** to open the web page.



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.

5.14.5 NAT Sessions Table

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

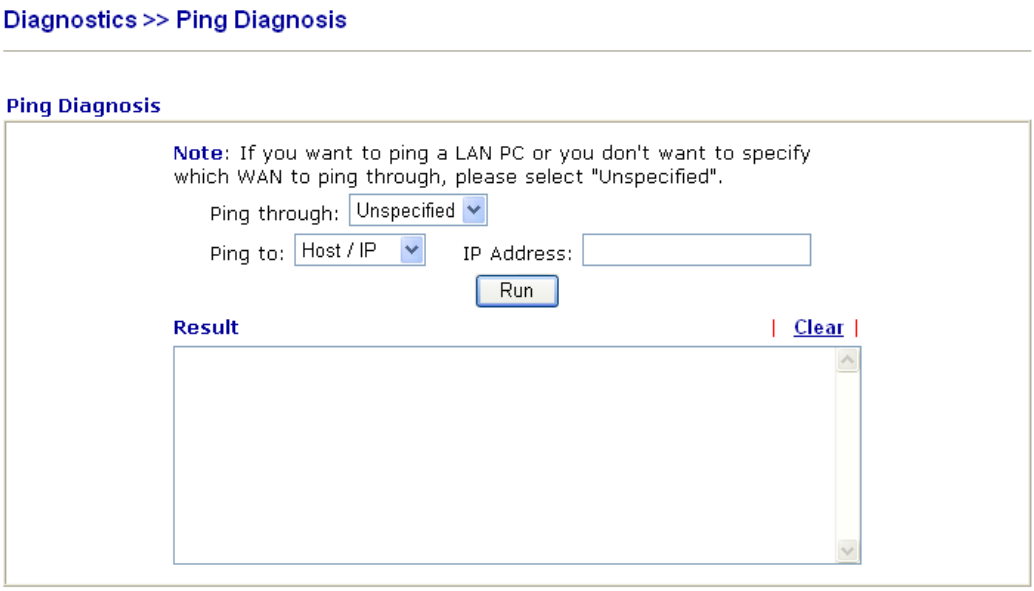


Private IP:Port	It indicates the source IP address and port of local PC.
#Pseudo Port	It indicates the temporary port of the router used for NAT.

Peer IP:Port	It indicates the destination IP address and port of remote host.
Interface	It displays the representing number for different interface.
Refresh	Click it to reload the page.

5.14.6 Ping Diagnosis

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

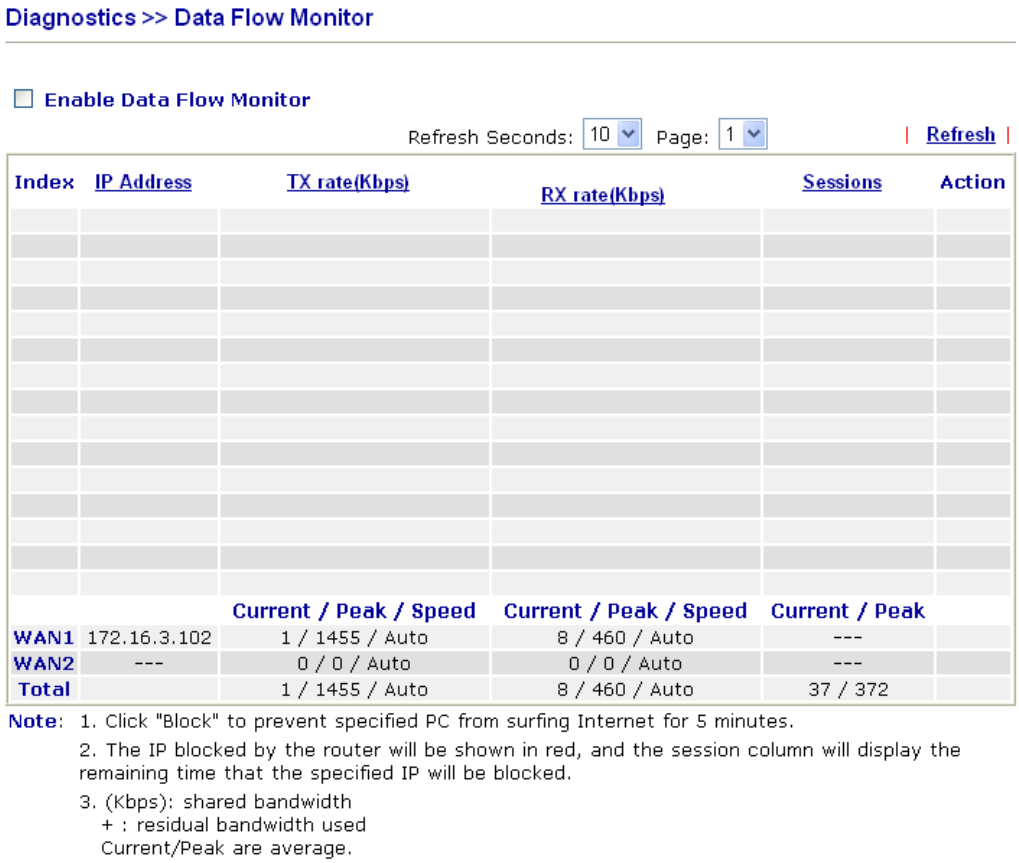


Ping through	Use the drop down list to choose the WAN interface that you want to ping through or choose **Unspecified** to be determined by the router automatically.
Ping to	Use the drop down list to choose the destination that you want to ping.
IP Address	Type in the IP address of the Host/IP that you 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.

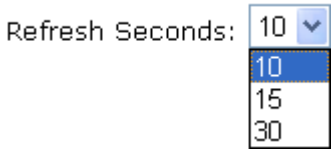
5.14.7 Data Flow Monitor

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.



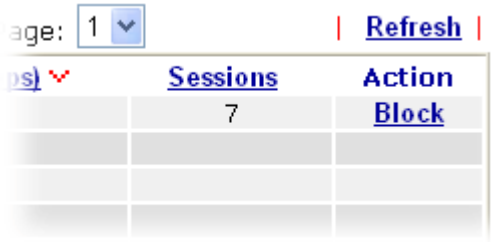
Enable Data Flow Monitor	Check this box to enable this function.
Refresh Seconds	Use the drop down list to choose the time interval of refreshing data flow that will be done by the system automatically.



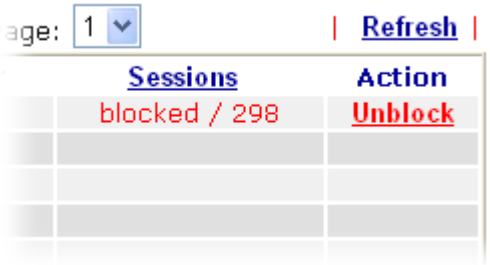
Refresh	Click this link to refresh this page manually.
Index	Display the number of the data flow.
IP Address	Display the IP address of the monitored device.
TX rate (kbps)	Display the transmission speed of the monitored device.
RX rate (kbps)	Display the receiving speed of the monitored device.
Sessions	Display the session number that you specified in Limit Session web page.

Action

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

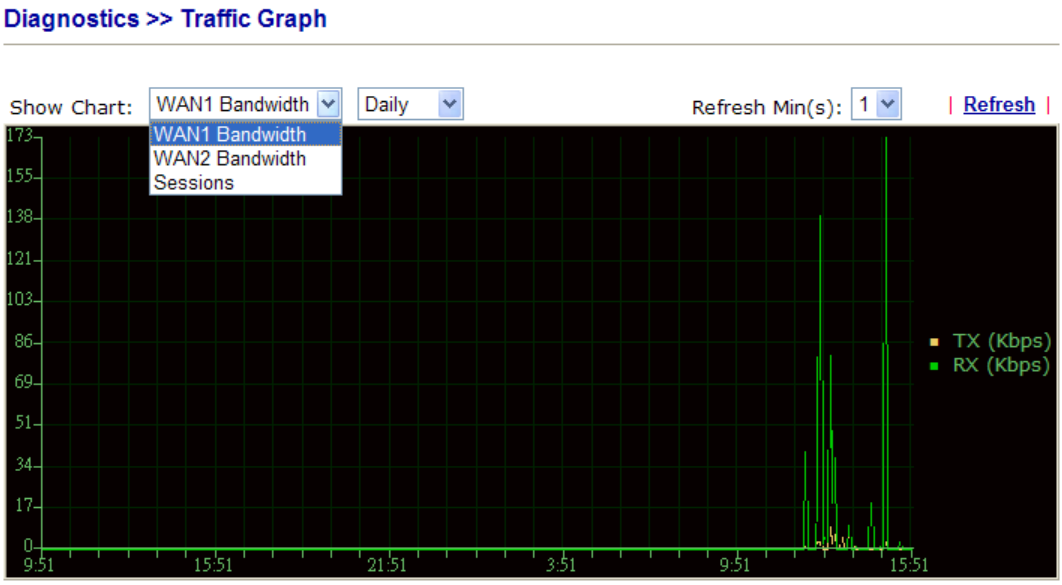


Unblock – the device with the IP address will be blocked in five minutes. The remaining time will be shown on the session column.



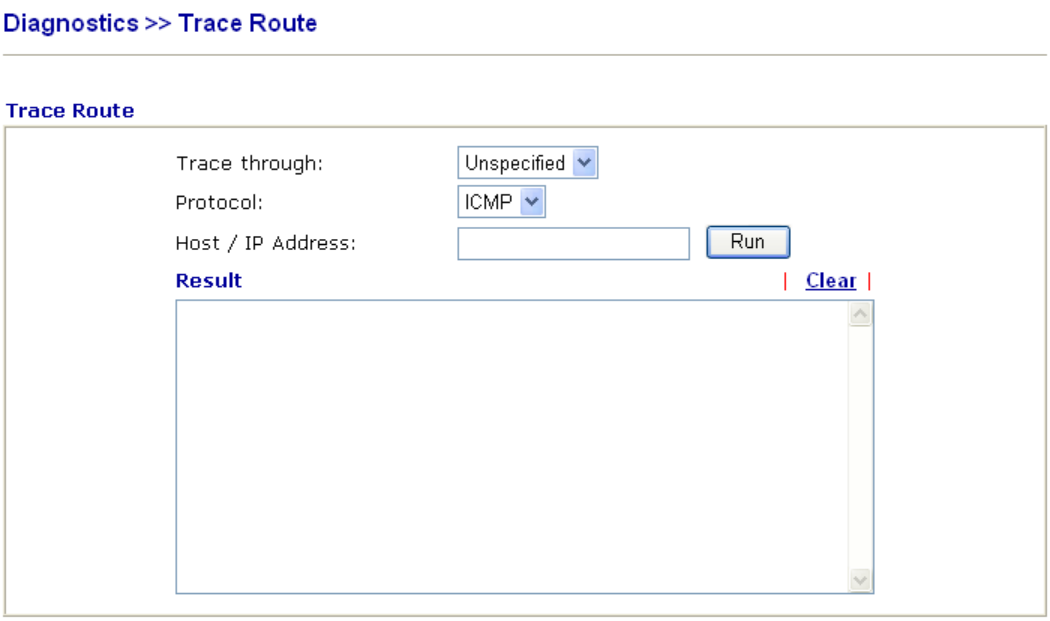
5.14.8 Traffic Graph

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.



5.14.9 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.



Trace through Use the drop down list to choose the WAN interface that you want to ping through or choose **Unspecified** to be determined by the router automatically.

Protocol Choose a protocol (ICMP or UDP) for such route.

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.

Chapter 6: Trouble Shooting

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

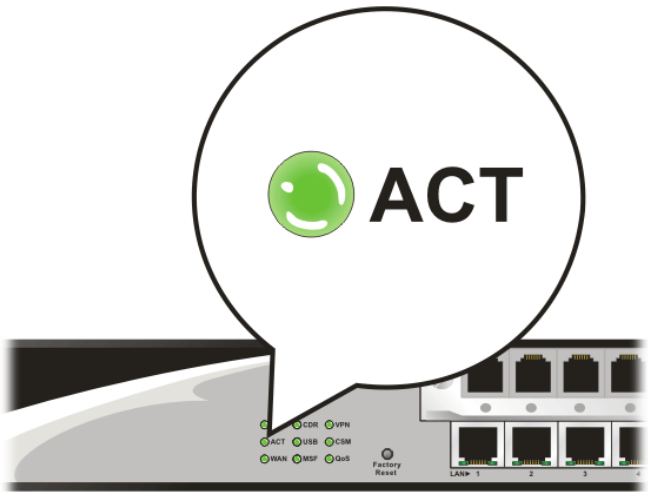
- Checking if the hardware status is OK or not.
- Checking if the network connection settings on your computer are OK or not.
- Pinging the router from your computer.
- Checking if the ISP settings are OK or not.
- Backing to factory default setting if necessary.

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

6.1 Checking If the Hardware Status Is OK or Not

Follow the steps below to verify the hardware status.

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



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

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

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

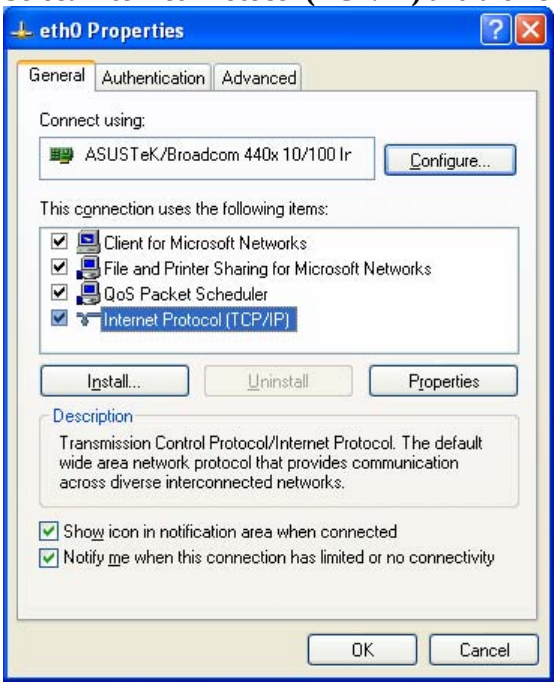
For Windows

> 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**.

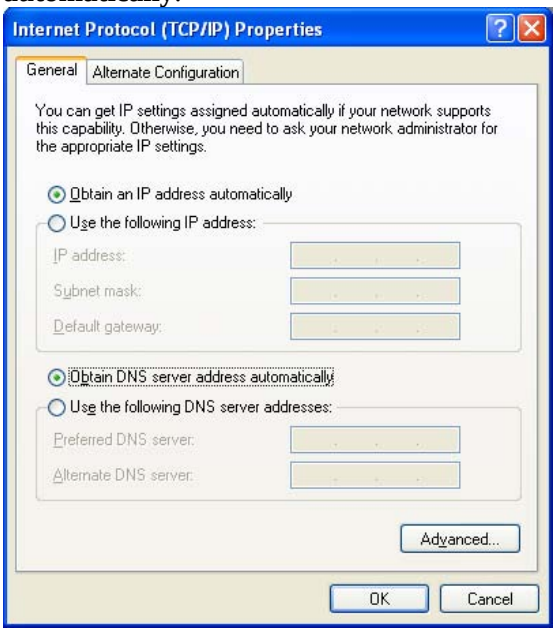
1. Go to **Control Panel** and then double-click on **Network Connections**.

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

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

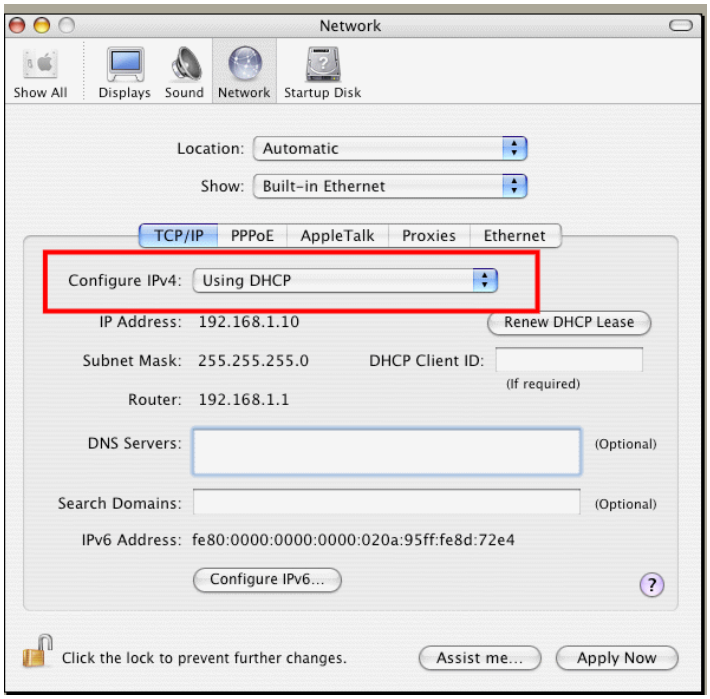


4. Select **Obtain an IP address automatically** and **Obtain DNS server address automatically**.



For Mac OS

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



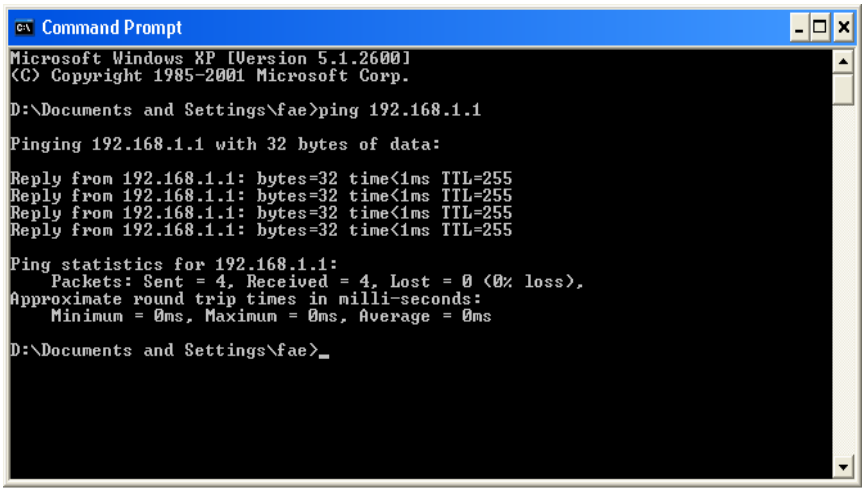
6.3 Pinging the Router from Your Computer

The default gateway IP address of the router is 192.168.1.1. For some reason, you might need to use "ping" command to check the link status of the router. **The most important thing is that the computer will receive a reply from 192.168.1.1.** If not, please check the IP address of your computer. We suggest you setting the network connection as **get IP automatically**. (Please refer to the section 6.2)

Please follow the steps below to ping the router correctly.

For Windows

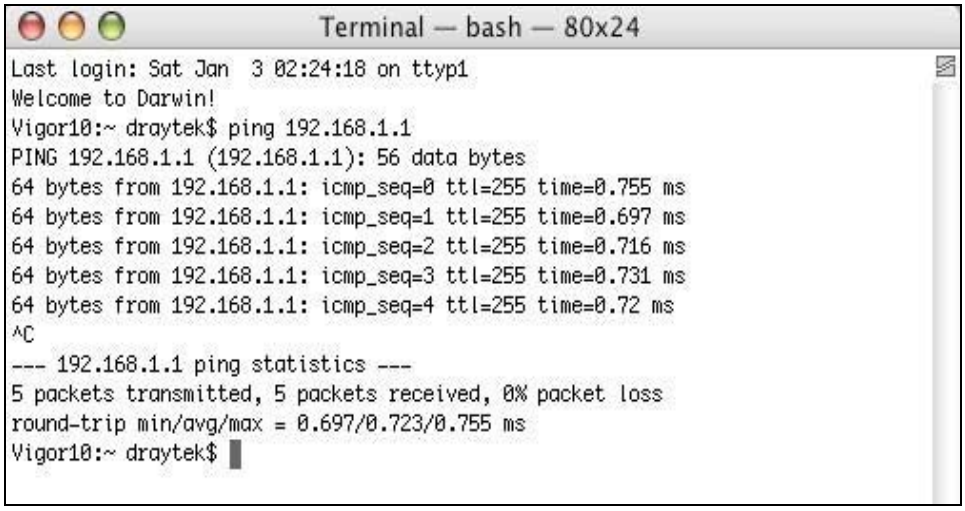
1. Open the **Command** Prompt window (from **Start menu> Run**).
2. Type **command** (for Windows 95/98/ME) or **cmd** (for Windows NT/ 2000/XP/Vista). The DOS command dialog will appear.



3. Type ping 192.168.1.1 and press [Enter]. If the link is OK, the line of **"Reply from 192.168.1.1:bytes=32 time<1ms TTL=255"** will appear.
4. If the line does not appear, please check the IP address setting of your computer.

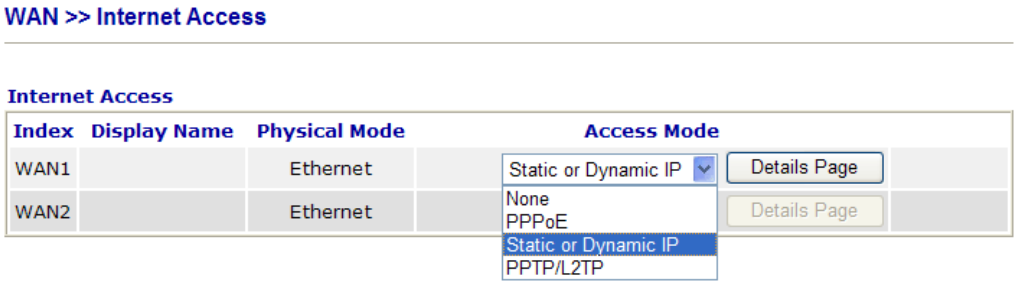
For Mac OS (Terminal)

1. Double click on the current used Mac OS on the desktop.
2. Open the **Application** folder and get into **Utilities**.
3. Double click **Terminal**. The Terminal window will appear.
4. Type **ping 192.168.1.1** and press [Enter]. If the link is OK, the line of **"64 bytes from 192.168.1.1: icmp_seq=0 ttl=255 time=xxxx ms**" will appear.



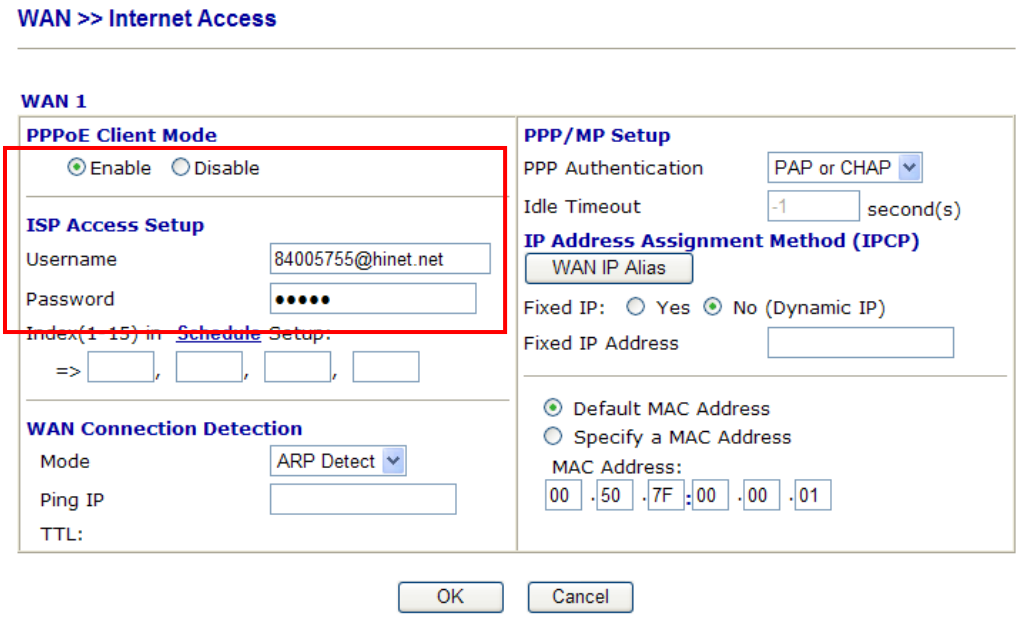
6.4 Checking If the ISP Settings are OK or Not

Open **Internet Access** page and then check whether the ISP settings are set correctly.



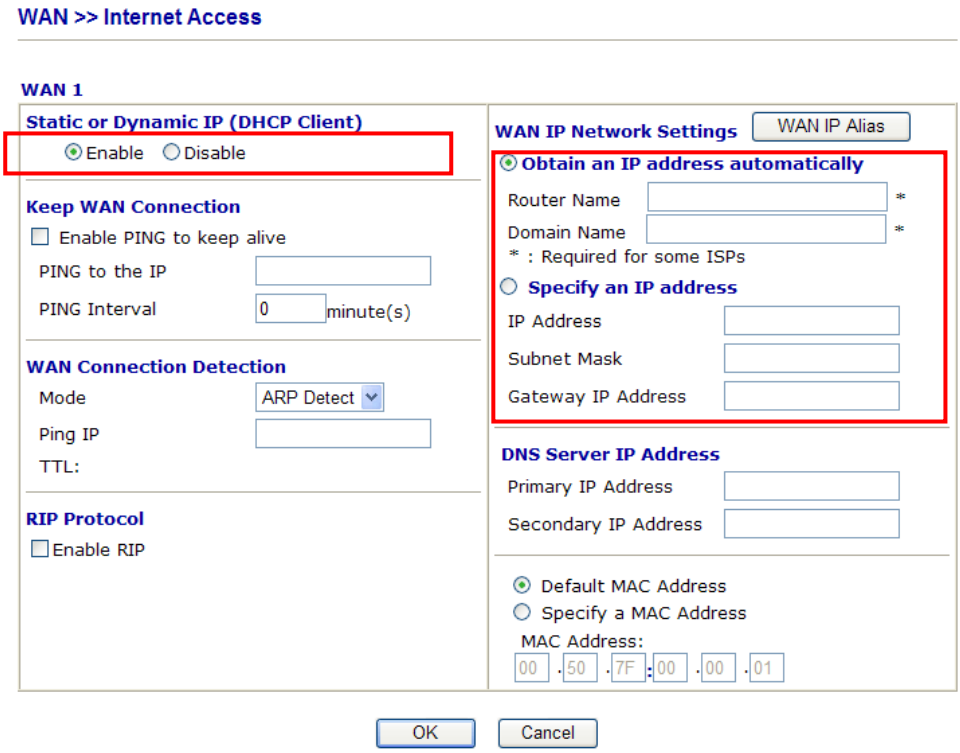
For PPPoE Users

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



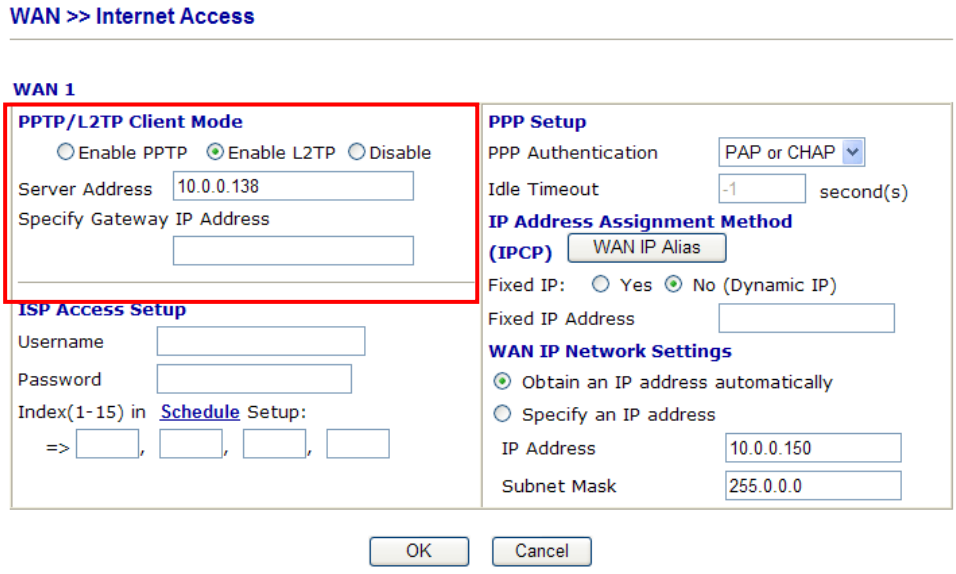
For Static/Dynamic IP Users

1. Check if the **Enable** option is selected.
2. Check if **Obtain an IP address automatically** for Dynamic IP setting is selected. Or check if **IP address, Subnet Mask** and **Gateway** are entered with correct values for Static IP setting that you **got from** your **ISP**.



For PPTP/L2TP Users

1. Check if the **Enable** option for **PPTP** Link is selected.
2. Check if **PPTP Server, Username, Password** and **WAN IP address** are set correctly (must identify with the values from your ISP).



6.5 Backing to Factory Default Setting If Necessary

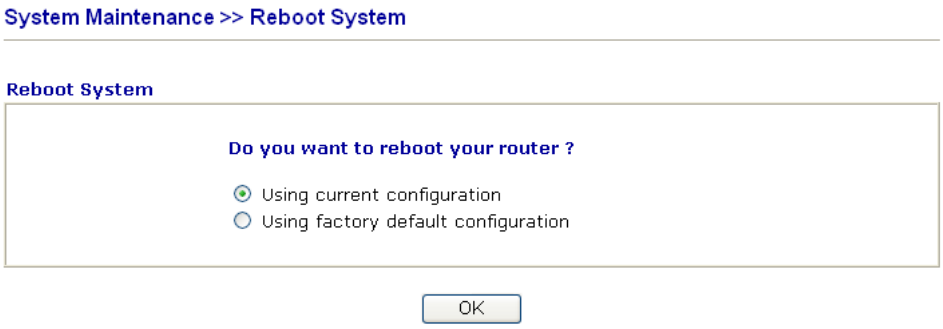
Sometimes, a wrong connection can be improved by returning to the default settings. Try to reset the router by software or hardware.

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

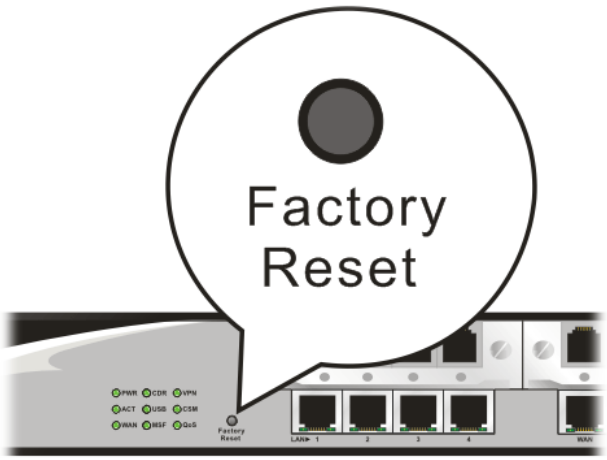
You can reset the router to factory default via Web page.

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 Contacting Your Dealer

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

Appendix: Hardware Specifications

Temperature	Operating : 0°C ~ 45°C
	Storage : -25°C ~ 70°C
Humidity	10% ~ 90% (non-condensing)
Max. Power Consumption	50 Watt (Max)
Dimension	L443 * W280.5 * H44 (mm)
Power	100-240V, 50-60Hz, 1.0/0.5A