DrayTek

Vigor*IPPBX* 3510 Series

Your reliable networking solutions partner

User's Guide

V.1.0

Vigor*IPPBX*3510/3500 Series User's Guide

Version: 1.0

Date: 18/09/2009

Copyright Information

Copyright Declarations

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

Trademarks

The following trademarks are used in this document:

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

Safety Instructions and Approval

Safety Instructions

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

Warranty

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

Be a Registered Owner

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

Firmware & Tools Updates

Due to the continuous evolution of DrayTek technology, all routers 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

1.2.1 For VigorIPPBX 3510 2
1.2.2 For VigorIPPBX 3500 4

1.3 Hardware Installation 6

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 Online Status.. 22

2.4 Saving Configuration.. 25

Chapter 3: Applications...27

3.1 Versatile PSTN and VoIP Trunk 27

3.2 Cost-effective Extendability by Integrated Analog-telephone Adapter (for
24 Conventional Aanalog Phones) & POE-switch for IP-based phones.................................... 29

Chapter 4: Other Applications 31

4.1 Create a LAN-to-LAN Connection Between Remote Office and Headquarter 31

4.2 Create a Remote Dial-in User Connection Between the Teleworker and Headquarter........ 38

4.3 QoS Setting Example.. 42

4.4 LAN – Created by Using NAT 46

4.5 Upgrade Firmware for Your Router 47

4.6 Request a certificate from a CA server on Windows CA Server.. 50

4.7 Request a CA Certificate and Set as Trusted on Windows CA Server 54

Chapter 5: Reference - Advanced Web Configuration...57

5.1 WAN 57

5.1.1 Basics of Internet Protocol (IP) Network.. 57
5.1.2 Network Connection by 3G USB Modem 58
5.1.3 General Setup... 58
5.1.4 Internet Access... 61
5.1.5 Load-Balance Policy... 68

5.2 LAN 70

5.2.1 Basics of LAN 70
5.2.2 General Setup........ 72
5.2.3 Static Route 75
5.2.4 VLAN........ 77
5.2.5 Bind IP to MAC 79

5.3 NAT 80

5.3.1 Port Redirection........ 80
5.3.2 DMZ Host........ 83
5.3.3 Open Ports........ 85

5.4 Firewall........ 88

5.4.1 Basics for Firewall........ 88
5.4.2 General Setup........ 90
5.4.3 Filter Setup 92
5.4.4 DoS Defense 99

5.5 Objects Settings........ 102

5.5.1 IP Object........ 102
5.5.2 IP Group 104
5.5.3 Service Type Object 105
5.5.4 Service Type Group........ 106
5.5.5 Keyword Object 107
5.5.6 Keyword Group........ 108
5.5.7 File Extension Object........ 109
5.5.8 IM Object 111
5.5.9 P2P Object........ 113
5.5.10 Misc Object........ 114

5.6 CSM 115

5.6.1 IM/P2P Filter Profile........ 117
5.6.2 URL Content Filter Profile........ 118
5.6.3 Web Content Filter Profile........ 122

5.7 Bandwidth Management 124

5.7.1 Sessions Limit........ 124
5.7.2 Bandwidth Limit 125
5.7.3 Quality of Service........ 126

5.8 Applications........ 133

5.8.1 Dynamic DNS 133
5.8.2 Schedule........ 135
5.8.3 RADIUS 137
5.8.4 UPnP........ 138
5.8.5 IGMP........ 140
5.8.6 Wake on LAN........ 141

5.9 VPN and Remote Access........ 142

5.9.1 Remote Access Control........ 142
5.9.2 PPP General Setup 143
5.9.3 IPSec General Setup 144
5.9.4 IPSec Peer Identity........ 145
5.9.5 Remote Dial-in User 147
5.9.6 LAN to LAN........ 149
5.9.7 Connection Management........ 156

5.10 Certificate Management........ 157

5.10.1 Local Certificate........ 157
5.10.2 Trusted CA Certificate 159
5.10.3 Certificate Backup........ 160

5.11 IP PBX 160

5.11.1 Extension 161
5.11.2 Line Setting 164
5.11.3 Dial Plan 167
5.11.4 PBX System 170
5.11.5 PBX Status 185

5.12 System Maintenance 186

5.12.1 System Status 186
5.12.2 TR-069 188
5.12.3 Administrator Password 189
5.12.4 Configuration Backup 189
5.12.5 Syslog/Mail Alert 191
5.12.6 Time and Date 193
5.12.7 Management 194
5.12.8 Reboot System 195
5.12.9 Firmware Upgrade 196

5.13 Diagnostics 197

5.13.1 Dial-out Trigger 197
5.13.2 Routing Table 198
5.13.3 ARP Cache Table 198
5.13.4 DHCP Table 199
5.13.5 NAT Sessions Table 199
5.13.6 Ping Diagnosis 200
5.13.7 Data Flow Monitor 201
5.13.8 Traffic Graph 202
5.13.9 Trace Route 203

Chapter 6: Trouble Shooting 205

6.1 Checking If the Hardware Status Is OK or Not 205

6.2 Checking If the Network Connection Settings on Your Computer Is OK or Not 206

6.3 Pinging the Router from Your Computer 208

6.4 Checking If the ISP Settings are OK or Not 209

6.5 Backing to Factory Default Setting If Necessary 211

6.6 Contacting Your Dealer 211

Appendix: Hardware Specifications 213

Chapter 1: Preface

VigorIPPBX 3510 is an ADSL and 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 2 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 50 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:

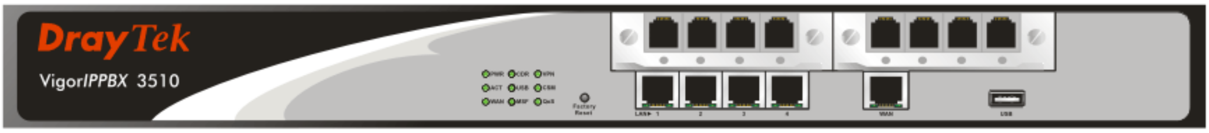
OK	Save and apply current settings.
Cancel	Cancel current settings and recover to the previous saved settings.
Clear	Clear all the selections and parameters settings, including selection from drop-down list. All the values must be reset with factory default settings.
Add	Add new settings for specified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

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

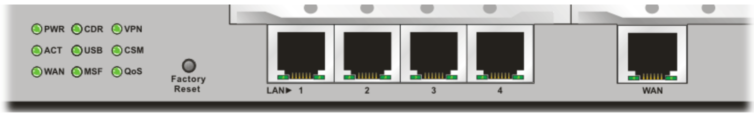
1.2 LED Indicators and Connectors

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

1.2.1 For VigorIPPBX 3510

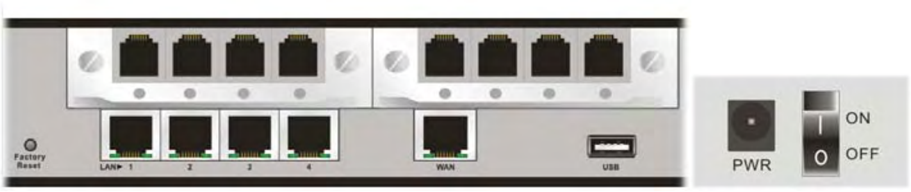


Description for LED



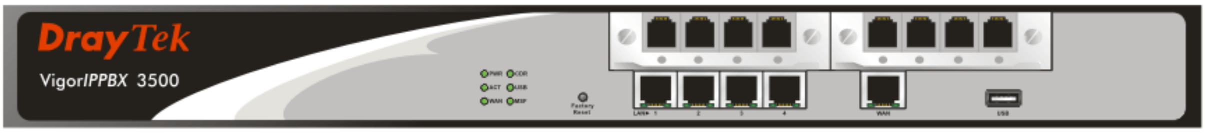
LED		Status	Explanation
PWR (Power)		On	The router is powered on.
		Off	The router is powered off.
ACT (Activity)		Blinking	The router is powered on and running normally.
		Off	The router is not ready or failed.
WAN		On	The WAN connection is ready.
		Blinking	It will blink while transmitting data.
CDR		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 2	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

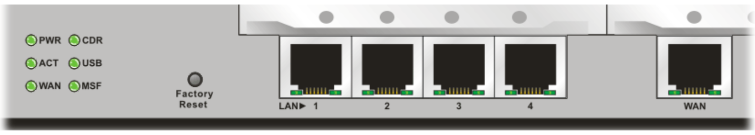


Interface	Description
Factory Reset	Restore the default settings. Usage: Turn on the router (ACT LED is blinking). Press the hole and keep for more than 5 seconds. When you see the ACT LED begins to blink rapidly than usual, release the button. Then the router will restart with the factory default configuration.
FXS	Connecter for telephone set.
FXO	Connecter for FXS interface of PABX.
LAN (1-4)	Connecters for local networked devices.
WAN	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.

1.2.2 For VigorIPPBX 3500

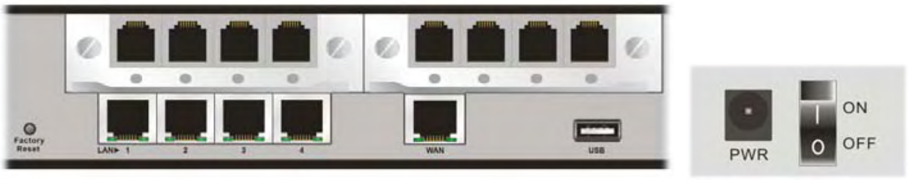


Description for LED



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 powered off.
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.
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	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



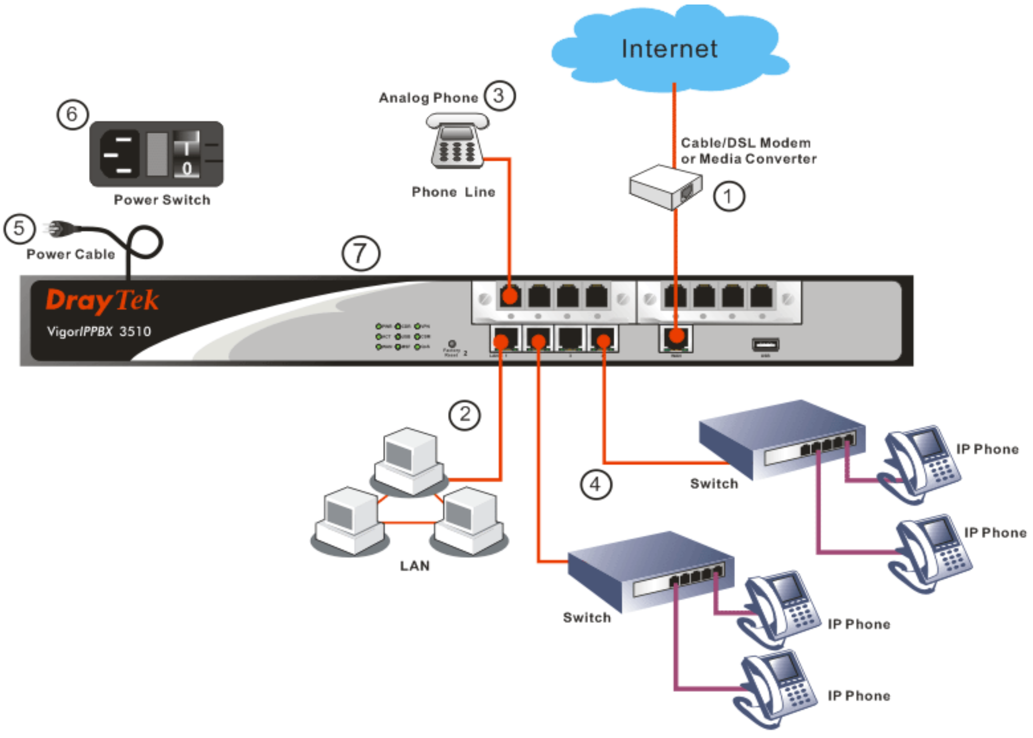
Interface	Description
Factory Reset	Restore the default settings. Usage: Turn on the router (ACT LED is blinking). Press the hole and keep for more than 5 seconds. When you see the ACT LED begins to blink rapidly than usual, release the button. Then the router will restart with the factory default configuration.
FXS	Connecter for telephone set.
FXO	Connecter for FXS interface of PABX.
LAN (1-4)	Connecters for local networked devices.
WAN	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 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.

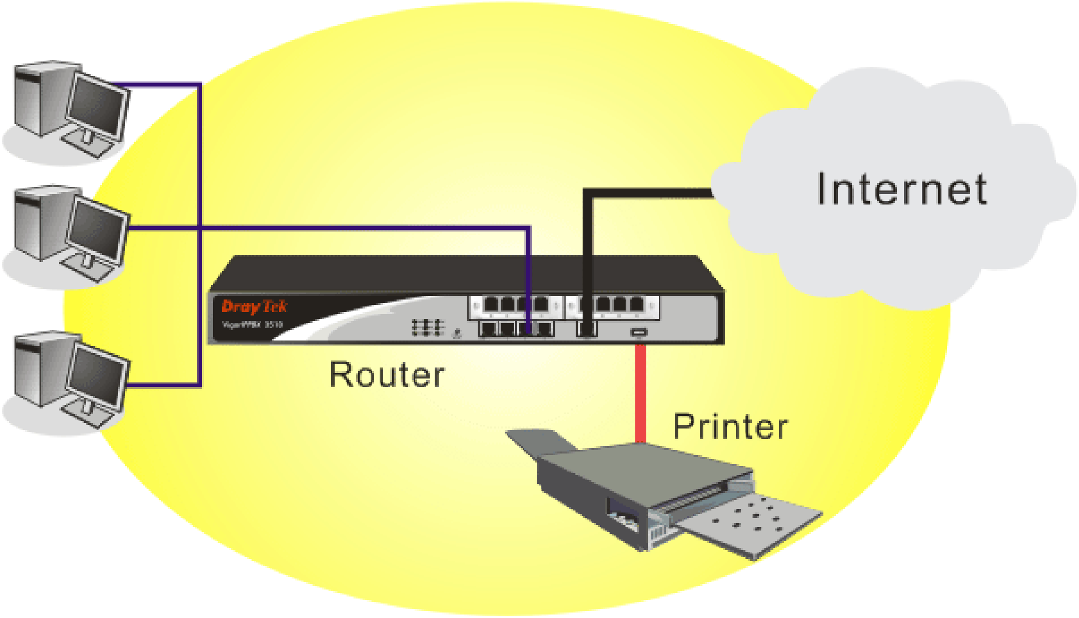
(For the detailed information of LED status, please refer to section 1.2.)



Caution: Each of the Phone ports can be connected to an analog phone only. Do not connect the phone ports to the telephone wall jack. Such connection might damage your router.

1.4 Printer Installation

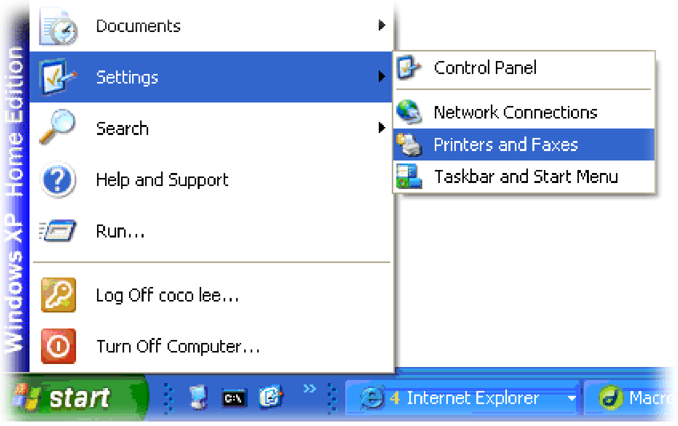
You can install a printer onto the router for sharing printing. All the PCs connected this router can print documents via the router. The example provided here is made based on Windows XP/2000. For Windows 98/SE, please visit www.draytek.com.



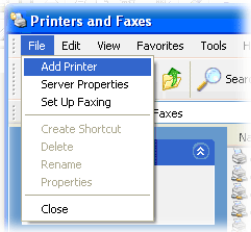
Before using it, please follow the steps below to configure settings for connected computers (or wireless clients).

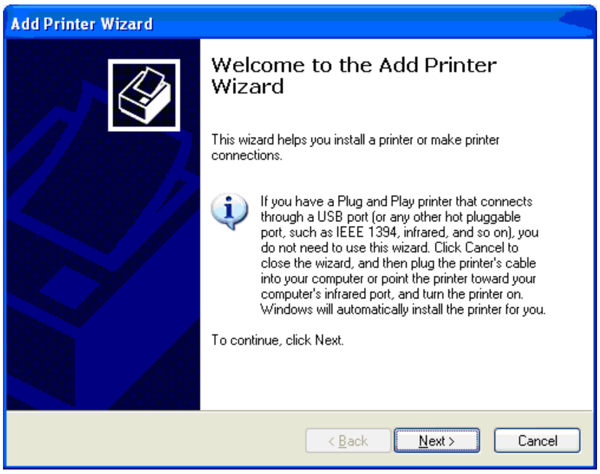
1. Connect the printer with the router through USB/parallel port.

2. Open **Start->Settings-> Printer and Faxes**.



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





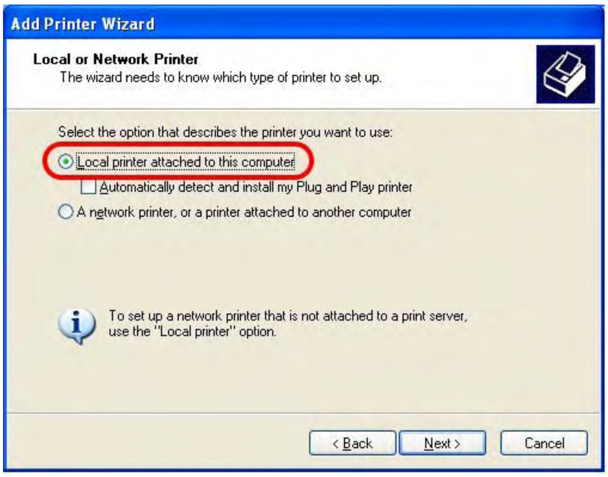
Welcome to the Add Printer Wizard

This wizard helps you install a printer or make printer connections.

If you have a Plug and Play printer that connects through a USB port (or any other hot pluggable port, such as IEEE 1394, infrared, and so on), you do not need to use this wizard. Click Cancel to close the wizard, and then plug the printer's cable into your computer or point the printer toward your computer's infrared port, and turn the printer on. Windows will automatically install the printer for you.

To continue, click Next.

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



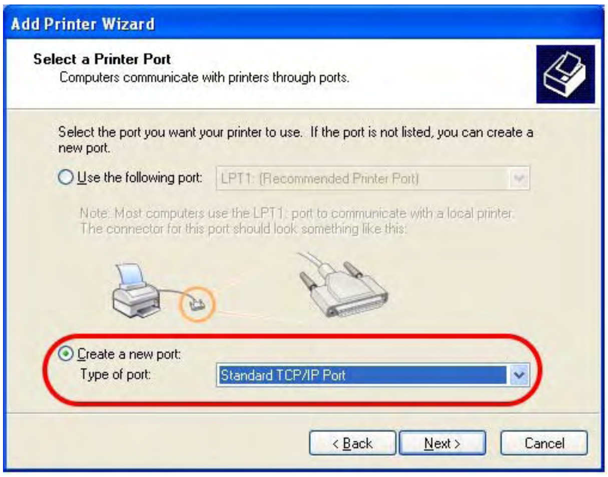
Local or Network Printer
The wizard needs to know which type of printer to set up.

Select the option that describes the printer you want to use:

● Local printer attached to this computer
□ Automatically detect and install my Plug and Play printer
○ A network printer, or a printer attached to another computer

To set up a network printer that is not attached to a print server, use the "Local printer" option.

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**.



Select a Printer Port
Computers communicate with printers through ports.

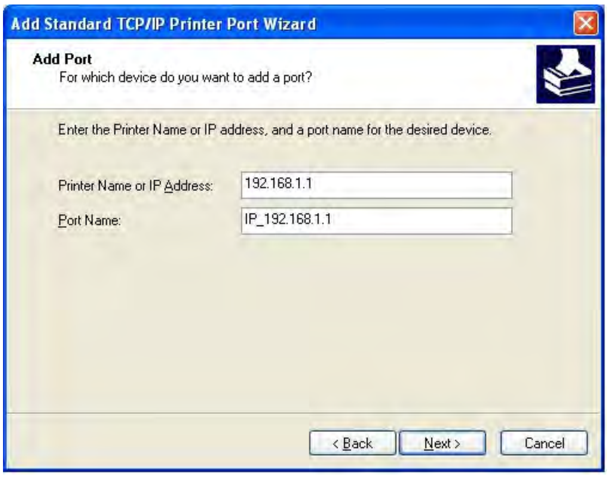
Select the port you want your printer to use. If the port is not listed, you can create a new port.

○ Use the following port: LPT1: (Recommended Printer Port)

Note: Most computers use the LPT1: port to communicate with a local printer. The connector for this port should look something like this:

● Create a new port:
Type of port: Standard TCP/IP Port

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**.



Add Standard TCP/IP Printer Port Wizard

Add Port

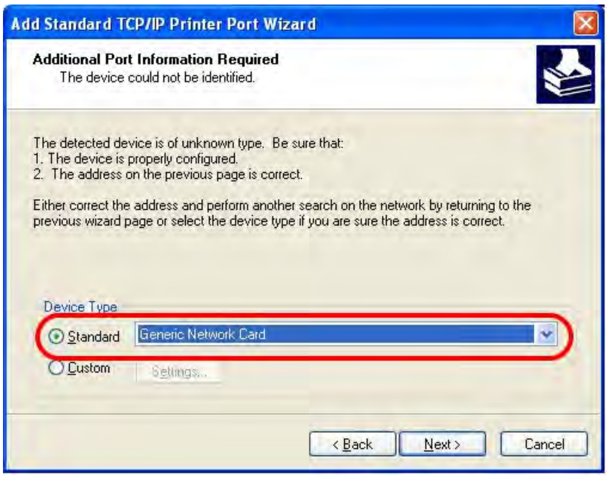
For which device do you want to add a port?

Enter the Printer Name or IP address, and a port name for the desired device.

Printer Name or IP Address: 192.168.1.1

Port Name: IP_192.168.1.1

7. Click Standard and choose Generic Network Card.



Add Standard TCP/IP Printer Port Wizard

Additional Port Information Required

The device could not be identified.

The detected device is of unknown type. Be sure that:
1. The device is properly configured.
2. The address on the previous page is correct.

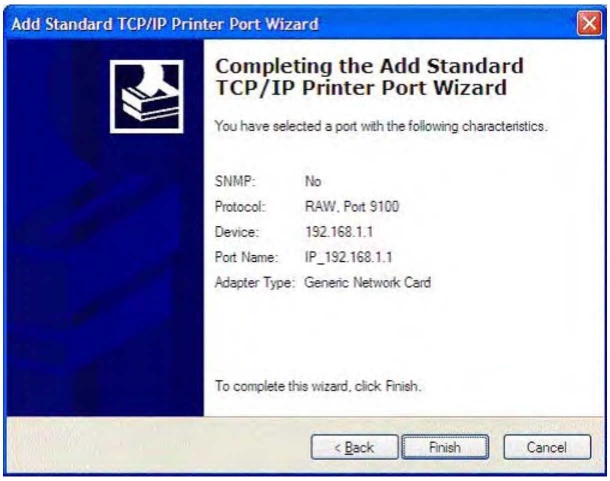
Either correct the address and perform another search on the network by returning to the previous wizard page or select the device type if you are sure the address is correct.

Device Type

● Standard: Generic Network Card

○ Custom

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



Add Standard TCP/IP Printer Port Wizard

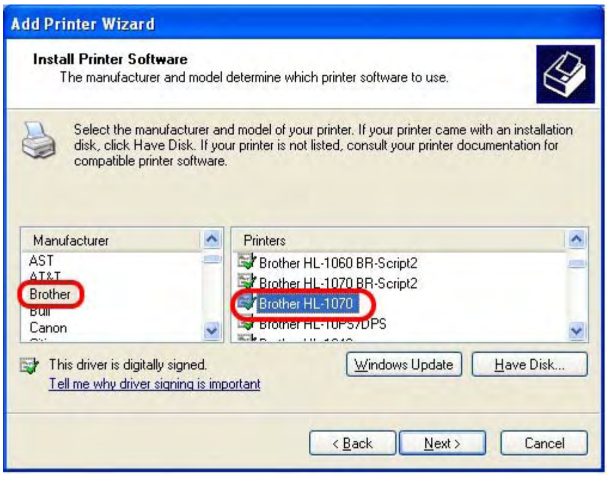
Completing the Add Standard TCP/IP Printer Port Wizard

You have selected a port with the following characteristics.

SNMP:	No
Protocol:	RAW, Port 9100
Device:	192.168.1.1
Port Name:	IP_192.168.1.1
Adapter Type:	Generic Network Card

To complete this wizard, 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**.



Add Printer Wizard

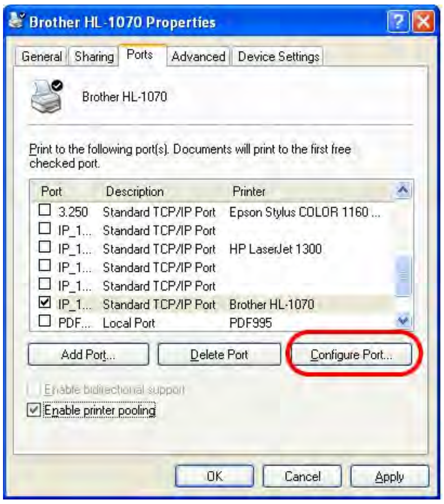
Install Printer Software
The manufacturer and model determine which printer software to use.

Select the manufacturer and model of your printer. If your printer came with an installation disk, click Have Disk. If your printer is not listed, consult your printer documentation for compatible printer software.

Manufacturer	Printers
AST	Brother HL-1060 BR-Script2
AT&T	Brother HL-1070 BR-Script2
Brother	Brother HL-1070
Bull	Brother HL-10PS/DPS
Canon	

This driver is digitally signed.
Tell me why driver signing is important

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.



Brother HL-1070 Properties

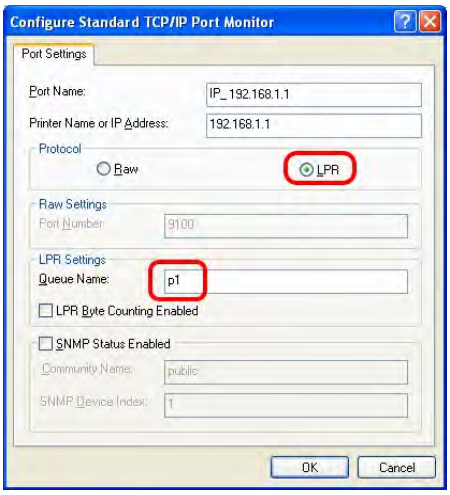
Brother HL-1070

Print to the following port(s). Documents will print to the first free checked port.

Port	Description	Printer
☐ 3.250	Standard TCP/IP Port	Epson Stylus COLOR 1160 ...
☐ IP_1...	Standard TCP/IP Port	
☐ IP_1...	Standard TCP/IP Port	HP LaserJet 1300
☐ IP_1...	Standard TCP/IP Port	
☐ IP_1...	Standard TCP/IP Port	
☑ IP_1...	Standard TCP/IP Port	Brother HL-1070
☐ PDF...	Local Port	PDF995

☐ Enable bidirectional support
☑ Enable printer pooling

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



Configure Standard TCP/IP Port Monitor

Port Settings

Port Name: IP_192.168.1.1

Printer Name or IP Address: 192.168.1.1

Protocol
○ Raw ● LPR

Raw Settings
Port Number: 9100

LPR Settings
Queue Name: p1

☐ LPR Byte Counting Enabled

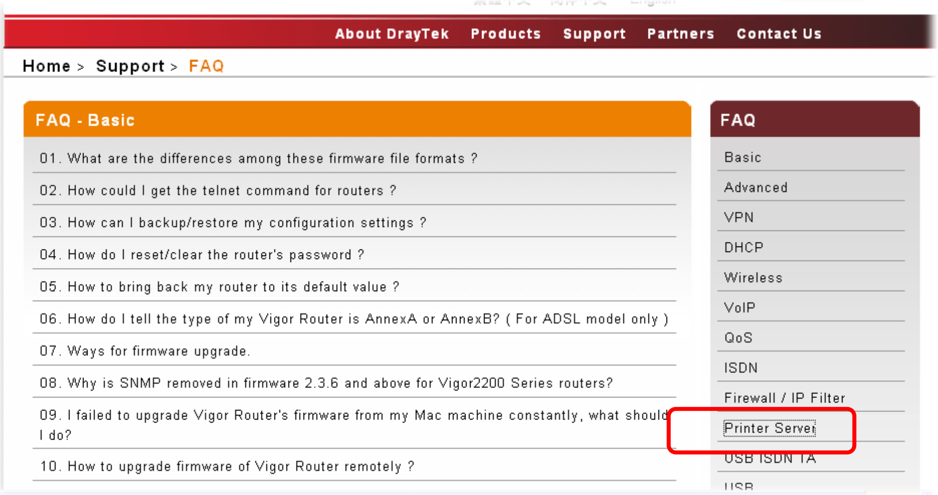
☐ SNMP Status Enabled

Community Name: public

SNMP Device Index: 1

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

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



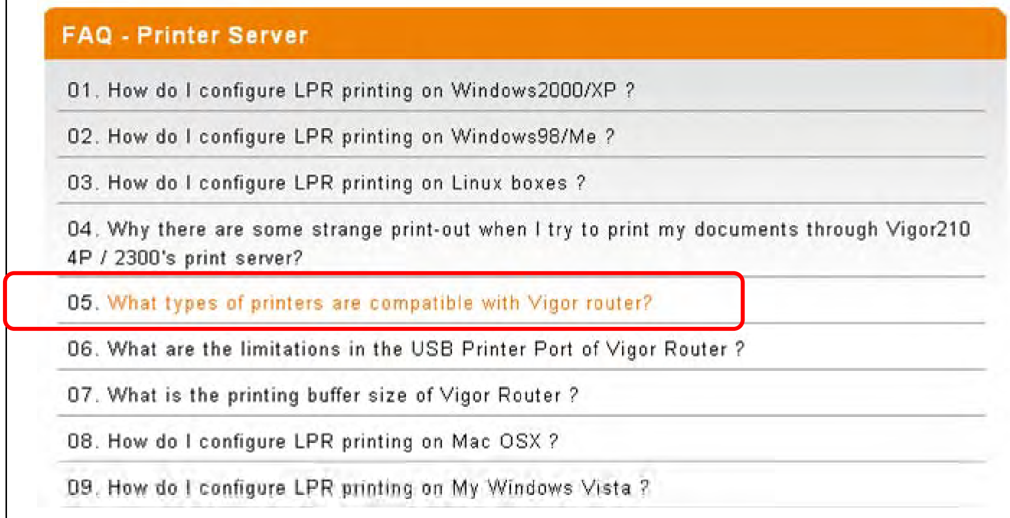
Home > Support > FAQ

FAQ - Basic

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

FAQ

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



FAQ - Printer Server

01. How do I configure LPR printing on Windows2000/XP ?
02. How do I configure LPR printing on Windows98/Me ?
03. How do I configure LPR printing on Linux boxes ?
04. Why there are some strange print-out when I try to print my documents through Vigor2104P / 2300's print server?
05. What types of printers are compatible with Vigor router?
06. What are the limitations in the USB Printer Port of Vigor Router ?
07. What is the printing buffer size of Vigor Router ?
08. How do I configure LPR printing on Mac OSX ?
09. How do I configure LPR printing on My Windows Vista ?

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

This page is left blank.

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.

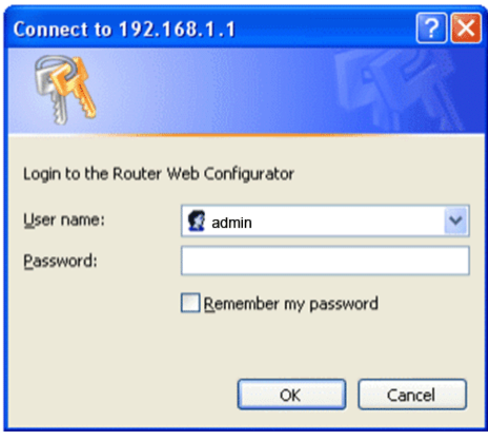
2.1 Changing Password

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.



Connect to 192.168.1.1

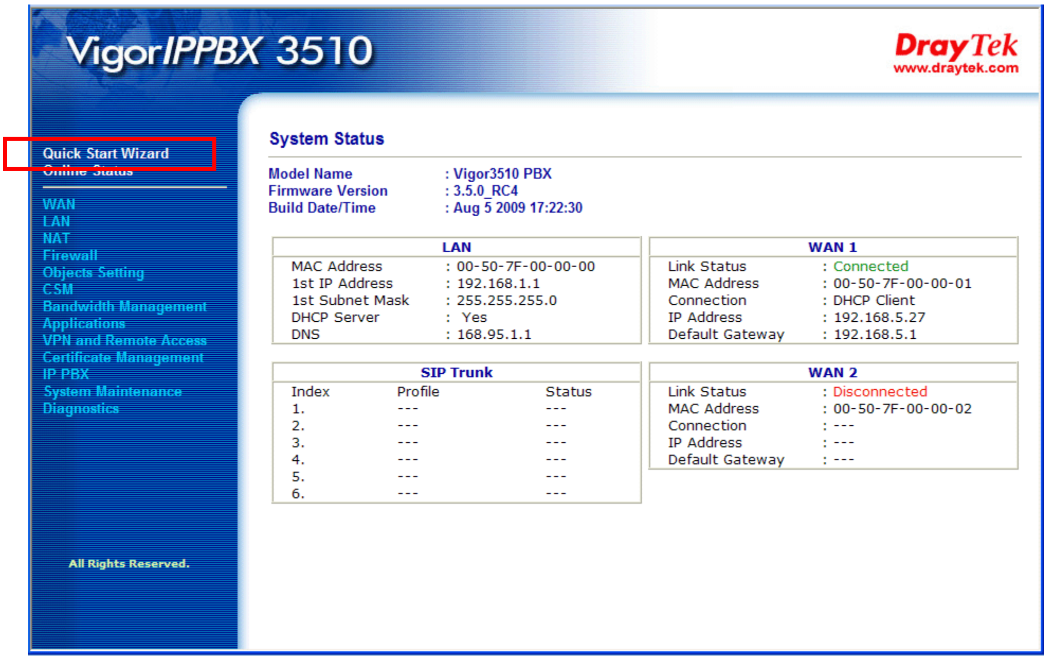
Login to the Router Web Configurator

User name: admin

Password:

□ Remember my password

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



System Status

Model Name : Vigor3510 PBX
Firmware Version : 3.5.0_RC4
Build Date/Time : Aug 5 2009 17:22:30

LAN	
MAC Address	: 00-50-7F-00-00-00
1st IP Address	: 192.168.1.1
1st Subnet Mask	: 255.255.255.0
DHCP Server	: Yes
DNS	: 168.95.1.1

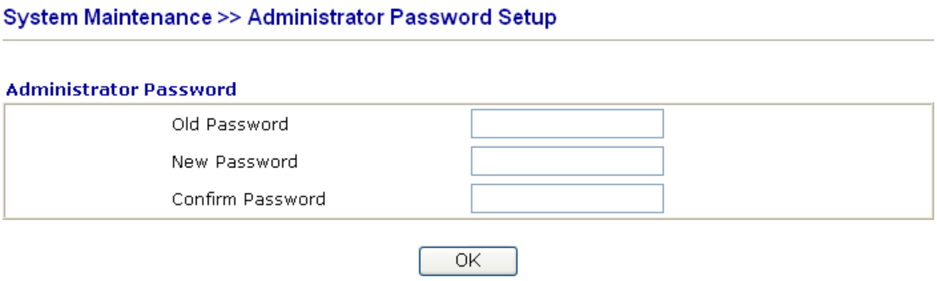
WAN 1	
Link Status	: Connected
MAC Address	: 00-50-7F-00-00-01
Connection	: DHCP Client
IP Address	: 192.168.5.27
Default Gateway	: 192.168.5.1

SIP Trunk		
Index	Profile	Status
1.	---	---
2.	---	---
3.	---	---
4.	---	---
5.	---	---
6.	---	---

WAN 2	
Link Status	: Disconnected
MAC Address	: 00-50-7F-00-00-02
Connection	: ---
IP Address	: ---
Default Gateway	: ---

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

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



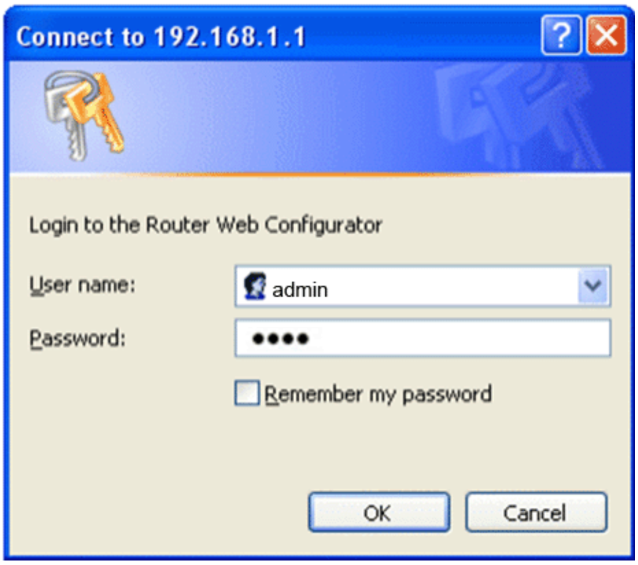
System Maintenance >> Administrator Password Setup

Administrator Password

Old Password
New Password
Confirm 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.



Connect to 192.168.1.1

Login to the Router Web Configurator

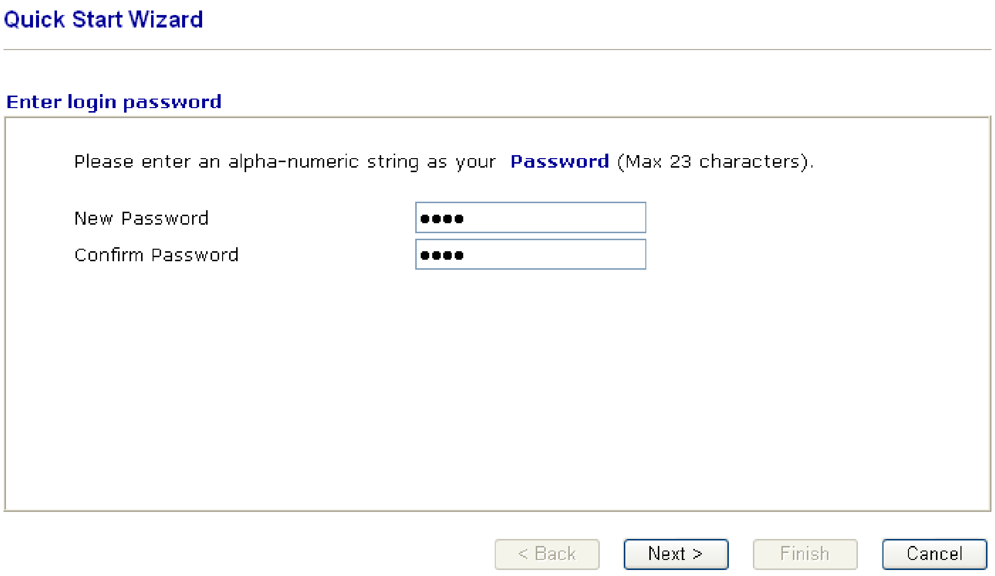
User name: admin

Password: ●●●●

□ Remember my password

2.2 Quick Start Wizard

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



Quick Start Wizard

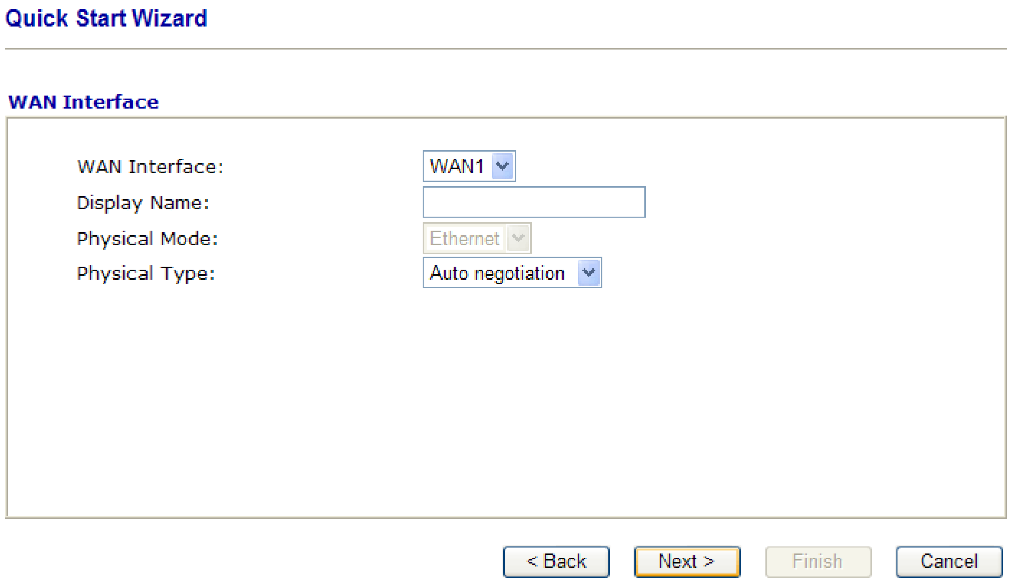
Enter login password

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

New Password ●●●●

Confirm Password ●●●●

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



Quick Start Wizard

WAN Interface

WAN Interface: WAN1

Display Name:

Physical Mode: Ethernet

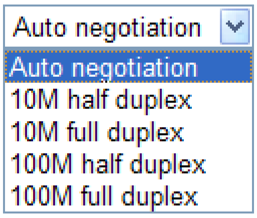
Physical Type: Auto negotiation

WAN Interface Specify which interface you use for network connection.

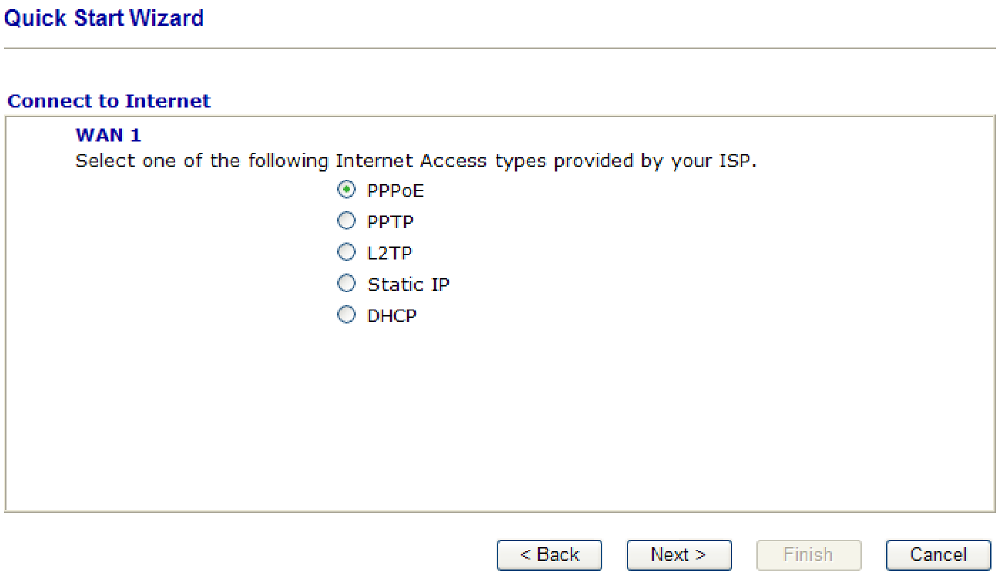
Display Name Type the name for this router.

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.



Quick Start Wizard

Connect to Internet

WAN 1

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

● PPPoE
○ PPTP
○ L2TP
○ Static IP
○ DHCP

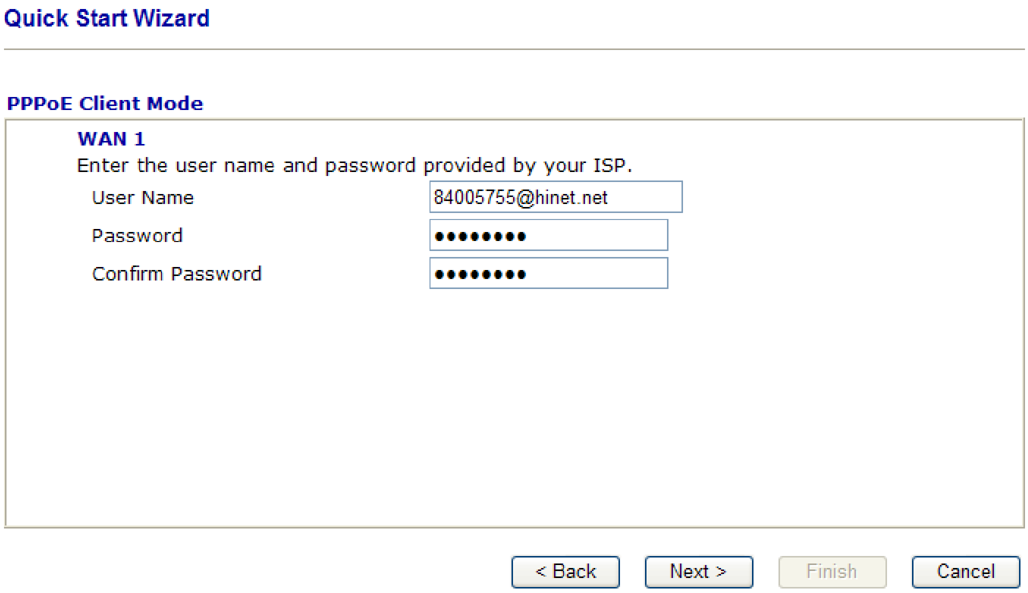
In the **Quick Start Wizard**, you can configure the router to access the Internet with different protocol/modes such as **PPPoE**, **PPTP, L2TP**, **Static IP** or **DHCP**. The router supports the DSL WAN interface for Internet access.

2.2.1 PPPoE

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

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

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



Quick Start Wizard

PPPoE Client Mode

WAN 1

Enter the user name and password provided by your ISP.

User Name: 84005755@hinet.net

Password: ••••••••

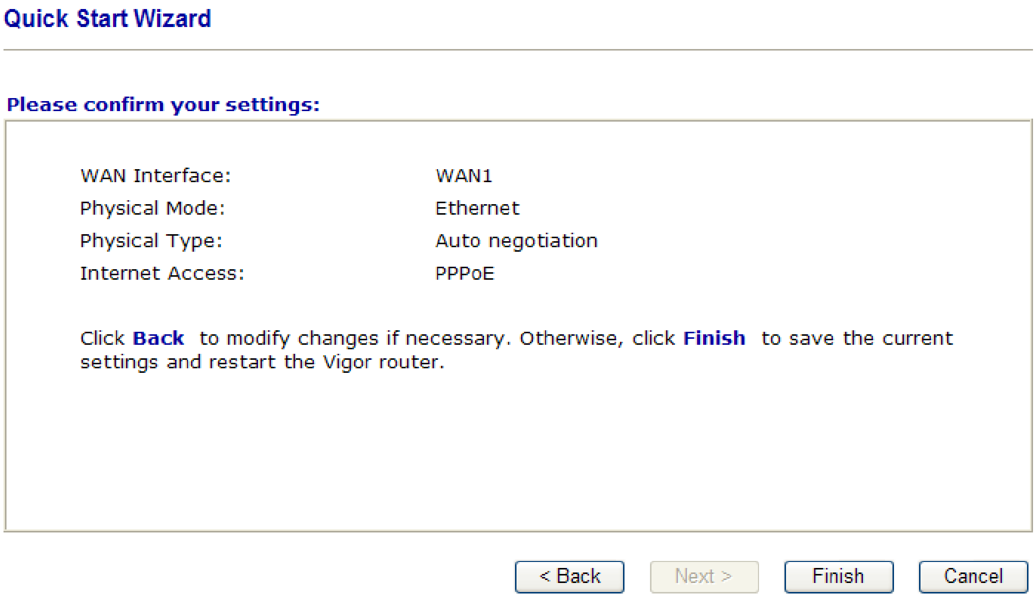
Confirm Password: ••••••••

User Name Assign a specific valid user name provided by the ISP.

Password Assign a valid password provided by the ISP.

Confirm Password Retype the password.

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



Quick Start Wizard

Please confirm your settings:

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

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

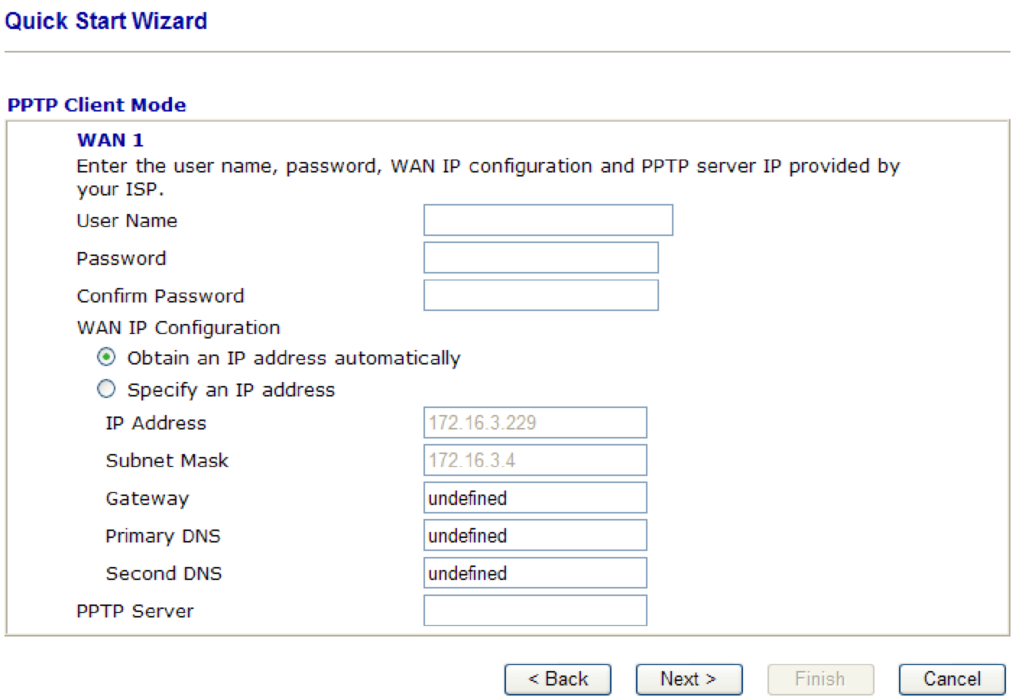
Click **Finish.** A page of **Quick Start Wizard Setup OK!!!** will appear. Then, the system status of this protocol will be shown.

Quick Start Wizard Setup OK !!!

2.2.2 PPTP/L2TP

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

PPTP Setting ---



Quick Start Wizard

PPTP Client Mode

WAN 1

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

User Name

Password

Confirm Password

WAN IP Configuration

● Obtain an IP address automatically

○ Specify an IP address

IP Address: 172.16.3.229

Subnet Mask: 172.16.3.4

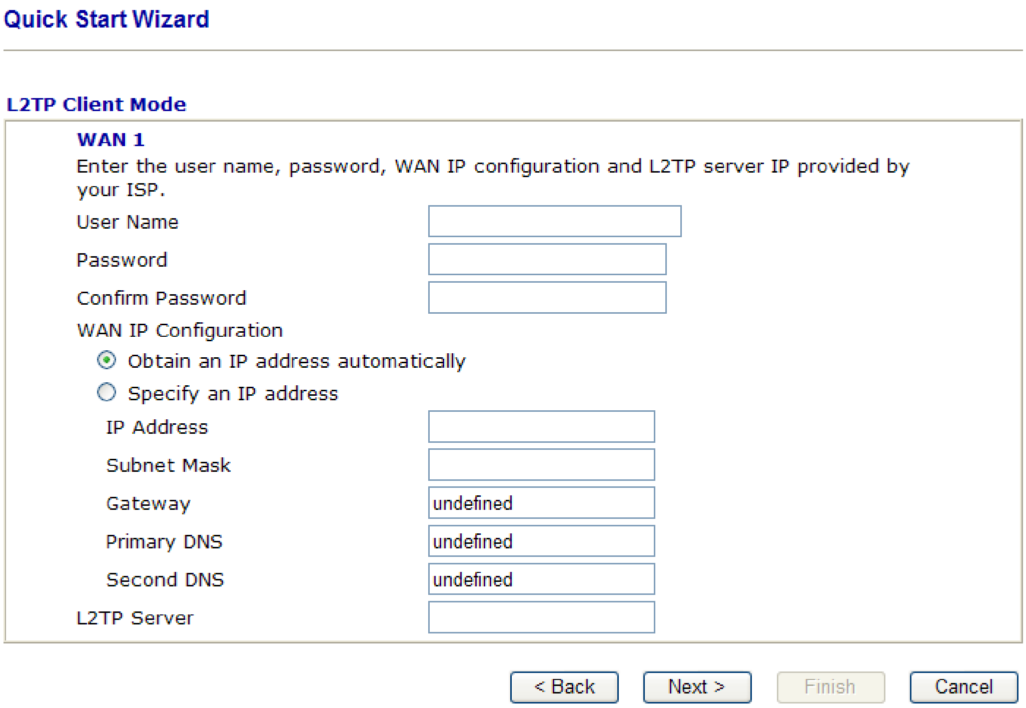
Gateway: undefined

Primary DNS: undefined

Second DNS: undefined

PPTP Server

L2TP Setting ---



Quick Start Wizard

L2TP Client Mode

WAN 1

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

User Name

Password

Confirm Password

WAN IP Configuration

● Obtain an IP address automatically

○ Specify an IP address

IP Address

Subnet Mask

Gateway: undefined

Primary DNS: undefined

Second DNS: undefined

L2TP Server

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.

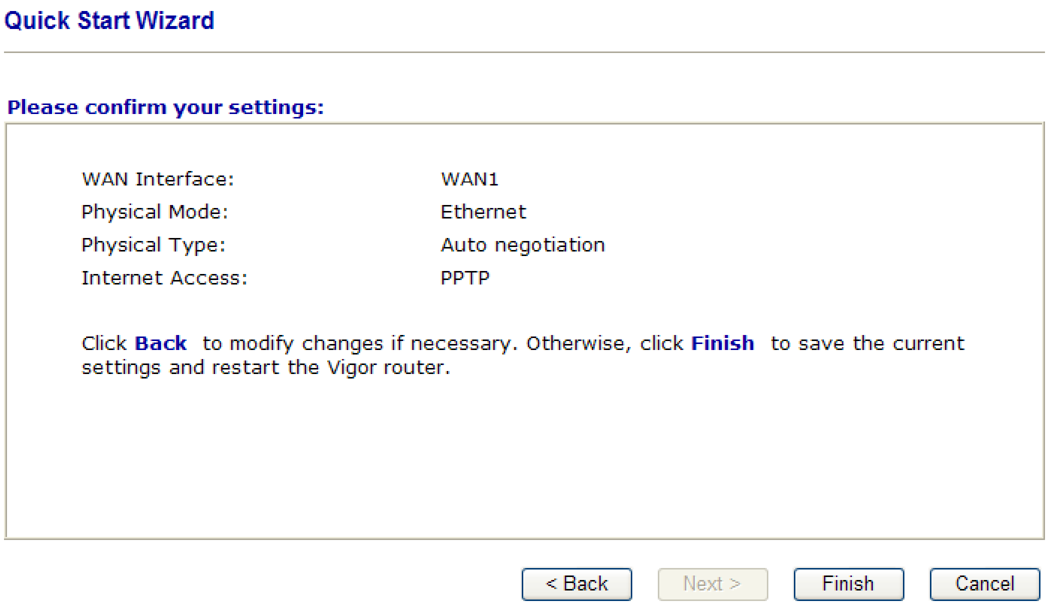
Obtain an IP address automatically

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.



Quick Start Wizard

Please confirm your settings:

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

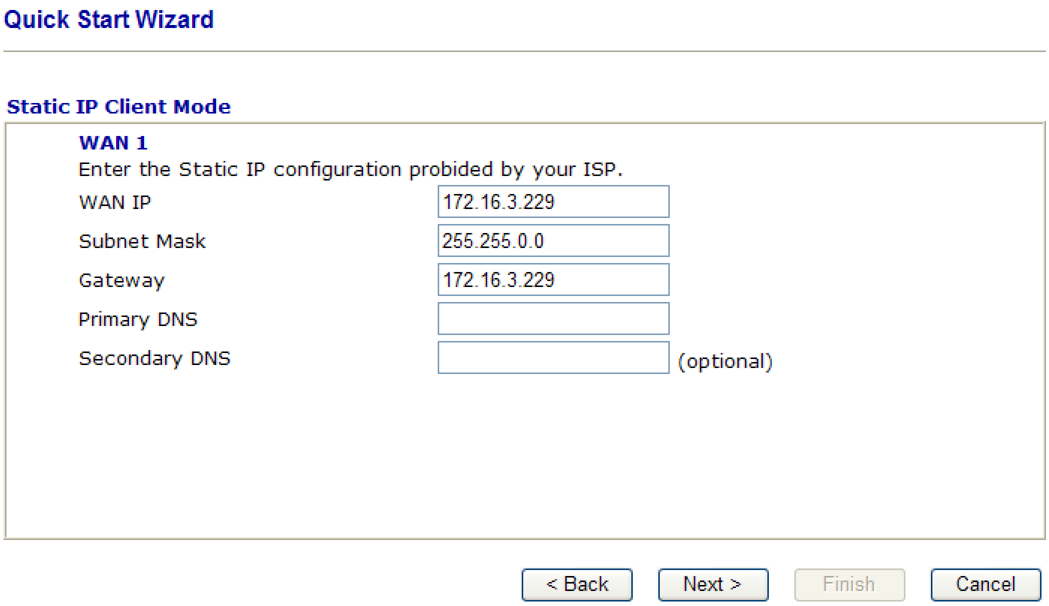
Click **Back** to modify changes if necessary. Otherwise, click **Finish** to save the current settings and restart the Vigor router.

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

Quick Start Wizard Setup OK !!!

2.2.3 Static IP

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



Quick Start Wizard

Static IP Client Mode

WAN 1

Enter the Static IP configuration probided by your ISP.

WAN IP	172.16.3.229
Subnet Mask	255.255.0.0
Gateway	172.16.3.229
Primary DNS	
Secondary DNS	(optional)

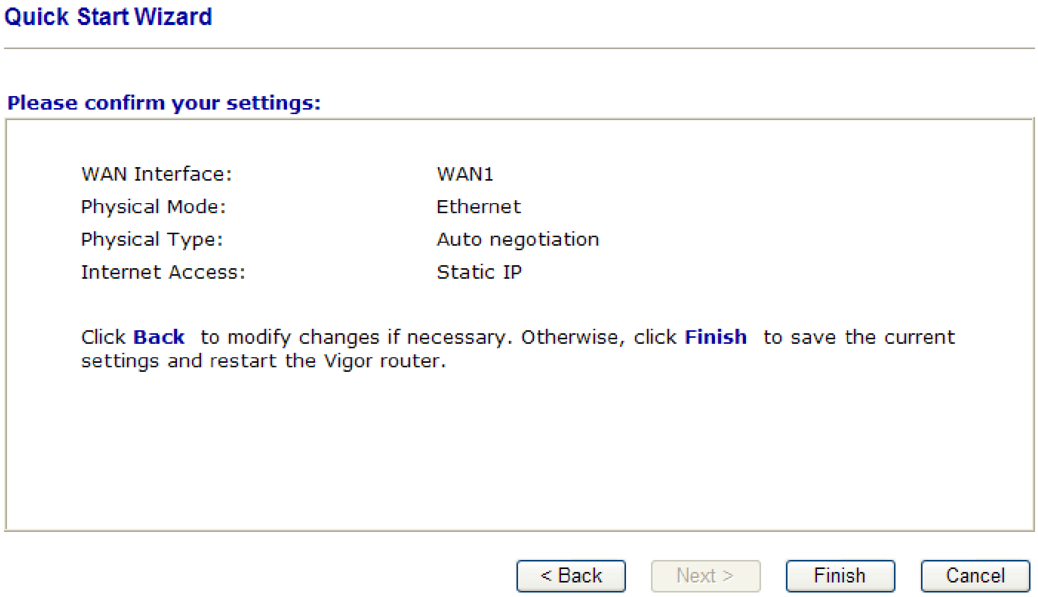
WANIP Address Type the IP address.

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.



Quick Start Wizard

Please confirm your settings:

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

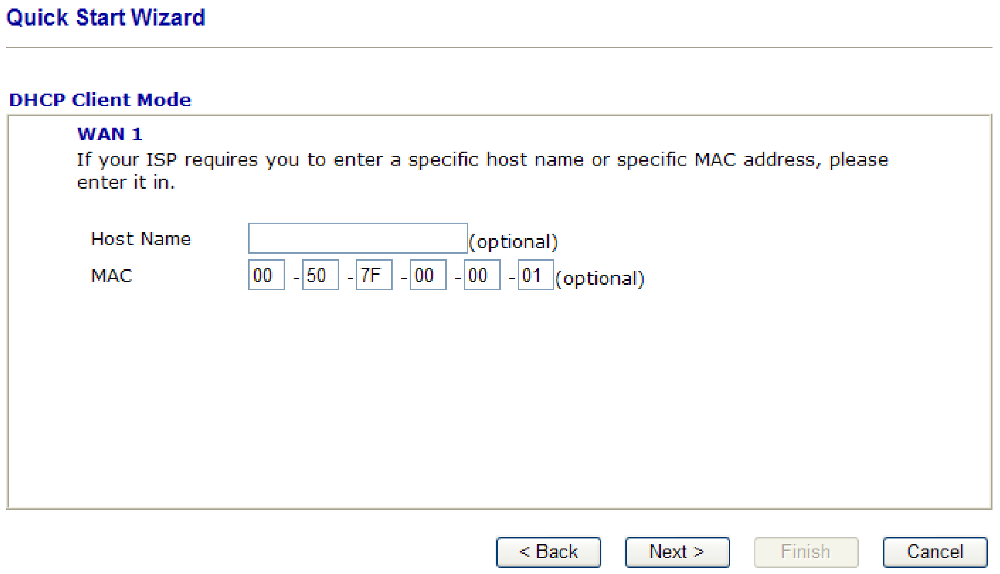
Click **Back** to modify changes if necessary. Otherwise, click **Finish** to save the current settings and restart the Vigor router.

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

Quick Start Wizard Setup OK !!!

2.2.4 DHCP

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



Quick Start Wizard

DHCP Client Mode

WAN 1

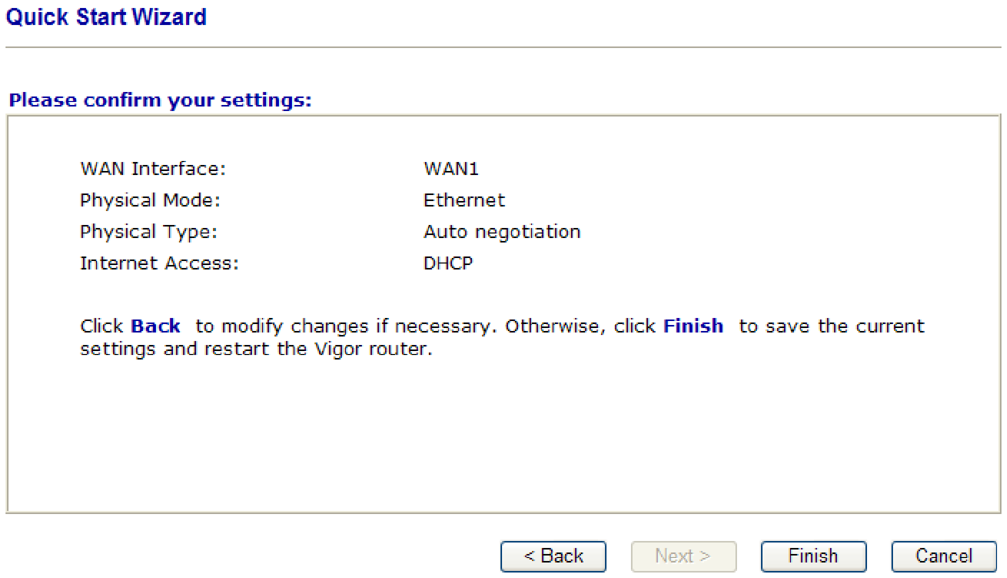
If your ISP requires you to enter a specific host name or specific MAC address, please enter it in.

Host Name		(optional)
MAC	00 - 50 - 7F - 00 - 00 - 01	(optional)

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.



Quick Start Wizard

Please confirm your settings:

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

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

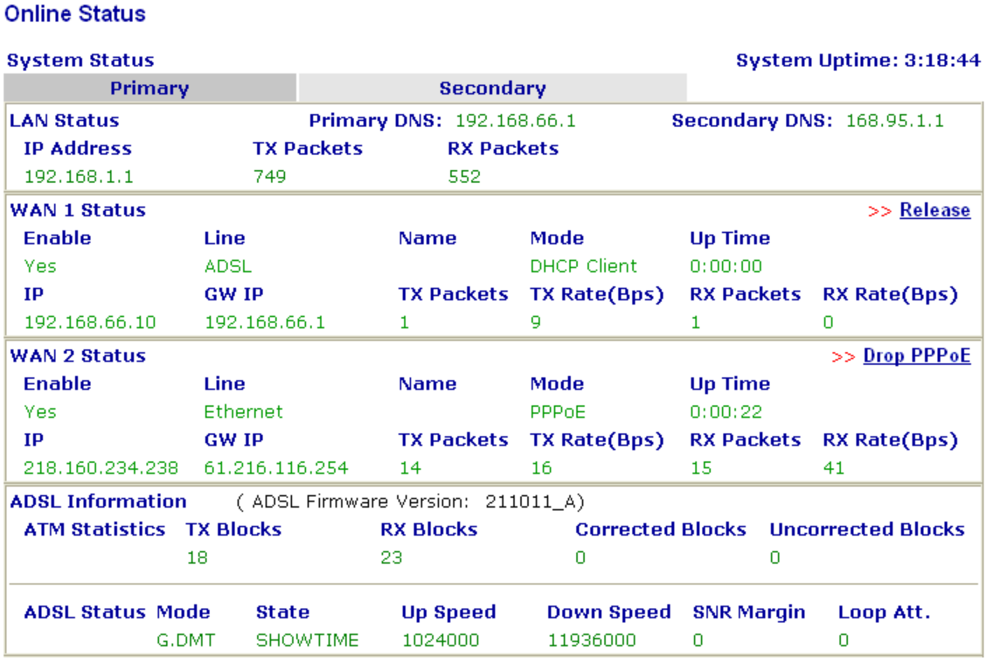
Click **Finish.** A page of **Quick Start Wizard Setup OK!!!** will appear. Then, the system status of this protocol will be shown.

Quick Start Wizard Setup OK !!!

2.3 Online Status

The online status shows the system status, WAN status, ADSL Information 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.

Online status for PPPoE



Online Status

System Status — System Uptime: 3:18:44

LAN Status — Primary DNS: 192.168.66.1 — Secondary DNS: 168.95.1.1

IP Address	TX Packets	RX Packets
192.168.1.1	749	552

WAN 1 Status — >> Release

Enable	Line	Name	Mode	Up Time	
Yes	ADSL		DHCP Client	0:00:00	
IP	**GW IP**	**TX Packets**	**TX Rate(Bps)**	**RX Packets**	**RX Rate(Bps)**
192.168.66.10	192.168.66.1	1	9	1	0

WAN 2 Status — >> Drop PPPoE

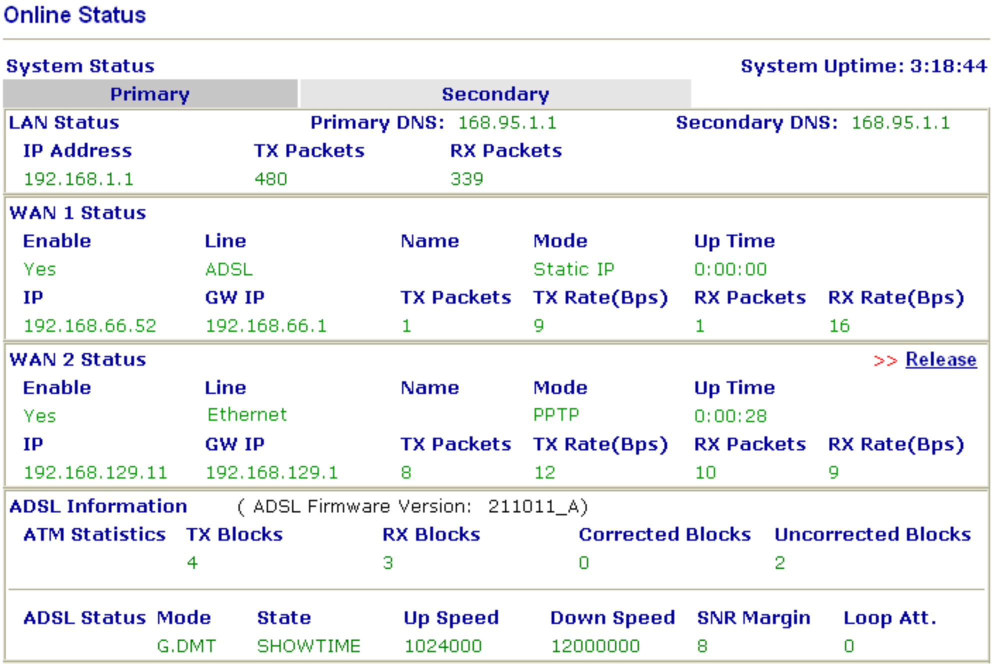
Enable	Line	Name	Mode	Up Time	
Yes	Ethernet		PPPoE	0:00:22	
IP	**GW IP**	**TX Packets**	**TX Rate(Bps)**	**RX Packets**	**RX Rate(Bps)**
218.160.234.238	61.216.116.254	14	16	15	41

ADSL Information (ADSL Firmware Version: 211011_A)

ATM Statistics	TX Blocks	RX Blocks	Corrected Blocks	Uncorrected Blocks
	18	23	0	0

ADSL Status	Mode	State	Up Speed	Down Speed	SNR Margin	Loop Att.
	G.DMT	SHOWTIME	1024000	11936000	0	0

Online status for PPTP



Online Status

System Status — System Uptime: 3:18:44

Primary | Secondary

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

IP Address	TX Packets	RX Packets
192.168.1.1	480	339

WAN 1 Status

Enable	Line	Name	Mode	Up Time	
Yes	ADSL		Static IP	0:00:00	
IP	**GW IP**	**TX Packets**	**TX Rate(Bps)**	**RX Packets**	**RX Rate(Bps)**
192.168.66.52	192.168.66.1	1	9	1	16

WAN 2 Status — >> Release

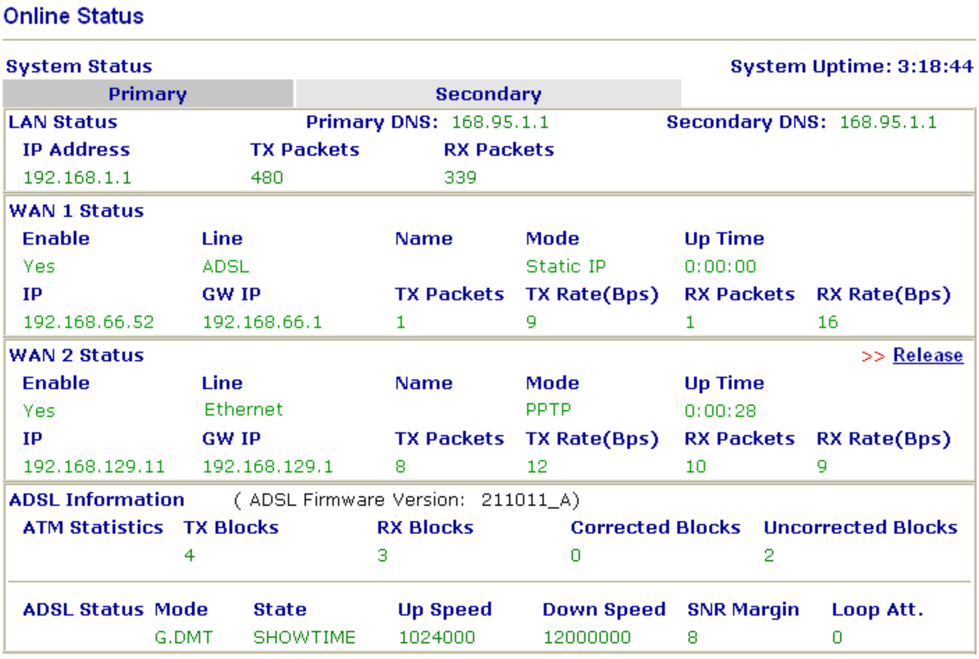
Enable	Line	Name	Mode	Up Time	
Yes	Ethernet		PPTP	0:00:28	
IP	**GW IP**	**TX Packets**	**TX Rate(Bps)**	**RX Packets**	**RX Rate(Bps)**
192.168.129.11	192.168.129.1	8	12	10	9

ADSL Information (ADSL Firmware Version: 211011_A)

ATM Statistics	TX Blocks	RX Blocks	Corrected Blocks	Uncorrected Blocks
	4	3	0	2

ADSL Status	Mode	State	Up Speed	Down Speed	SNR Margin	Loop Att.
	G.DMT	SHOWTIME	1024000	12000000	8	0

Online status for Static IP



Online Status

System Status — System Uptime: 3:18:44

Primary | Secondary

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

IP Address	TX Packets	RX Packets
192.168.1.1	480	339

WAN 1 Status

Enable	Line	Name	Mode	Up Time	
Yes	ADSL		Static IP	0:00:00	
IP	**GW IP**	**TX Packets**	**TX Rate(Bps)**	**RX Packets**	**RX Rate(Bps)**
192.168.66.52	192.168.66.1	1	9	1	16

WAN 2 Status — >> Release

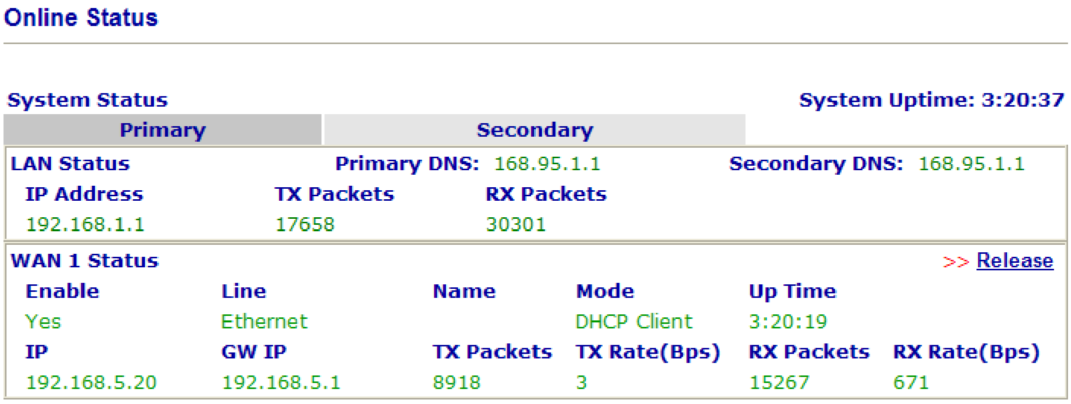
Enable	Line	Name	Mode	Up Time	
Yes	Ethernet		PPTP	0:00:28	
IP	**GW IP**	**TX Packets**	**TX Rate(Bps)**	**RX Packets**	**RX Rate(Bps)**
192.168.129.11	192.168.129.1	8	12	10	9

ADSL Information (ADSL Firmware Version: 211011_A)

ATM Statistics	TX Blocks	RX Blocks	Corrected Blocks	Uncorrected Blocks
	4	3	0	2

ADSL Status	Mode	State	Up Speed	Down Speed	SNR Margin	Loop Att.
	G.DMT	SHOWTIME	1024000	12000000	8	0

Online status for DHCP



Online Status

System Status — System Uptime: 3:20:37

Primary | Secondary

LAN Status		Primary DNS: 168.95.1.1	Secondary DNS: 168.95.1.1
IP Address	TX Packets	RX Packets	
192.168.1.1	17658	30301	

WAN 1 Status — >> Release

Enable	Line	Name	Mode	Up Time	
Yes	Ethernet		DHCP Client	3:20:19	
IP	GW IP	TX Packets	TX Rate(Bps)	RX Packets	RX Rate(Bps)
192.168.5.20	192.168.5.1	8918	3	15267	671

Detailed explanation is shown below:

Primary DNS Displays the IP address of the primary DNS.

Secondary DNS Displays the IP address of the secondary DNS.

LAN Status

IP Address Displays the IP address of the LAN interface.

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

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

WAN Status

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

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

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

Up Time Displays the total uptime of the interface.

IP Displays the IP address of the WAN interface.

GW IP Displays the IP address of the default gateway.

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

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

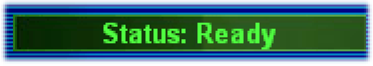
RX Packets Displays the total number of received packets at the WAN interface.

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

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

2.4 Saving Configuration

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



Status: Ready

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

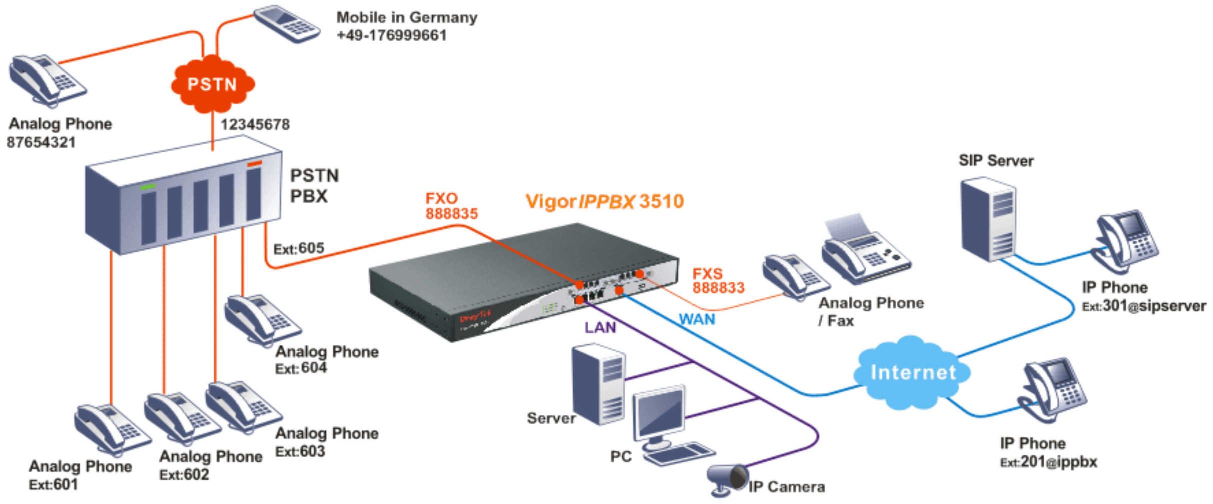
Settings Saved means your settings are saved once you click **Finish** or **OK** button.

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

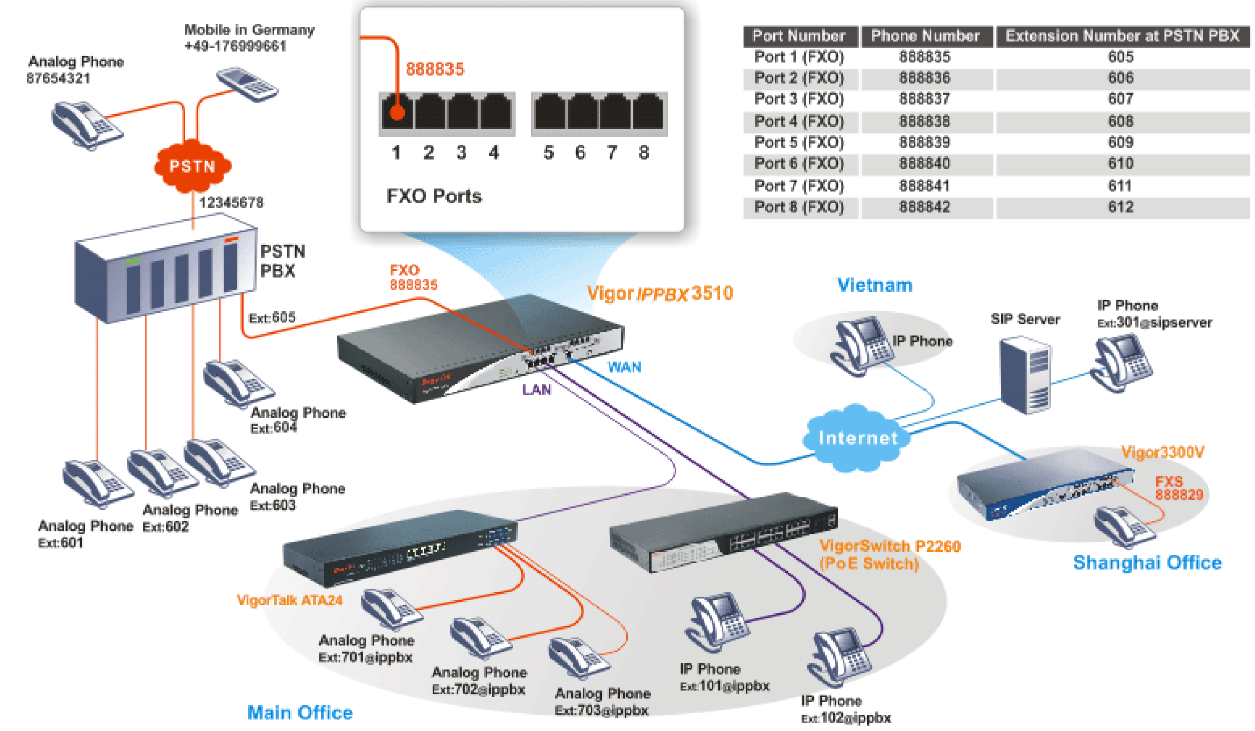


- The establishment of IP registration is made through WAN port.
- The remote IP -based phone with ext. 301 is registered at a SIP server.
- The remote IP -based phone with ext. 201 is registered at remote site.
- The analog phone or fax machine is connected to FXS module. The said VoIP No. is 888833.
- 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 Aanalog 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]

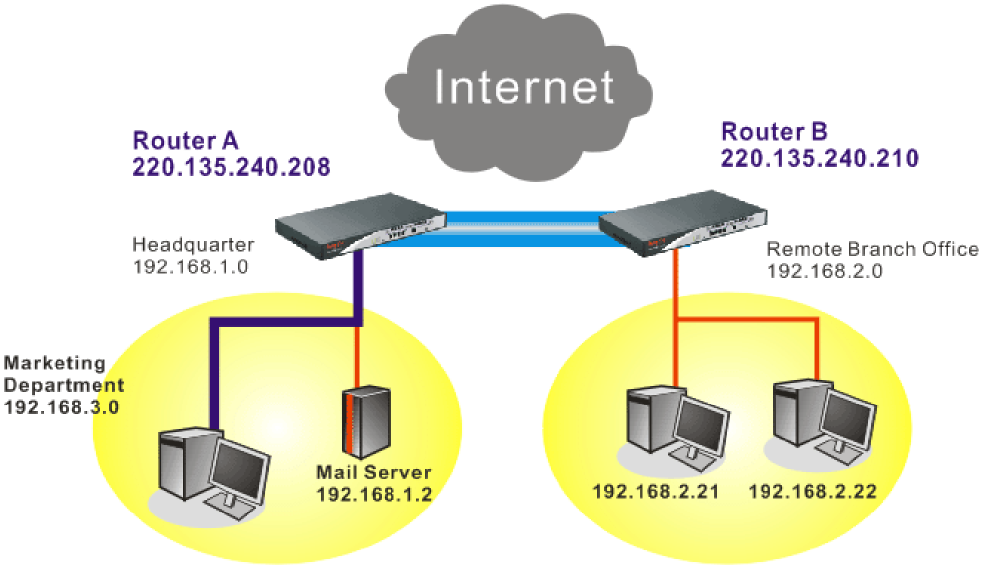
- The IP phone with ext. No. 201 made a call to remote analog phone (No. 87654321): Press 888835#. After getting through you will hear the dial tone, press outside line **0** and then press the PSTN number 87654321.
- The analog phone with VoIP number 88829 in Shanghai made a call to the remote mobile 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**
VigorIPPBX3510	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	

Chapter 4: Other Applications

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

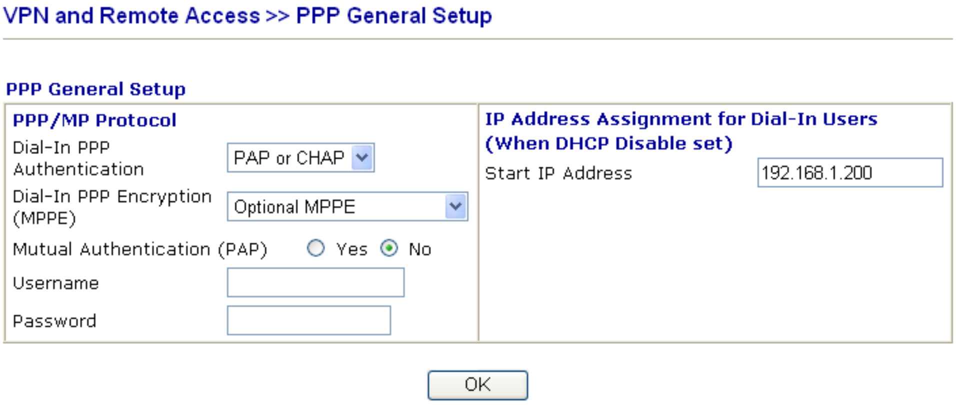
The most common case is that you may want to connect to network securely, such as the remote branch office and headquarter. According to the network structure as shown in the below illustration, you may follow the steps to create a LAN-to-LAN profile. These two networks (LANs) should NOT have the same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



VPN and Remote Access >> PPP General Setup

PPP General Setup

PPP/MP Protocol

Dial-In PPP Authentication: PAP or CHAP

Dial-In PPP Encryption (MPPE): Optional MPPE

Mutual Authentication (PAP): ○ Yes ● No

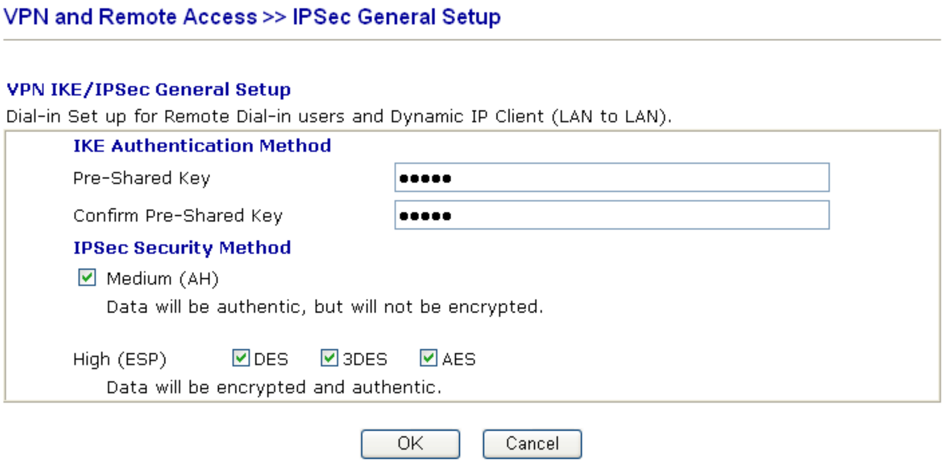
Username:

Password:

IP Address Assignment for Dial-In Users (When DHCP Disable set)

Start IP Address: 192.168.1.200

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



VPN and Remote Access >> IPSec General Setup

VPN IKE/IPSec General Setup

Dial-in Set up for Remote Dial-in users and Dynamic IP Client (LAN to LAN).

IKE Authentication Method

Pre-Shared Key: ●●●●●

Confirm Pre-Shared Key: ●●●●●

IPSec Security Method

☑ Medium (AH)

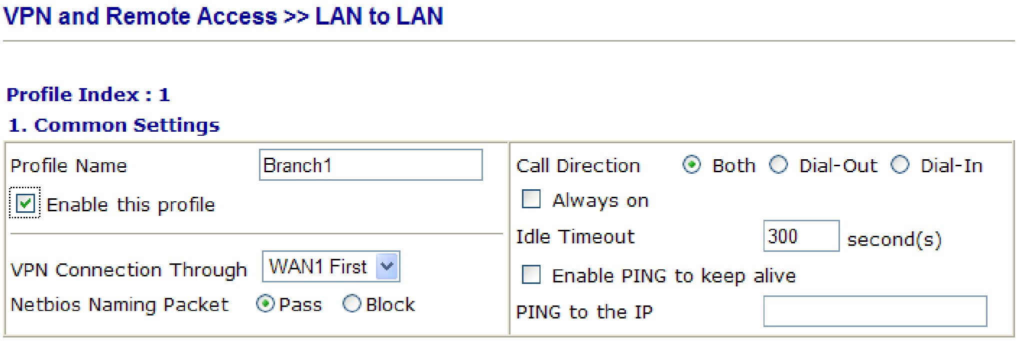
Data will be authentic, but will not be encrypted.

High (ESP) ☑ DES ☑ 3DES ☑ AES

Data will be encrypted and authentic.

3. Go to **LAN-to-LAN**. Click on one index number to edit a profile.

4. Set **Common Settings** as shown below. You should enable both of VPN connections because any one of the parties may start the VPN connection.



VPN and Remote Access >> LAN to LAN

Profile Index : 1

1. Common Settings

Profile Name: Branch1

☑ Enable this profile

VPN Connection Through: WAN1 First

Netbios Naming Packet: ● Pass ○ Block

Call Direction: ● Both ○ Dial-Out ○ Dial-In

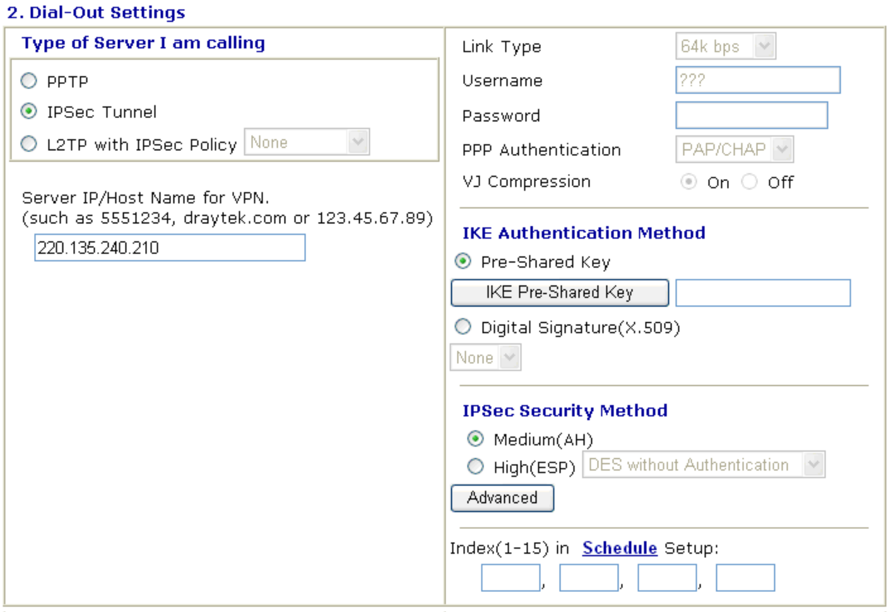
□ Always on

Idle Timeout: 300 second(s)

□ Enable PING to keep alive

PING to the IP:

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



2. Dial-Out Settings

Type of Server I am calling

○ PPTP
● IPSec Tunnel
○ L2TP with IPSec Policy [None]

Server IP/Host Name for VPN.
(such as 5551234, draytek.com or 123.45.67.89)
220.135.240.210

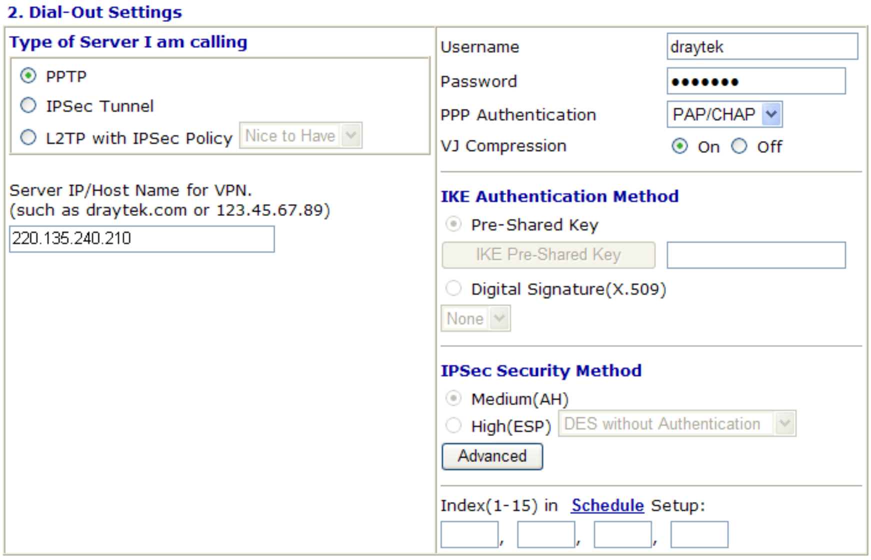
Link Type	64k bps
Username	???
Password	
PPP Authentication	PAP/CHAP
VJ Compression	● On ○ Off

IKE Authentication Method
● Pre-Shared Key
IKE Pre-Shared Key
○ Digital Signature(X.509)
None

IPSec Security Method
● Medium(AH)
○ High(ESP) DES without Authentication
Advanced

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

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



2. Dial-Out Settings

Type of Server I am calling

● PPTP
○ IPSec Tunnel
○ L2TP with IPSec Policy [Nice to Have]

Server IP/Host Name for VPN.
(such as draytek.com or 123.45.67.89)
220.135.240.210

Username	draytek
Password	●●●●●●●
PPP Authentication	PAP/CHAP
VJ Compression	● On ○ Off

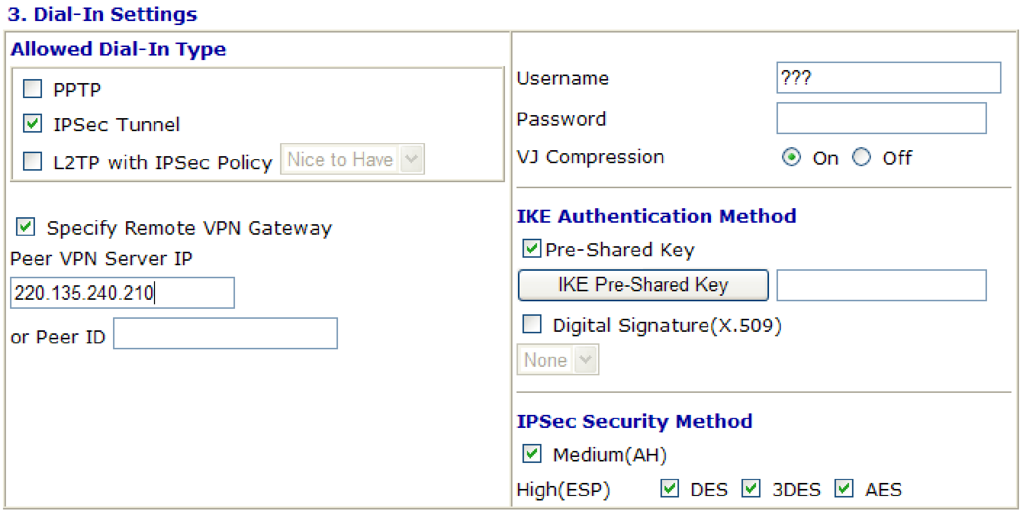
IKE Authentication Method
● Pre-Shared Key
IKE Pre-Shared Key
○ Digital Signature(X.509)
None

IPSec Security Method
● Medium(AH)
○ High(ESP) DES without Authentication
Advanced

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

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.



3. Dial-In Settings

Allowed Dial-In Type

□ PPTP
☑ IPSec Tunnel
□ L2TP with IPSec Policy [Nice to Have]

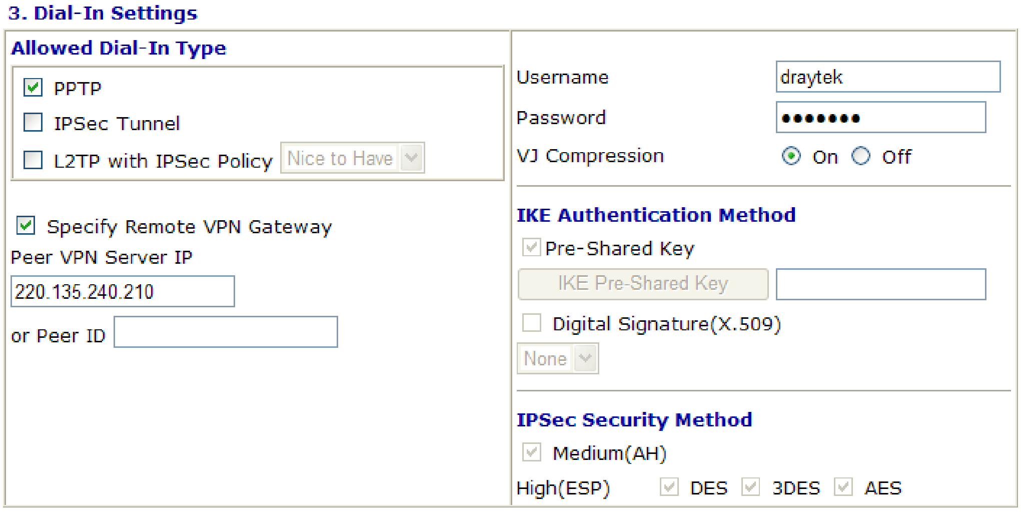
☑ Specify Remote VPN Gateway
Peer VPN Server IP
220.135.240.210
or Peer ID

Username ???
Password
VJ Compression ● On ○ Off

IKE Authentication Method
☑ Pre-Shared Key
IKE Pre-Shared Key
□ Digital Signature(X.509)
None

IPSec Security Method
☑ Medium(AH)
High(ESP) ☑ DES ☑ 3DES ☑ AES

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



3. Dial-In Settings

Allowed Dial-In Type

☑ PPTP
□ IPSec Tunnel
□ L2TP with IPSec Policy [Nice to Have]

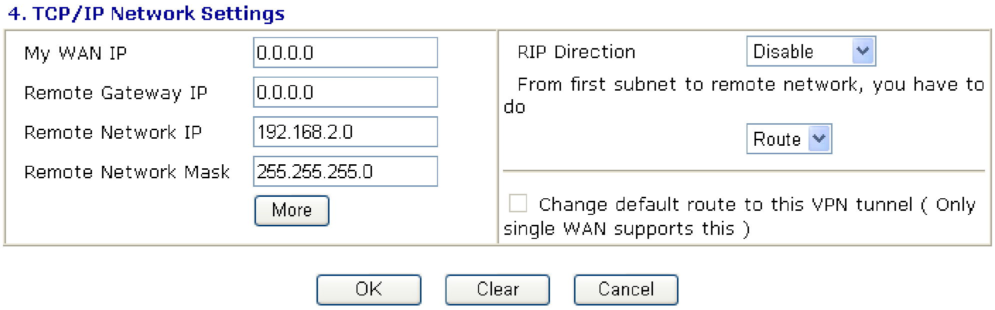
☑ Specify Remote VPN Gateway
Peer VPN Server IP
220.135.240.210
or Peer ID

Username draytek
Password •••••••
VJ Compression ● On ○ Off

IKE Authentication Method
☑ Pre-Shared Key
IKE Pre-Shared Key
□ Digital Signature(X.509)
None

IPSec Security Method
☑ Medium(AH)
High(ESP) ☑ DES ☑ 3DES ☑ AES

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.



4. TCP/IP Network Settings

My WAN IP 0.0.0.0
Remote Gateway IP 0.0.0.0
Remote Network IP 192.168.2.0
Remote Network Mask 255.255.255.0
More

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

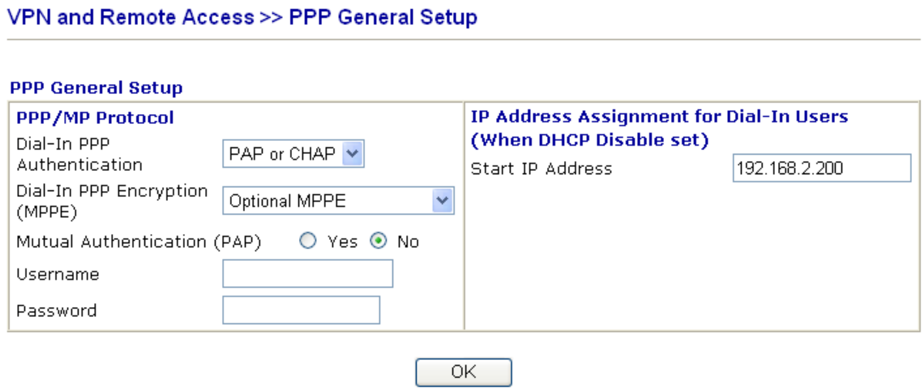
□ Change default route to this VPN tunnel (Only single WAN supports this)

OK Clear Cancel

Settings in Router B in the remote office:

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

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



VPN and Remote Access >> PPP General Setup

PPP General Setup

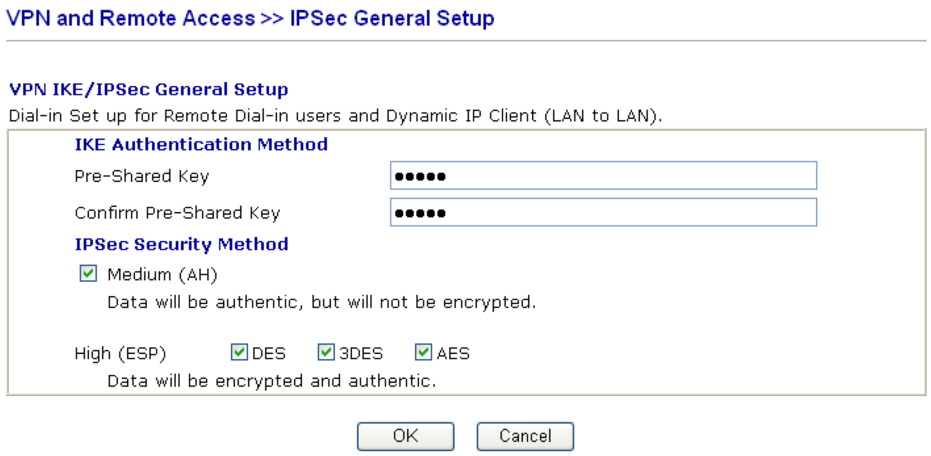
PPP/MP Protocol

Dial-In PPP Authentication	PAP or CHAP
Dial-In PPP Encryption (MPPE)	Optional MPPE
Mutual Authentication (PAP)	○ Yes ● No
Username	
Password	

IP Address Assignment for Dial-In Users (When DHCP Disable set)

Start IP Address	192.168.2.200

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



VPN and Remote Access >> IPSec General Setup

VPN IKE/IPSec General Setup

Dial-in Set up for Remote Dial-in users and Dynamic IP Client (LAN to LAN).

IKE Authentication Method

Pre-Shared Key	●●●●●
Confirm Pre-Shared Key	●●●●●

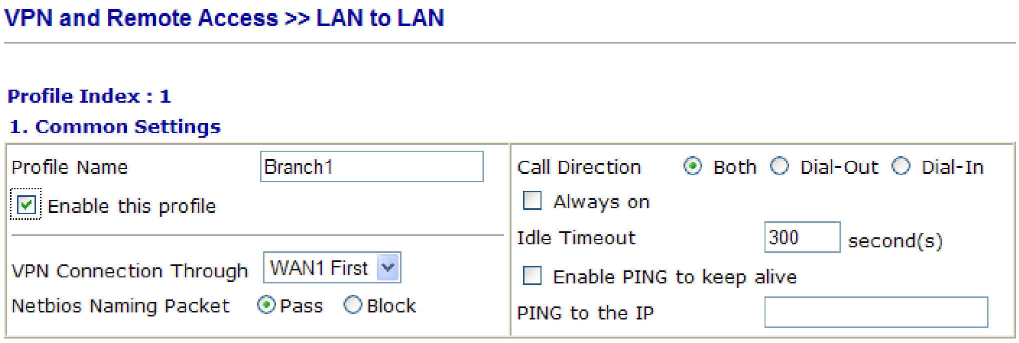
IPSec Security Method

☑ Medium (AH)
Data will be authentic, but will not be encrypted.

High (ESP) ☑ DES ☑ 3DES ☑ AES
Data will be encrypted and authentic.

3. Go to **LAN-to-LAN**. Click on one index number to edit a profile.

4. Set **Common Settings** as shown below. You should enable both of VPN connections because any one of the parties may start the VPN connection.



VPN and Remote Access >> LAN to LAN

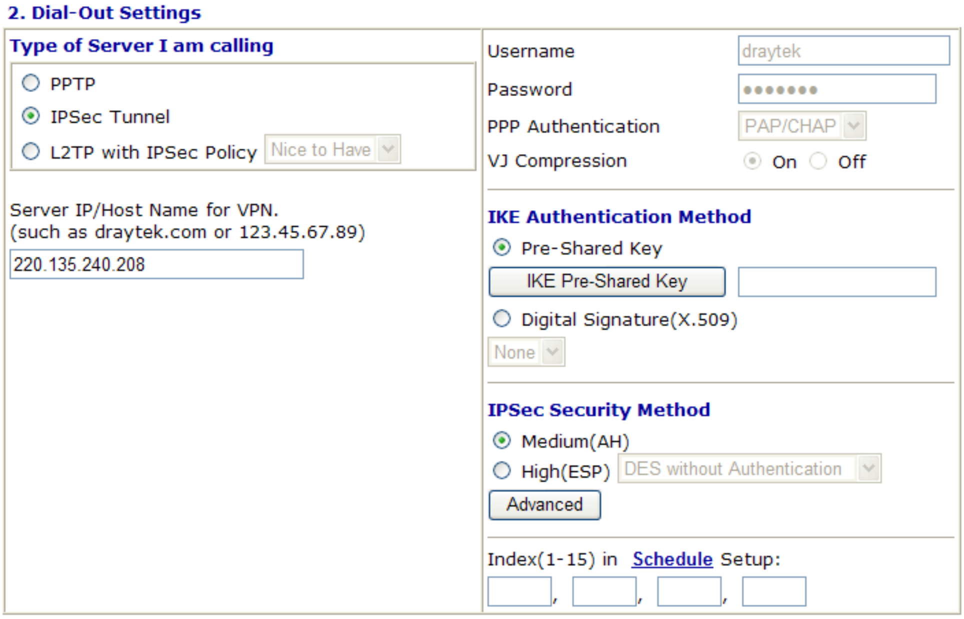
Profile Index : 1

1. Common Settings

Profile Name	Branch1
☑ Enable this profile	
VPN Connection Through	WAN1 First
Netbios Naming Packet	● Pass ○ Block
Call Direction	● Both ○ Dial-Out ○ Dial-In
□ Always on	
Idle Timeout	300 second(s)
□ Enable PING to keep alive	
PING to the IP	

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

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



2. Dial-Out Settings

Type of Server I am calling

○ PPTP
● IPSec Tunnel
○ L2TP with IPSec Policy Nice to Have

Server IP/Host Name for VPN.
(such as draytek.com or 123.45.67.89)
220.135.240.208

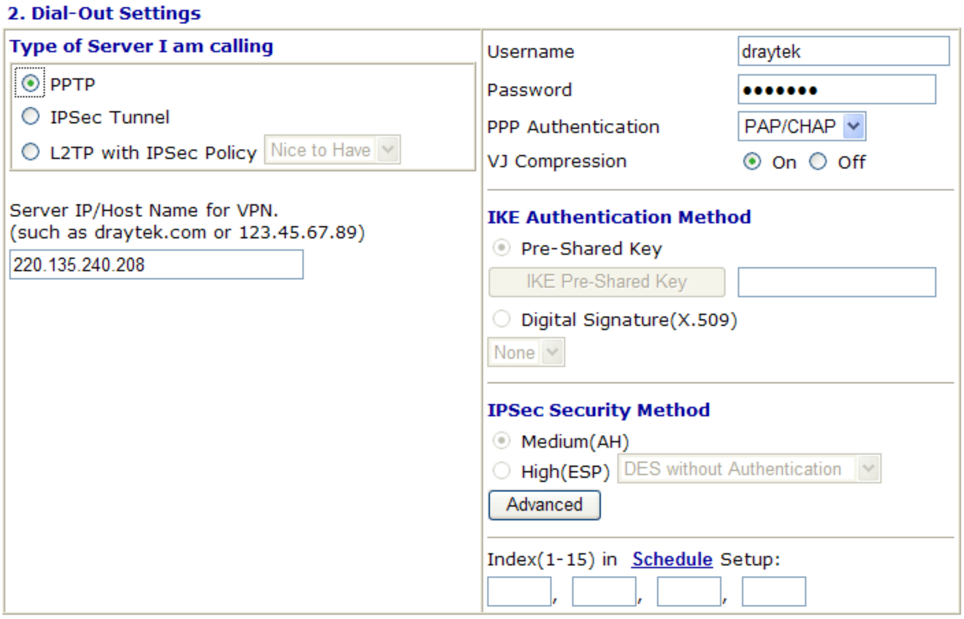
Username: draytek
Password: •••••••
PPP Authentication: PAP/CHAP
VJ Compression: ● On ○ Off

IKE Authentication Method
● Pre-Shared Key
IKE Pre-Shared Key
○ Digital Signature(X.509)
None

IPSec Security Method
● Medium(AH)
○ High(ESP) DES without Authentication
Advanced

Index(1-15) in Schedule Setup:

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



2. Dial-Out Settings

Type of Server I am calling

● PPTP
○ IPSec Tunnel
○ L2TP with IPSec Policy Nice to Have

Server IP/Host Name for VPN.
(such as draytek.com or 123.45.67.89)
220.135.240.208

Username: draytek
Password: •••••••
PPP Authentication: PAP/CHAP
VJ Compression: ● On ○ Off

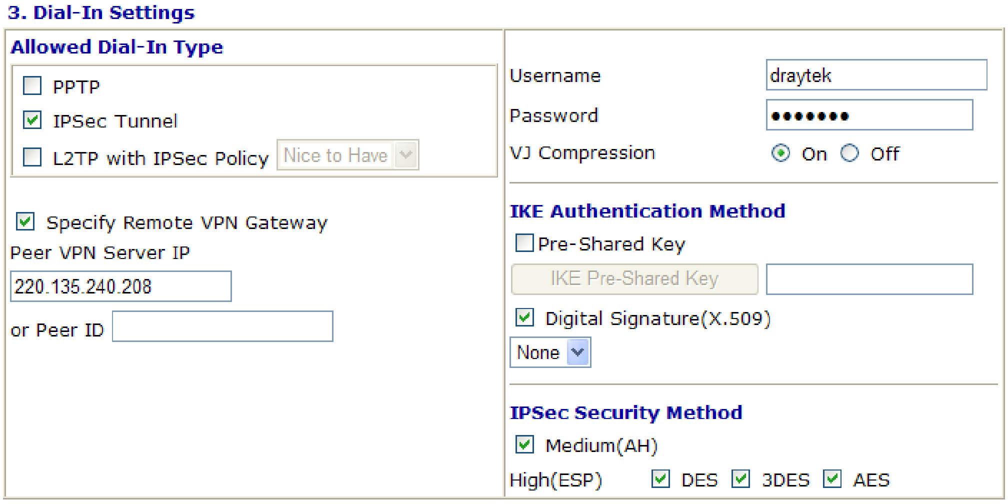
IKE Authentication Method
● Pre-Shared Key
IKE Pre-Shared Key
○ Digital Signature(X.509)
None

IPSec Security Method
● Medium(AH)
○ High(ESP) DES without Authentication
Advanced

Index(1-15) in Schedule Setup:

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.



3. Dial-In Settings

Allowed Dial-In Type

□ PPTP

☑ IPSec Tunnel

□ L2TP with IPSec Policy: Nice to Have

☑ Specify Remote VPN Gateway

Peer VPN Server IP: 220.135.240.208

or Peer ID:

Username: draytek

Password: •••••••

VJ Compression: ● On ○ Off

IKE Authentication Method

□ Pre-Shared Key

IKE Pre-Shared Key:

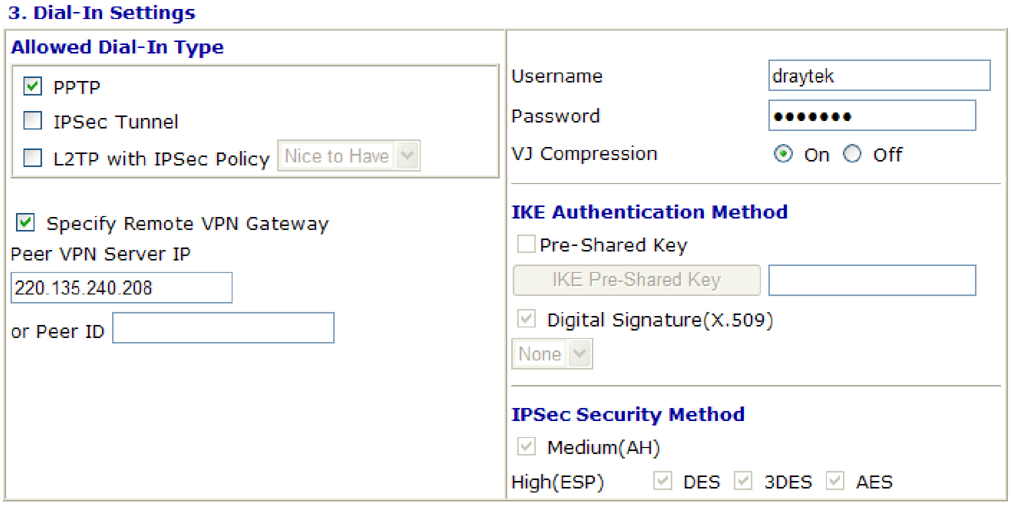
☑ Digital Signature(X.509): None

IPSec Security Method

☑ Medium(AH)

High(ESP) ☑ DES ☑ 3DES ☑ AES

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



3. Dial-In Settings

Allowed Dial-In Type

☑ PPTP

□ IPSec Tunnel

□ L2TP with IPSec Policy: Nice to Have

☑ Specify Remote VPN Gateway

Peer VPN Server IP: 220.135.240.208

or Peer ID:

Username: draytek

Password: •••••••

VJ Compression: ● On ○ Off

IKE Authentication Method

□ Pre-Shared Key

IKE Pre-Shared Key:

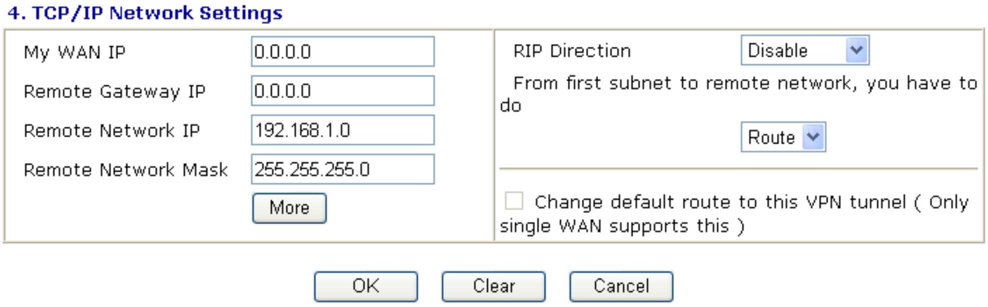
☑ Digital Signature(X.509): None

IPSec Security Method

☑ Medium(AH)

High(ESP) ☑ DES ☑ 3DES ☑ AES

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. TCP/IP Network Settings

My WAN IP: 0.0.0.0

Remote Gateway IP: 0.0.0.0

Remote Network IP: 192.168.1.0

Remote Network Mask: 255.255.255.0

More

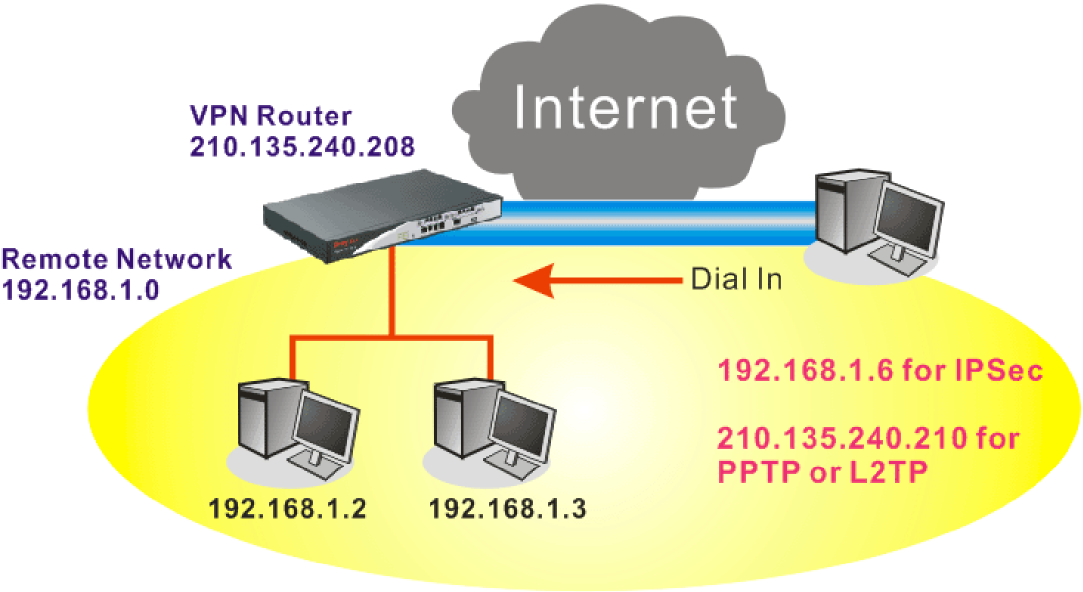
RIP Direction: Disable

From first subnet to remote network, you have to do: Route

□ Change default route to this VPN tunnel (Only single WAN supports this)

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

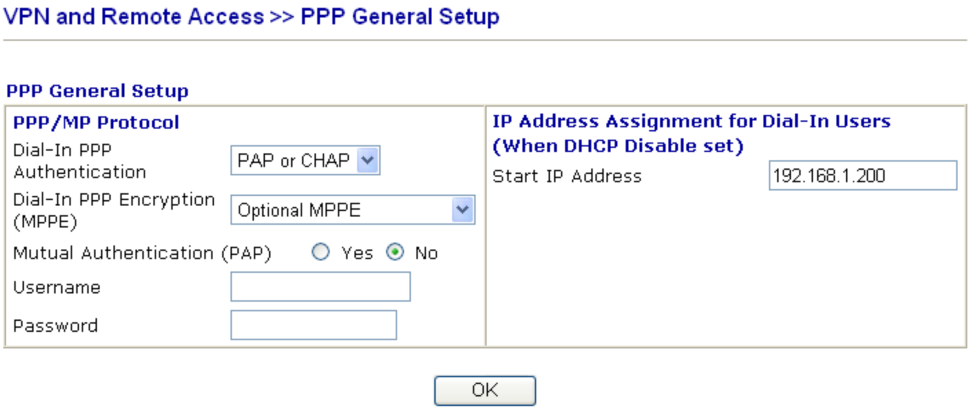
The other common case is that you, as a teleworker, may want to connect to the enterprise network securely. According to the network structure as shown in the below illustration, you may follow the steps to create a Remote User Profile and install Smart VPN Client on the remote host.



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**.



VPN and Remote Access >> PPP General Setup

PPP General Setup

PPP/MP Protocol

Dial-In PPP Authentication: PAP or CHAP

Dial-In PPP Encryption (MPPE): Optional MPPE

Mutual Authentication (PAP): ○ Yes ● No

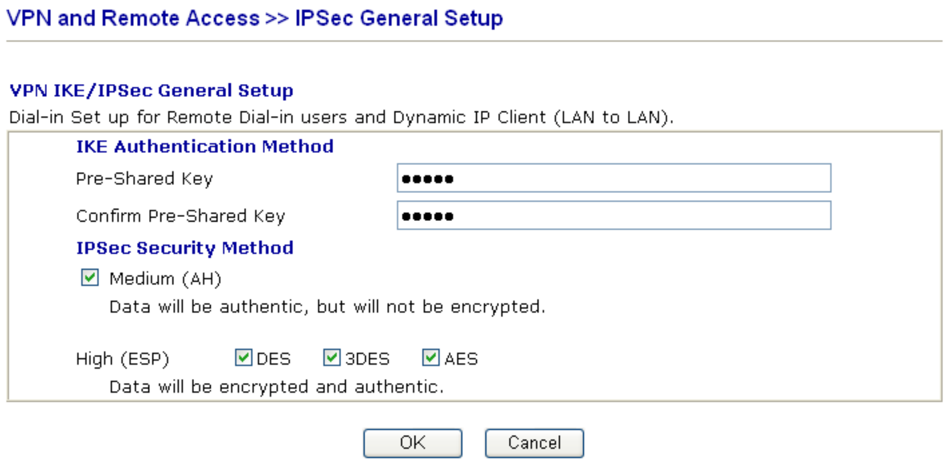
Username:

Password:

IP Address Assignment for Dial-In Users (When DHCP Disable set)

Start IP Address: 192.168.1.200

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



VPN and Remote Access >> IPSec General Setup

VPN IKE/IPSec General Setup

Dial-in Set up for Remote Dial-in users and Dynamic IP Client (LAN to LAN).

IKE Authentication Method

Pre-Shared Key: ●●●●●

Confirm Pre-Shared Key: ●●●●●

IPSec Security Method

☑ Medium (AH)

Data will be authentic, but will not be encrypted.

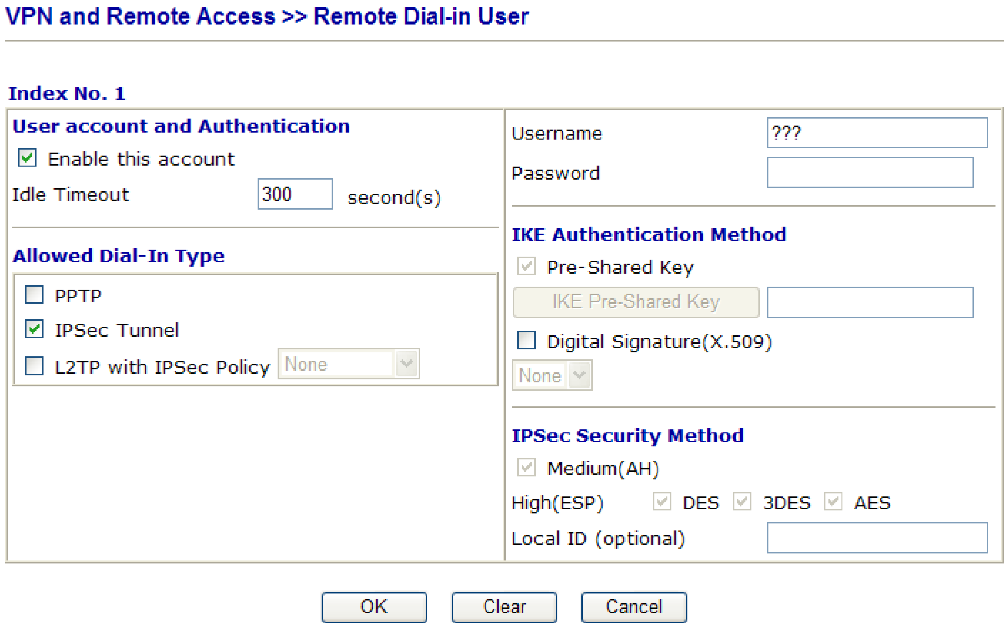
High (ESP) ☑ DES ☑ 3DES ☑ AES

Data will be encrypted and authentic.

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.



VPN and Remote Access >> Remote Dial-in User

Index No. 1

User account and Authentication

☑ Enable this account

Idle Timeout: 300 second(s)

Allowed Dial-In Type

□ PPTP

☑ IPSec Tunnel

□ L2TP with IPSec Policy: None

Username: ???

Password:

IKE Authentication Method

☑ Pre-Shared Key

IKE Pre-Shared Key:

□ Digital Signature(X.509): None

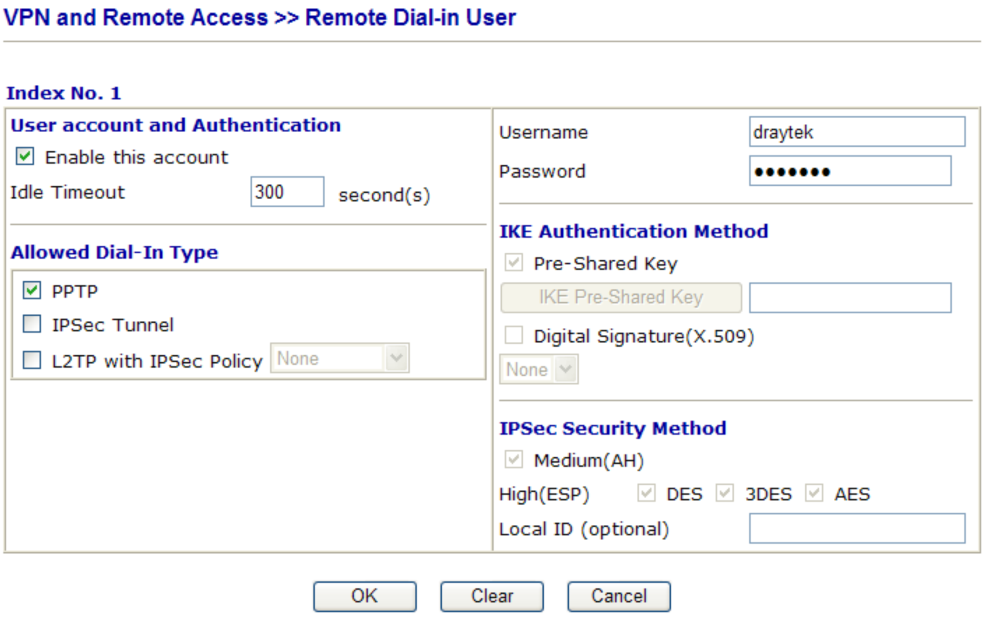
IPSec Security Method

☑ Medium(AH)

High(ESP) ☑ DES ☑ 3DES ☑ AES

Local ID (optional):

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.



VPN and Remote Access >> Remote Dial-in User

Index No. 1

User account and Authentication

☑ Enable this account

Idle Timeout 300 second(s)

Allowed Dial-In Type

☑ PPTP

□ IPSec Tunnel

□ L2TP with IPSec Policy None

Username draytek

Password •••••••

IKE Authentication Method

☑ Pre-Shared Key

IKE Pre-Shared Key

□ Digital Signature(X.509)

None

IPSec Security Method

☑ Medium(AH)

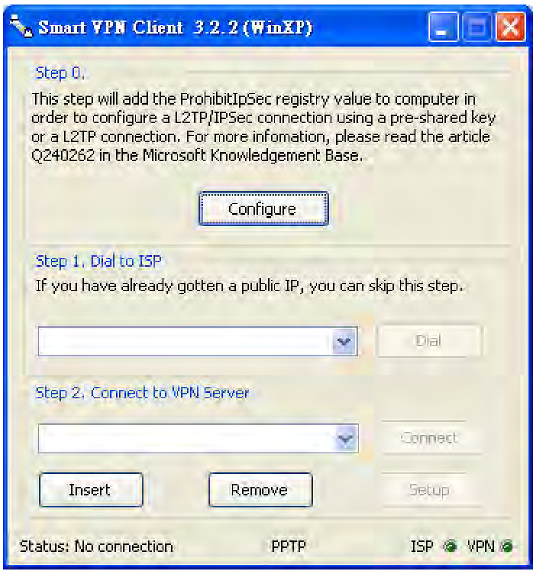
High(ESP) ☑ DES ☑ 3DES ☑ AES

Local ID (optional)

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.



Smart VPN Client 3.2.2 (WinXP)

Step 0.

This step will add the ProhibitIpSec registry value to computer in order to configure a L2TP/IPSec connection using a pre-shared key or a L2TP connection. For more infomation, please read the article Q240262 in the Microsoft Knowledgement Base.

Step 1. Dial to ISP

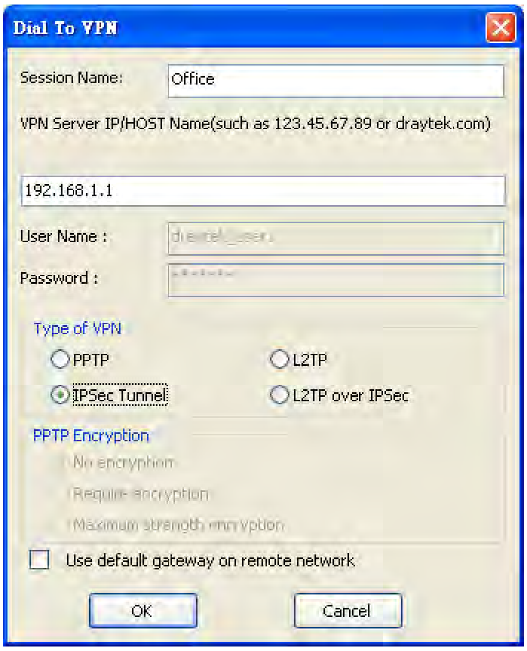
If you have already gotten a public IP, you can skip this step.

Step 2. Connect to VPN Server

Status: No connection PPTP ISP VPN

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,



Session Name: Office

VPN Server IP/HOST Name(such as 123.45.67.89 or draytek.com)

192.168.1.1

User Name : draytek_user

Password : ******

Type of VPN

○ PPTP ○ L2TP

● IPSec Tunnel ○ L2TP over IPSec

PPTP Encryption

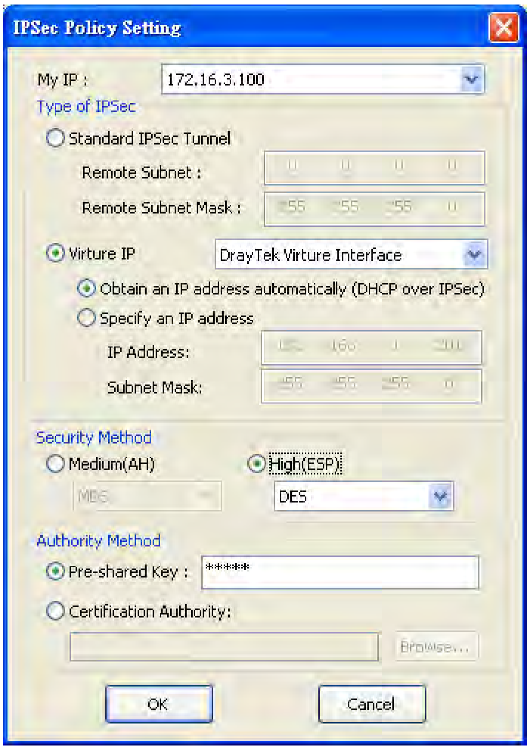
No encryption

Require encryption

Maximum strength encryption

□ Use default gateway on remote network

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.



My IP : 172.16.3.100

Type of IPSec

○ Standard IPSec Tunnel

Remote Subnet : 0 . 0 . 0 . 0

Remote Subnet Mask : 255 . 255 . 255 . 0

● Virture IP DrayTek Virture Interface

● Obtain an IP address automatically (DHCP over IPSec)

○ Specify an IP address

IP Address: 192 . 168 . 1 . 200

Subnet Mask: 255 . 255 . 255 . 0

Security Method

○ Medium(AH) ● High(ESP)

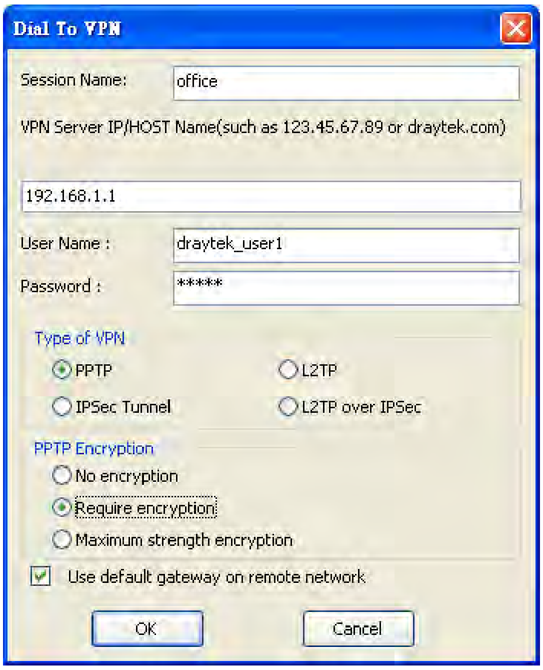
MD5 DES

Authority Method

● Pre-shared Key : ******

○ Certification Authority:

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.



Dial To VPN

Session Name: office

VPN Server IP/HOST Name(such as 123.45.67.89 or draytek.com)

192.168.1.1

User Name : draytek_user1

Password : *****

Type of VPN

● PPTP ○ L2TP

○ IPSec Tunnel ○ L2TP over IPSec

PPTP Encryption

○ No encryption

● Require encryption

○ Maximum strength encryption

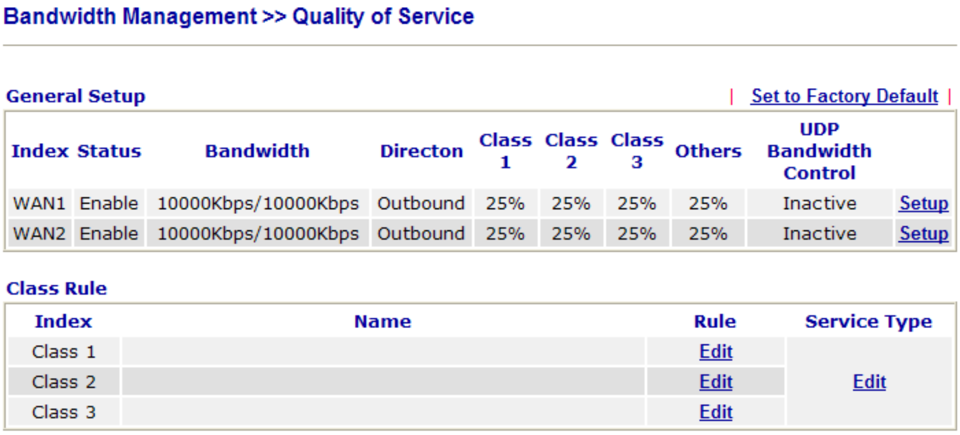
☑ Use default gateway on remote network

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.**



Bandwidth Management >> Quality of Service

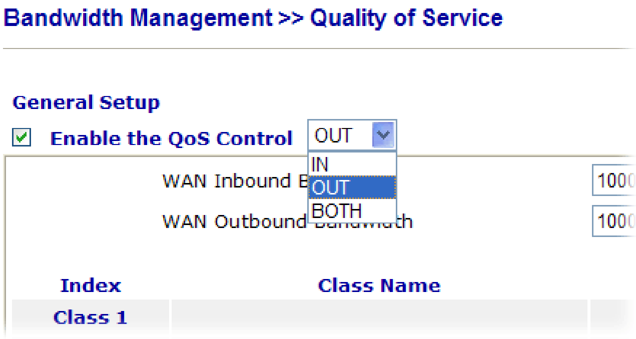
General Setup | Set to Factory Default |

Index	Status	Bandwidth	Directon	Class 1	Class 2	Class 3	Others	UDP Bandwidth Control	
WAN1	Enable	10000Kbps/10000Kbps	Outbound	25%	25%	25%	25%	Inactive	Setup
WAN2	Enable	10000Kbps/10000Kbps	Outbound	25%	25%	25%	25%	Inactive	Setup

Class Rule

Index	Name	Rule	Service Type
Class 1		Edit	Edit
Class 2		Edit	
Class 3		Edit	

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



Bandwidth Management >> Quality of Service

General Setup

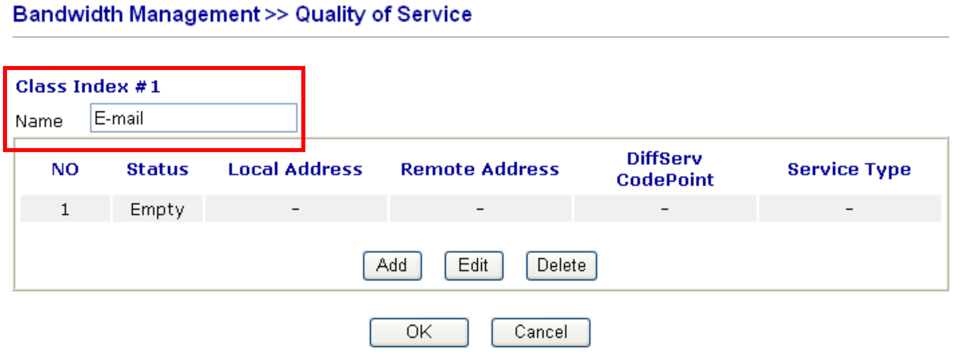
☑ Enable the QoS Control [OUT ▾]

WAN Inbound B... 1000

WAN Outbound ...th 1000

Index	Class Name
Class 1	

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



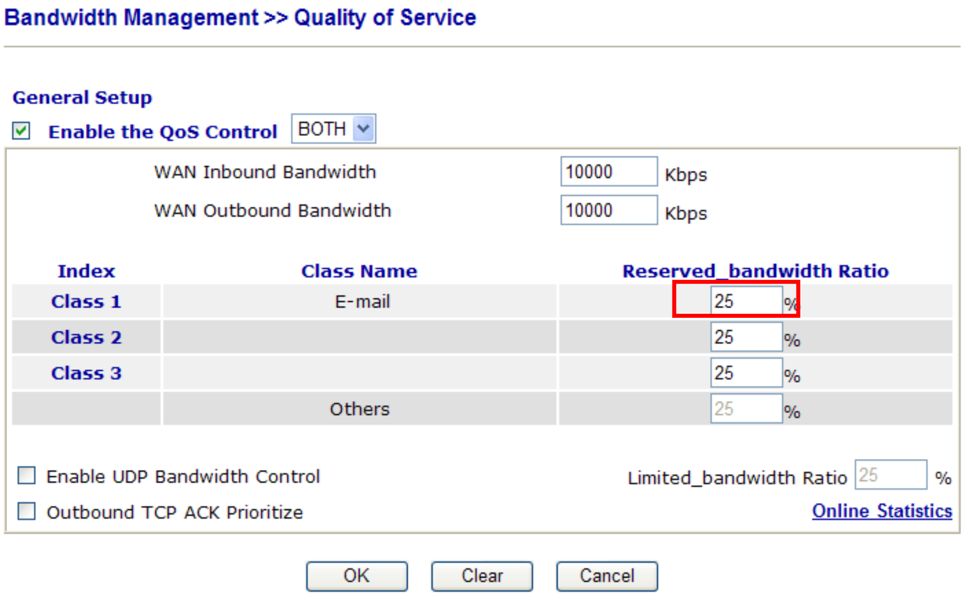
Bandwidth Management >> Quality of Service

Class Index #1

Name: E-mail

NO	Status	Local Address	Remote Address	DiffServ CodePoint	Service Type
1	Empty	-	-	-	-

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



Bandwidth Management >> Quality of Service

General Setup

☑ Enable the QoS Control [BOTH ▾]

WAN Inbound Bandwidth 10000 Kbps

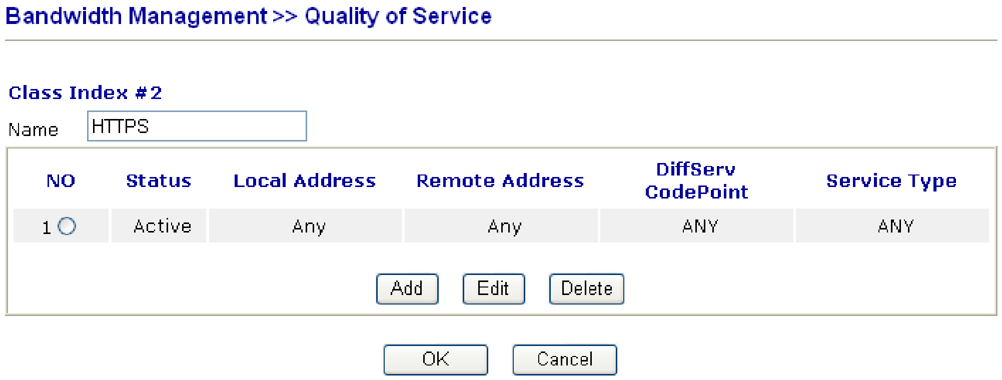
WAN Outbound Bandwidth 10000 Kbps

Index	Class Name	Reserved_bandwidth Ratio
Class 1	E-mail	25 %
Class 2		25 %
Class 3		25 %
	Others	25 %

☐ Enable UDP Bandwidth Control   Limited_bandwidth Ratio 25 %

☐ Outbound TCP ACK Prioritize

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**.



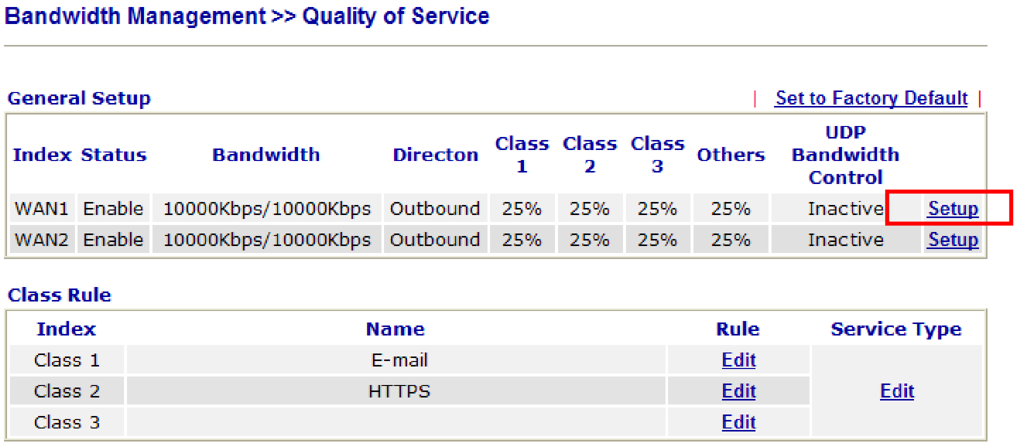
Bandwidth Management >> Quality of Service

Class Index #2

Name HTTPS

NO	Status	Local Address	Remote Address	DiffServ CodePoint	Service Type
1 ○	Active	Any	Any	ANY	ANY

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



Bandwidth Management >> Quality of Service

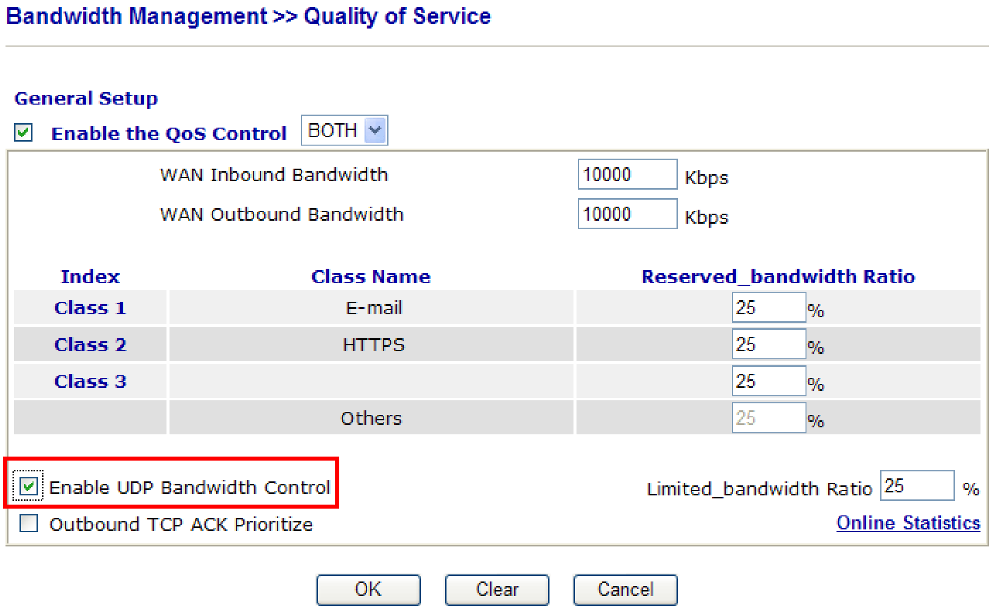
General Setup | Set to Factory Default |

Index	Status	Bandwidth	Directon	Class 1	Class 2	Class 3	Others	UDP Bandwidth Control	
WAN1	Enable	10000Kbps/10000Kbps	Outbound	25%	25%	25%	25%	Inactive	Setup
WAN2	Enable	10000Kbps/10000Kbps	Outbound	25%	25%	25%	25%	Inactive	Setup

Class Rule

Index	Name	Rule	Service Type
Class 1	E-mail	Edit	Edit
Class 2	HTTPS	Edit	
Class 3		Edit	

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



Bandwidth Management >> Quality of Service

General Setup

☑ Enable the QoS Control BOTH

WAN Inbound Bandwidth 10000 Kbps

WAN Outbound Bandwidth 10000 Kbps

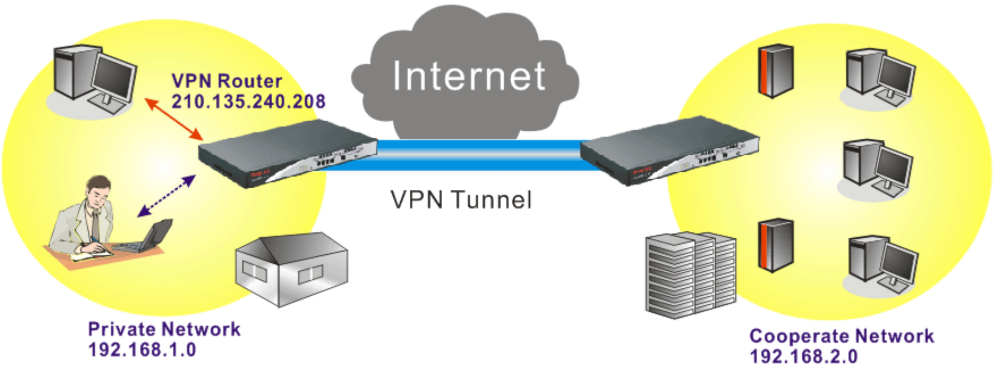
Index	Class Name	Reserved_bandwidth Ratio
Class 1	E-mail	25 %
Class 2	HTTPS	25 %
Class 3		25 %
	Others	25 %

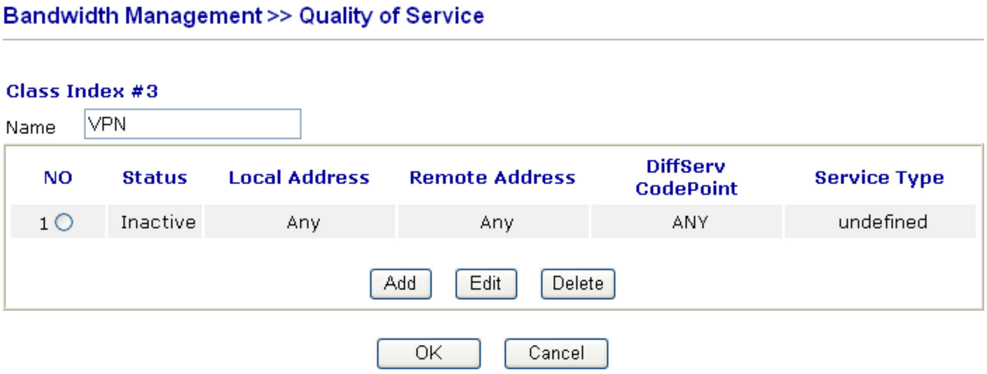
☑ Enable UDP Bandwidth Control Limited_bandwidth Ratio 25 %

☐ Outbound TCP ACK Prioritize

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.





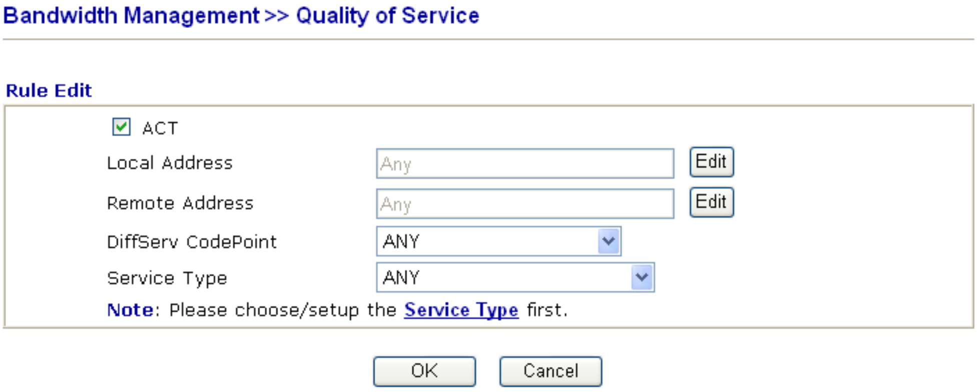
Bandwidth Management >> Quality of Service

Class Index #3

Name: VPN

NO	Status	Local Address	Remote Address	DiffServ CodePoint	Service Type
1 ○	Inactive	Any	Any	ANY	undefined

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



Bandwidth Management >> Quality of Service

Rule Edit

☑ ACT

Local Address: Any

Remote Address: Any

DiffServ CodePoint: ANY

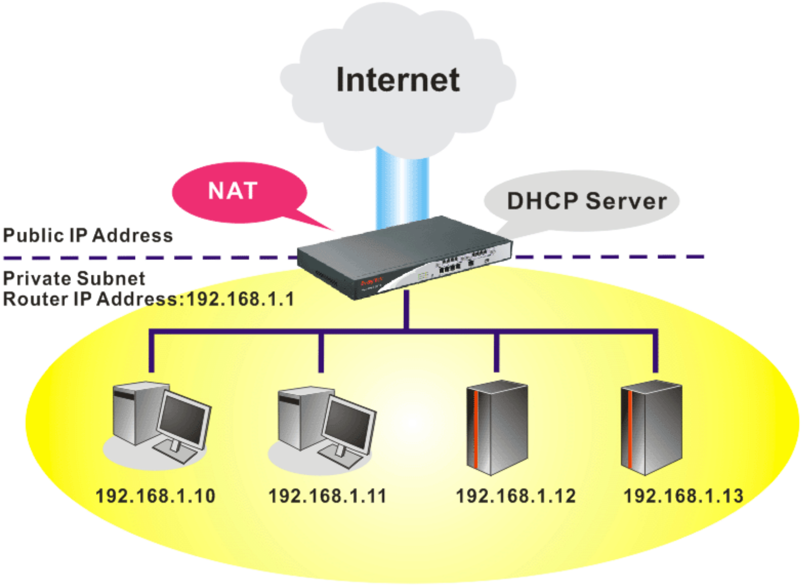
Service Type: ANY

Note: Please choose/setup the Service Type first.

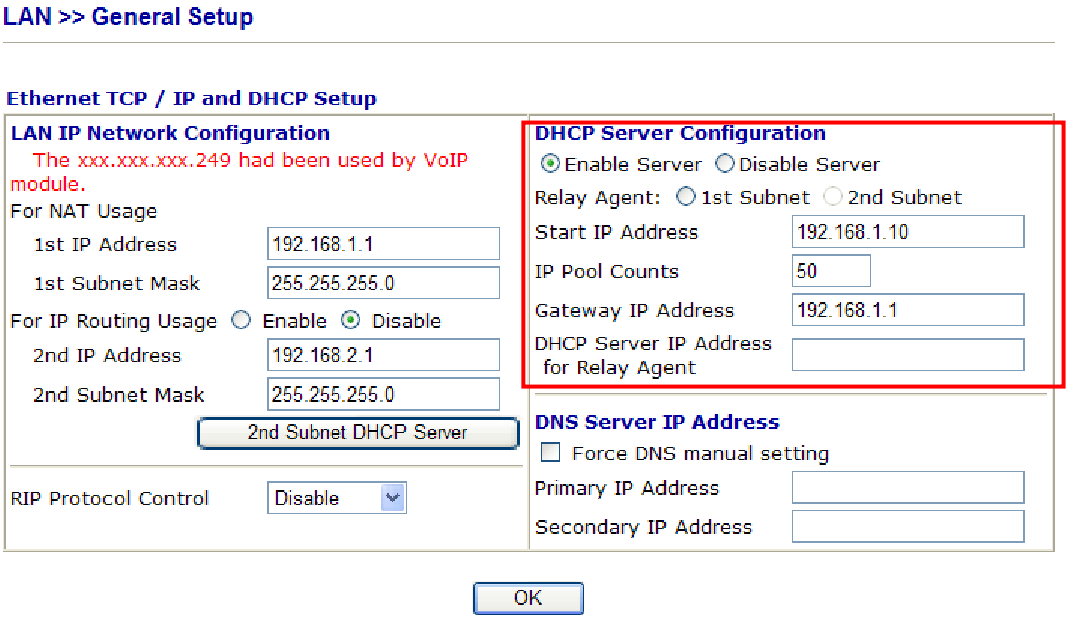
10. Then click **Edit** of **Local Address** to set a worker’s subnet address. Click **Edit** of **Remote Address** to set headquarter’s IP address. Leave other fields and click **OK**.

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.



LAN >> General Setup

Ethernet TCP / IP and DHCP Setup

LAN IP Network Configuration

The xxx.xxx.xxx.249 had been used by VoIP module.

For NAT Usage

1st IP Address	192.168.1.1
1st Subnet Mask	255.255.255.0
For IP Routing Usage	○ Enable ● Disable
2nd IP Address	192.168.2.1
2nd Subnet Mask	255.255.255.0
RIP Protocol Control	Disable

DHCP Server Configuration

● Enable Server ○ Disable Server

Relay Agent: ○ 1st Subnet ○ 2nd Subnet

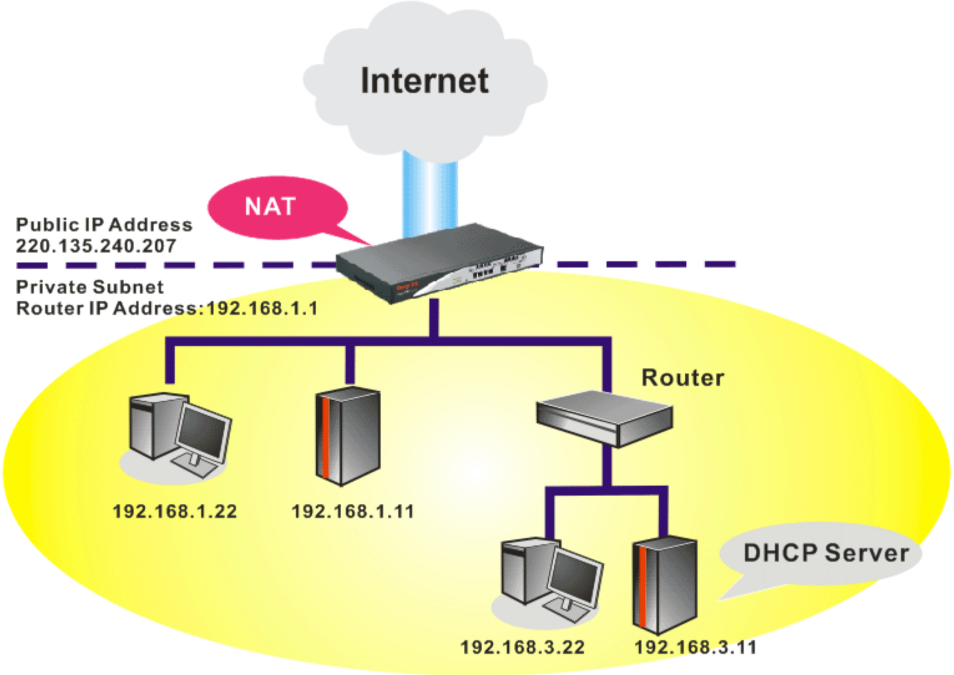
Start IP Address	192.168.1.10
IP Pool Counts	50
Gateway IP Address	192.168.1.1
DHCP Server IP Address for Relay Agent	

DNS Server IP Address

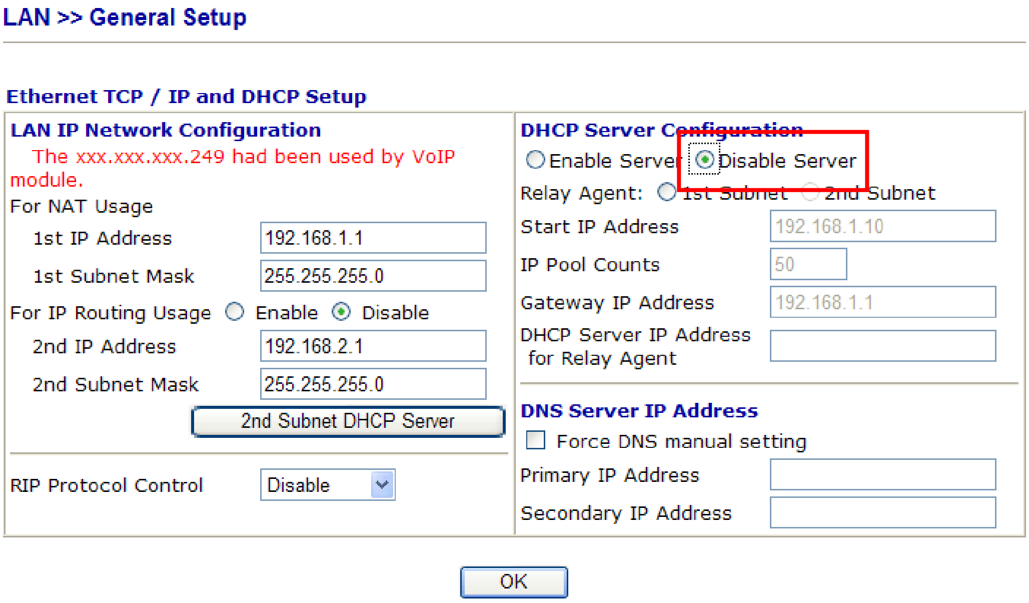
□ Force DNS manual setting

Primary IP Address	
Secondary IP Address	

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



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



LAN >> General Setup

Ethernet TCP / IP and DHCP Setup

LAN IP Network Configuration

The xxx.xxx.xxx.249 had been used by VoIP module.

For NAT Usage

1st IP Address	192.168.1.1
1st Subnet Mask	255.255.255.0
For IP Routing Usage	○ Enable ● Disable
2nd IP Address	192.168.2.1
2nd Subnet Mask	255.255.255.0
RIP Protocol Control	Disable

DHCP Server Configuration

○ Enable Server ● Disable Server

Relay Agent: ○ 1st Subnet ○ 2nd Subnet

Start IP Address	192.168.1.10
IP Pool Counts	50
Gateway IP Address	192.168.1.1
DHCP Server IP Address for Relay Agent	

DNS Server IP Address

□ Force DNS manual setting

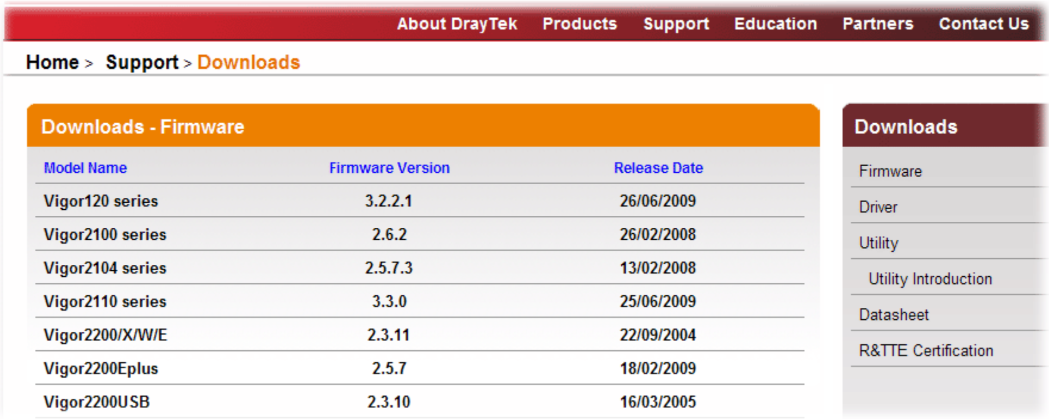
Primary IP Address	
Secondary IP Address	

4.5 Upgrade Firmware for Your Router

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

1. Go to **www.draytek.com**.

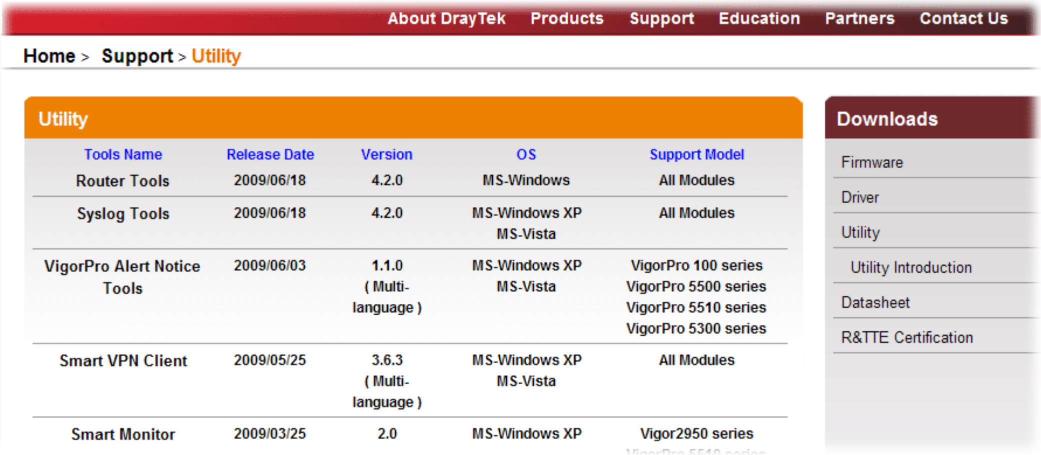
2. Access into **Support** >> **Downloads**. Please find out **Firmware** menu and click it. Search the model you have and click on it to download the newly update firmware for your router.



Downloads - Firmware

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

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

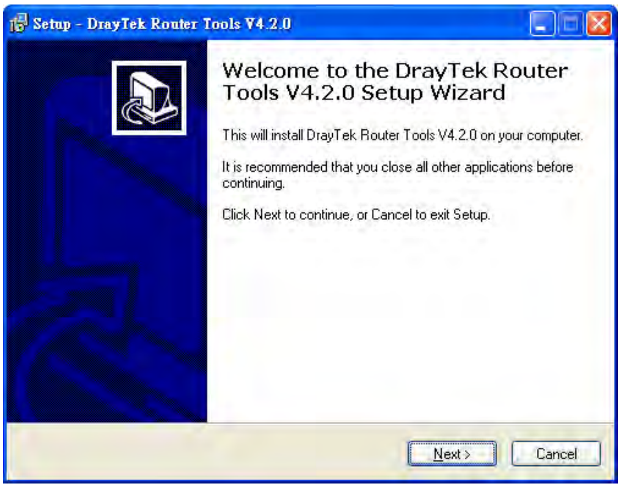


Utility

Tools Name	Release Date	Version	OS	Support Model
Router Tools	2009/06/18	4.2.0	MS-Windows	All Modules
Syslog Tools	2009/06/18	4.2.0	MS-Windows XP MS-Vista	All Modules
VigorPro Alert Notice Tools	2009/06/03	1.1.0 (Multi-language)	MS-Windows XP MS-Vista	VigorPro 100 series VigorPro 5500 series VigorPro 5510 series VigorPro 5300 series
Smart VPN Client	2009/05/25	3.6.3 (Multi-language)	MS-Windows XP MS-Vista	All Modules
Smart Monitor	2009/03/25	2.0	MS-Windows XP	Vigor2950 series

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

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



Welcome to the DrayTek Router Tools V4.2.0 Setup Wizard

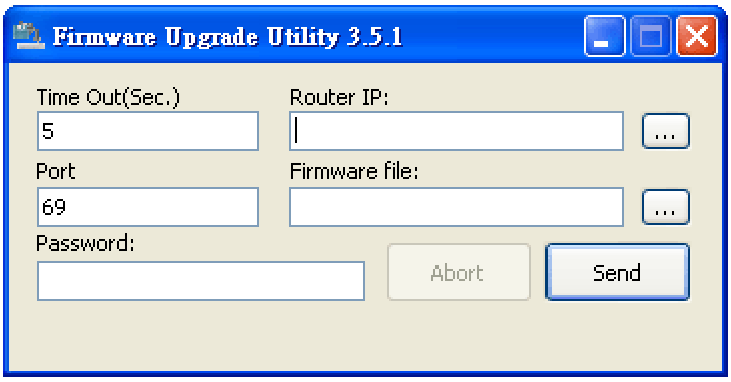
This will install DrayTek Router Tools V4.2.0 on your computer.

It is recommended that you close all other applications before continuing.

Click Next to continue, or Cancel to exit Setup.

6. Follow the onscreen instructions to install the tool. Finally, click **Finish** to end the installation.

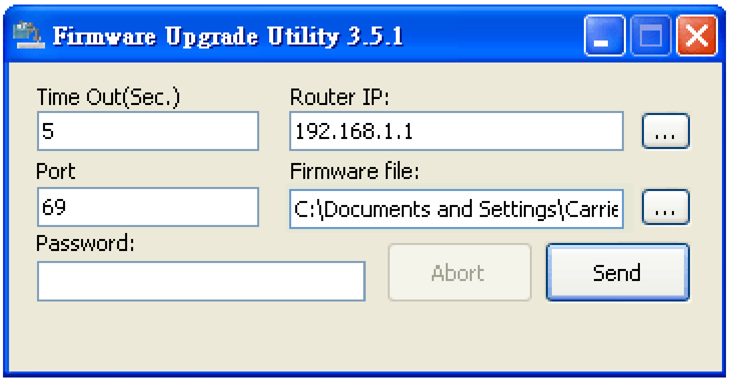
7. From the **Start** menu, open **Programs** and choose **Router Tools XXX** >> **Firmware Upgrade Utility**.



Time Out(Sec.): 5
Port: 69

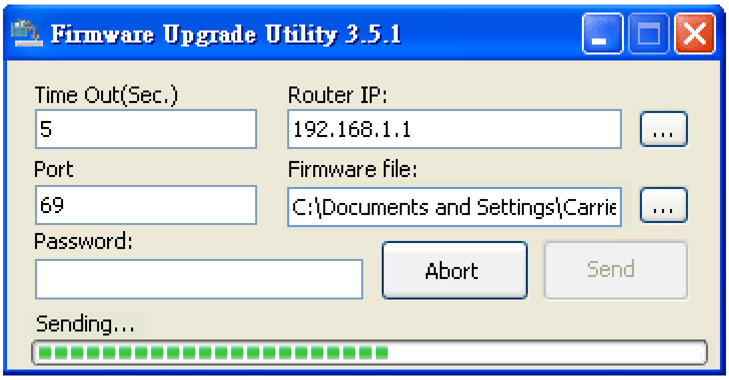
8. Type in your router IP, usually **192.168.1.1**.

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



Time Out(Sec.): 5
Router IP: 192.168.1.1
Port: 69
Firmware file: C:\Documents and Settings\Carrie

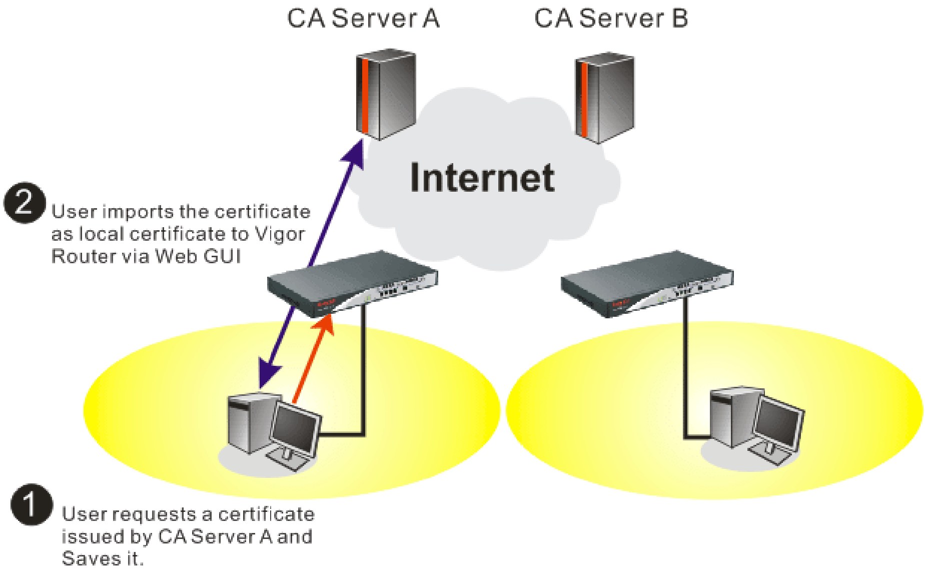
10. Click **Send**.



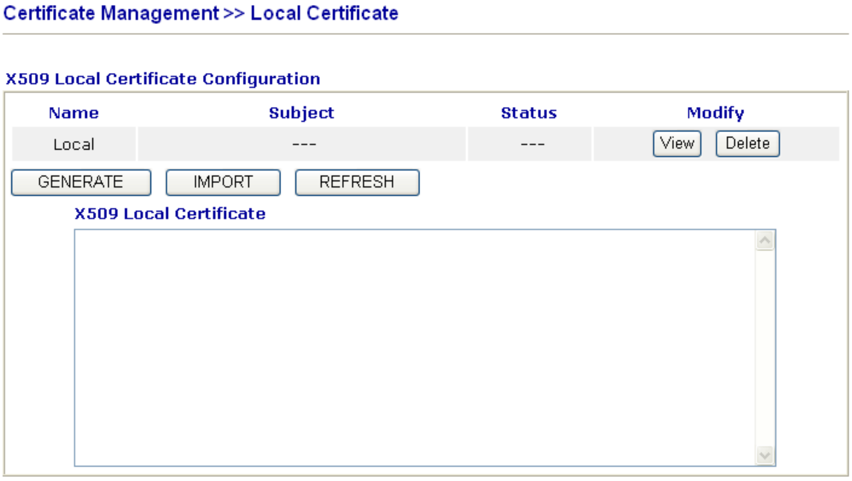
Time Out(Sec.): 5
Router IP: 192.168.1.1
Port: 69
Firmware file: C:\Documents and Settings\Carrie
Sending...

Now the firmware update is finished.

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


CA Server A
CA Server B
Internet
2 User imports the certificate as local certificate to Vigor Router via Web GUI
1 User requests a certificate issued by CA Server A and Saves it.

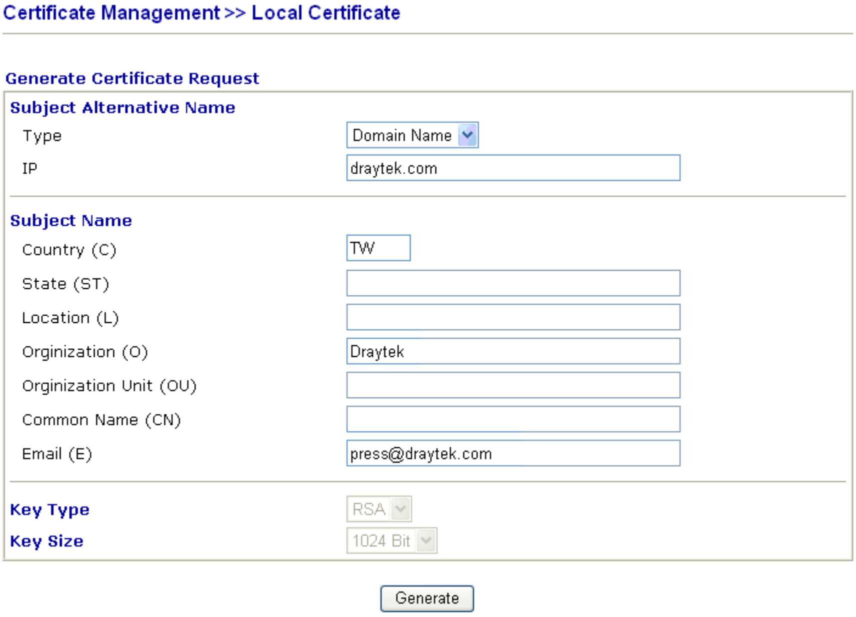
1. Go to **Certificate Management** and choose **Local Certificate**.


Certificate Management >> Local Certificate

X509 Local Certificate Configuration

Name	Subject	Status	Modify
Local	---	---	View Delete

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



Certificate Management >> Local Certificate

Generate Certificate Request

Subject Alternative Name

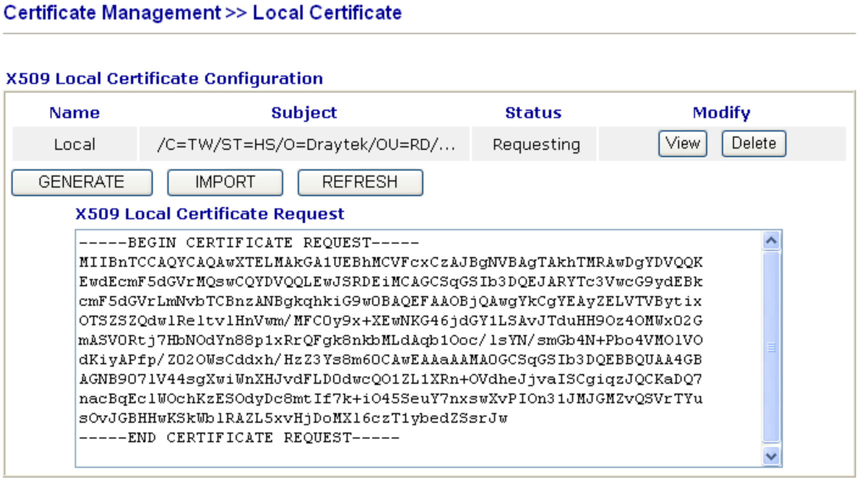
Type	Domain Name
IP	draytek.com

Subject Name

Country (C)	TW
State (ST)	
Location (L)	
Orginization (O)	Draytek
Orginization Unit (OU)	
Common Name (CN)	
Email (E)	press@draytek.com

Key Type	RSA
Key Size	1024 Bit

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



Certificate Management >> Local Certificate

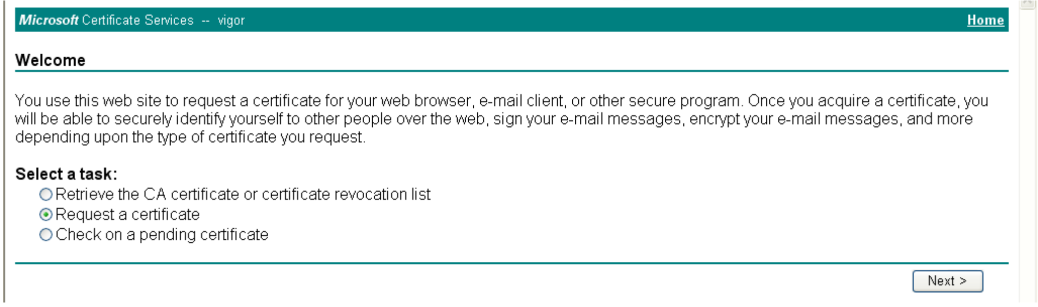
X509 Local Certificate Configuration

Name	Subject	Status	Modify
Local	/C=TW/ST=HS/O=Draytek/OU=RD/...	Requesting	View Delete

X509 Local Certificate Request

```
-----BEGIN CERTIFICATE REQUEST-----
MIIBnTCCAQYCAQAwXTELMAkGA1UEBhMCVFcxCzAJBgNVBAgTAkhTMRAwDgYDVQQK
EwdEcmF5dGVrMQswCQYDVQQLEwJSRDEiMCAGCSqGSIb3DQEJARYTc3VwcG9ydEBk
cmF5dGVrLmNvbTCBnzANBgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEAyZELVTVBytix
OTSZSZQdwlReltvlHnVwm/MFCOy9x+XEwNKG46jdGY1LSAvJTduHH9Oz4OMWxO2G
mASVORtj7HbNOdYn88p1xRrQFgk8nkbMLdAqb1Ooc/lsYN/smGb4N+Pbo4VMOlVO
dKiyAPfp/ZO2OWsCddxh/HzZ3Ys8m6OCAwEAAaAAMA0GCSqGSIb3DQEBBQUAA4GB
AGNB9O7lV44sgXwiWnXHJvdFLDOdwcQO1ZL1XRn+OVdheJjvaISCgiqzJQCKaDQ7
nacBqEclWOchKzESOdyDc8mtIf7k+iO45SeuY7nxswXvPIOn31JMJGMZvQSVrTYu
sOvJGBHHwKSkWblRAZL5xvHjDoMXl6czT1ybedZSsrJw
-----END CERTIFICATE REQUEST-----
```

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



Microsoft Certificate Services -- vigor Home

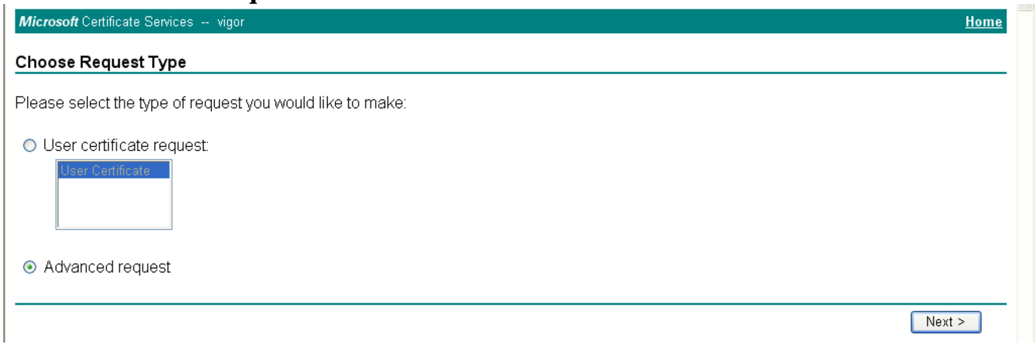
Welcome

You use this web site to request a certificate for your web browser, e-mail client, or other secure program. Once you acquire a certificate, you will be able to securely identify yourself to other people over the web, sign your e-mail messages, encrypt your e-mail messages, and more depending upon the type of certificate you request.

Select a task:

○ Retrieve the CA certificate or certificate revocation list
● Request a certificate
○ Check on a pending certificate

Select **Advanced request**.



Microsoft Certificate Services -- vigor — Home

Choose Request Type

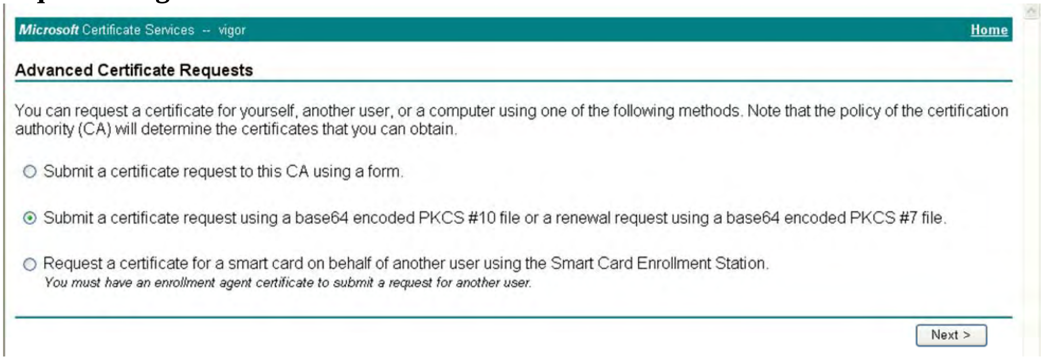
Please select the type of request you would like to make:

○ User certificate request:

User Certificate

● Advanced request

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



Microsoft Certificate Services -- vigor — Home

Advanced Certificate Requests

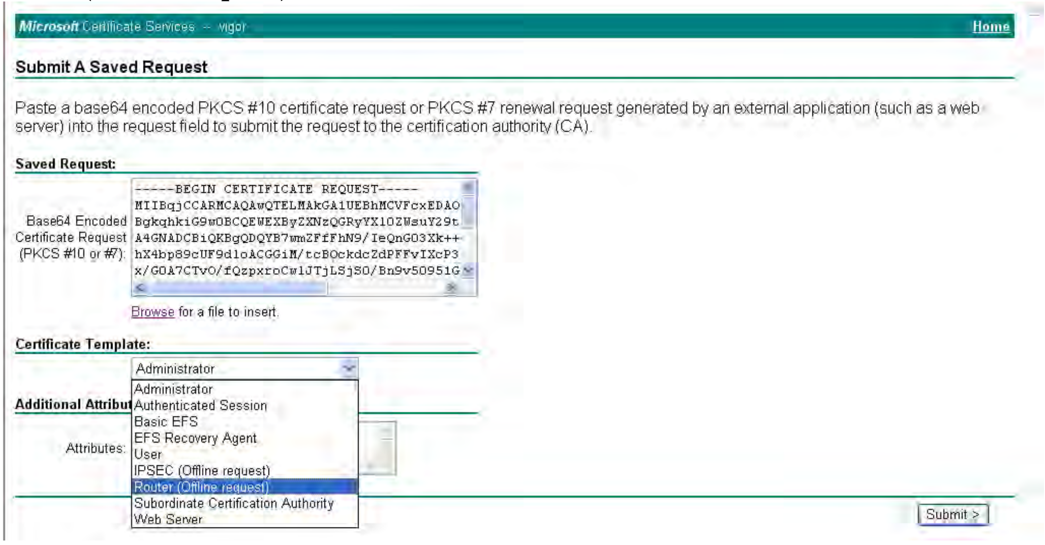
You can request a certificate for yourself, another user, or a computer using one of the following methods. Note that the policy of the certification authority (CA) will determine the certificates that you can obtain.

○ Submit a certificate request to this CA using a form.

● Submit a certificate request using a base64 encoded PKCS #10 file or a renewal request using a base64 encoded PKCS #7 file.

○ Request a certificate for a smart card on behalf of another user using the Smart Card Enrollment Station.
You must have an enrollment agent certificate to submit a request for another user.

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



Microsoft Certificate Services -- vigor — Home

Submit A Saved Request

Paste a base64 encoded PKCS #10 certificate request or PKCS #7 renewal request generated by an external application (such as a web server) into the request field to submit the request to the certification authority (CA).

Saved Request:

Base64 Encoded Certificate Request (PKCS #10 or #7):

```
-----BEGIN CERTIFICATE REQUEST-----
MIIBqjCCARMCAQAwQTELMAkGA1UEBhMCVFcxEDAO
BgkqhkiG9w0BCQEWEXByZXNzQGRyYX10ZWsuY29t
A4GNADCBiQKBgQDQYB7wmZFfFhN9/IeQnG03Xk++
hX4bp89cUF9dloACGGiM/tcBOckdcZdPFFvIXcP3
x/G0A7CTvO/fQzpxroCwlJTjLSjS0/Bn9v50951G
```

Browse for a file to insert.

Certificate Template:

Administrator

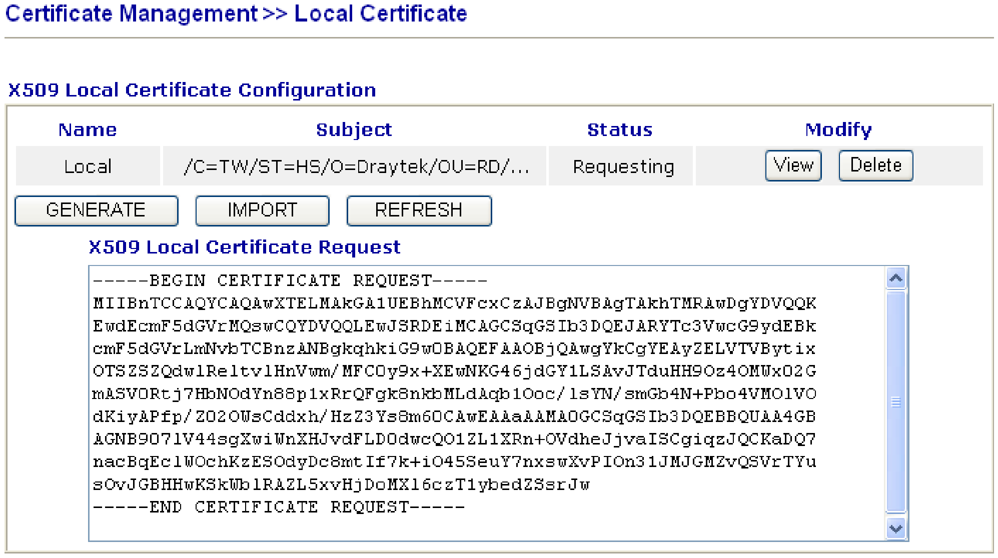
Additional Attribut

Attributes:

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

5. Back to Vigor router, go to **Local Certificate**. Click **IMPORT** button and browse the file to import the certificate (.cer file) into Vigor router. When finished, click refresh

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



Certificate Management >> Local Certificate

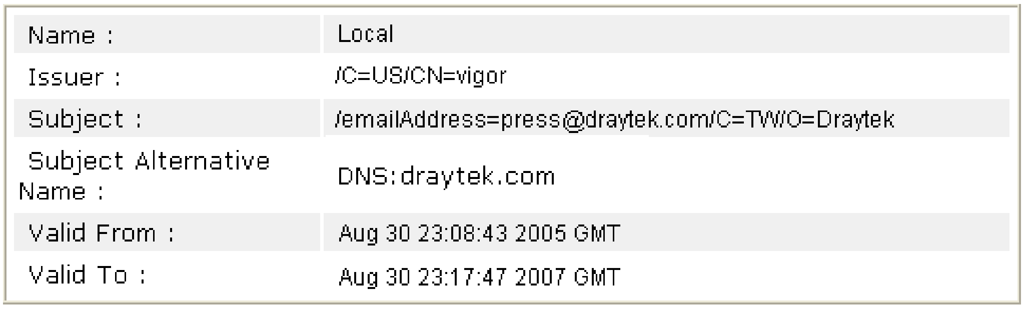
X509 Local Certificate Configuration

Name	Subject	Status	Modify
Local	/C=TW/ST=HS/O=Draytek/OU=RD/...	Requesting	View Delete

X509 Local Certificate Request

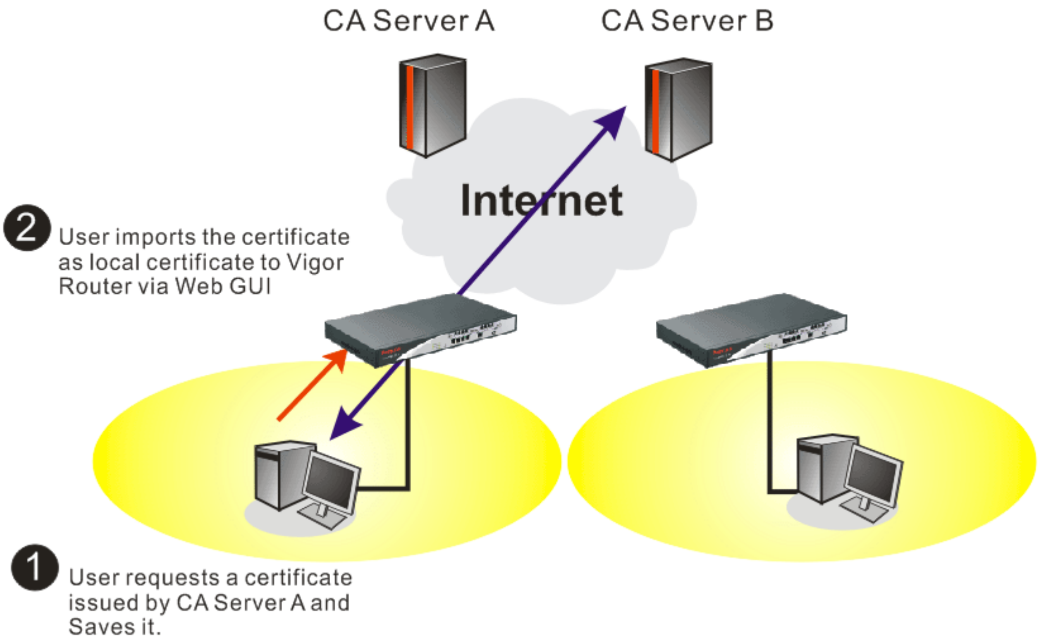
```
-----BEGIN CERTIFICATE REQUEST-----
MIIBnTCCAQYCAQAwXTELMAkGA1UEBhMCVFcxCzAJBgNVBAgTAkhTMRAwDgYDVQQK
EwdEcmF5dGVrMQswCQYDVQQLEwJSRDEiMCAGCSqGSIb3DQEJARYTc3VwcG9ydEBk
cmF5dGVrLmNvbTCBnzANBgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEAyZELVTVBytix
OTSZSZQdwlReltvlHnVwm/MFCOy9x+XEwNKG46jdGY1LSAvJTduHH9Oz4OMWx02G
mASVORtj7HbNOdYn88p1xRrQFgk8nkbMLdAqb1Ooc/lsYN/smGb4N+Pbo4VMO1VO
dKiyAPfp/ZO2OWsCddxh/HzZ3Ys8m6OCAwEAAaAAMA0GCSqGSIb3DQEBBQUAA4GB
AGNB907lV44sgXwiWnXHJvdFLDOdwcQO1ZL1XRn+OVdheJjvaISCgiqzJQCKaDQ7
nacBqEclWOchKzESOdyDc8mtIf7k+iO45SeuY7nxswXvPIOn31JMJGMZvQSVrTYu
sOvJGBHHwKSkWblRAZL5xvHjDoMXl6czT1ybedZSsrJw
-----END CERTIFICATE REQUEST-----
```

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

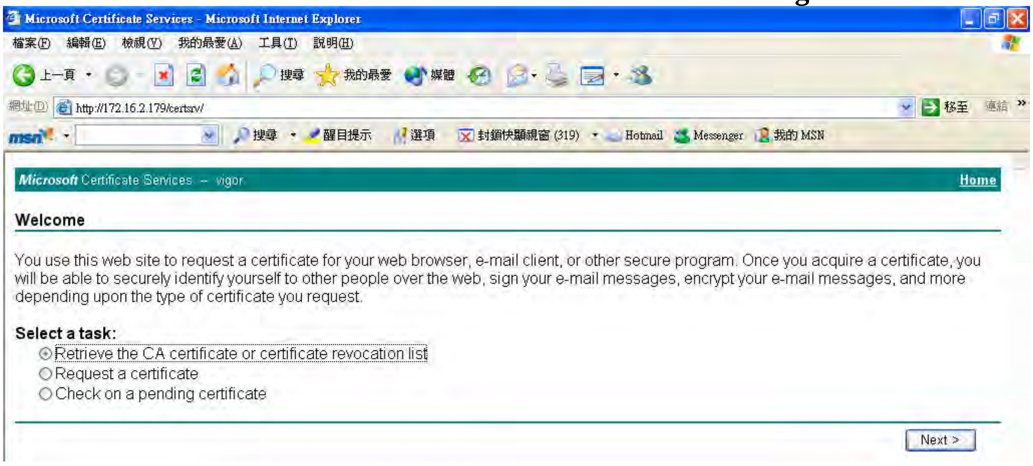


Name :	Local
Issuer :	/C=US/CN=vigor
Subject :	/emailAddress=press@draytek.com/C=TW/O=Draytek
Subject Alternative Name :	DNS:draytek.com
Valid From :	Aug 30 23:08:43 2005 GMT
Valid To :	Aug 30 23:17:47 2007 GMT

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


CA Server A
CA Server B
Internet
2
User imports the certificate as local certificate to Vigor Router via Web GUI
1
User requests a certificate issued by CA Server A and Saves it.

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**.


Microsoft Certificate Services - Microsoft Internet Explorer
檔案(F) 編輯(E) 檢視(V) 我的最愛(A) 工具(T) 說明(H)
上一頁
搜尋
我的最愛
媒體
網址(D) http://172.16.2.179/certsrv/
移至
連結
搜尋
醒目提示
選項
封鎖快顯視窗 (319)
Hotmail
Messenger
我的 MSN

Microsoft Certificate Services -- vigor **Home**

Welcome

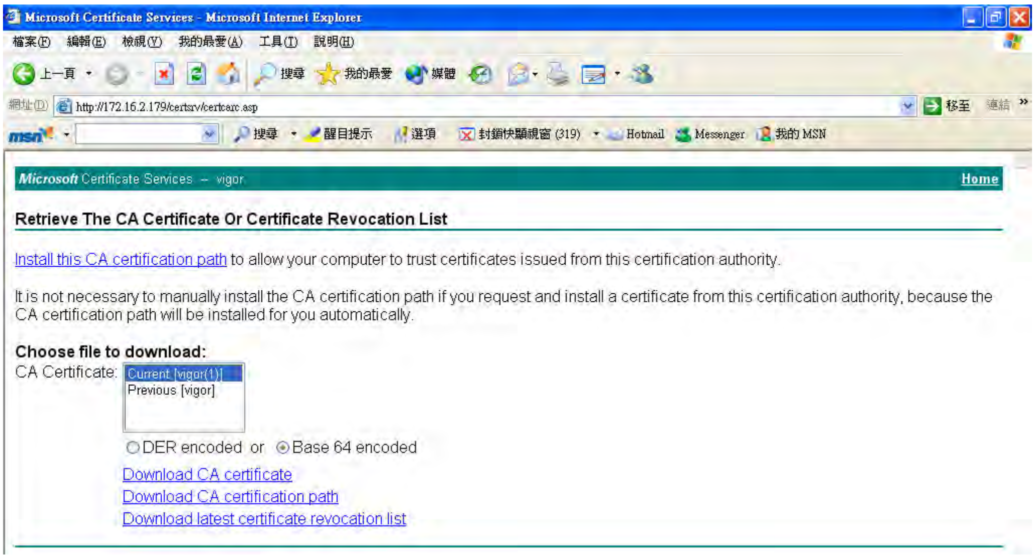
You use this web site to request a certificate for your web browser, e-mail client, or other secure program. Once you acquire a certificate, you will be able to securely identify yourself to other people over the web, sign your e-mail messages, encrypt your e-mail messages, and more depending upon the type of certificate you request.

Select a task:

● Retrieve the CA certificate or certificate revocation list
○ Request a certificate
○ Check on a pending certificate

Next >

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



Microsoft Certificate Services - Microsoft Internet Explorer
http://172.16.2.179/certsrv/certcarc.asp

Microsoft Certificate Services -- vigor | Home

Retrieve The CA Certificate Or Certificate Revocation List

Install this CA certification path to allow your computer to trust certificates issued from this certification authority.

It is not necessary to manually install the CA certification path if you request and install a certificate from this certification authority, because the CA certification path will be installed for you automatically.

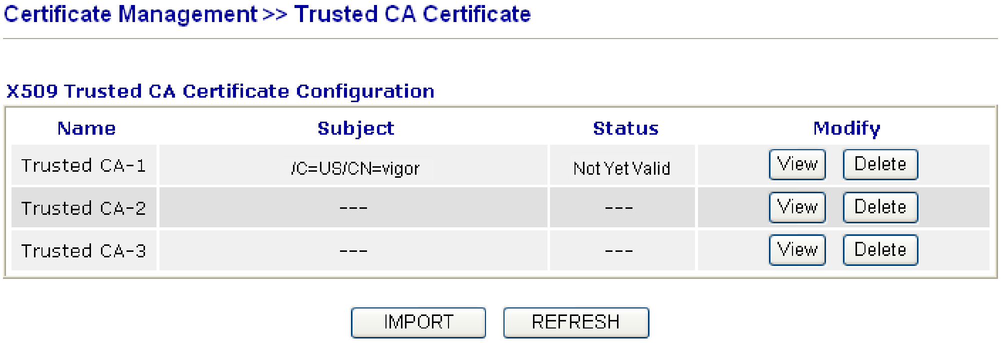
Choose file to download:

CA Certificate: Current [vigor(1)]
Previous [vigor]

○ DER encoded or ● Base 64 encoded

Download CA certificate
Download CA certification path
Download latest certificate revocation list

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.

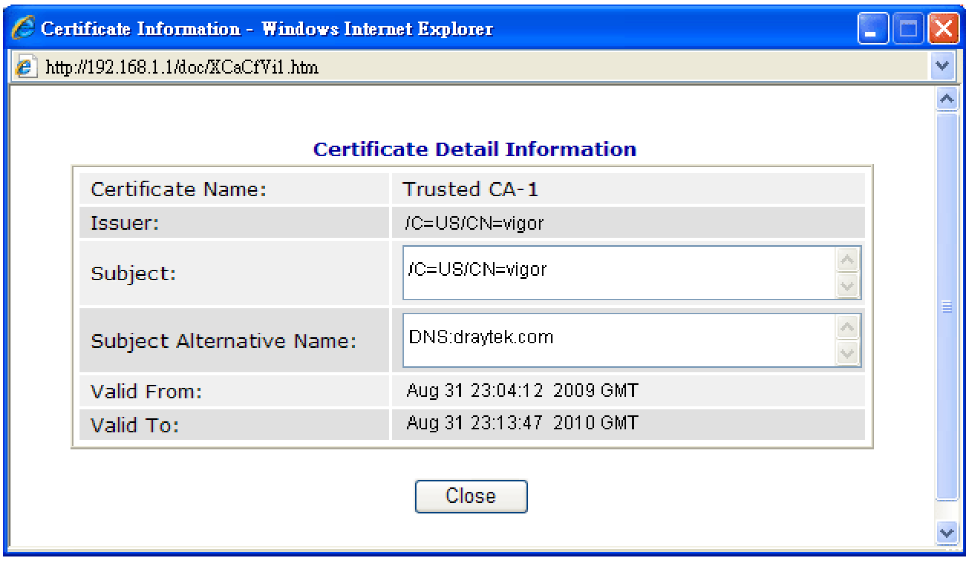


Certificate Management >> Trusted CA Certificate

X509 Trusted CA Certificate Configuration

Name	Subject	Status	Modify
Trusted CA-1	/C=US/CN=vigor	Not Yet Valid	View Delete
Trusted CA-2	---	---	View Delete
Trusted CA-3	---	---	View Delete

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



Certificate Information - Windows Internet Explorer
http://192.168.1.1/doc/XCaCfVi1.htm

Certificate Detail Information

Certificate Name:	Trusted CA-1
Issuer:	/C=US/CN=vigor
Subject:	/C=US/CN=vigor
Subject Alternative Name:	DNS:draytek.com
Valid From:	Aug 31 23:04:12 2009 GMT
Valid To:	Aug 31 23:13:47 2010 GMT

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

This page is left blank.

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.

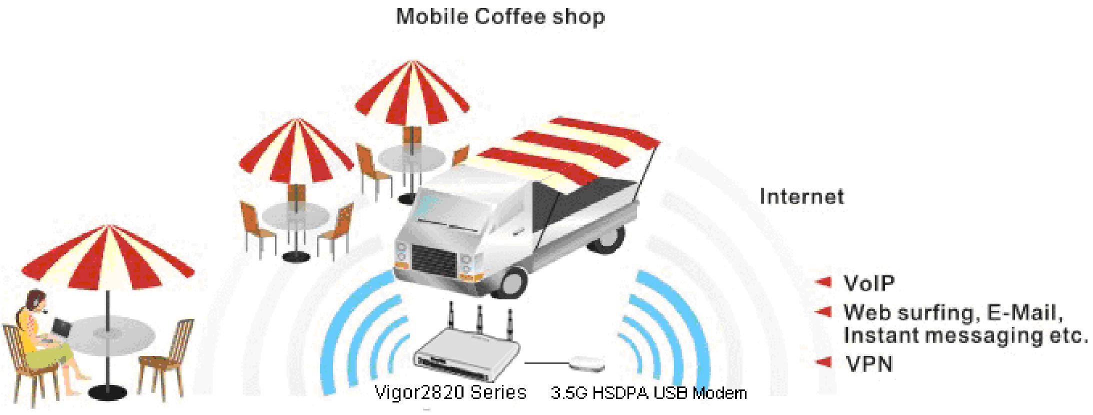
Get Your Public IP Address from ISP

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

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

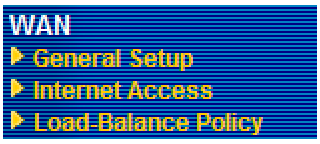
5.1.2 Network Connection by 3G USB Modem

For 3G mobile communication through Access Point is popular more and more, Vigor3510 adds the function of 3G network connection for such purpose. By connecting 3G USB Modem to the USB port of Vigor3510, it can support HSDPA/UMTS/EDGE/GPRS/GSM and the future 3G standard (HSUPA, etc). Vigor3510 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.



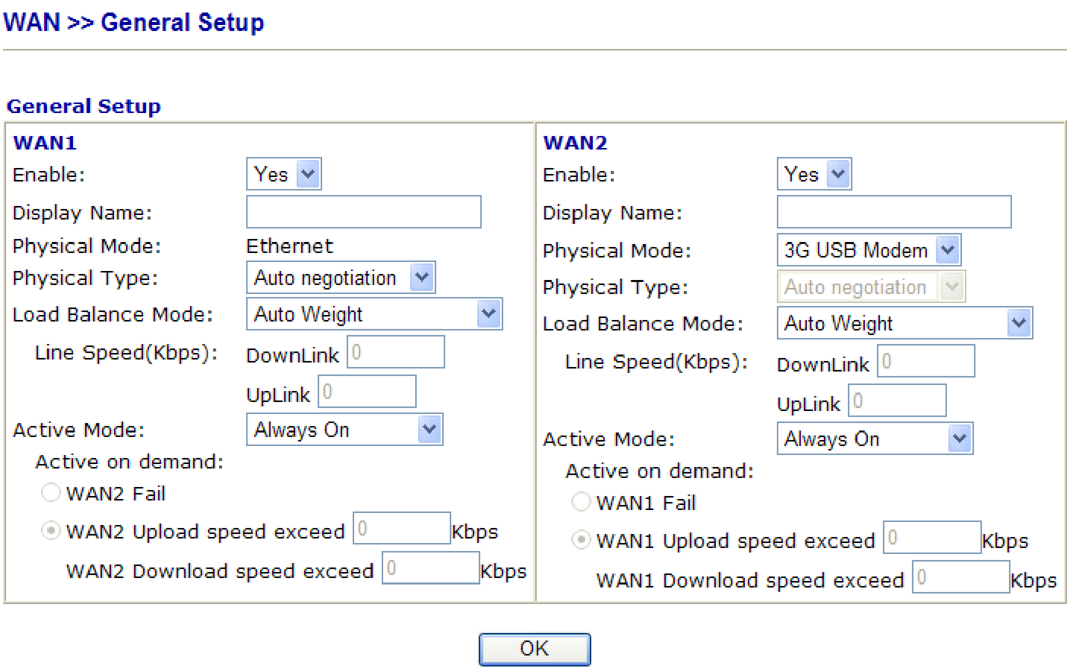
5.1.3 General Setup

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 LAN1 port) can connect to different ISPs, Even if the ISPs use different technology to provide telecommunication service (such as DSL, Cable modem, etc.). If any connection problem occurred on one of the ISP connections, all the traffic will be guided and switched to the normal communication port for proper operation. Please configure WAN1 and WAN2 settings.

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

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



WAN >> General Setup

General Setup

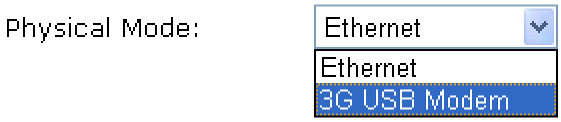
WAN1		WAN2	
Enable:	Yes	Enable:	Yes
Display Name:		Display Name:	
Physical Mode:	Ethernet	Physical Mode:	3G USB Modem
Physical Type:	Auto negotiation	Physical Type:	Auto negotiation
Load Balance Mode:	Auto Weight	Load Balance Mode:	Auto Weight
Line Speed(Kbps):	DownLink 0	Line Speed(Kbps):	DownLink 0
	UpLink 0		UpLink 0
Active Mode:	Always On	Active Mode:	Always On
Active on demand:		Active on demand:	
○ WAN2 Fail		○ WAN1 Fail	
● WAN2 Upload speed exceed 0 Kbps		● WAN1 Upload speed exceed 0 Kbps	
WAN2 Download speed exceed 0 Kbps		WAN1 Download speed exceed 0 Kbps	

OK

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

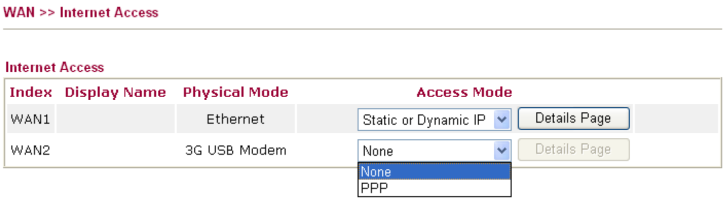
Display Name Type the description for the WAN1/WAN2 interface.

Physical Mode For WAN1, the physical connection is done and fixed through Ethernet port; yet the physical connection for WAN2 is done through an Ethernet port (P1) or USB port.



Physical Mode: Ethernet

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.

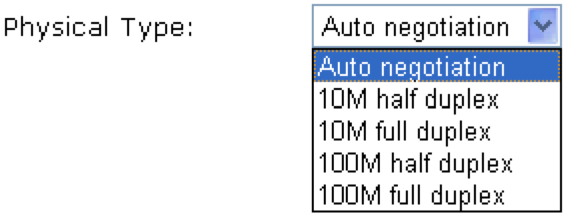


WAN >> Internet Access

Internet Access

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

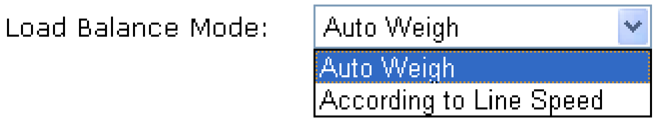
Physical Type You can change the physical type for WAN2 or choose **Auto negotiation** for determined by the system.



Physical Type: Auto negotiation

Load Balance Mode

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



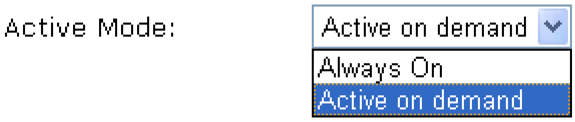
Load Balance Mode: Auto Weigh

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.



Active Mode: Active on demand

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

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

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

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

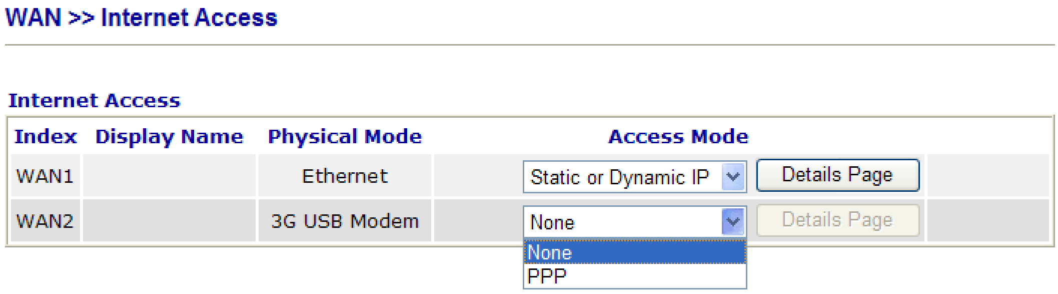
WAN1 Fail – It means the connection for WAN2 will be activated when WAN1 is failed.

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

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

5.1.4 Internet Access

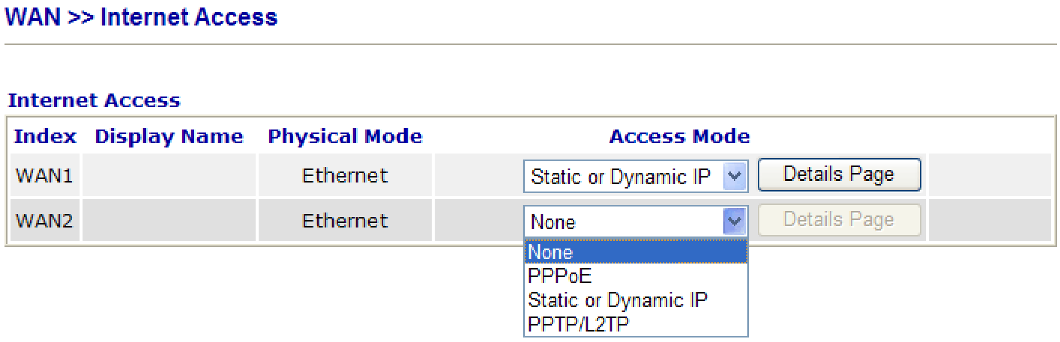
For the router supports dual WAN function, the users can set different WAN settings (for WAN1/WAN2) for Internet Access. Due to different Physical Mode for WAN1 and WAN2, the Access Mode for these two connections also varies slightly.



WAN >> Internet Access

Internet Access

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



WAN >> Internet Access

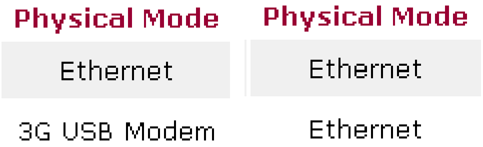
Internet Access

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

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.

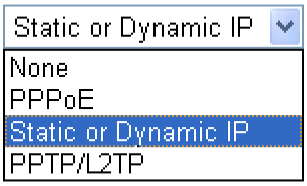
Display Name It shows the name of the WAN1/WAN2 that entered in general setup.

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



Physical Mode	Physical Mode
Ethernet	Ethernet
3G USB Modem	Ethernet

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.

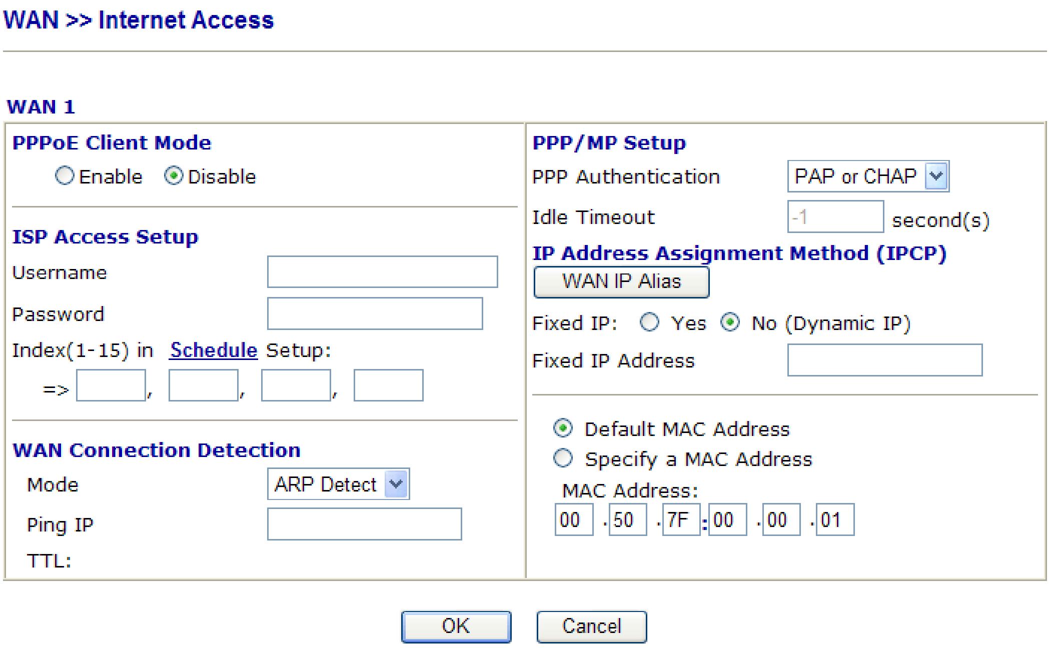


There are three access modes provided for PPPoE, Static or Dynamic IP and PPTP/L2TP.

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..



WAN >> Internet Access

WAN 1

PPPoE Client Mode
○ Enable ● Disable

ISP Access Setup
Username
Password
Index(1-15) in Schedule Setup:
=> , , ,

WAN Connection Detection
Mode: ARP Detect
Ping IP
TTL:

PPP/MP Setup
PPP Authentication: PAP or CHAP
Idle Timeout: -1 second(s)

IP Address Assignment Method (IPCP)
WAN IP Alias
Fixed IP: ○ Yes ● No (Dynamic IP)
Fixed IP Address

● Default MAC Address
○ Specify a MAC Address
MAC Address:
00 . 50 . 7F : 00 . 00 . 01

OK Cancel

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.

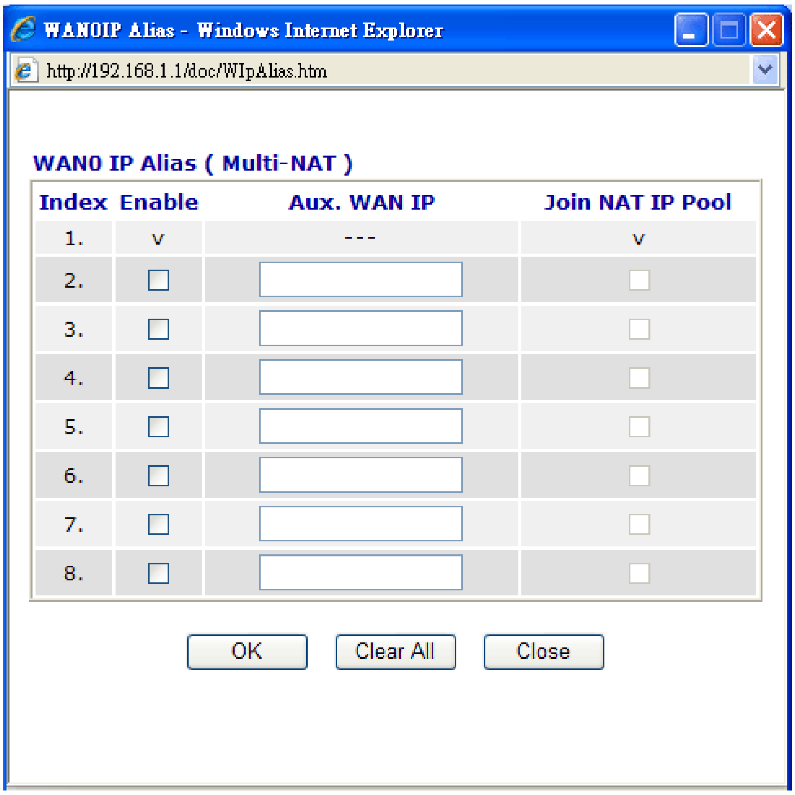
PPP/MP Setup **PPP Authentication** – Select **PAP only** or **PAP or CHAP** for PPP. If you want to connect to Internet all the time, you can check **Always On**.
Idle Timeout – Set the timeout for breaking down the Internet after passing through the time without any action.

IP Address Usually ISP dynamically assigns IP address to you each time you

Assignment Method (IPCP)

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.


WAN0IP Alias - Windows Internet Explorer
http://192.168.1.1/doc/WIpAlias.htm
OK
Clear All
Close

WAN0 IP Alias (Multi-NAT)

Index	Enable	Aux. WAN IP	Join NAT IP Pool
1.	v	---	v
2.	□		□
3.	□		□
4.	□		□
5.	□		□
6.	□		□
7.	□		□
8.	□		□

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.

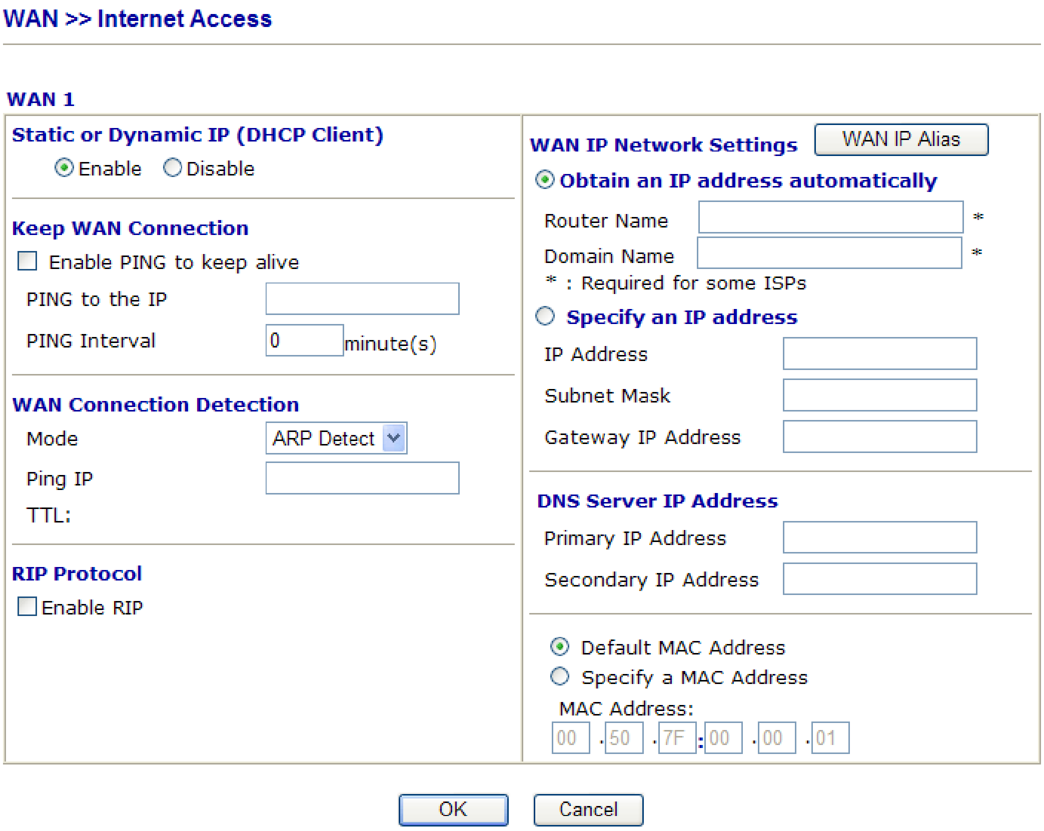
Specify a MAC Address – Type the MAC address for the router manually.

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.



WAN >> Internet Access

WAN 1

Static or Dynamic IP (DHCP Client)

● Enable ○ Disable

Keep WAN Connection

□ Enable PING to keep alive

PING to the IP

PING Interval 0 minute(s)

WAN Connection Detection

Mode ARP Detect

Ping IP

TTL:

RIP Protocol

□ Enable RIP

WAN IP Network Settings WAN IP Alias

● Obtain an IP address automatically

Router Name *

Domain Name *

* : Required for some ISPs

○ Specify an IP address

IP Address

Subnet Mask

Gateway IP Address

DNS Server IP Address

Primary IP Address

Secondary IP Address

● Default MAC Address

○ Specify a MAC Address

MAC Address: 00 . 50 . 7F : 00 . 00 . 01

OK Cancel

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.

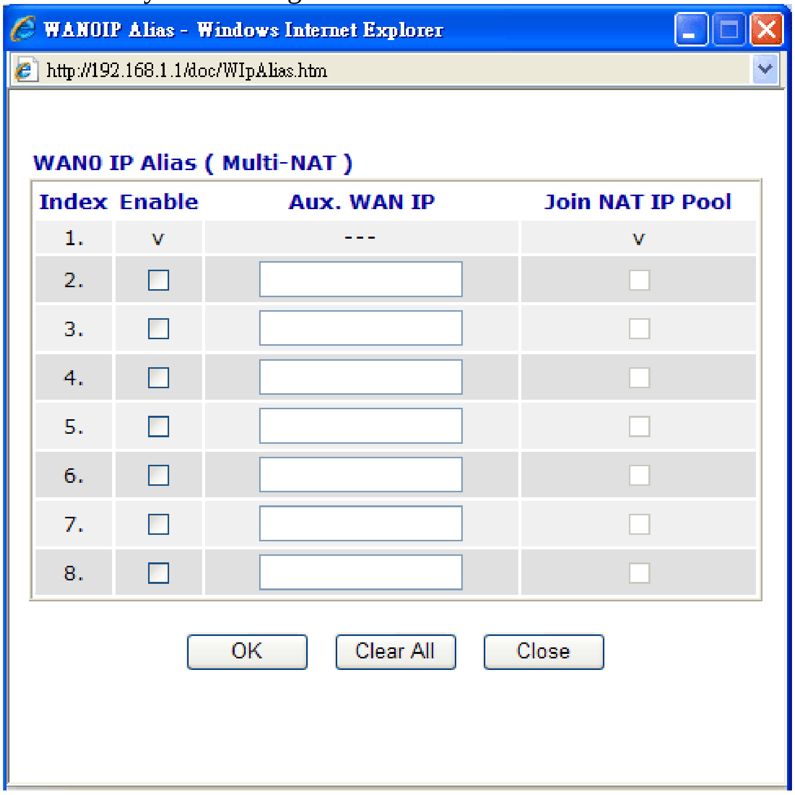
RIP Protocol

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.


WAN0IP Alias - Windows Internet Explorer
http://192.168.1.1/doc/WIpAlias.htm

WAN0 IP Alias (Multi-NAT)

Index	Enable	Aux. WAN IP	Join NAT IP Pool
1.	v	---	v
2.	□		□
3.	□		□
4.	□		□
5.	□		□
6.	□		□
7.	□		□
8.	□		□

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.

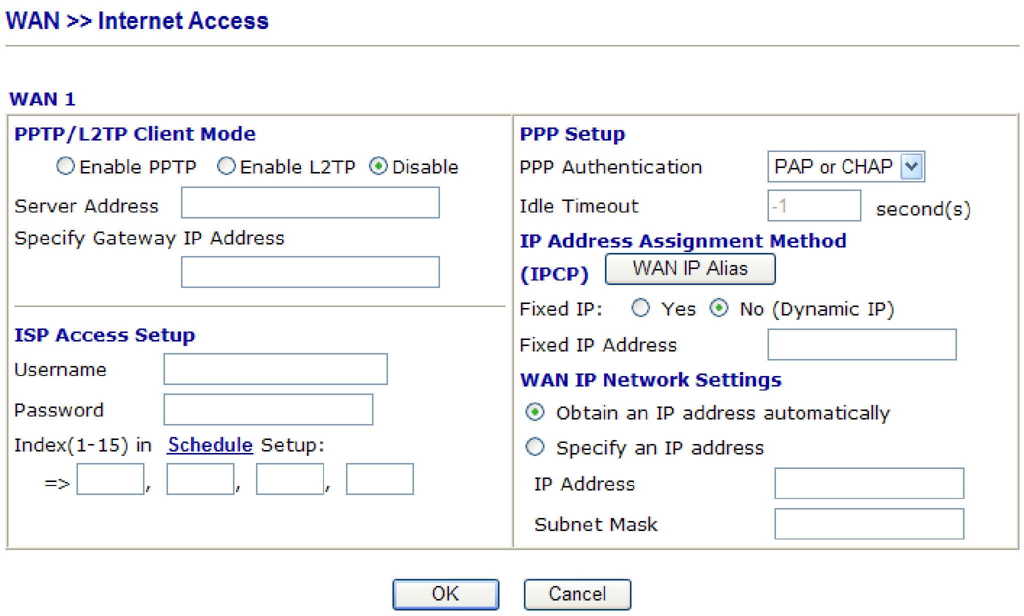
Default MAC Address : Click this radio button to use default MAC address for the router.

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.



WAN >> Internet Access

WAN 1

PPTP/L2TP Client Mode

○ Enable PPTP ○ Enable L2TP ● Disable

Server Address

Specify Gateway IP Address

ISP Access Setup

Username

Password

Index(1-15) in Schedule Setup:

=> , , ,

PPP Setup

PPP Authentication: PAP or CHAP

Idle Timeout: -1 second(s)

IP Address Assignment Method (IPCP) WAN IP Alias

Fixed IP: ○ Yes ● No (Dynamic IP)

Fixed IP Address

WAN IP Network Settings

● Obtain an IP address automatically

○ Specify an IP address

IP Address

Subnet Mask

OK Cancel

PPTP/L2TP Client Mode

Enable PPTP- Click this radio button to enable a PPTP client to establish a tunnel to a DSL modem on the WAN interface.
Enable L2TP - Click this radio button to enable a L2TP client to establish a tunnel to a DSL modem 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

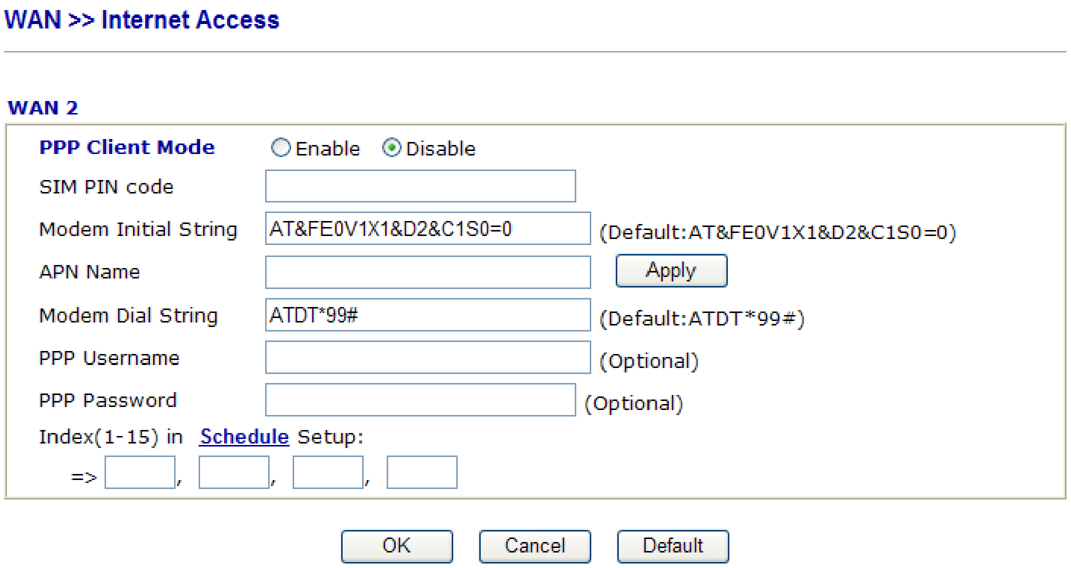
Obtain an IP address automatically – Click this button to obtain

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.



WAN >> Internet Access

WAN 2

PPP Client Mode	○ Enable ● Disable	
SIM PIN code		
Modem Initial String	AT&FE0V1X1&D2&C1S0=0	(Default:AT&FE0V1X1&D2&C1S0=0)
APN Name		Apply
Modem Dial String	ATDT*99#	(Default:ATDT*99#)
PPP Username		(Optional)
PPP Password		(Optional)
Index(1-15) in Schedule Setup:	=> , , ,	

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).

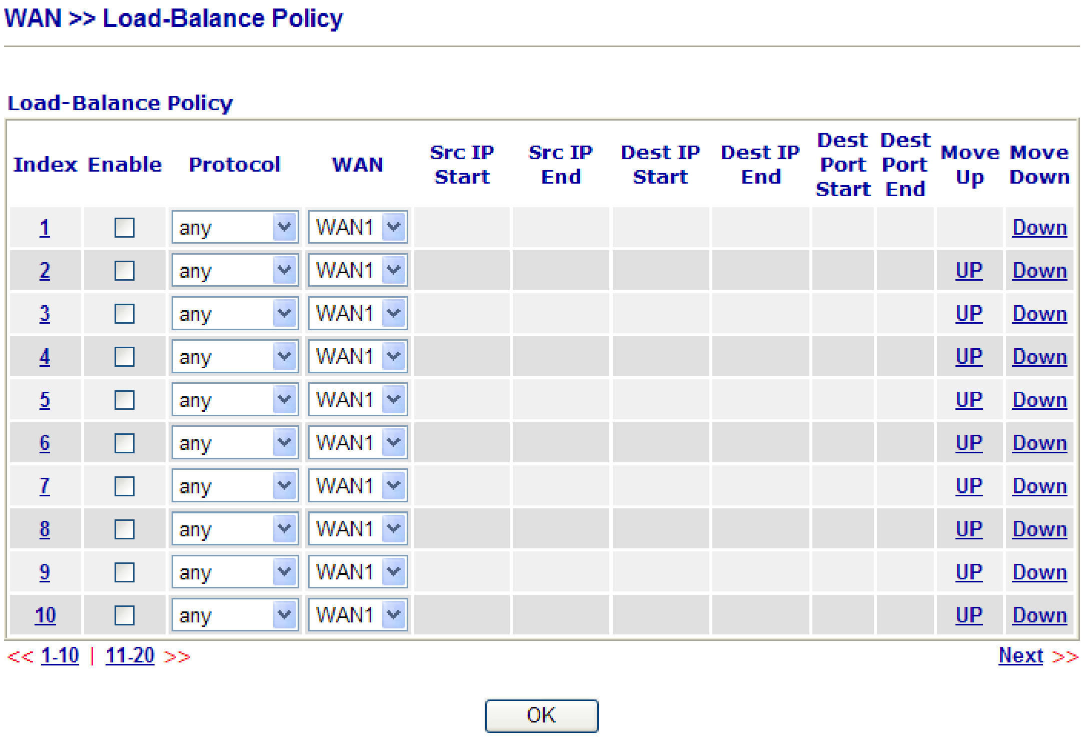
PPP Password Type the PPP password (optional).

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.



WAN >> Load-Balance Policy

Load-Balance Policy

Index	Enable	Protocol	WAN	Src IP Start	Src IP End	Dest IP Start	Dest IP End	Dest Port Start	Dest Port End	Move Up	Move Down
1	□	any	WAN1								Down
2	□	any	WAN1							UP	Down
3	□	any	WAN1							UP	Down
4	□	any	WAN1							UP	Down
5	□	any	WAN1							UP	Down
6	□	any	WAN1							UP	Down
7	□	any	WAN1							UP	Down
8	□	any	WAN1							UP	Down
9	□	any	WAN1							UP	Down
10	□	any	WAN1							UP	Down

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.

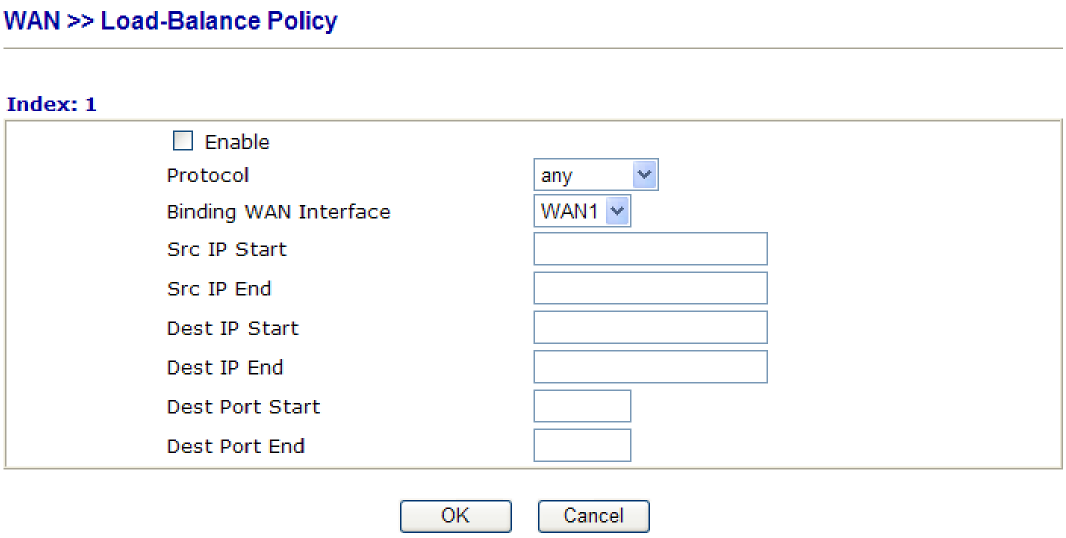
Dest IP End Displays the IP address for the end of the destination IP.

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.



WAN >> Load-Balance Policy

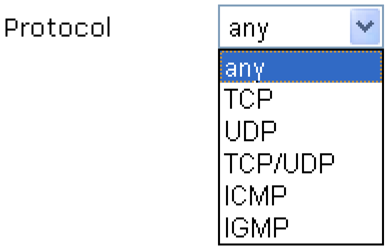
Index: 1

☐ Enable

Protocol	any
Binding WAN Interface	WAN1
Src IP Start	
Src IP End	
Dest IP Start	
Dest IP End	
Dest Port Start	
Dest Port End	

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.

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.

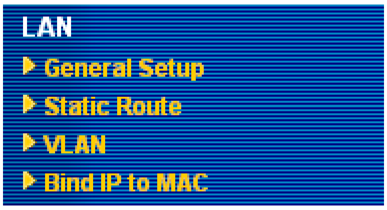
Dest IP End Type the destination IP end for the specified WAN interface. If this field is blank, it means that all the destination IPs will be passed through the WAN interface.

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.

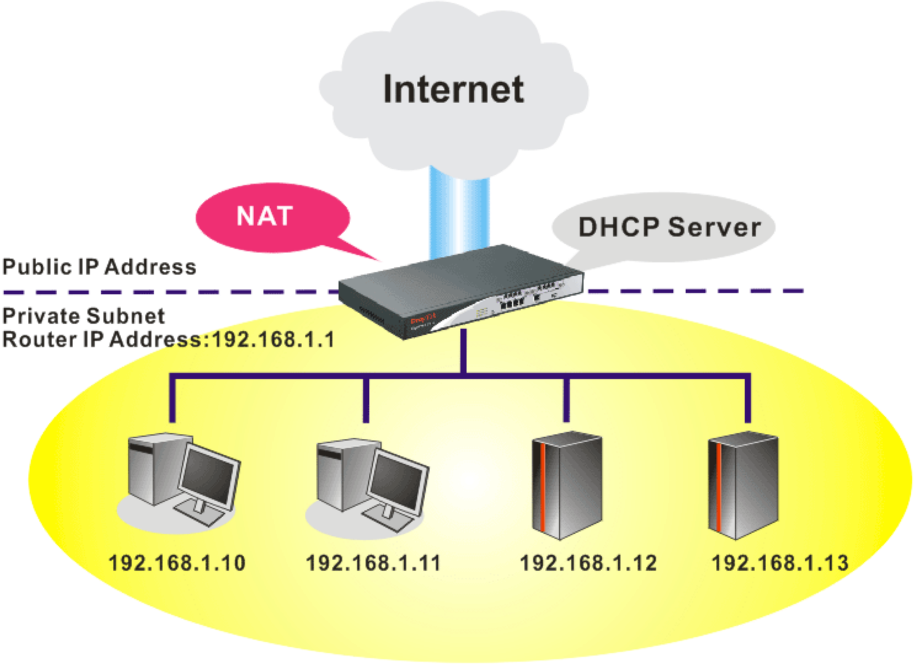
5.2 LAN

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.

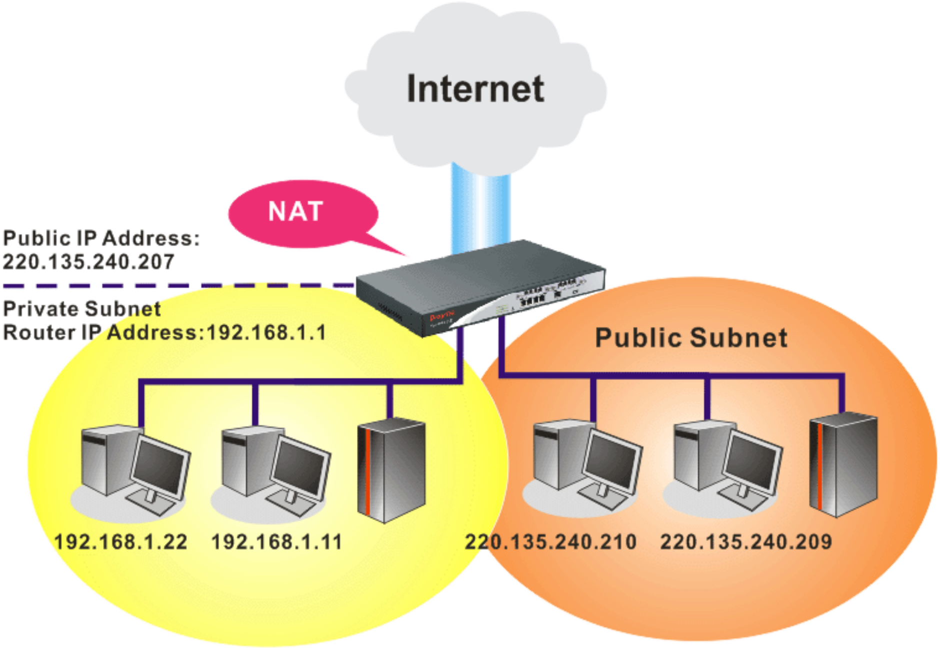


5.2.1 Basics of LAN

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)

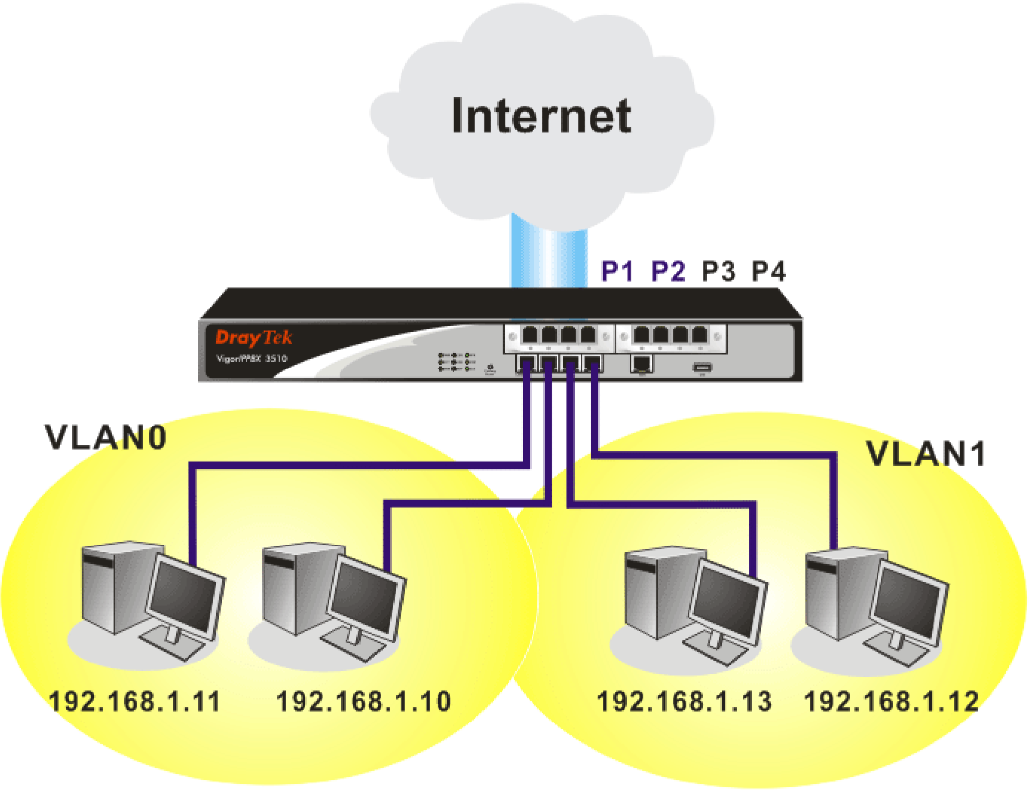
Vigor router will exchange routing information with neighboring routers using the RIP to accomplish IP routing. This allows users to change the information of the router such as IP address and the routers will automatically inform for each other.

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

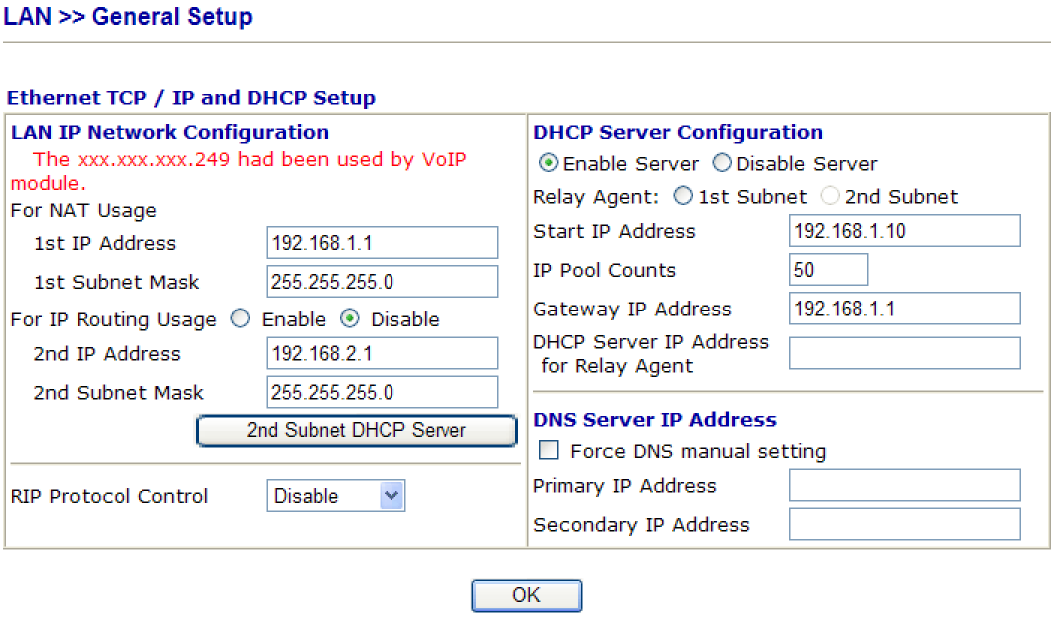
You can group local hosts by physical ports and create up to 4 virtual LANs. To manage the communication between different groups, please set up rules in Virtual LAN (VLAN) function and the rate of each.



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**.



LAN >> General Setup

Ethernet TCP / IP and DHCP Setup

LAN IP Network Configuration

The xxx.xxx.xxx.249 had been used by VoIP module.

For NAT Usage

1st IP Address	192.168.1.1
1st Subnet Mask	255.255.255.0
For IP Routing Usage	○ Enable ● Disable
2nd IP Address	192.168.2.1
2nd Subnet Mask	255.255.255.0

RIP Protocol Control: Disable

DHCP Server Configuration

● Enable Server ○ Disable Server

Relay Agent: ○ 1st Subnet ○ 2nd Subnet

Start IP Address	192.168.1.10
IP Pool Counts	50
Gateway IP Address	192.168.1.1
DHCP Server IP Address for Relay Agent	

DNS Server IP Address

□ Force DNS manual setting

Primary IP Address	
Secondary IP Address	

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

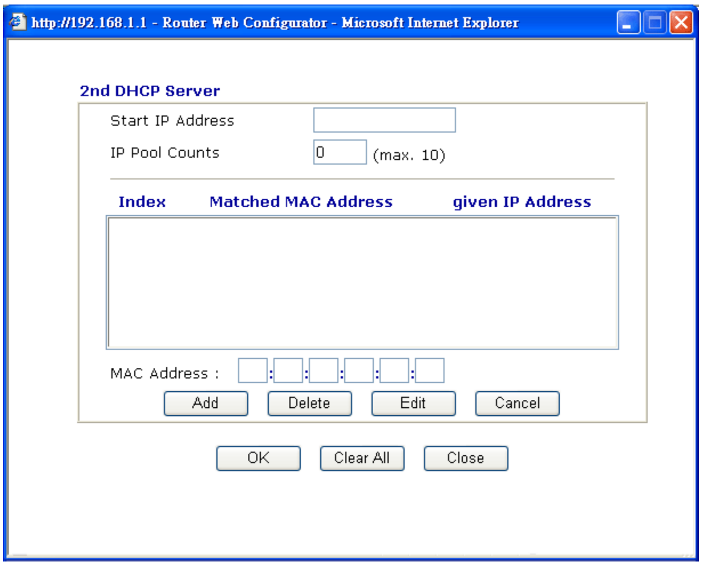
1st Subnet Mask Type in an address code that determines the size of the network. (Default: 255.255.255.0/ 24)

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

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

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

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



http://192.168.1.1 - Router Web Configurator - Microsoft Internet Explorer

2nd DHCP Server

Start IP Address

IP Pool Counts 0 (max. 10)

Index	Matched MAC Address	given IP Address

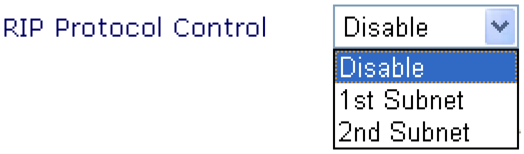
MAC Address : : : : : :

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

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

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

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



RIP Protocol Control: Disable

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.

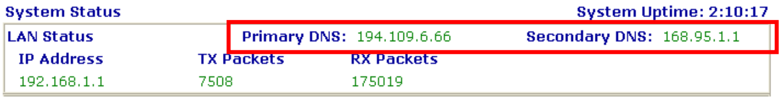
If you want to use another DHCP server in the network other than the Vigor Router's, you can let Relay Agent help you to redirect the DHCP request to the specified location.
Enable Server - Let the router assign IP address to every host in the LAN.
Disable Server – Let you manually assign IP address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



System Status | System Uptime: 2:10:17

LAN Status		Primary DNS: 194.109.6.66	Secondary DNS: 168.95.1.1
IP Address	TX Packets	RX Packets	
192.168.1.1	7508	175019	

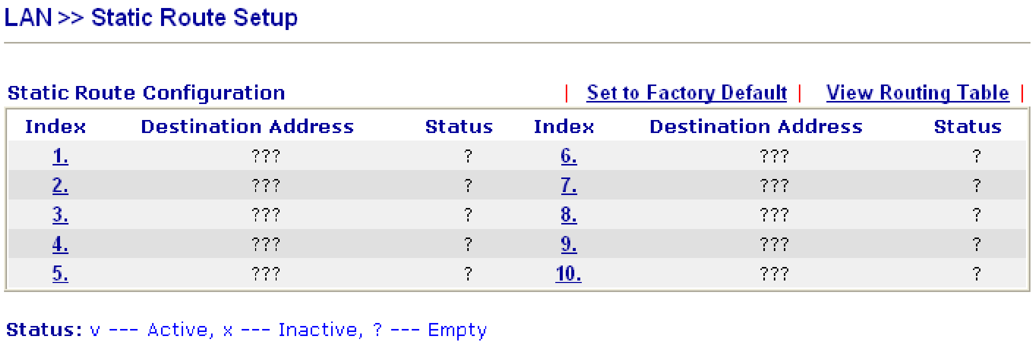
If both the Primary IP and Secondary IP Address fields are left empty, the router will assign its own IP address to local users as a DNS proxy server and maintain a DNS cache.

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

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

5.2.3 Static Route

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



LAN >> Static Route Setup

Static Route Configuration | Set to Factory Default | View Routing Table |

Index	Destination Address	Status	Index	Destination Address	Status
1.	???	?	6.	???	?
2.	???	?	7.	???	?
3.	???	?	8.	???	?
4.	???	?	9.	???	?
5.	???	?	10.	???	?

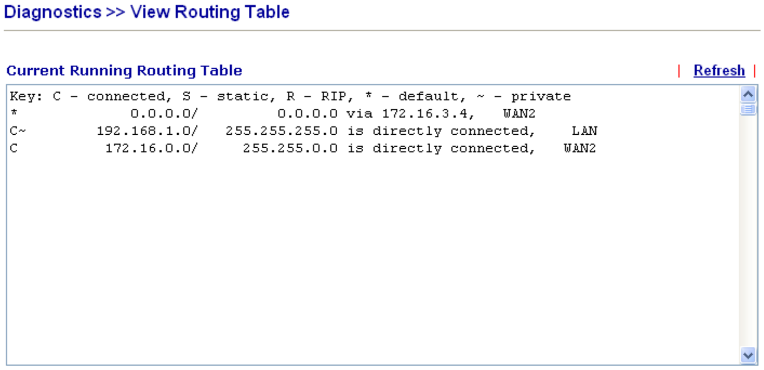
Status: v --- Active, x --- Inactive, ? --- Empty

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

Destination Address Displays the destination address of the static route.

Status Displays the status of the static route.

Viewing Routing Table Displays the routing table for your reference.



Diagnostics >> View Routing Table

Current Running Routing Table | Refresh |

```
Key: C - connected, S - static, R - RIP, * - default, ~ - private
*          0.0.0.0/         0.0.0.0 via 172.16.3.4,    WAN2
C~       192.168.1.0/   255.255.255.0 is directly connected,    LAN
C         172.16.0.0/     255.255.0.0 is directly connected,   WAN2
```

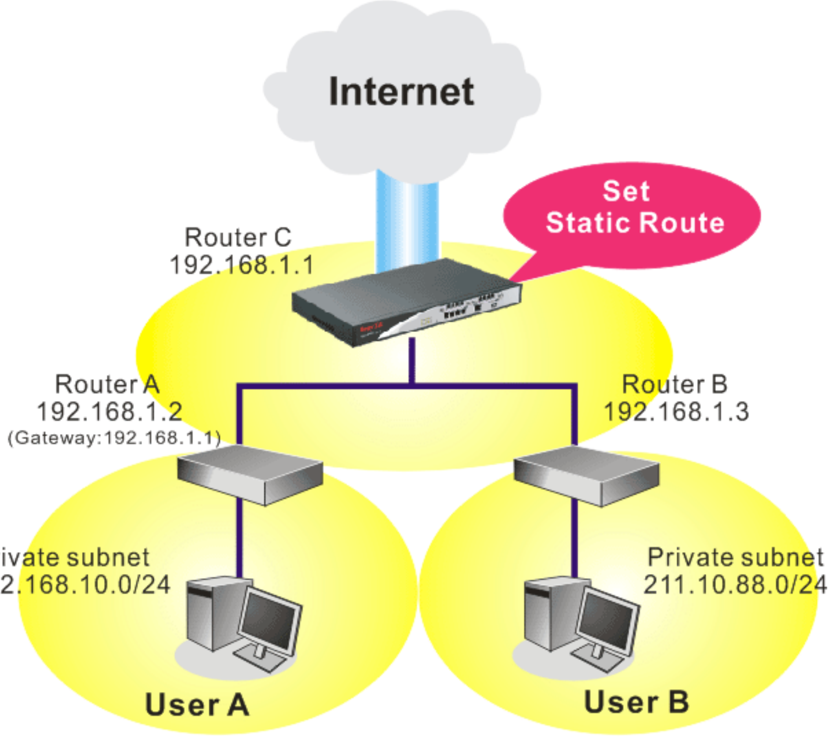
Add Static Routes to Private and Public Networks

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.

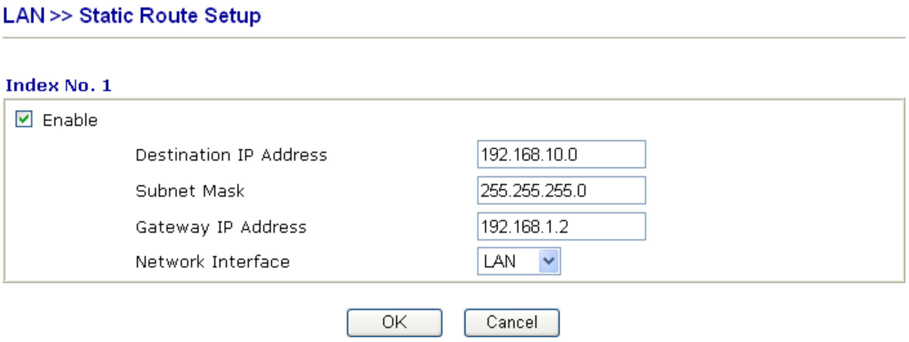
Before setting Static Route, user A cannot talk to user B for Router A can only forward recognized packets to its default gateway Main Router.



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**.

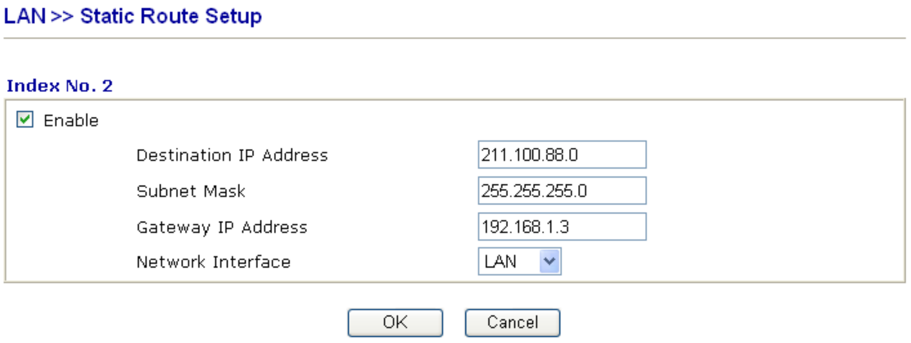

LAN >> Static Route Setup

Index No. 1

☑ Enable

Destination IP Address	192.168.10.0
Subnet Mask	255.255.255.0
Gateway IP Address	192.168.1.2
Network Interface	LAN

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.



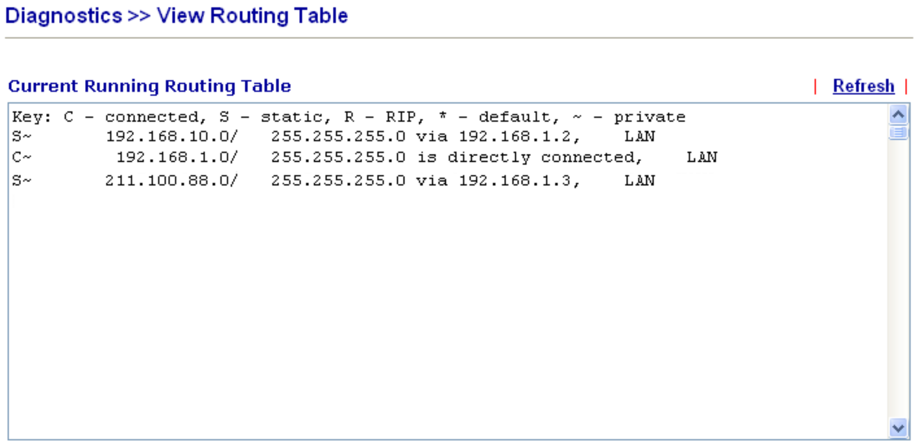
LAN >> Static Route Setup

Index No. 2

☑ Enable

Destination IP Address	211.100.88.0
Subnet Mask	255.255.255.0
Gateway IP Address	192.168.1.3
Network Interface	LAN

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



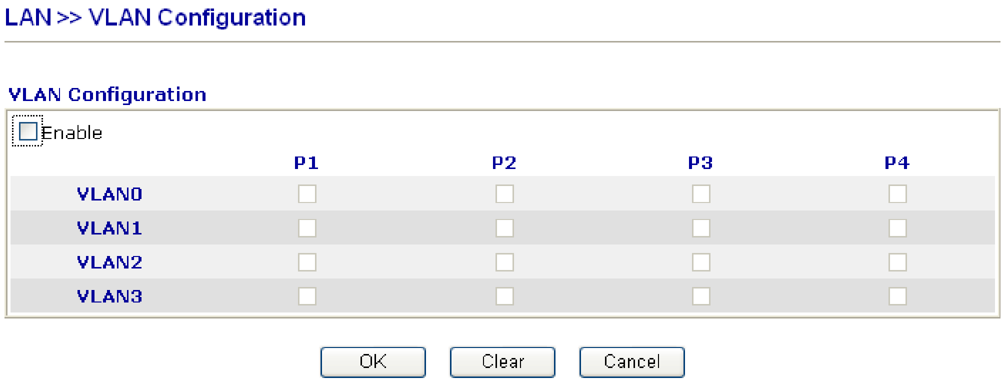
Diagnostics >> View Routing Table

Current Running Routing Table

```
Key: C - connected, S - static, R - RIP, * - default, ~ - private
S~       192.168.10.0/   255.255.255.0 via 192.168.1.2,     LAN
C~        192.168.1.0/   255.255.255.0 is directly connected,    LAN
S~       211.100.88.0/   255.255.255.0 via 192.168.1.3,     LAN
```

5.2.4 VLAN

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



LAN >> VLAN Configuration

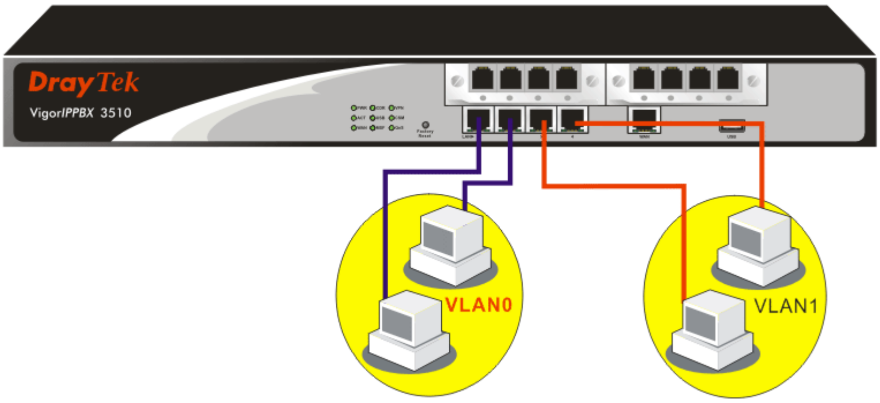
VLAN Configuration

☐ Enable

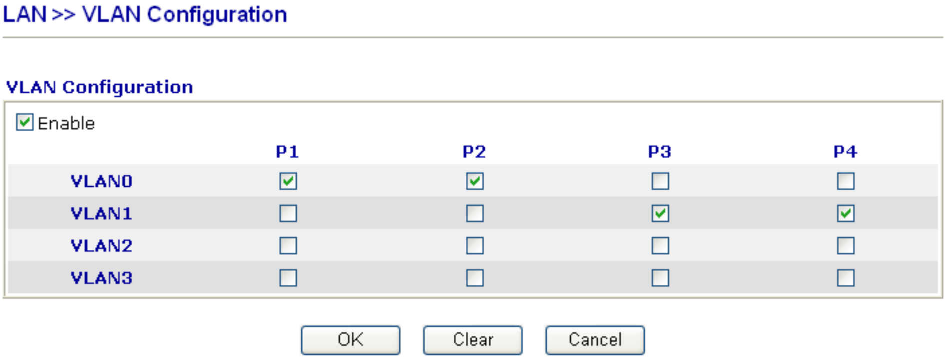
	P1	P2	P3	P4
VLAN0	☐	☐	☐	☐
VLAN1	☐	☐	☐	☐
VLAN2	☐	☐	☐	☐
VLAN3	☐	☐	☐	☐

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

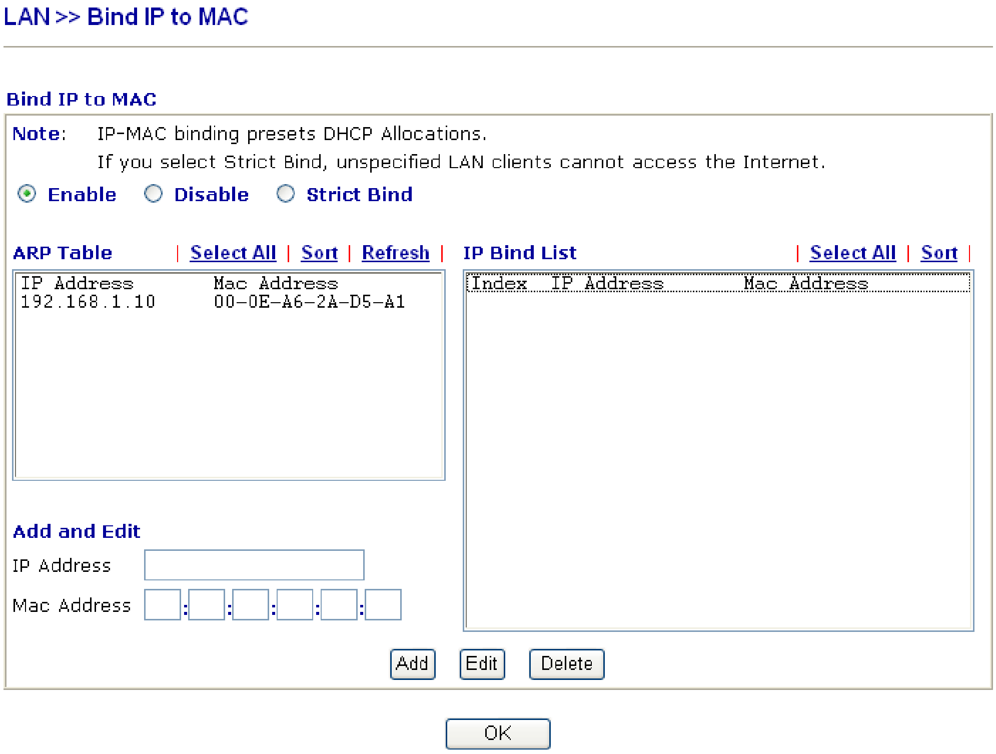
	P1	P2	P3	P4
VLAN0	☑	☑	□	□
VLAN1	□	□	☑	☑
VLAN2	□	□	□	□
VLAN3	□	□	□	□

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.



LAN >> Bind IP to MAC

Bind IP to MAC

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

● Enable ○ Disable ○ Strict Bind

ARP Table | Select All | Sort | Refresh |

```
IP Address        Mac Address
192.168.1.10      00-0E-A6-2A-D5-A1
```

IP Bind List | Select All | Sort |

```
Index  IP Address          Mac Address
```

Add and Edit

IP Address

Mac Address : : : : :

Enable Click this radio button to invoke this function. However, IP/MAC which is not listed in IP Bind List also can connect to Internet.

Disable Click this radio button to disable this function. All the settings on this page will be invalid.

Strict Bind Click this radio button to block the connection of the IP/MAC which is not listed in IP Bind List.

ARP Table This table is the LAN ARP table of this router. The information for IP and MAC will be displayed in this field. Each pair of IP and MAC address listed in ARP table can be selected and added to IP Bind List by clicking **Add** below.

Add and Edit **IP Address** – Type the IP address that will be used for the specified MAC address.
Mac Address – Type the MAC address that is used to bind with the assigned IP address.

Refresh It is used to refresh the ARP table. When there is one new PC added to the LAN, you can click this link to obtain the newly ARP table information.

IP Bind List It displays a list for the IP bind to MAC information.

Add It allows you to add the one you choose from the ARP table or the IP/MAC address typed in **Add and Edit** to the table of **IP Bind List**.

Edit It allows you to edit and modify the selected IP address and MAC address that you create before.

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.

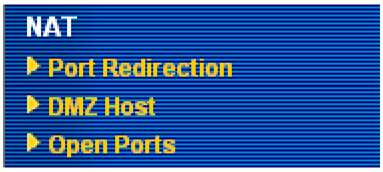
When the outgoing packets destined to some public server on the Internet reach the NAT router, the router will change its source address into the public IP address of the router, select the available public port, and then forward it. At the same time, the router shall list an entry in a table to memorize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

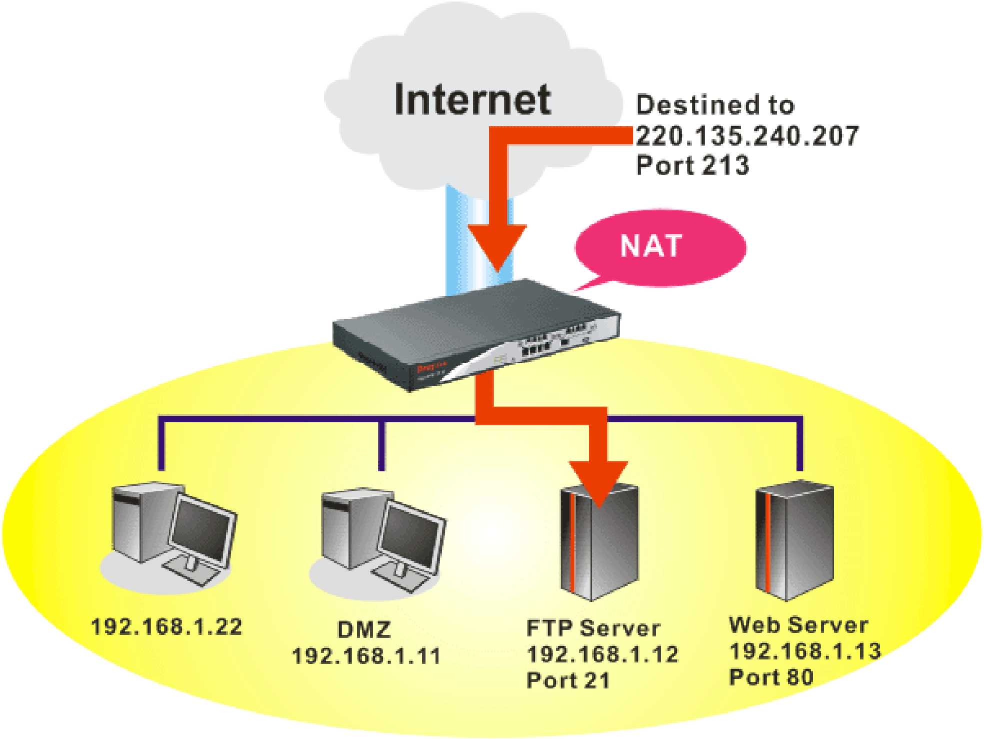
> On NAT page, you will see the private IP address defined in RFC-1918. Usually we use the 192.168.1.0/24 subnet for the router. As stated before, the NAT facility can map one or more IP addresses and/or service ports into different specified services. In other words, the NAT function can be achieved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

Below shows the menu items for NAT.



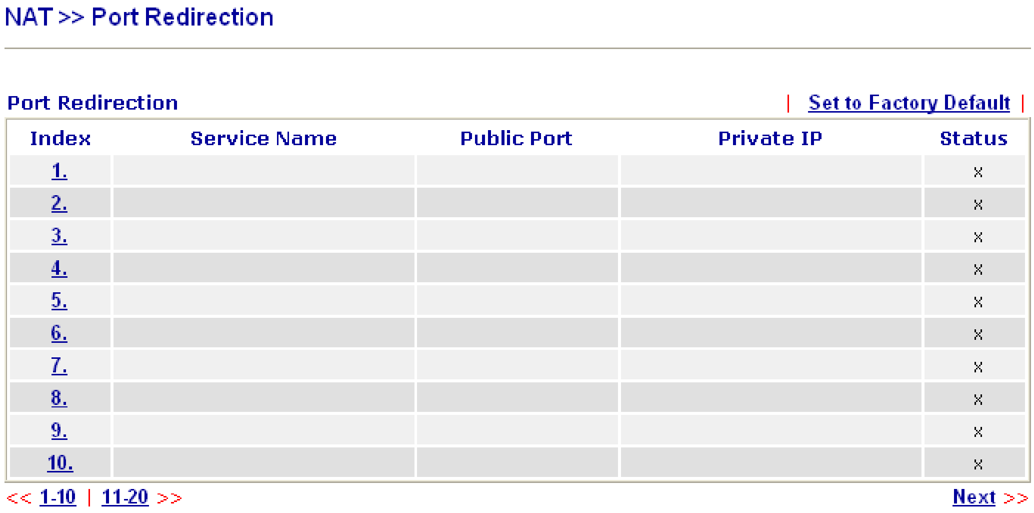
5.3.1 Port Redirection

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.



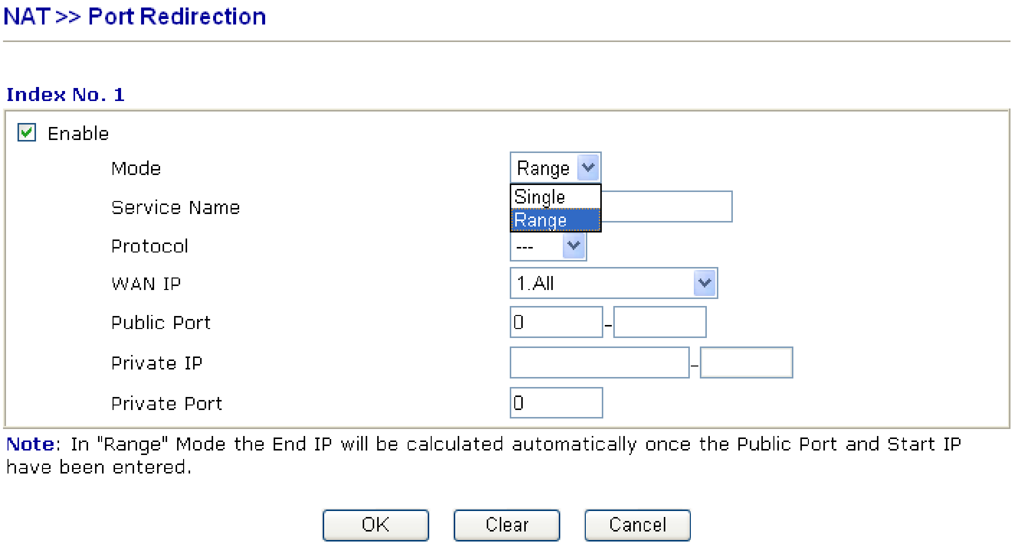
NAT >> Port Redirection

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.


NAT >> Port Redirection

Index No. 1

☑ Enable

Mode	Range
Service Name	
Protocol	---
WAN IP	1.All
Public Port	0 -
Private IP	-
Private Port	0

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

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.

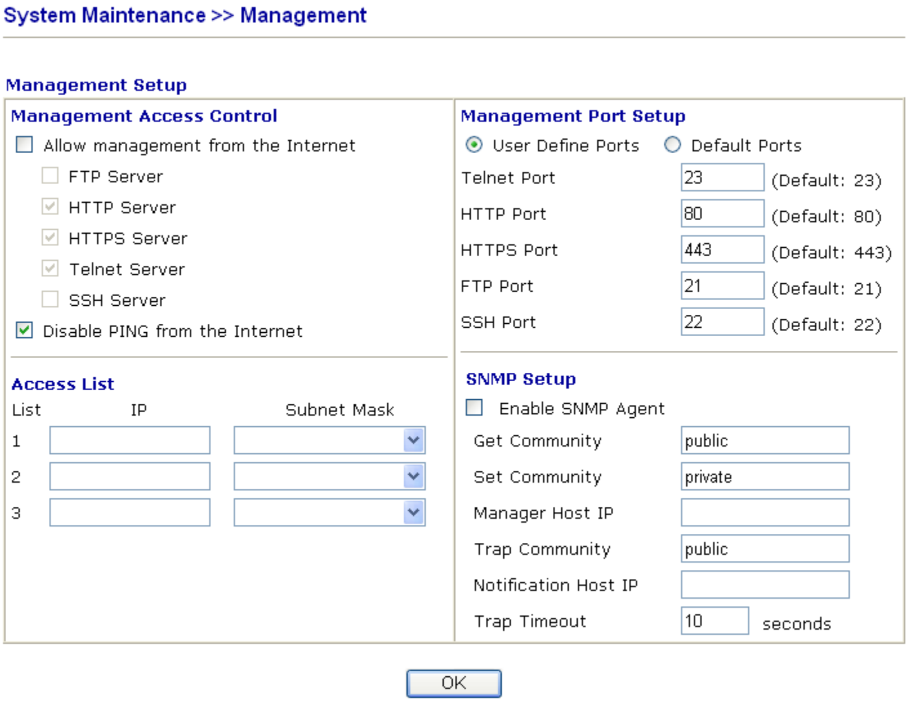
Private IP Specify the private IP address of the internal host providing the service. If you choose **Range** as the port redirection mode, you will see two boxes on this field. Type a complete IP address in the first box (as the starting point) and the fourth digits in the second box (as the end point).

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.



System Maintenance >> Management

Management Setup

Management Access Control

□ Allow management from the Internet
□ FTP Server
☑ HTTP Server
☑ HTTPS Server
☑ Telnet Server
□ SSH Server
☑ Disable PING from the Internet

Access List

List	IP	Subnet Mask
1		
2		
3		

Management Port Setup

● User Define Ports ○ Default Ports

Telnet Port	23	(Default: 23)
HTTP Port	80	(Default: 80)
HTTPS Port	443	(Default: 443)
FTP Port	21	(Default: 21)
SSH Port	22	(Default: 22)

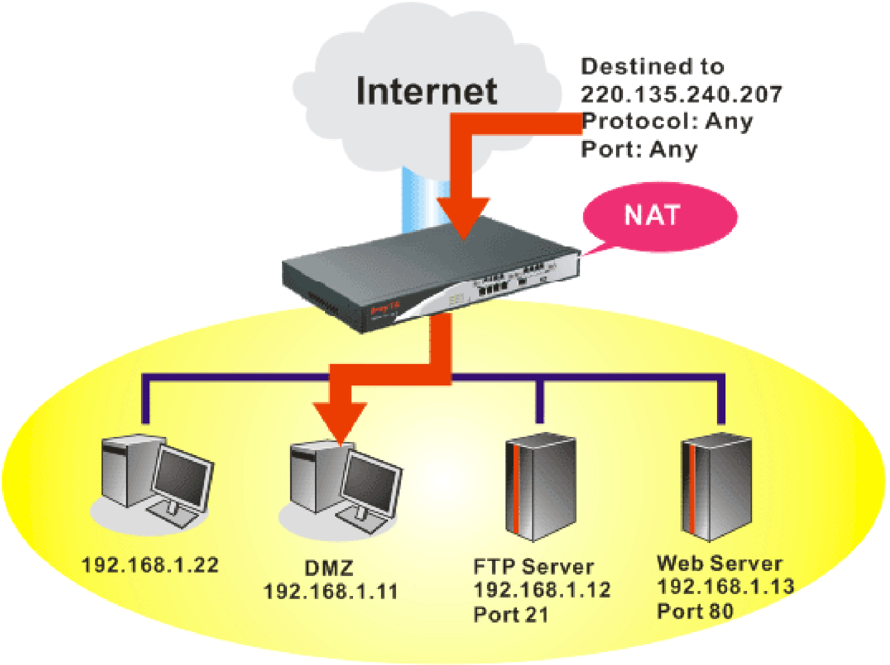
SNMP Setup

□ Enable SNMP Agent

Get Community	public	
Set Community	private	
Manager Host IP		
Trap Community	public	
Notification Host IP		
Trap Timeout	10	seconds

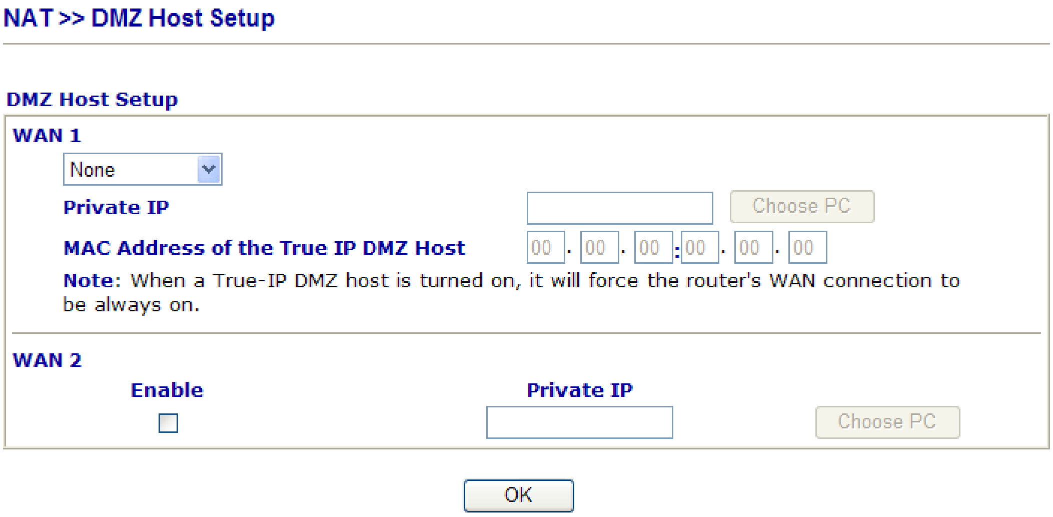
5.3.2 DMZ Host

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:



NAT >> DMZ Host Setup

DMZ Host Setup

WAN 1

None

Private IP

Choose PC

MAC Address of the True IP DMZ Host 00 . 00 . 00 : 00 . 00 . 00

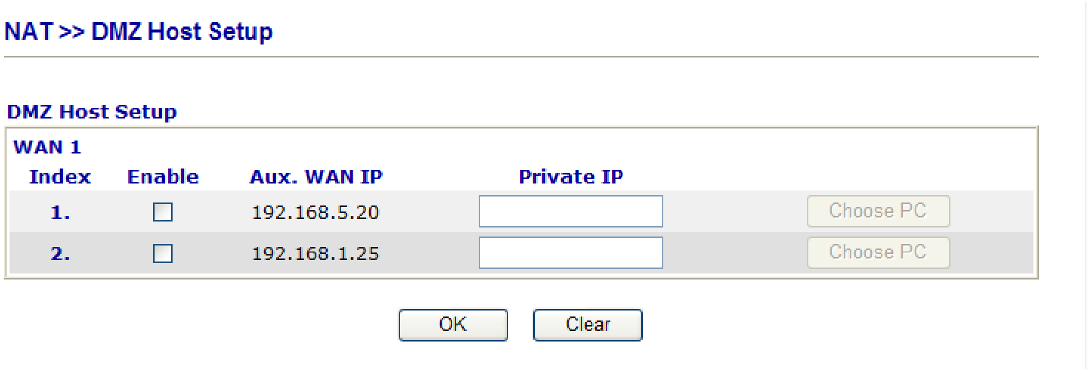
Note: When a True-IP DMZ host is turned on, it will force the router's WAN connection to be always on.

WAN 2

Enable	Private IP	
□		Choose PC

OK

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.



NAT >> DMZ Host Setup

DMZ Host Setup

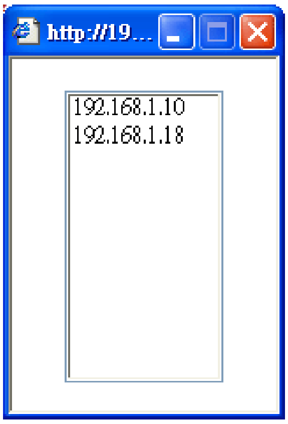
WAN 1

Index	Enable	Aux. WAN IP	Private IP	
1.	□	192.168.5.20		Choose PC
2.	□	192.168.1.25		Choose PC

Enable Check to enable the DMZ Host function.

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

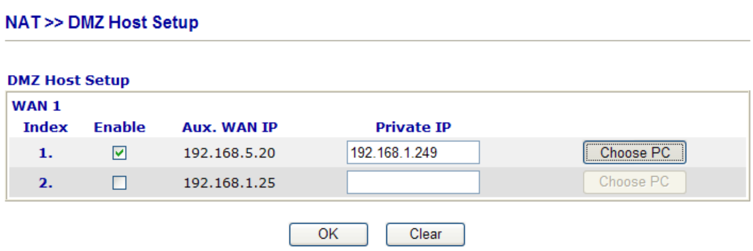
Choose PC Click this button and then a window will automatically pop up, as depicted below. The window consists of a list of private IP addresses of all hosts in your LAN network. Select one private IP address in the list to be the DMZ host.



http://19...

192.168.1.10
192.168.1.18

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



NAT >> DMZ Host Setup

DMZ Host Setup

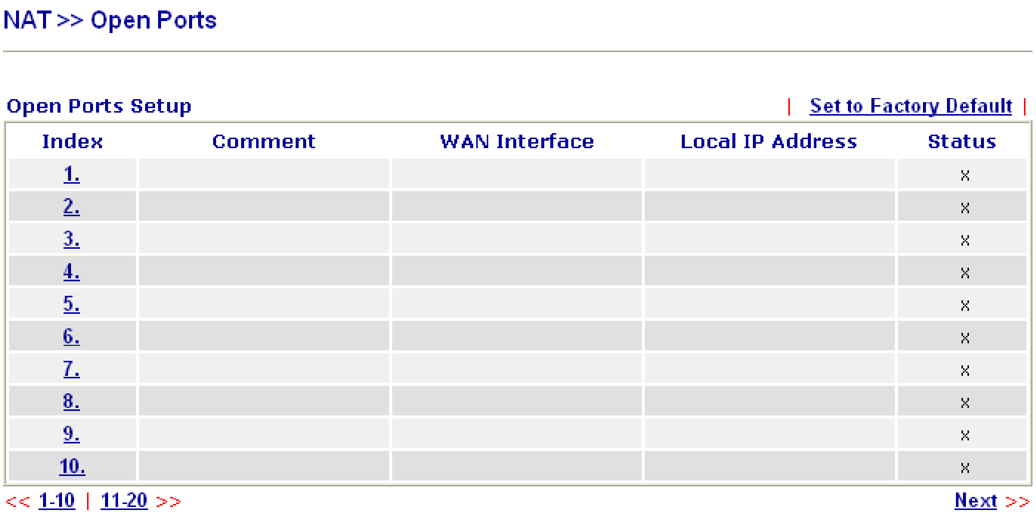
WAN 1

Index	Enable	Aux. WAN IP	Private IP	
1.	☑	192.168.5.20	192.168.1.249	Choose PC
2.	□	192.168.1.25		Choose PC

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:



NAT >> Open Ports

Open Ports Setup | Set to Factory Default |

Index	Comment	WAN Interface	Local IP Address	Status
1.				x
2.				x
3.				x
4.				x
5.				x
6.				x
7.				x
8.				x
9.				x
10.				x

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

Index Indicate the relative number for the particular entry that you want to offer service in a local host. You should click the appropriate index number to edit or clear the corresponding entry.

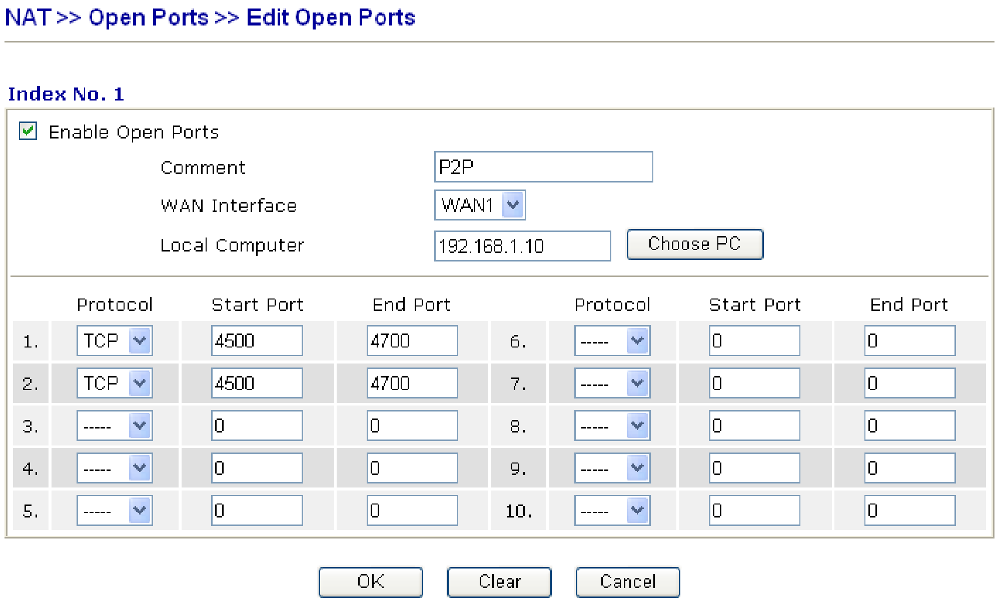
Comment Specify the name for the defined network service.

WAN Interface Display the WAN interface for the entry.

Local IP Address Display the private IP address of the local host offering the service.

Status Display the state for the corresponding entry. X or V is to represent the **Inactive** or **Active** state.

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



NAT >> Open Ports >> Edit Open Ports

Index No. 1

☑ Enable Open Ports

Comment	P2P
WAN Interface	WAN1
Local Computer	192.168.1.10 [Choose PC]

	Protocol	Start Port	End Port		Protocol	Start Port	End Port
1.	TCP	4500	4700	6.	-----	0	0
2.	TCP	4500	4700	7.	-----	0	0
3.	-----	0	0	8.	-----	0	0
4.	-----	0	0	9.	-----	0	0
5.	-----	0	0	10.	-----	0	0

Enable Open Ports Check to enable this entry.

Comment Make a name for the defined network application/service.

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

Local Computer Enter the private IP address of the local host or click **Choose PC** to select one.

Choose PC Click this button and, subsequently, a window having a list of private IP addresses of local hosts will automatically pop up. Select the appropriate IP address of the local host in the list.

Protocol Specify the transport layer protocol. It could be **TCP**, **UDP**, or ----- (none) for selection.

Start Port Specify the starting port number of the service offered by the local host.

End Port Specify the ending port number of the service offered by the local host.

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:

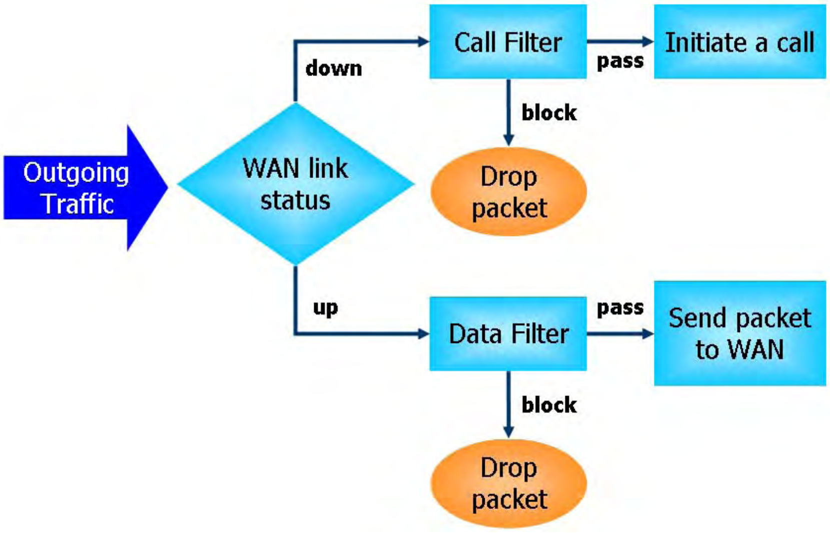
- User-configurable IP filter (Call Filter/ Data Filter).
- Stateful Packet Inspection (SPI): tracks packets and denies unsolicited incoming data
- Selectable Denial of Service (DoS) /Distributed DoS (DDoS) attacks protection

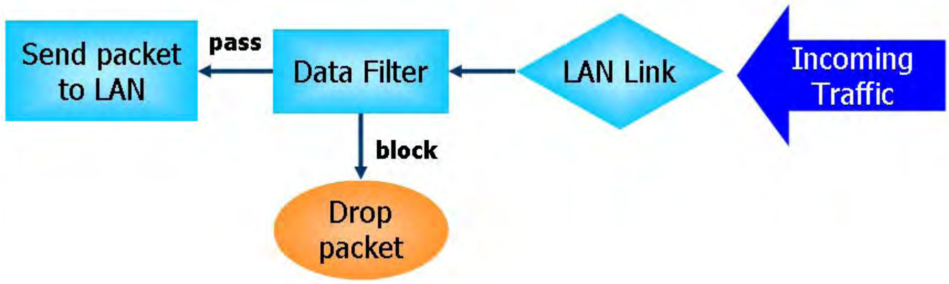
IP Filters

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.

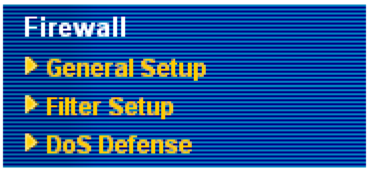
The **DoS Defense** function enables the Vigor router to inspect every incoming packet based on the attack signature database. Any malicious packet that might duplicate itself to paralyze the host in the secure LAN will be strictly blocked and a Syslog message will be sent as warning, if you set up Syslog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

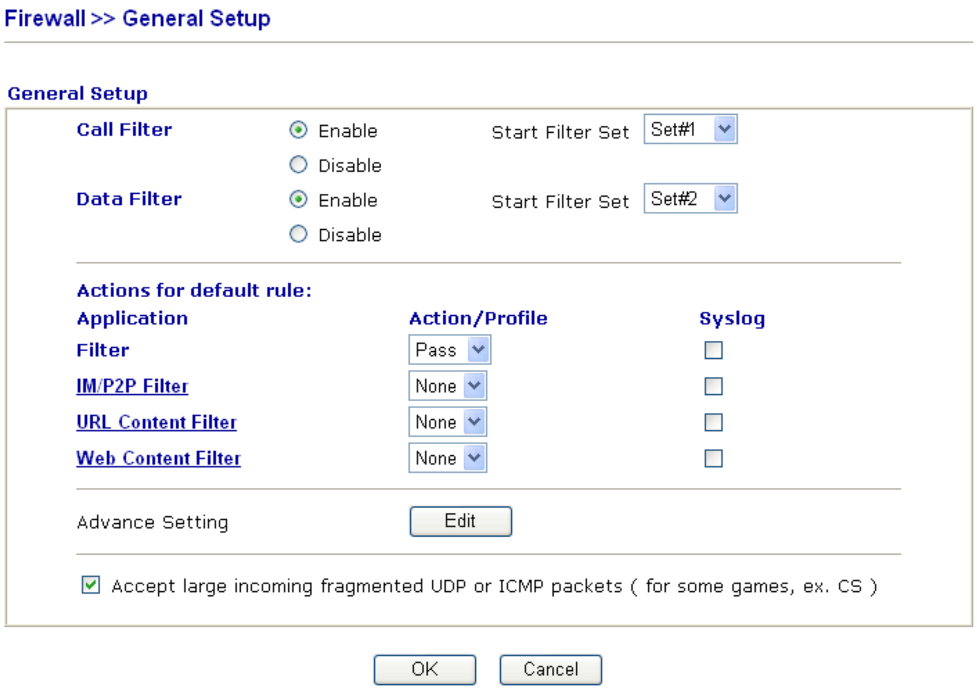
Below shows the menu items for Firewall.



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.



Firewall >> General Setup

General Setup

Call Filter ● Enable ○ Disable Start Filter Set Set#1

Data Filter ● Enable ○ Disable Start Filter Set Set#2

Actions for default rule:

Application	Action/Profile	Syslog
Filter	Pass	□
IM/P2P Filter	None	□
URL Content Filter	None	□
Web Content Filter	None	□

Advance Setting Edit

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

OK Cancel

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

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

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

IM/P2P Filter Select one of the **IM/P2P Filter Profile** settings (created in **CSM>> IM/P2P Filter**) for applying with this router. Please set at least one profile for choosing in **CSM>> IM/P2P Filter Profile** web page first. For troubleshooting needs, you can specify to record information for **IM/P2P Filter Profile** by checking the Log box. It will be sent to Syslog server. Please refer to section 5.14.5 **Syslog/Mail Alert** for more detailed information.

URL Content Filter Select one of the **URL Content Filter Profile** settings (created in **CSM>> URL Content Filter 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 5.14.5 **Syslog/Mail Alert** for more detailed information.

Web Content Filter Select one of the **Web Content Filter Profile** settings (created in **CSM>> Web Content Filter Profile**) for applying with this router.

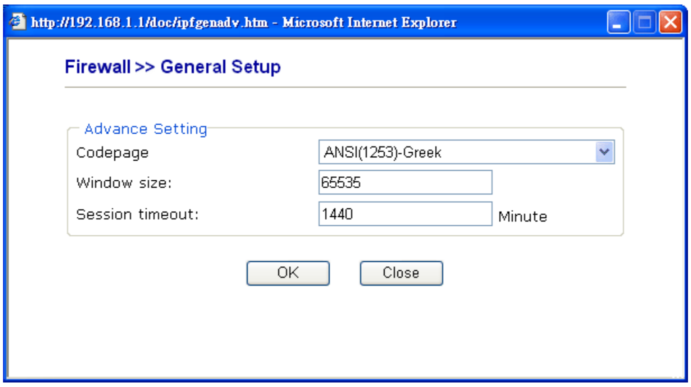
Please set at least one profile for anti-virus in **CSM>> Web Content Filter Profile** web page first. For troubleshooting needs, you can specify to record information for **Web Content Filter Profile** by checking the Log box. It will be sent to Syslog server. Please refer to section 5.14.5 **Syslog/Mail 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.



http://192.168.1.1/doc/ipfgenadv.htm - Microsoft Internet Explorer

Firewall >> General Setup

Advance Setting

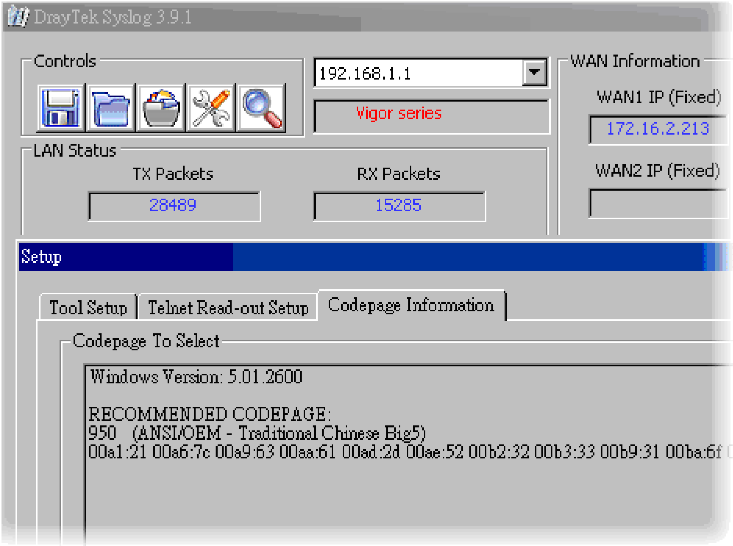
Codepage: ANSI(1253)-Greek

Window size: 65535

Session timeout: 1440 Minute

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.



DrayTek Syslog 3.9.1

Controls: 192.168.1.1

Vigor series

WAN Information

WAN1 IP (Fixed): 172.16.2.213

WAN2 IP (Fixed):

LAN Status

TX Packets: 28489

RX Packets: 15285

Setup

Codepage To Select

```
Windows Version: 5.01.2600

RECOMMENDED CODEPAGE:
950   (ANSI/OEM - Traditional Chinese Big5)
00a1:21 00a6:7c 00a9:63 00aa:61 00ad:2d 00ae:52 00b2:32 00b3:33 00b9:31 00ba:6f
```

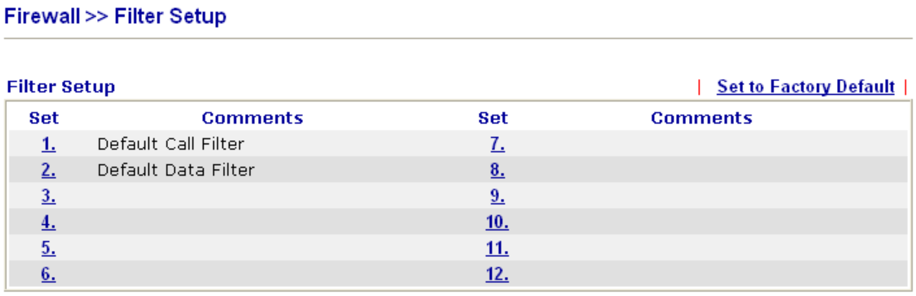
Window size – It determines the size of TCP protocol (0~65535). The more the value is, the better the performance will be. However, if the network is not stable, small value will be proper.

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

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

5.4.3 Filter Setup

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

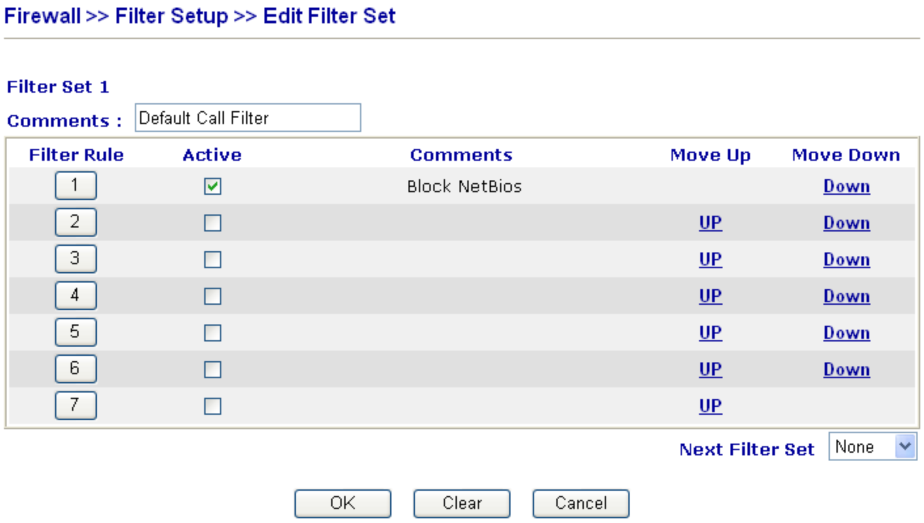


Firewall >> Filter Setup

Filter Setup | Set to Factory Default |

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

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



Firewall >> Filter Setup >> Edit Filter Set

Filter Set 1

Comments : Default Call Filter

Filter Rule	Active	Comments	Move Up	Move Down
1	☑	Block NetBios		Down
2	□		UP	Down
3	□		UP	Down
4	□		UP	Down
5	□		UP	Down
6	□		UP	Down
7	□		UP	

Next Filter Set None

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

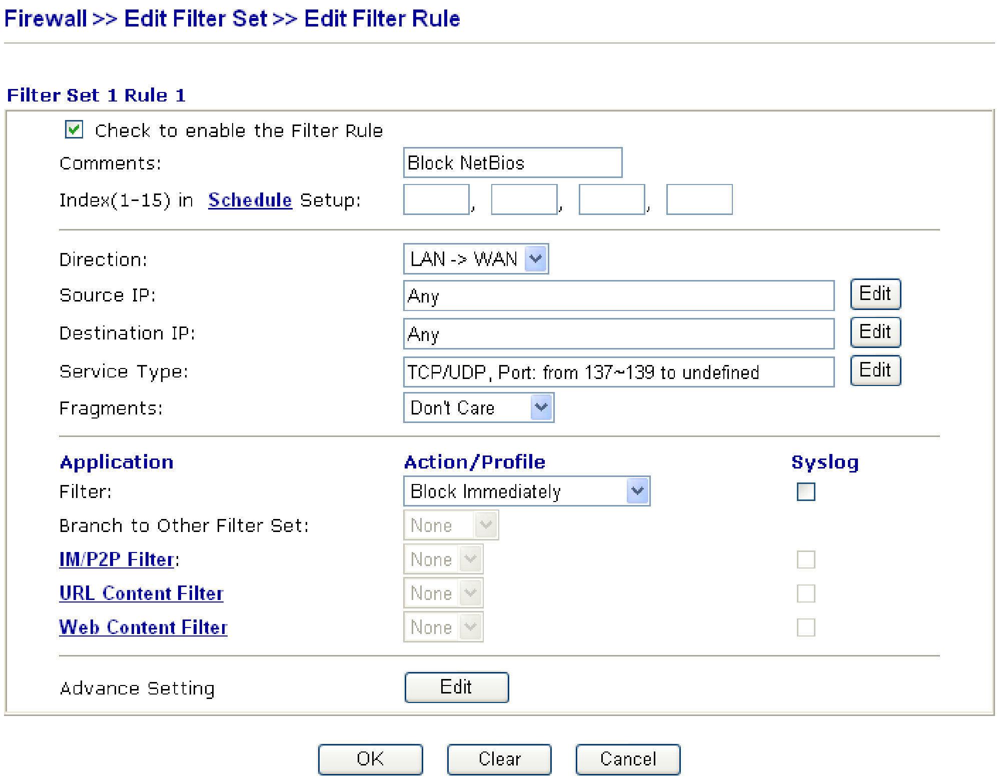
Active Enable or disable the filter rule.

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

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

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

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



Firewall >> Edit Filter Set >> Edit Filter Rule

Filter Set 1 Rule 1

☑ Check to enable the Filter Rule

Comments:	Block NetBios
Index(1-15) in Schedule Setup:	, , ,
Direction:	LAN -> WAN
Source IP:	Any [Edit]
Destination IP:	Any [Edit]
Service Type:	TCP/UDP, Port: from 137~139 to undefined [Edit]
Fragments:	Don't Care

Application	Action/Profile	Syslog
Filter:	Block Immediately	□
Branch to Other Filter Set:	None	
IM/P2P Filter:	None	□
URL Content Filter	None	□
Web Content Filter	None	□

Advance Setting [Edit]

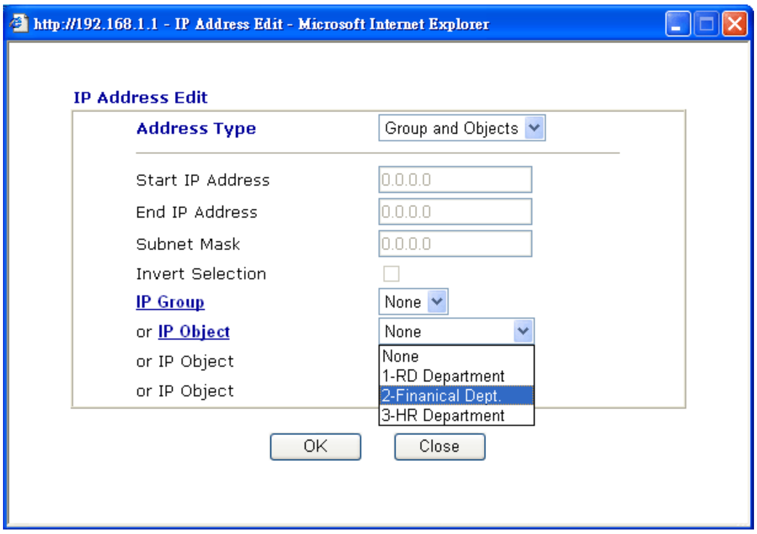
Check to enable the Filter Rule Check this box to enable the filter rule.

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

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


http://192.168.1.1 - IP Address Edit - Microsoft Internet Explorer

IP Address Edit

Address Type: Group and Objects

Start IP Address: 0.0.0.0

End IP Address: 0.0.0.0

Subnet Mask: 0.0.0.0

Invert Selection: □

IP Group: None

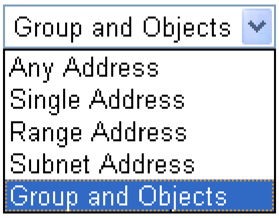
or IP Object: None

or IP Object

or IP Object

None
1-RD Department
2-Finanical Dept.
3-HR Department
OK
Close

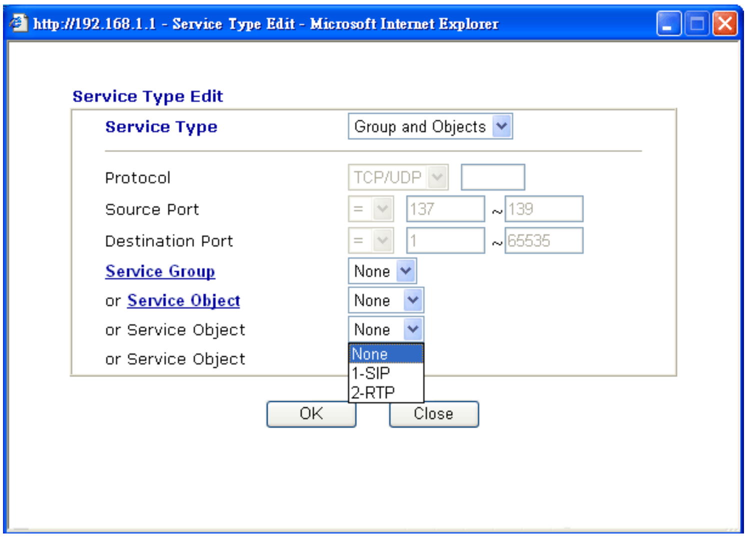
To set the IP address manually, please choose **Any Address/Single Address/Range Address/Subnet Address** as the Address Type and type them in this dialog. In addition, if you want to use the IP range from defined groups or objects, please choose **Group and Objects** as the Address Type.



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.


http://192.168.1.1 - Service Type Edit - Microsoft Internet Explorer

Service Type Edit

Service Type: Group and Objects

Protocol: TCP/UDP

Source Port: = 137 ~ 139

Destination Port: = 1 ~ 65535

Service Group: None

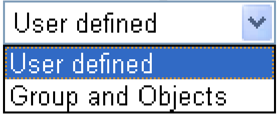
or Service Object: None

or Service Object: None

or Service Object

None
1-SIP
2-RTP
OK
Close

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



Protocol - Specify the protocol(s) which this filter rule will apply to.
Source/Destination Port -
(=) – when the first and last value are the same, it indicates one port; when the first and last values are different, it indicates a range for the port and available for this service type.
(!=) – when the first and last value are the same, it indicates all the ports except the port defined here; when the first and last values are different, it indicates that all the ports except the range defined here are available for this service type.
(>) – the port number greater than this value is available.
(<) – the port number less than this value is available for this profile.
Service Group/Object - Use the drop down list to choose the one that you want.

Fragments

Specify the action for fragmented packets. And it is used for **Data Filter** only.
Don't care -No action will be taken towards fragmented packets.
Unfragmented -Apply the rule to unfragmented packets.
Fragmented - Apply the rule to fragmented packets.
Too Short - Apply the rule only to packets that are too short to contain a complete header.

Filter

Specifies the action to be taken when packets match the rule.
Block Immediately - Packets matching the rule will be dropped immediately.
Pass Immediately - Packets matching the rule will be passed immediately.
Block If No Further Match - A packet matching the rule, and that does not match further rules, will be dropped.
Pass If No Further Match - A packet matching the rule, and that does not match further rules, will be passed through.

Branch to other Filter Set

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

IM/P2P Filter

Select one of the **IM/P2P Filter Profile** settings (created in **CSM>> IM/P2P Filter**) for applying with this router. Please set at least one profile for choosing in **CSM>> IM/P2P Filter Profile** web page first. For troubleshooting needs, you can specify to record information for **IM/P2P Filter Profile** by checking the Log box. It will be sent to Syslog server. Please refer to section 5.14.5 **Syslog/Mail Alert** for more detailed information.

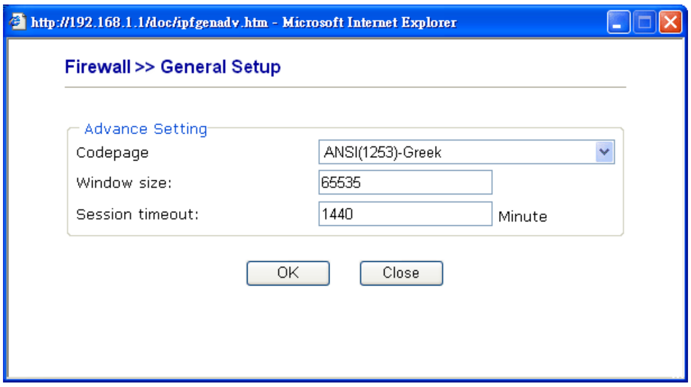
URL Content Filter

Select one of the **URL Content Filter** profile settings (created in **CSM>> URL Content Filter**) for applying with this router. Please set at least one profile for choosing in **CSM>> URL Content Filter** web page first. For troubleshooting needs, you can specify to record information for **URL Content Filter** by checking the Log box. It will be sent to Syslog server. Please refer to section 5.14.5 **Syslog/Mail Alert** for more detailed information.

Web Content Filter Select one of the **Web Content Filter** profile settings (created in **CSM>> Web Content Filter**) for applying with this router. Please set at least one profile for anti-virus in **CSM>> Web Content Filter** web page first. For troubleshooting needs, you can specify to record information for **Web Content Filter** by checking the Log box. It will be sent to Syslog server. Please refer to section 5.14.5 **Syslog/Mail Alert** for more detailed information.

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

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



http://192.168.1.1/doc/ipfgenadv.htm - Microsoft Internet Explorer

Firewall >> General Setup

Advance Setting

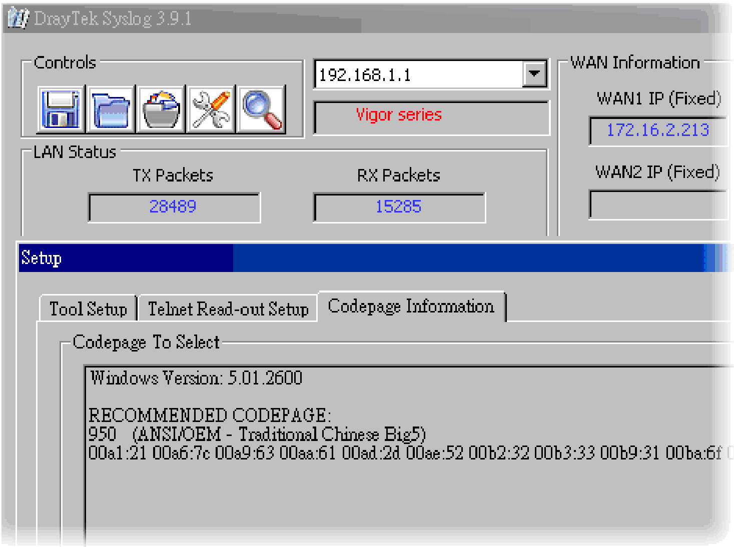
Codepage: ANSI(1253)-Greek

Window size: 65535

Session timeout: 1440 Minute

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.



192.168.1.1

Vigor series

WAN Information

WAN1 IP (Fixed) 172.16.2.213

WAN2 IP (Fixed)

TX Packets 28489

RX Packets 15285

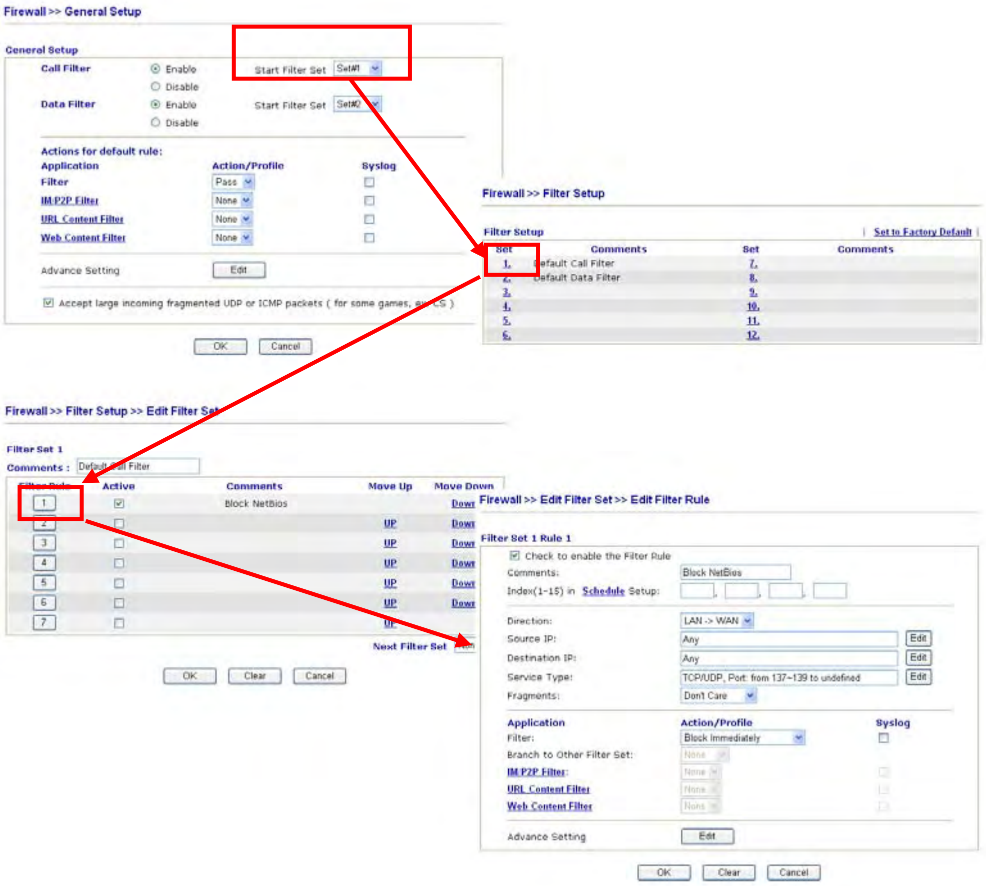
```
Windows Version: 5.01.2600

RECOMMENDED CODEPAGE:
950   (ANSI/OEM - Traditional Chinese Big5)
00a1:21 00a6:7c 00a9:63 00aa:61 00ad:2d 00ae:52 00b2:32 00b3:33 00b9:31 00ba:6f
```

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

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

Example

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



Firewall >> General Setup

General Setup

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

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

Actions for default rule:

Application	Action/Profile	Syslog
Filter	Pass	□
IM/P2P Filter	None	□
URL Content Filter	None	□
Web Content Filter	None	□

Advance Setting: Edit

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

Firewall >> Filter Setup

Filter Setup | Set to Factory Default |

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

Firewall >> Filter Setup >> Edit Filter Set

Filter Set 1

Comments : Default Call Filter

Filter Rule	Active	Comments	Move Up	Move Down
1	☑	Block NetBios		Down
2	□		UP	Down
3	□		UP	Down
4	□		UP	Down
5	□		UP	Down
6	□		UP	Down
7	□		UP	

Next Filter Set

Firewall >> Edit Filter Set >> Edit Filter Rule

Filter Set 1 Rule 1

☑ Check to enable the Filter Rule

Comments: Block NetBios

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

Direction: LAN -> WAN

Source IP: Any

Destination IP: Any

Service Type: TCP/UDP, Port: from 137~139 to undefined

Fragments: Don't Care

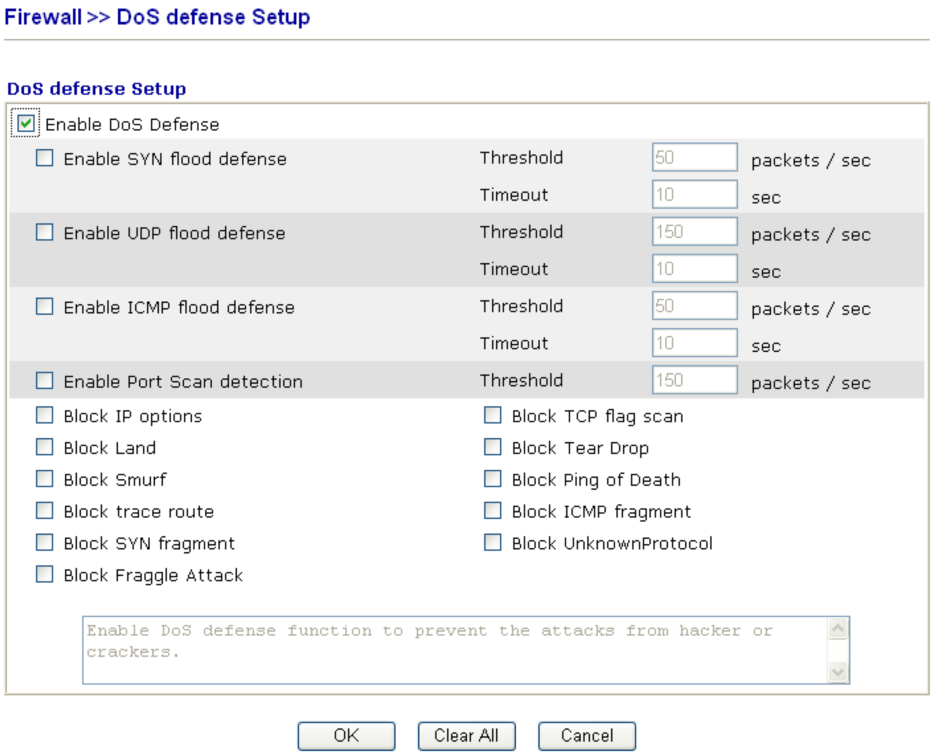
Application	Action/Profile	Syslog
Filter:	Block Immediately	□
Branch to Other Filter Set:	None	
IM/P2P Filter:	None	□
URL Content Filter	None	□
Web Content Filter	None	□

Advance Setting: Edit

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.



Firewall >> DoS defense Setup

DoS defense Setup

☑ Enable DoS Defense

□ Enable SYN flood defense	Threshold	50	packets / sec
	Timeout	10	sec
□ Enable UDP flood defense	Threshold	150	packets / sec
	Timeout	10	sec
□ Enable ICMP flood defense	Threshold	50	packets / sec
	Timeout	10	sec
□ Enable Port Scan detection	Threshold	150	packets / sec

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

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

Enable Dos Defense Check the box to activate the DoS Defense Functionality.

Enable SYN flood defense Check the box to activate the SYN flood defense function. Once detecting the Threshold of the TCP SYN packets from the Internet has exceeded the defined value, the Vigor router will start to randomly discard the subsequent TCP SYN packets for a period defined in Timeout. The goal for this is prevent the TCP SYN packets' attempt to exhaust the limited-resource of Vigor router. By default, the threshold and timeout values are set to 50 packets per second and 10 seconds, respectively.

Enable UDP flood defense Check the box to activate the UDP flood defense function. Once detecting the Threshold of the UDP packets from the Internet has exceeded the defined value, the Vigor router will start to randomly discard the subsequent UDP packets for a period defined in Timeout. The default setting for threshold and timeout are 150 packets per second and 10 seconds, respectively.

Enable ICMP flood defense Check the box to activate the ICMP flood defense function. Similar to the UDP flood defense function, once if the Threshold of ICMP packets from Internet has exceeded the defined value, the router will discard the ICMP echo requests coming from the Internet. The default setting for threshold and timeout are 50 packets per second and 10 seconds, respectively.

Enable PortScan detection Port Scan attacks the Vigor router by sending lots of packets to many ports in an attempt to find ignorant services would respond. Check the box to activate the Port Scan detection. Whenever detecting this malicious exploration behavior by monitoring the port-scanning Threshold rate, the Vigor router will send out a warning. By default, the Vigor router sets the threshold as 150 packets per second.

Block IP options Check the box to activate the Block IP options function. The Vigor router will ignore any IP packets with IP option field in the datagram header. The reason for limitation is IP option appears to be a vulnerability of the security for the LAN because it will carry significant information, such as security, TCC (closed user group) parameters, a series of Internet addresses, routing messages...etc. An eavesdropper outside might learn the details of your private networks.

Block Land Check the box to enforce the Vigor router to defense the Land attacks. The Land attack combines the SYN attack technology with IP spoofing. A Land attack occurs when an attacker sends spoofed SYN packets with the identical source and destination addresses, as well as the port number to victims.

Block Smurf Check the box to activate the Block Smurf function. The Vigor router will ignore any broadcasting ICMP echo request.

Block trace router Check the box to enforce the Vigor router not to forward any trace route packets.

Block SYN fragment Check the box to activate the Block SYN fragment function. The Vigor router will drop any packets having SYN flag and more fragment bit set.

Block Fraggle Attack Check the box to activate the Block fraggle Attack function. Any broadcast UDP packets received from the Internet is blocked. Activating the DoS/DDoS defense functionality might block some legal packets. For example, when you activate the fraggle attack defense, all broadcast UDP packets coming from the Internet are blocked. Therefore, the RIP packets from the Internet might be dropped.

Block TCP flag scan Check the box to activate the Block TCP flag scan function. Any TCP packet with anomaly flag setting is dropped. Those scanning activities include *no flag scan*, *FIN without ACK scan*, *SYN FINscan*, *Xmas scan* and *full Xmas scan*.

Block Tear Drop Check the box to activate the Block Tear Drop function. Many machines may crash when receiving ICMP datagrams (packets) that exceed the maximum length. To avoid this type of attack, the Vigor router is designed to be capable of discarding any fragmented ICMP packets with a length greater than 1024 octets.

Block Ping of Death Check the box to activate the Block Ping of Death function. This attack involves the perpetrator sending overlapping packets to the target hosts so that those target hosts will hang once they re-construct the packets. The Vigor routers will block any packets realizing this attacking activity.

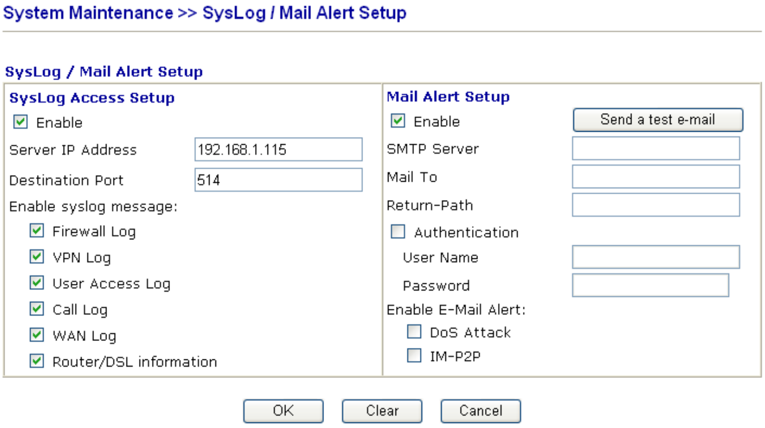
Block ICMP Fragment Check the box to activate the Block ICMP fragment function. Any ICMP packets with more fragment bit set are dropped.

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

Warning Messages

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

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



System Maintenance >> SysLog / Mail Alert Setup

SysLog / Mail Alert Setup

SysLog Access Setup

☑ Enable

Server IP Address: 192.168.1.115

Destination Port: 514

Enable syslog message:

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

Mail Alert Setup

☑ Enable

SMTP Server:

Mail To:

Return-Path:

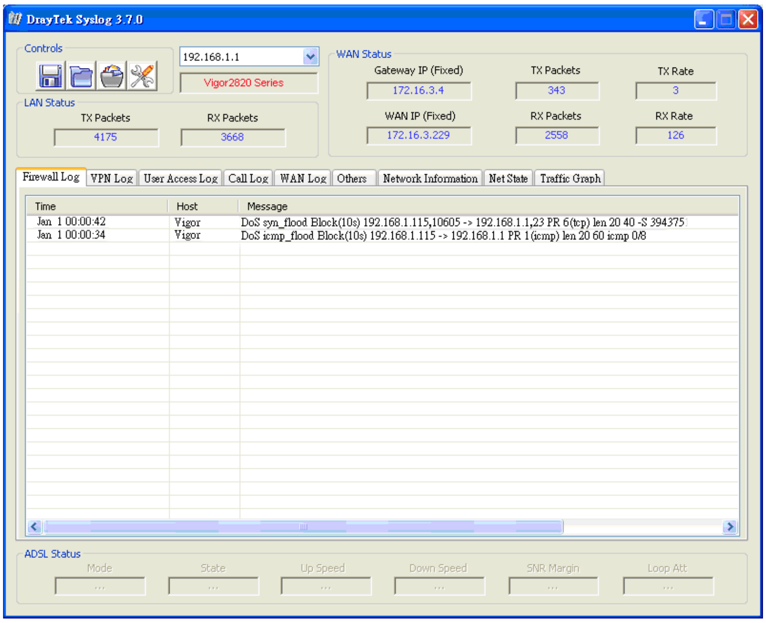
☐ Authentication

User Name:

Password:

Enable E-Mail Alert:

☐ DoS Attack
☐ IM-P2P



DrayTek Syslog 3.7.0

Controls: 192.168.1.1 — Vigor2820 Series

LAN Status

TX Packets: 4175
RX Packets: 3668

WAN Status

Gateway IP (Fixed): 172.16.3.4
TX Packets: 343
TX Rate: 3
WAN IP (Fixed): 172.16.3.229
RX Packets: 2558
RX Rate: 126

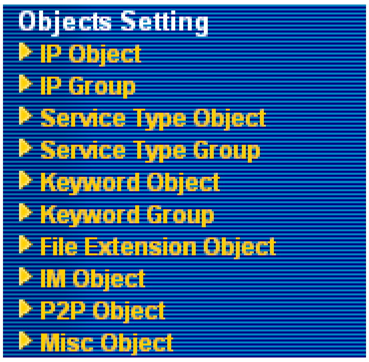
Time	Host	Message
Jan 1 00:00:42	Vigor	DoS syn_flood Block(10s) 192.168.1.115,10605 -> 192.168.1.1,23 PR 6(tcp) len 20 40 -S 394375
Jan 1 00:00:34	Vigor	DoS icmp_flood Block(10s) 192.168.1.115 -> 192.168.1.1 PR 1(icmp) len 20 60 icmp 0/8

ADSL Status

Mode	State	Up Speed	Down Speed	SNR Margin	Loop Att
...	...	...	...	...	...

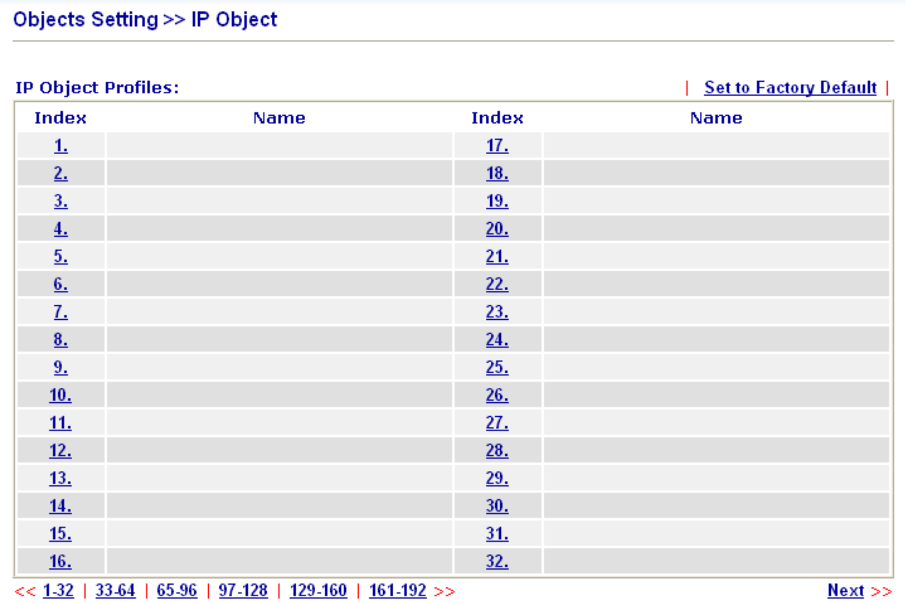
5.5 Objects Settings

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.



Objects Setting >> IP Object

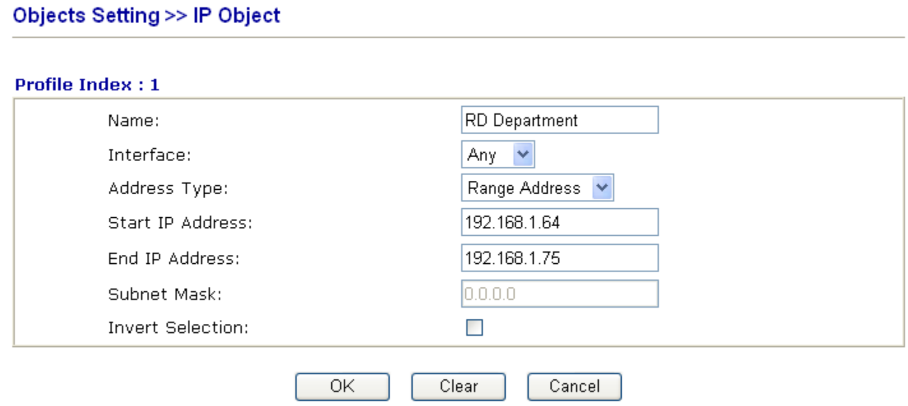
IP Object Profiles: | Set to Factory Default |

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

<< 1-32 | 33-64 | 65-96 | 97-128 | 129-160 | 161-192 >> Next >>

Set to Factory Default Clear all profiles.

Click the number under Index column for settings in detail.

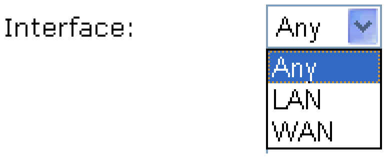


Objects Setting >> IP Object

Profile Index : 1

Name:	RD Department
Interface:	Any
Address Type:	Range Address
Start IP Address:	192.168.1.64
End IP Address:	192.168.1.75
Subnet Mask:	0.0.0.0
Invert Selection:	□

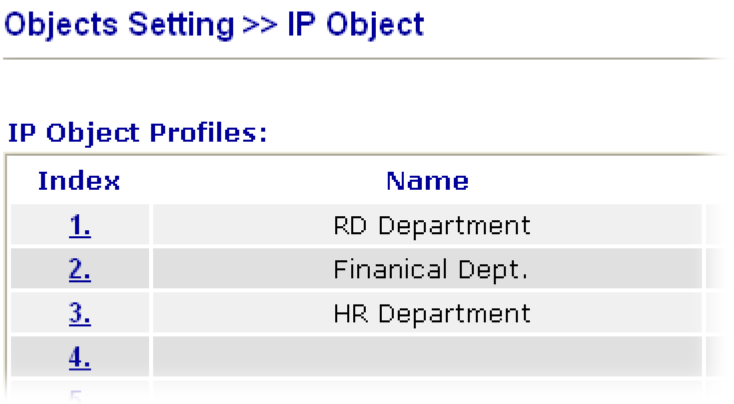
Name	Type a name for this profile. Maximum 15 characters are allowed.
Interface	Choose a proper interface (WAN, LAN or Any).


Interface: 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.

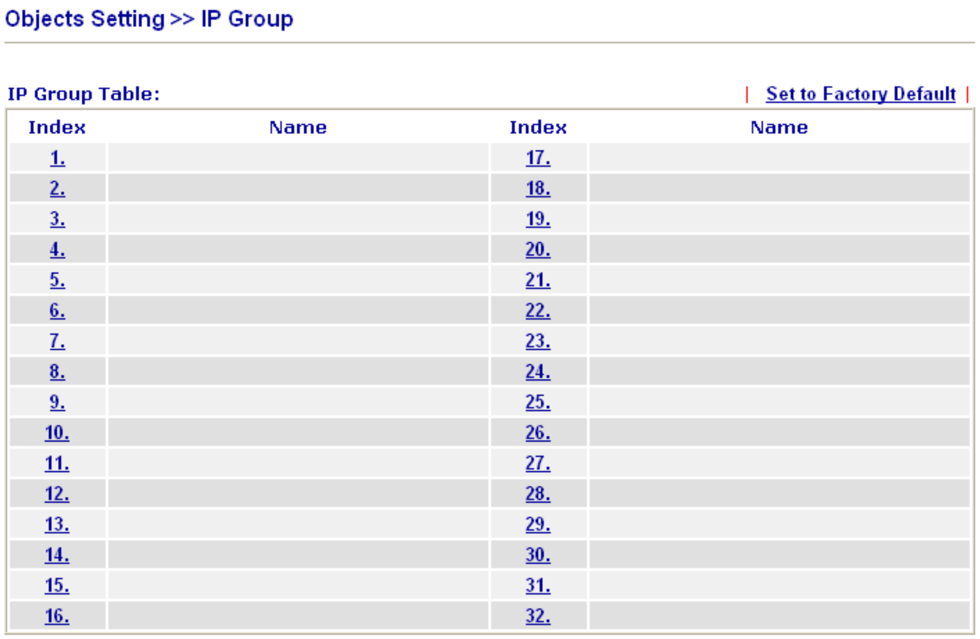

Objects Setting >> IP Object

IP Object Profiles:

Index	Name
1.	RD Department
2.	Finanical Dept.
3.	HR Department
4.	

5.5.2 IP Group

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



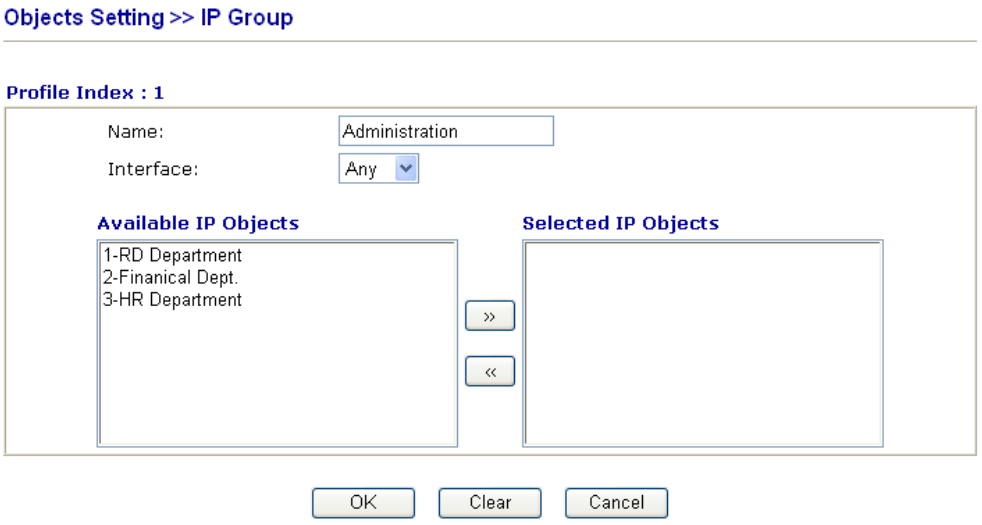
Objects Setting >> IP Group

IP Group Table: | Set to Factory Default |

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

Set to Factory Default Clear all profiles.

Click the number under Index column for settings in detail.



Objects Setting >> IP Group

Profile Index : 1

Name: Administration

Interface: Any

Available IP Objects

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

Selected IP Objects

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

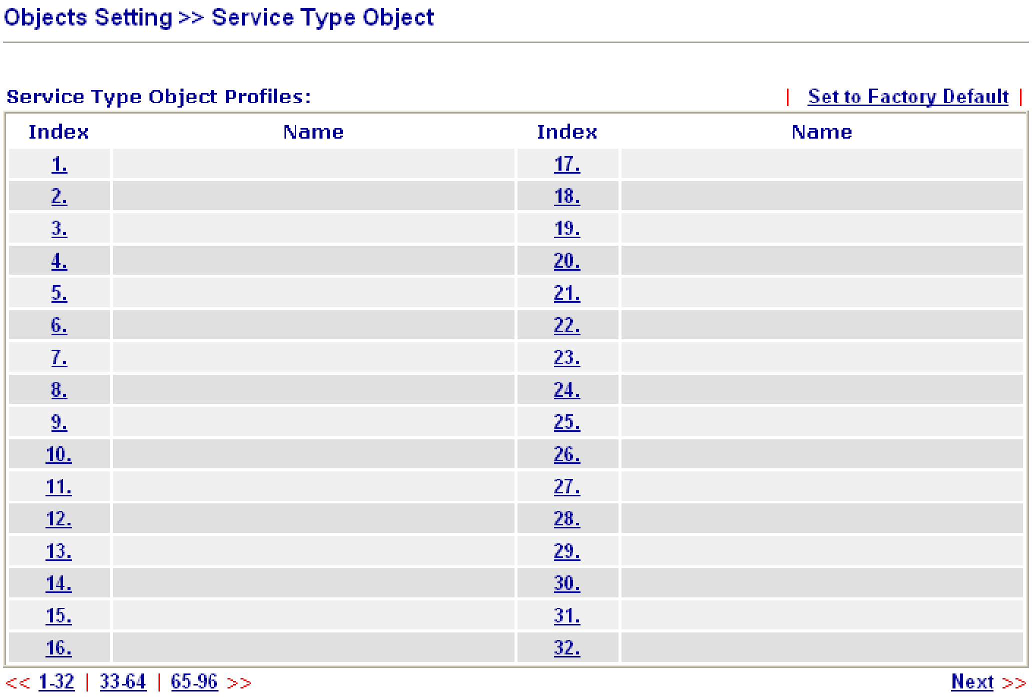
Interface Choose WAN, LAN or Any to display all the available IP objects with the specified interface.

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.



Objects Setting >> Service Type Object

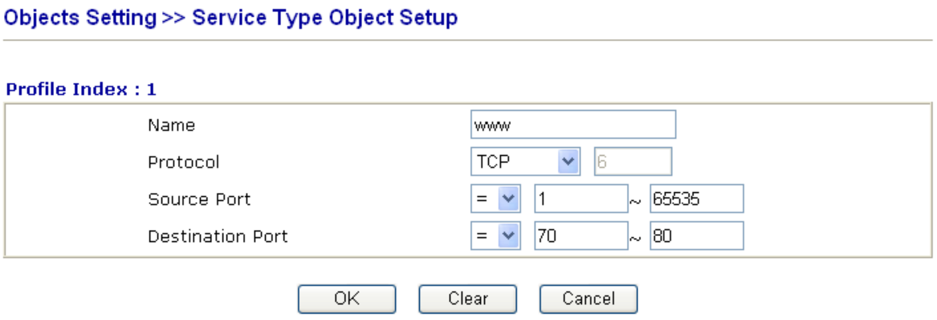
Service Type Object Profiles: | Set to Factory Default |

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

<< 1-32 | 33-64 | 65-96 >> Next >>

Set to Factory Default Clear all profiles.

Click the number under Index column for settings in detail.



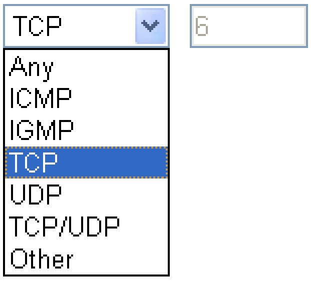
Objects Setting >> Service Type Object Setup

Profile Index : 1

Name	www
Protocol	TCP 6
Source Port	= 1 ~ 65535
Destination Port	= 70 ~ 80

Name Type a name for this profile.

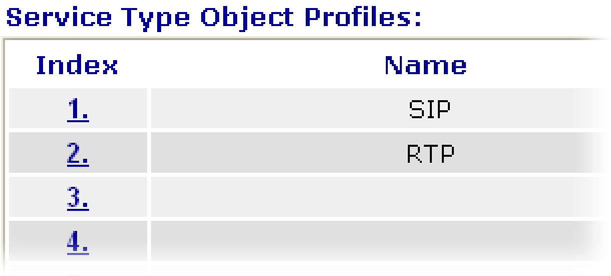
Protocol Specify the protocol(s) which this profile will apply to.



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.

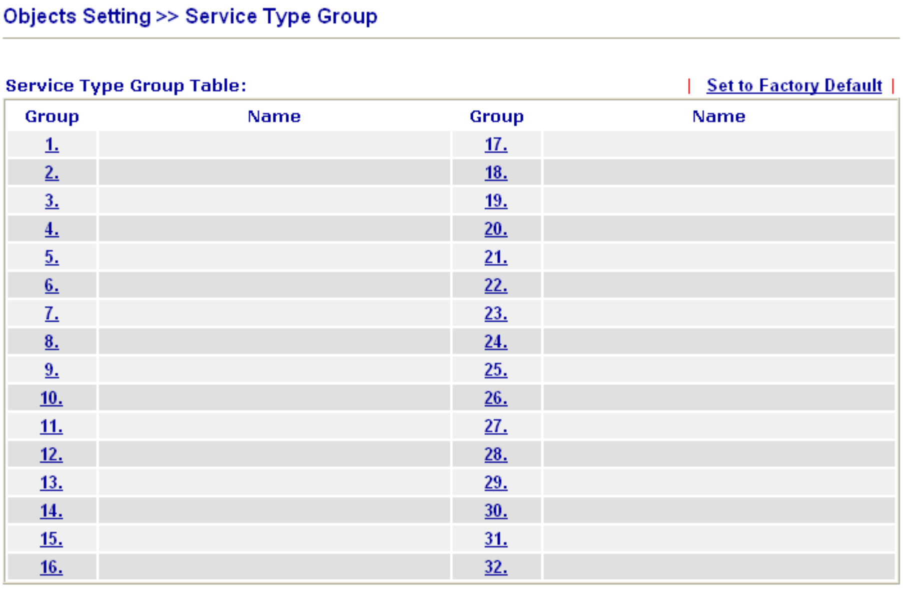


Service Type Object Profiles:

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.



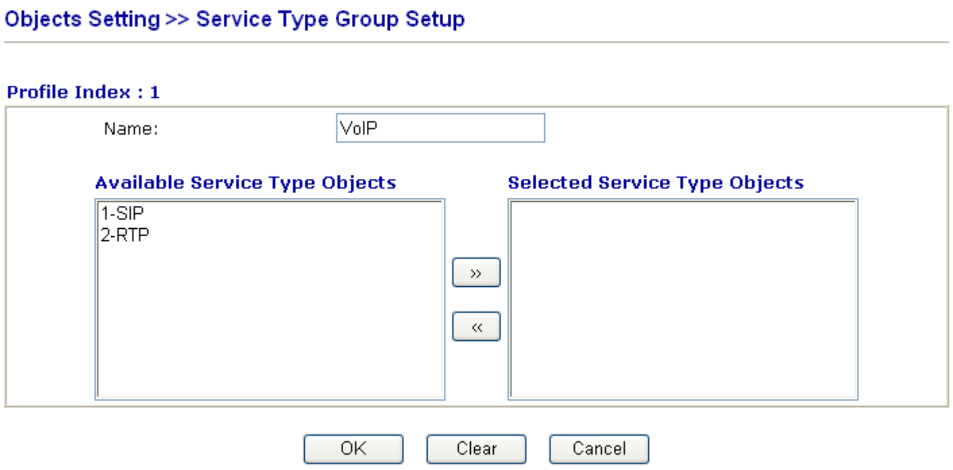
Objects Setting >> Service Type Group

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.



Objects Setting >> Service Type Group Setup

Profile Index : 1

Name: VoIP

Available Service Type Objects

1-SIP
2-RTP

Selected Service Type Objects

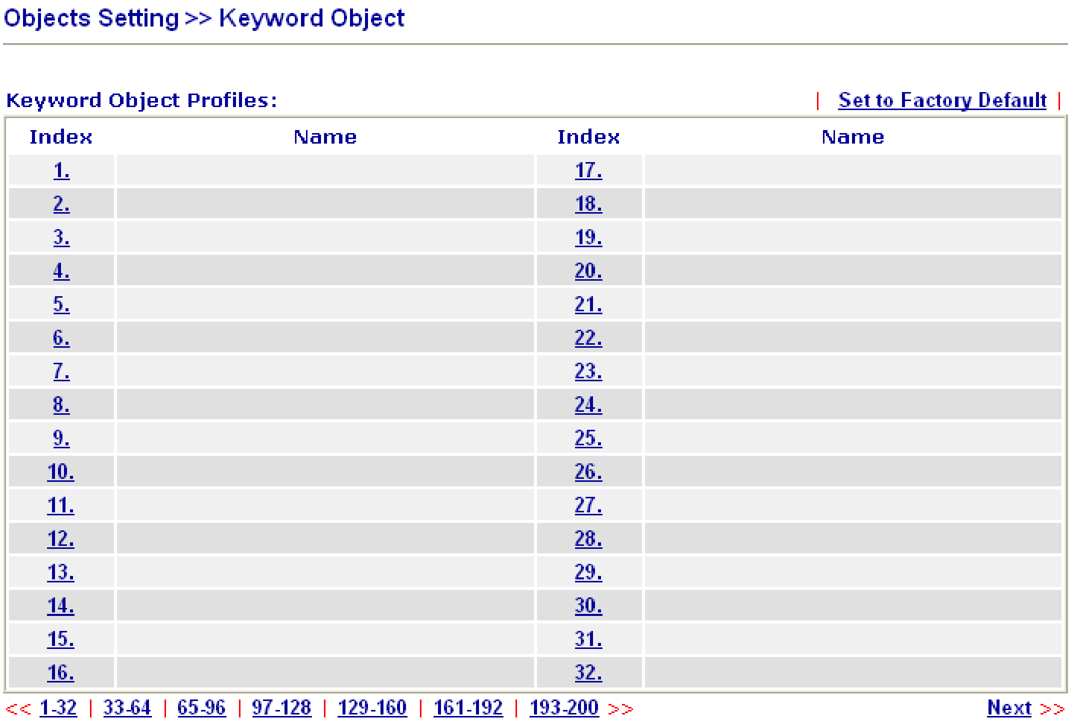
Name Type a name for this profile.

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.**



Objects Setting >> Keyword Object

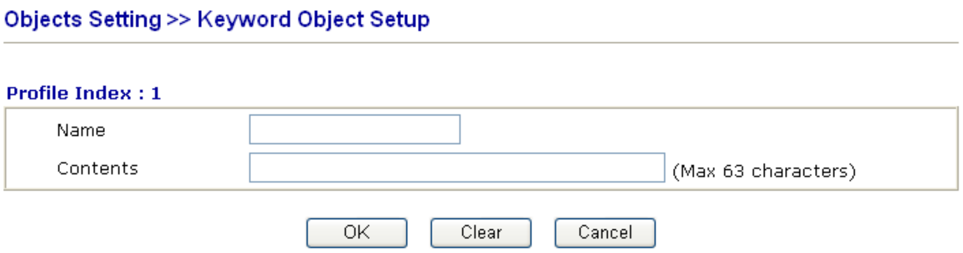
Keyword Object Profiles: | Set to Factory Default |

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

<< 1-32 | 33-64 | 65-96 | 97-128 | 129-160 | 161-192 | 193-200 >> Next >>

Set to Factory Default Clear all profiles.

Click the number under Index column for setting in detail.



Objects Setting >> Keyword Object Setup

Profile Index : 1

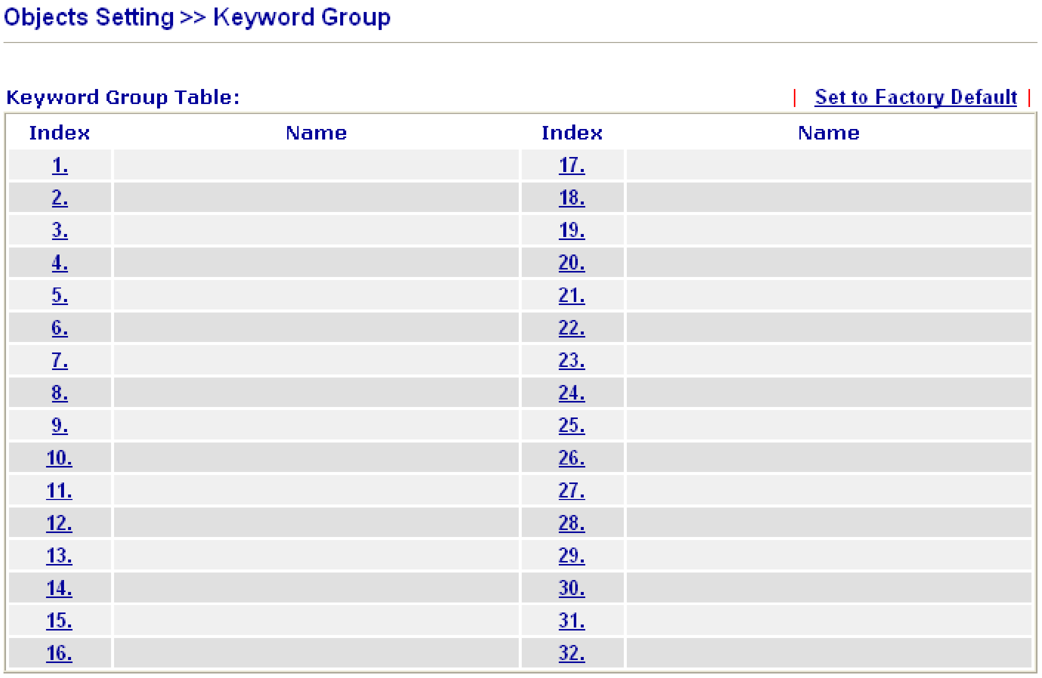
Name		
Contents		(Max 63 characters)

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**.



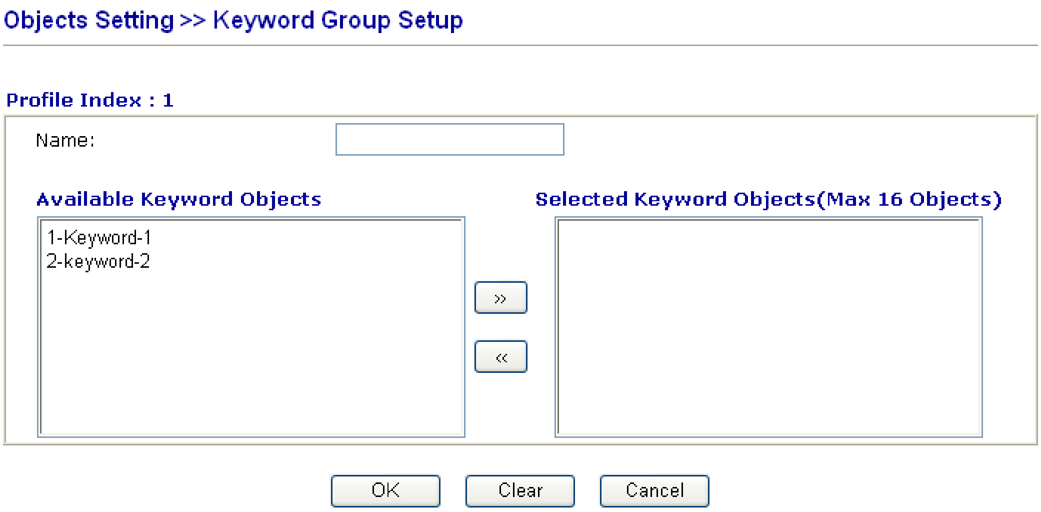
Objects Setting >> Keyword Group

Keyword Group Table:

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

Set to Factory Default Clear all profiles.

Click the number under Index column for setting in detail.



Objects Setting >> Keyword Group Setup

Profile Index : 1

Name:

Available Keyword Objects

1-Keyword-1
2-keyword-2

Selected Keyword Objects(Max 16 Objects)

Name Type a name for this group.

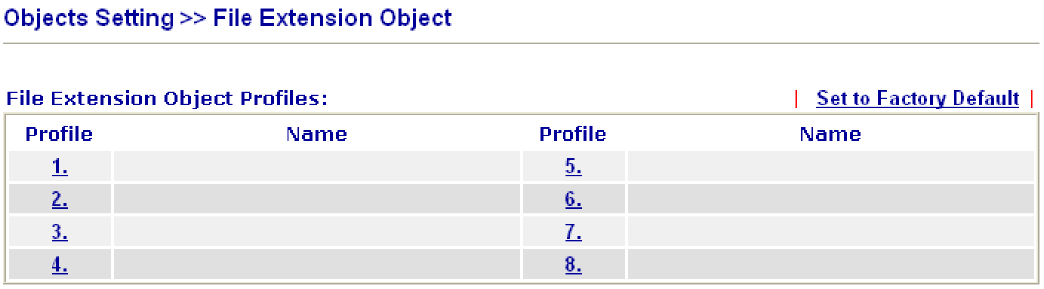
Available Keyword Objects You can gather keyword objects from Keyword Object page within one keyword group. All the available Keyword objects that you have created will be shown in this box.

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

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.



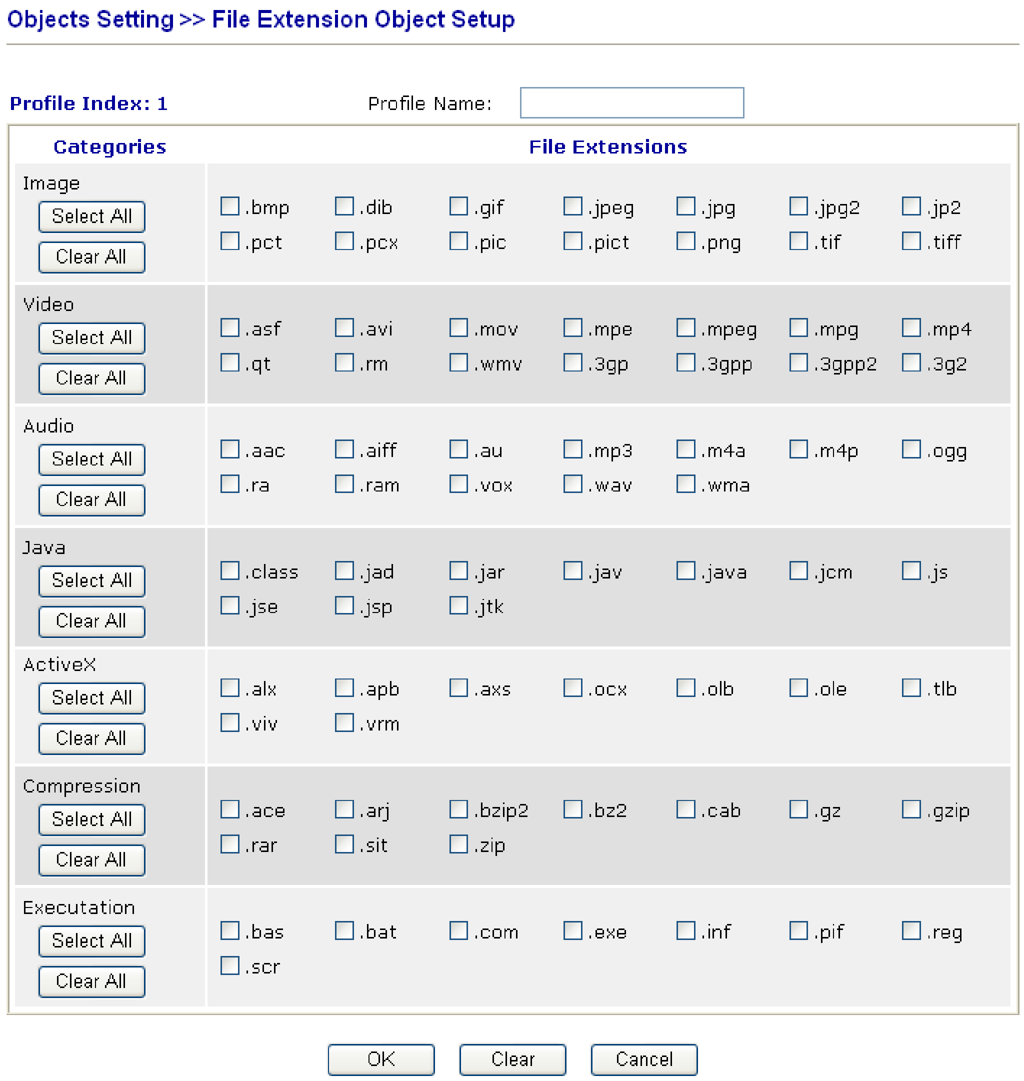
Objects Setting >> File Extension Object

File Extension Object Profiles: | Set to Factory Default |

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

Set to Factory Default Clear all profiles.

Click the number under Profile column for configuration in details.



Objects Setting >> File Extension Object Setup

Profile Index: 1 Profile Name:

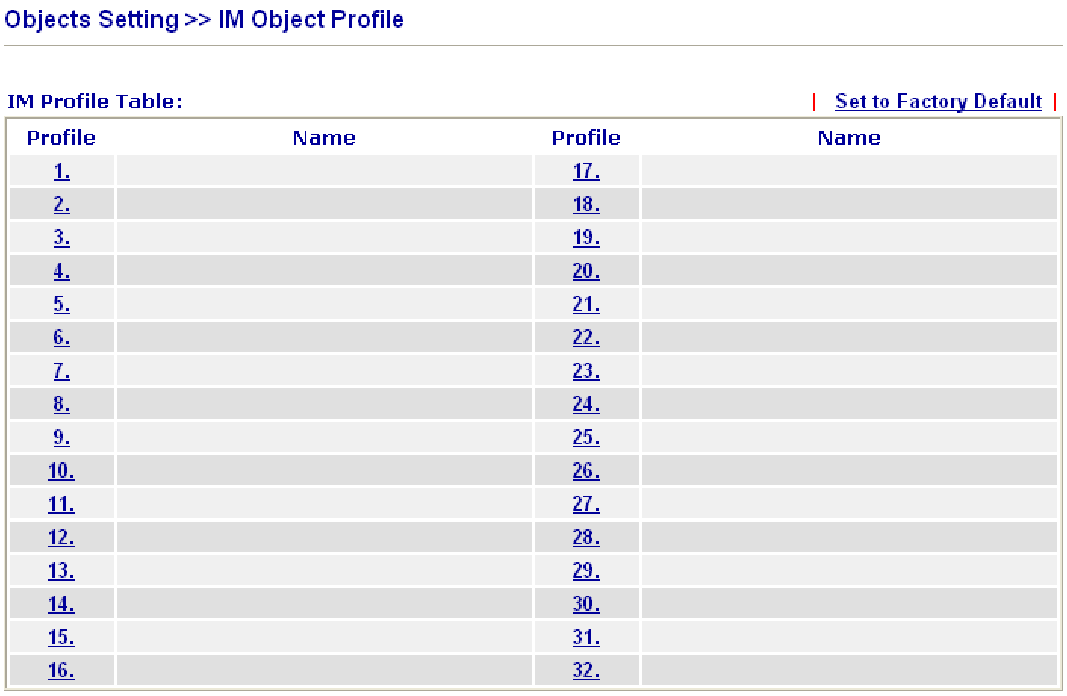
Categories	File Extensions						
Image Select All Clear All	□ .bmp	□ .dib	□ .gif	□ .jpeg	□ .jpg	□ .jpg2	□ .jp2
	□ .pct	□ .pcx	□ .pic	□ .pict	□ .png	□ .tif	□ .tiff
Video Select All Clear All	□ .asf	□ .avi	□ .mov	□ .mpe	□ .mpeg	□ .mpg	□ .mp4
	□ .qt	□ .rm	□ .wmv	□ .3gp	□ .3gpp	□ .3gpp2	□ .3g2
Audio Select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

Profile Name Type a name for this profile.

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

5.5.8 IM Object

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



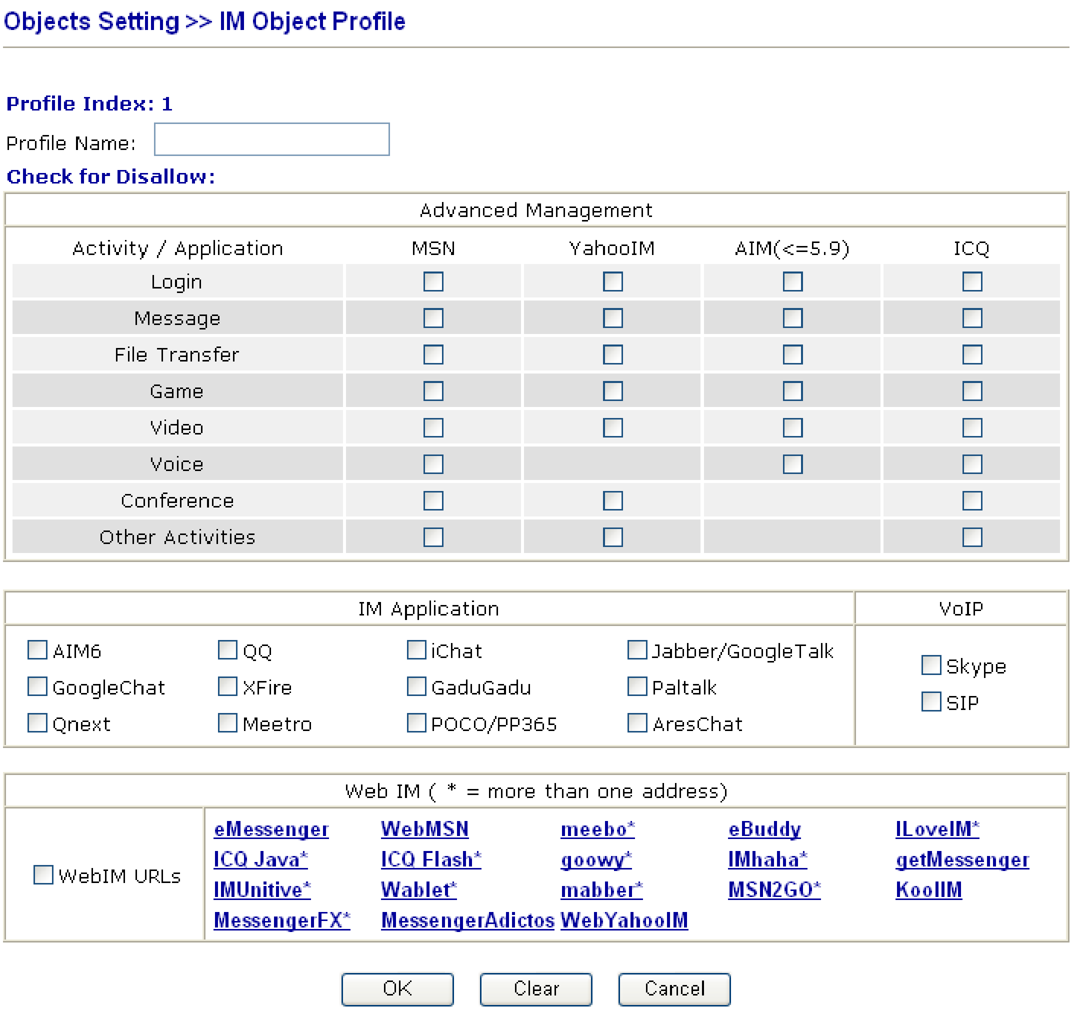
Objects Setting >> IM Object Profile

IM Profile Table: | Set to Factory Default |

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

Set to Factory Default Clear all profiles.

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



Objects Setting >> IM Object Profile

Profile Index: 1

Profile Name:

Check for Disallow:

Advanced Management

Activity / Application	MSN	YahooIM	AIM(<=5.9)	ICQ
Login	□	□	□	□
Message	□	□	□	□
File Transfer	□	□	□	□
Game	□	□	□	□
Video	□	□	□	□
Voice	□		□	□
Conference	□	□		□
Other Activities	□	□		□

IM Application				VoIP
□ AIM6	□ QQ	□ iChat	□ Jabber/GoogleTalk	□ Skype
□ GoogleChat	□ XFire	□ GaduGadu	□ Paltalk	□ SIP
□ Qnext	□ Meetro	□ POCO/PP365	□ AresChat	

Web IM (* = more than one address)

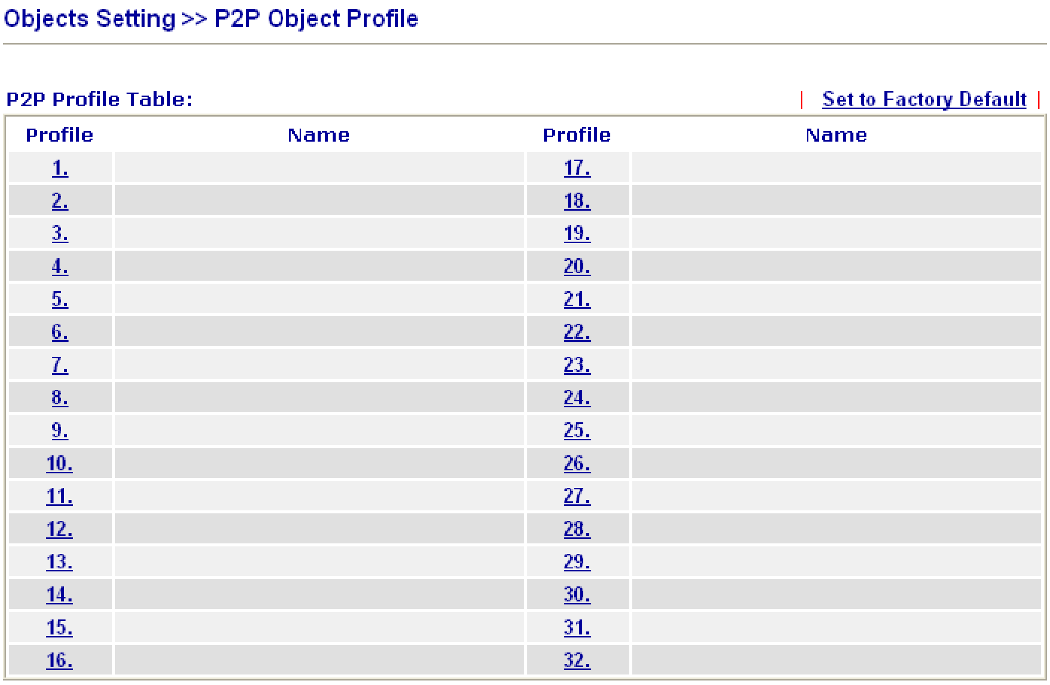
□ WebIM URLs	eMessenger	WebMSN	meebo*	eBuddy	ILoveIM*
	ICQ Java*	ICQ Flash*	goowy*	IMhaha*	getMessenger
	IMUnitive*	Wablet*	mabber*	MSN2GO*	KoolIM
	MessengerFX*	MessengerAdictos	WebYahooIM		

Profile Name Type a name for this profile.

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

5.5.9 P2P Object

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



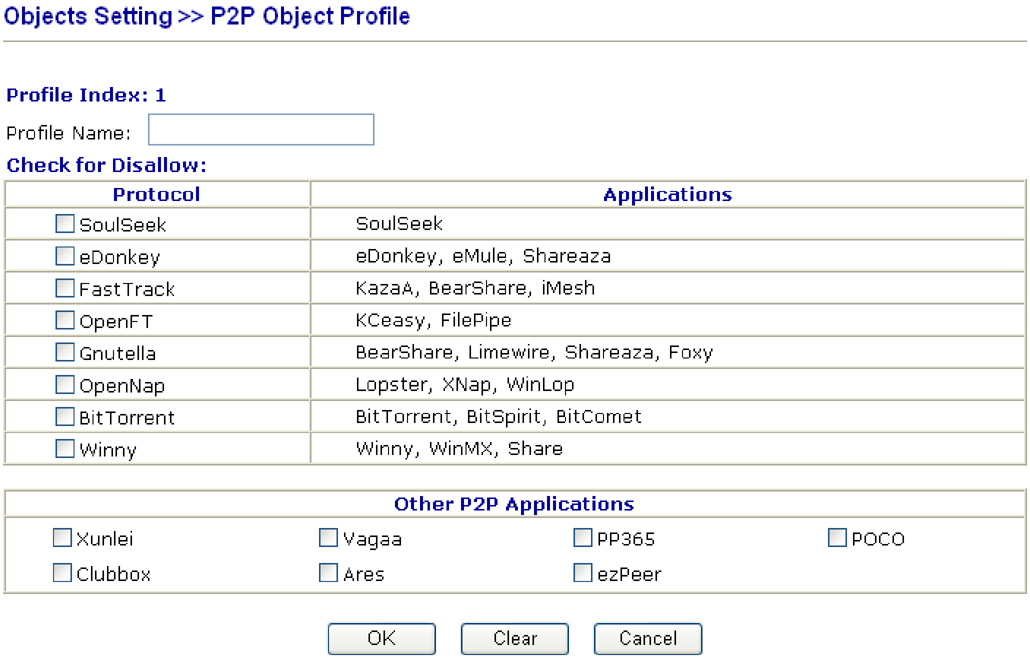
Objects Setting >> P2P Object Profile

P2P Profile Table: | Set to Factory Default |

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

Set to Factory Default Clear all profiles.

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



Objects Setting >> P2P Object Profile

Profile Index: 1

Profile Name:

Check for Disallow:

Protocol	Applications
□ SoulSeek	SoulSeek
□ eDonkey	eDonkey, eMule, Shareaza
□ FastTrack	KazaA, BearShare, iMesh
□ OpenFT	KCeasy, FilePipe
□ Gnutella	BearShare, Limewire, Shareaza, Foxy
□ OpenNap	Lopster, XNap, WinLop
□ BitTorrent	BitTorrent, BitSpirit, BitComet
□ Winny	Winny, WinMX, Share

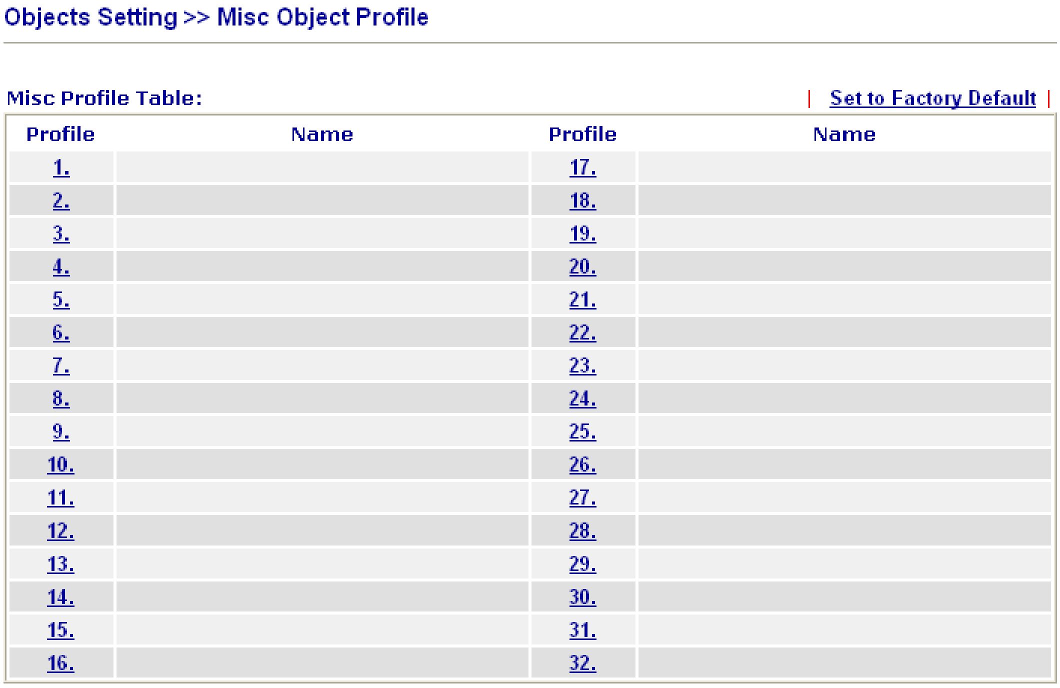
Other P2P Applications			
□ Xunlei	□ Vagaa	□ PP365	□ POCO
□ Clubbox	□ Ares	□ ezPeer	

Profile Name Type a name for this profile.

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

5.5.10 Misc Object

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



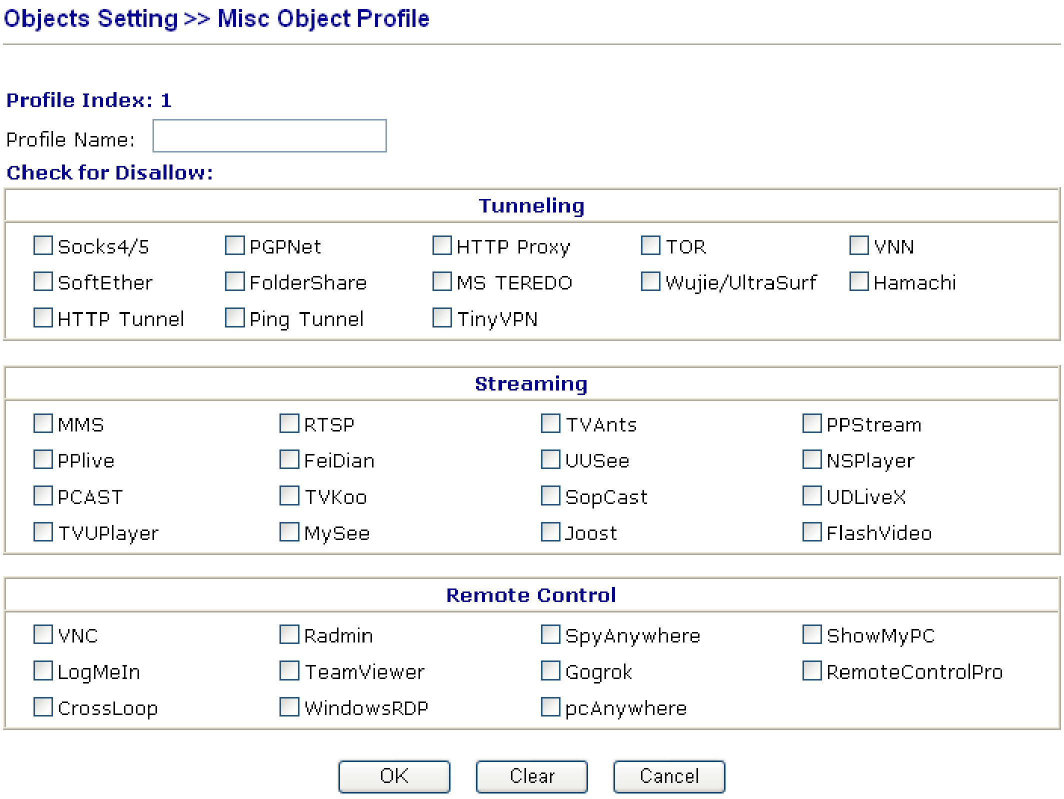
Objects Setting >> Misc Object Profile

Misc Profile Table: | Set to Factory Default |

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

Set to Factory Default Clear all profiles.

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



Objects Setting >> Misc Object Profile

Profile Index: 1

Profile Name:

Check for Disallow:

Tunneling

□ Socks4/5	□ PGPNet	□ HTTP Proxy	□ TOR	□ VNN
□ SoftEther	□ FolderShare	□ MS TEREDO	□ Wujie/UltraSurf	□ Hamachi
□ HTTP Tunnel	□ Ping Tunnel	□ TinyVPN		

Streaming

□ MMS	□ RTSP	□ TVAnts	□ PPStream
□ PPlive	□ FeiDian	□ UUSee	□ NSPlayer
□ PCAST	□ TVKoo	□ SopCast	□ UDLiveX
□ TVUPlayer	□ MySee	□ Joost	□ FlashVideo

Remote Control

□ VNC	□ Radmin	□ SpyAnywhere	□ ShowMyPC
□ LogMeIn	□ TeamViewer	□ Gogrok	□ RemoteControlPro
□ CrossLoop	□ WindowsRDP	□ pcAnywhere	

Profile Name Type a name for this profile.

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

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.

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

IM/P2P Filter

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

URL Content Filter

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

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

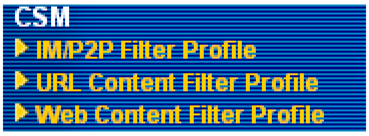
On the other hand, Vigor router can prevent user from accidentally downloading malicious codes from web pages. It's very common that malicious codes conceal in the executable objects, such as ActiveX, Java Applet, compressed files, and other executable files. Once downloading these types of files from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

Web Content Filter

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

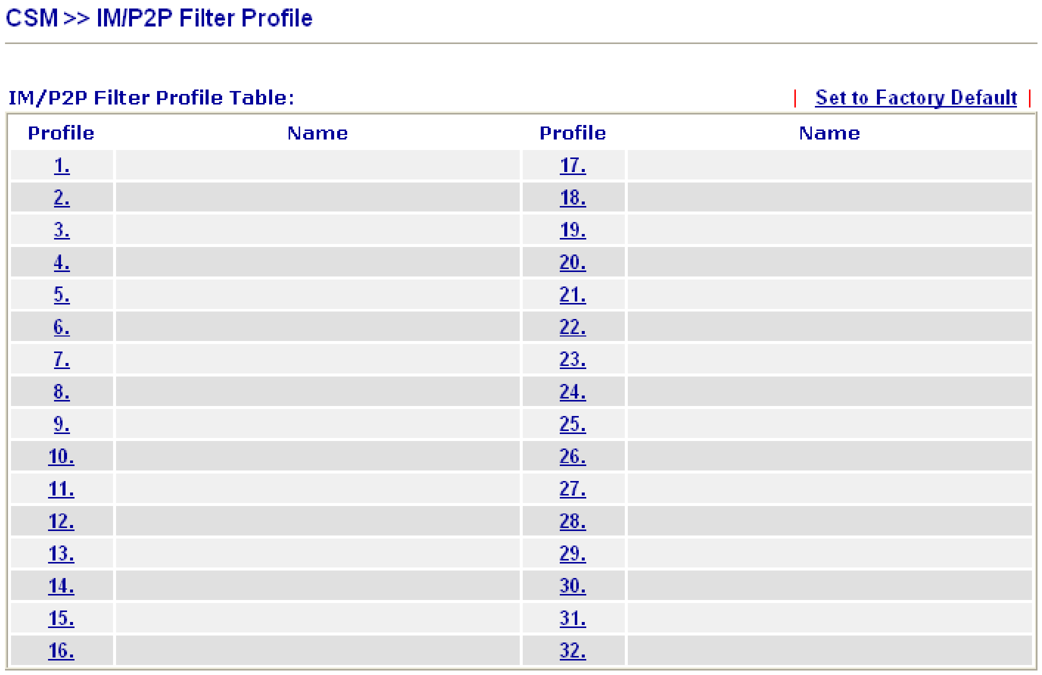
Once you have activated your Web Filtering service in Vigor router and chosen the categories of website you wish to restrict, each URL address requested (e.g.www.bbc.co.uk) will be checked against our server database. This database is updated as frequent as daily by a global team of Internet researchers.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

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



5.6.1 IM/P2P Filter Profile

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



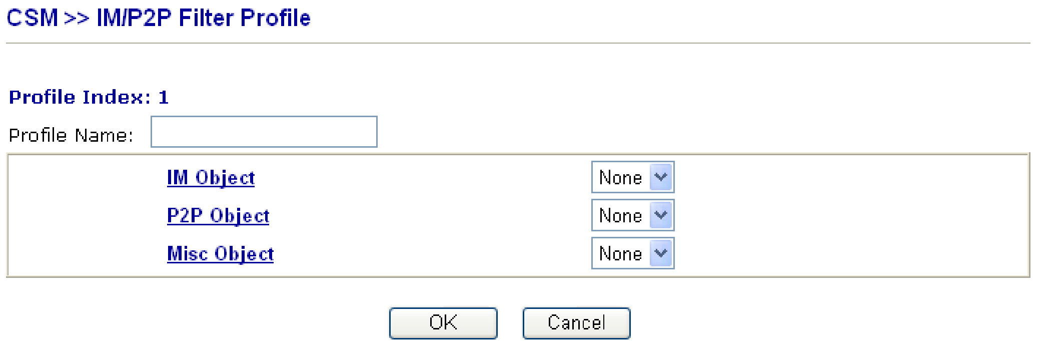
CSM >> IM/P2P Filter Profile

IM/P2P Filter Profile Table:

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

Set to Factory Default Clear all profiles.

Click the number under Index column for settings in detail.



CSM >> IM/P2P Filter Profile

Profile Index: 1

Profile Name:

IM Object	None
P2P Object	None
Misc Object	None

Profile Name Type a name for the CSM profile.

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

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.

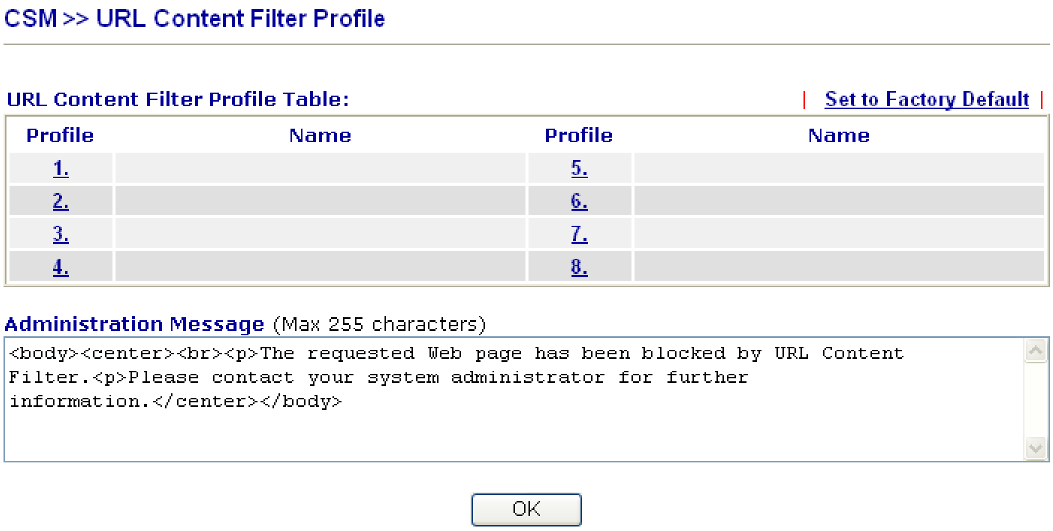
Once a user type in or click on an URL with objectionable keywords, URL keyword blocking facility will decline the HTTP request to that web page thus can limit user’s access to the website. You may imagine **URL Content Filter** as a well-trained convenience-store clerk who won’t sell adult magazines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



CSM >> URL Content Filter Profile

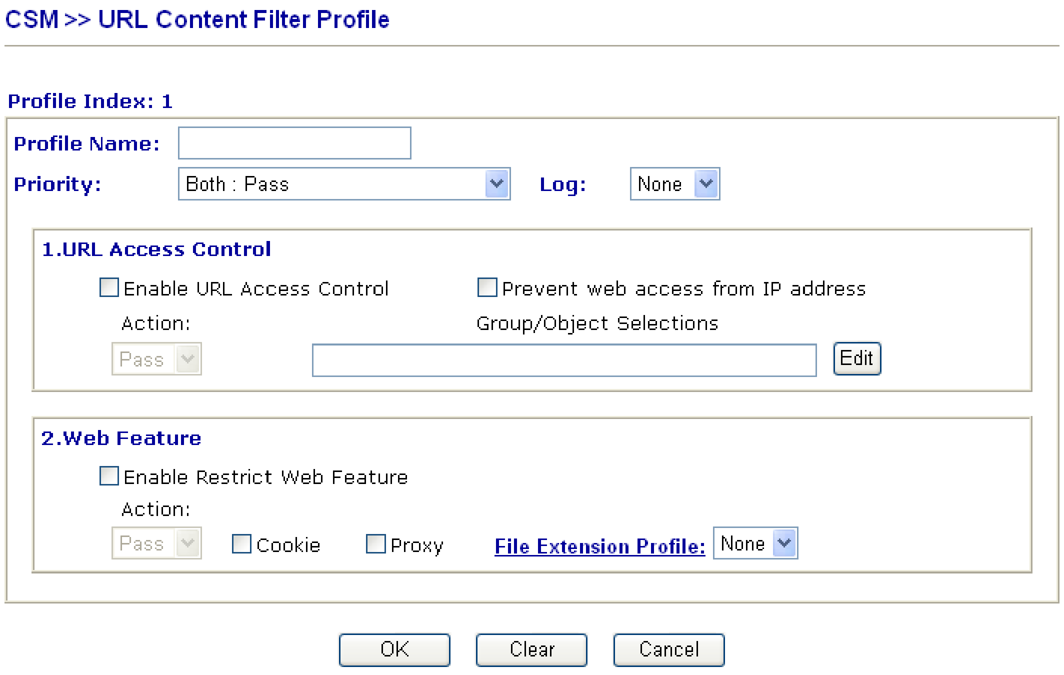
URL Content Filter Profile Table: | Set to Factory Default |

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

Administration Message (Max 255 characters)

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

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



CSM >> URL Content Filter Profile

Profile Index: 1

Profile Name:

Priority: Both : Pass   Log: None

1.URL Access Control

□ Enable URL Access Control   □ Prevent web access from IP address

Action: Pass   Group/Object Selections:

2.Web Feature

□ Enable Restrict Web Feature

Action: Pass   □ Cookie   □ Proxy   File Extension Profile: None

Profile Name Type the name for such profile.

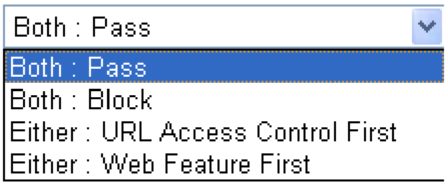
Priority It determines the action that this router will apply.

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.

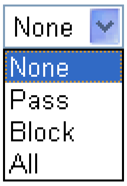


Log **None** – There is no log file will be recorded for this profile.

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

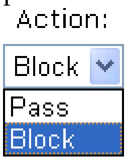
Enable URL Access Control - Check the box to activate URL Access Control. Note that the priority for **URL Access Control** is higher than **Restrict Web Feature**. If the web content match the setting set in URL Access Control, the router will execute the action specified in this field and ignore the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

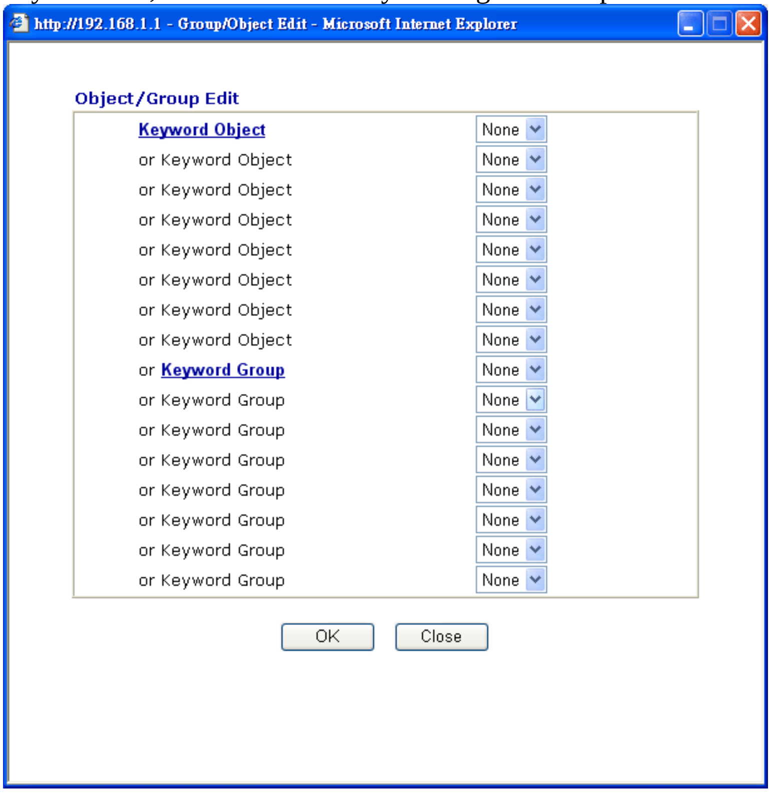
Action – This setting is available only when **Either : URL Access Control First** or **Either : Web Feature First** is selected. ***Pass* -** Allow accessing into the corresponding webpage with the keywords listed on the box below.

***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.



http://192.168.1.1 - Group/Object Edit - Microsoft Internet Explorer

Object/Group Edit

Keyword Object	None
or Keyword Object	None
or Keyword Object	None
or Keyword Object	None
or Keyword Object	None
or Keyword Object	None
or Keyword Object	None
or Keyword Object	None
or Keyword Group	None
or Keyword Group	None
or Keyword Group	None
or Keyword Group	None
or Keyword Group	None
or Keyword Group	None
or Keyword Group	None
or Keyword Group	None

Web Feature

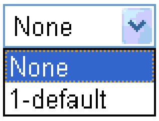
Enable Restrict Web Feature - Check this box to make the keyword being blocked or passed.

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.

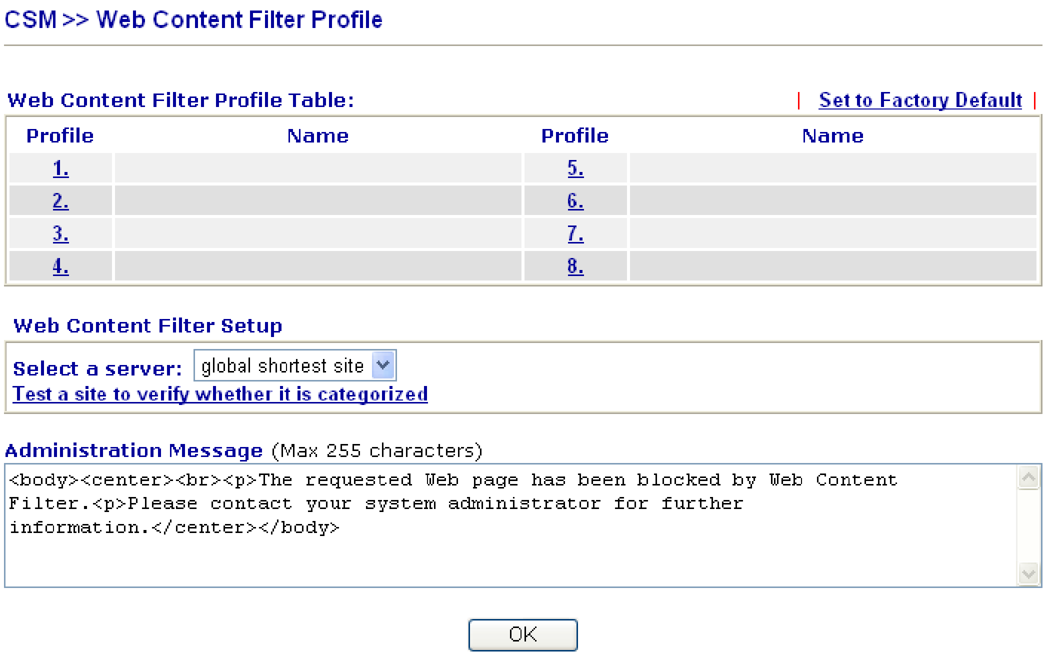


5.6.3 Web Content Filter Profile

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

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

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



CSM >> Web Content Filter Profile

Web Content Filter Profile Table: | Set to Factory Default |

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

Web Content Filter Setup

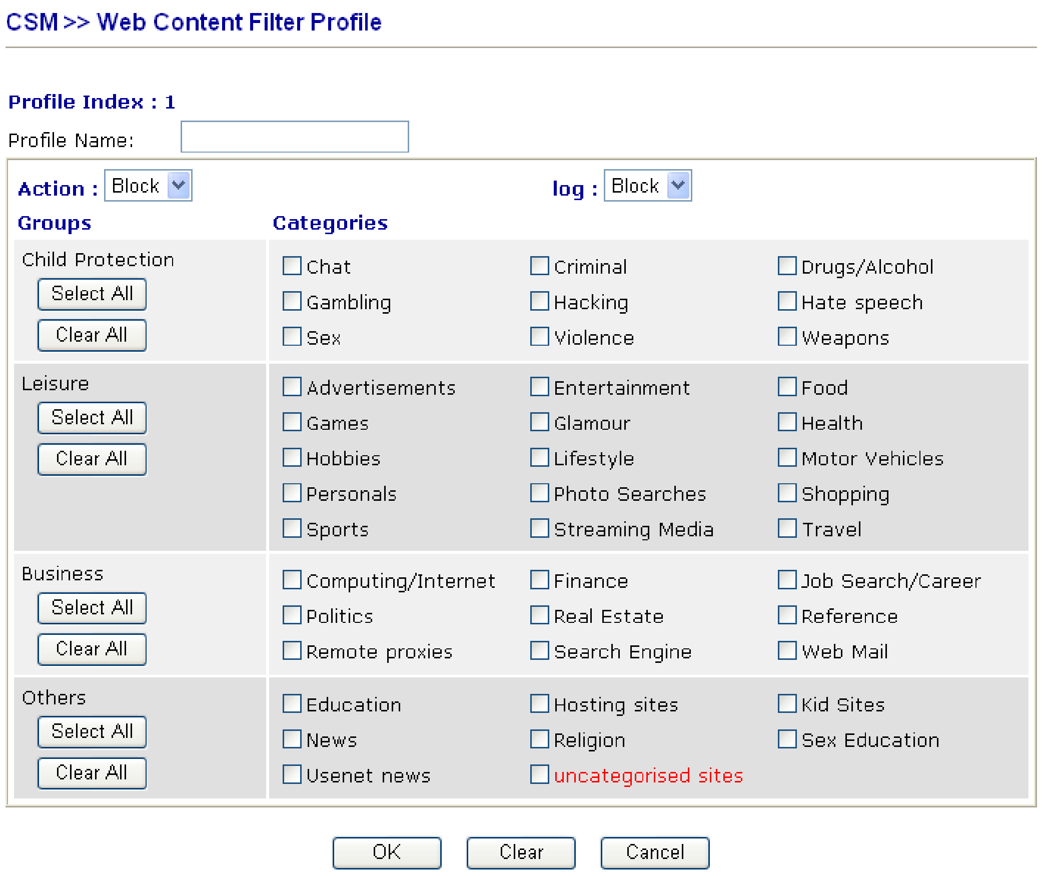
Select a server: global shortest site

Test a site to verify whether it is categorized

Administration Message (Max 255 characters)

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

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



CSM >> Web Content Filter Profile

Profile Index : 1

Profile Name:

Action : Block

log : Block

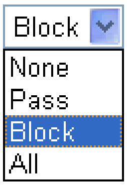
Groups	Categories		
Child Protection Select All Clear All	□ Chat □ Gambling □ Sex	□ Criminal □ Hacking □ Violence	□ Drugs/Alcohol □ Hate speech □ Weapons
Leisure Select All Clear All	□ Advertisements □ Games □ Hobbies □ Personals □ Sports	□ Entertainment □ Glamour □ Lifestyle □ Photo Searches □ Streaming Media	□ Food □ Health □ Motor Vehicles □ Shopping □ Travel
Business Select All Clear All	□ Computing/Internet □ Politics □ Remote proxies	□ Finance □ Real Estate □ Search Engine	□ Job Search/Career □ Reference □ Web Mail
Others Select All Clear All	□ Education □ News □ Usenet news	□ Hosting sites □ Religion □ uncategorised sites	□ Kid Sites □ Sex Education

Action

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

Log

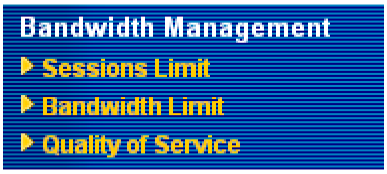
None – There is no log file will be recorded for this profile.
Pass – Only the log about Pass will be recorded in Syslog.
Block – Only the log about Block will be recorded in Syslog.
All – All the actions (Pass and Block) will be recorded in Syslog.



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

5.7 Bandwidth Management

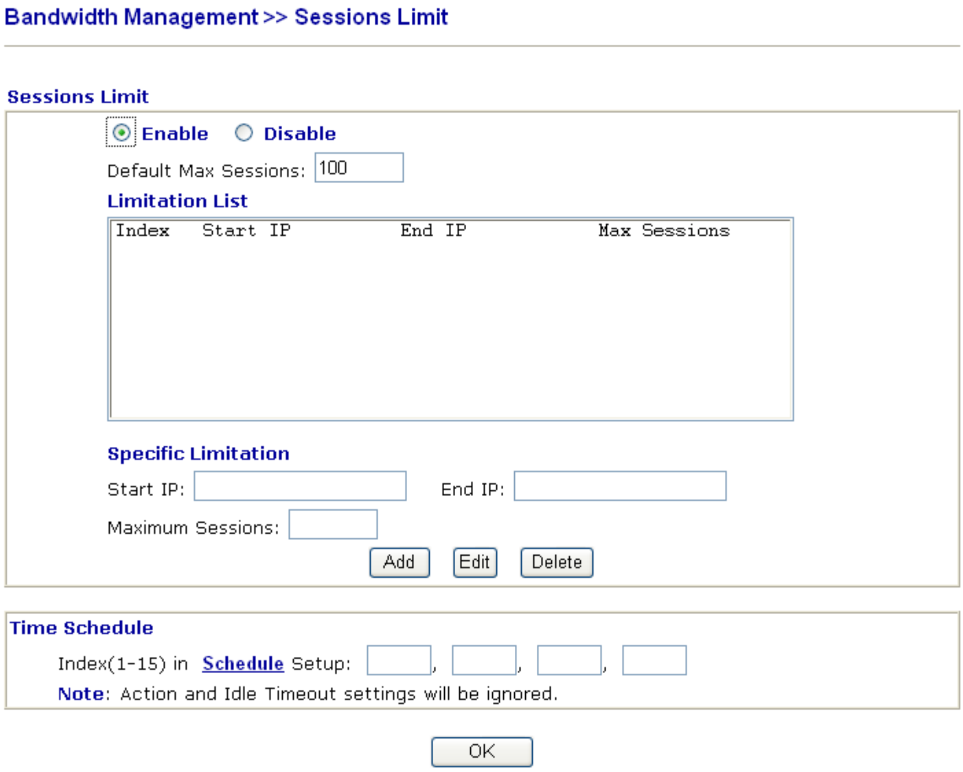
Below shows the menu items for Bandwidth Management.



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.



Bandwidth Management >> Sessions Limit

Sessions Limit

● Enable ○ Disable

Default Max Sessions: 100

Limitation List

```
Index   Start IP          End IP            Max Sessions
```

Specific Limitation

Start IP: End IP:

Maximum Sessions:

Time Schedule

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

Note: Action and Idle Timeout settings will be ignored.

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

Enable Click this button to activate the function of limit session.

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

Default session limit Defines the default session number used for each computer in LAN.

Limitation List Displays a list of specific limitations that you set on this web page.

Start IP Defines the start IP address for limit session.

End IP Defines the end IP address for limit session.

Maximum 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.

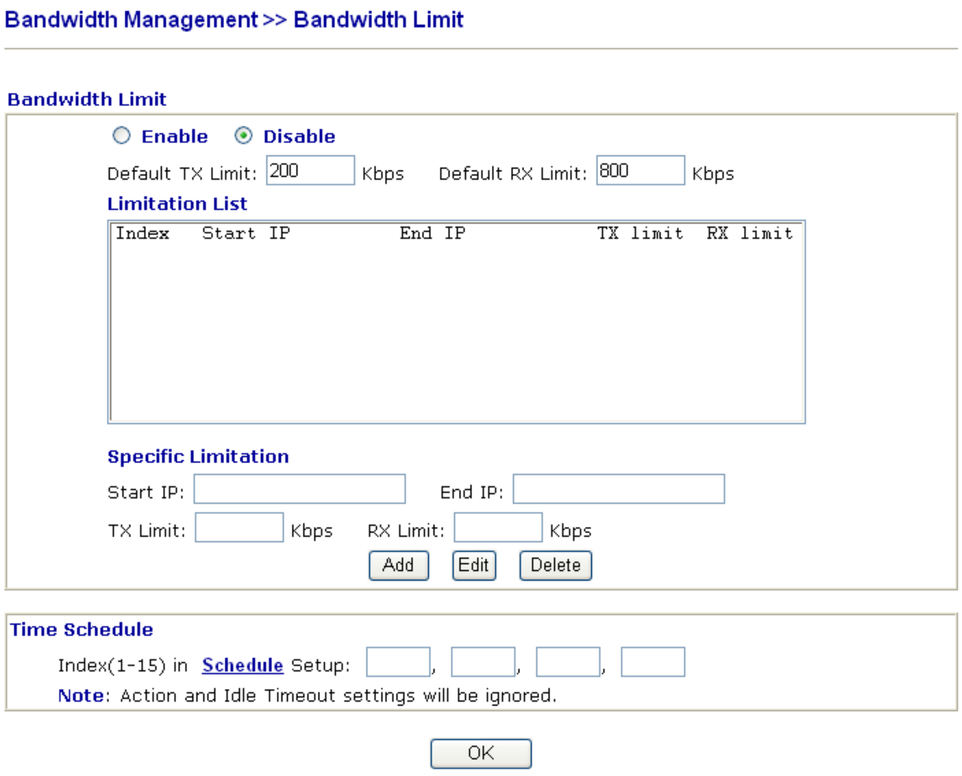
Delete Remove the selected settings existing on the limitation list.

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.



Bandwidth Management >> Bandwidth Limit

Bandwidth Limit

○ Enable ● Disable

Default TX Limit: 200 Kbps Default RX Limit: 800 Kbps

Limitation List

Index Start IP End IP TX limit RX limit

Specific Limitation

Start IP: End IP:

TX Limit: Kbps RX Limit: Kbps

Time Schedule

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

Note: Action and Idle Timeout settings will be ignored.

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

Enable Click this button to activate the function of limit bandwidth.

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:

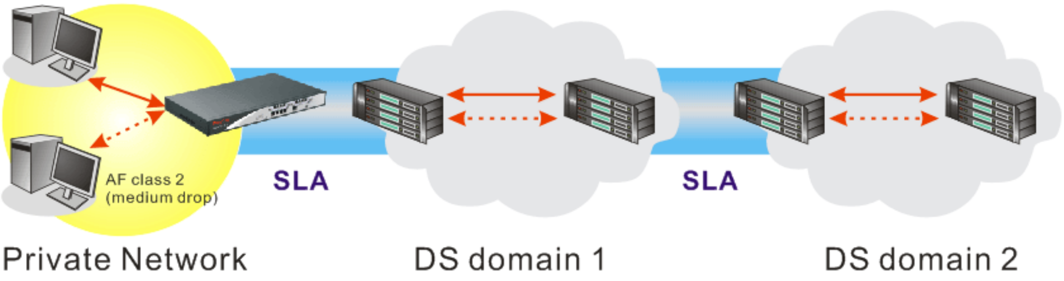
- Classification: Identifying low-latency or crucial applications and marking them for high-priority service level enforcement throughout the network.
- Scheduling: Based on classification of service level to assign packets to queues and associated service types

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.

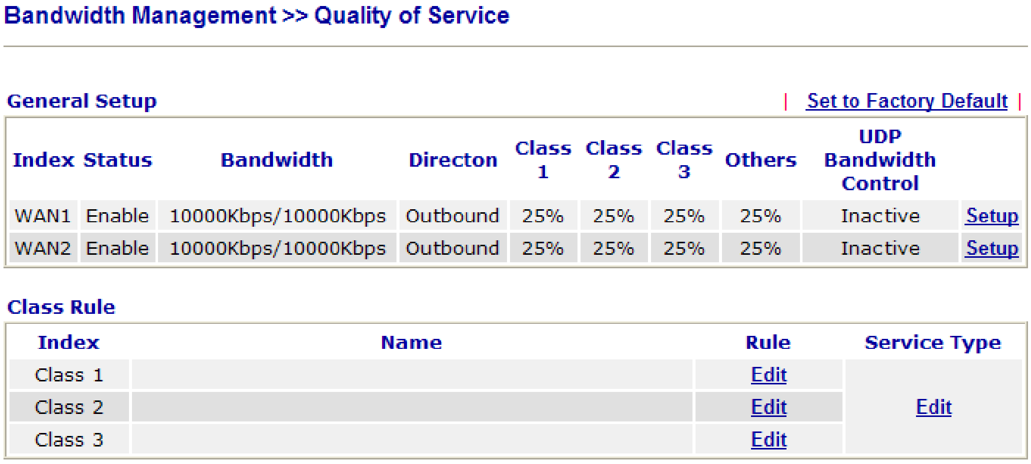
In a QoS-enabled network, or Differentiated Service (DiffServ or DS) framework, a DS domain owner should sign a Service License Agreement (SLA) with other DS domain owners to define the service level provided toward traffic from different domains. Then each DS node in these domains will perform the priority 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.



Bandwidth Management >> Quality of Service

General Setup | Set to Factory Default |

Index	Status	Bandwidth	Directon	Class 1	Class 2	Class 3	Others	UDP Bandwidth Control	
WAN1	Enable	10000Kbps/10000Kbps	Outbound	25%	25%	25%	25%	Inactive	Setup
WAN2	Enable	10000Kbps/10000Kbps	Outbound	25%	25%	25%	25%	Inactive	Setup

Class Rule

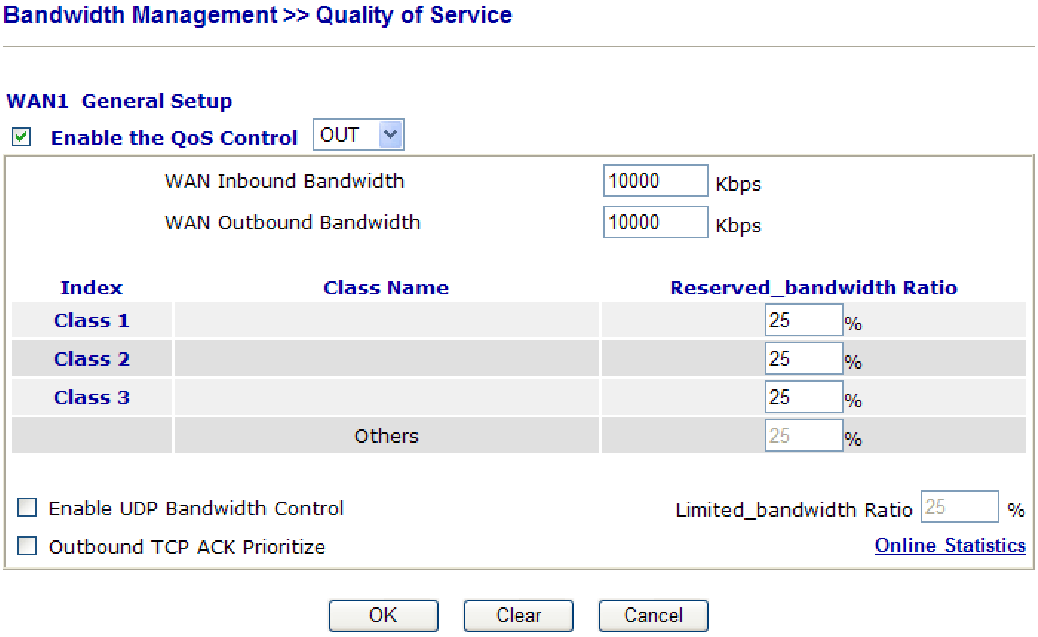
Index	Name	Rule	Service Type
Class 1		Edit	Edit
Class 2		Edit	
Class 3		Edit	

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

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

General Setup for WAN Interface

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



Bandwidth Management >> Quality of Service

WAN1 General Setup

☑ Enable the QoS Control: OUT

WAN Inbound Bandwidth: 10000 Kbps

WAN Outbound Bandwidth: 10000 Kbps

Index	Class Name	Reserved_bandwidth Ratio
Class 1		25 %
Class 2		25 %
Class 3		25 %
	Others	25 %

□ Enable UDP Bandwidth Control — Limited_bandwidth Ratio: 25 %

□ Outbound TCP ACK Prioritize

Enable the QoS Control The factory default for this setting is checked.
Please also define which traffic the QoS Control settings will apply to.
IN- apply to incoming traffic only.
OUT-apply to outgoing traffic only.
BOTH- apply to both incoming and outgoing traffic.
Check this box and click **OK**, then click **Setup** link again.
You will see the **Online Statistics** link appearing on this page.

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

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

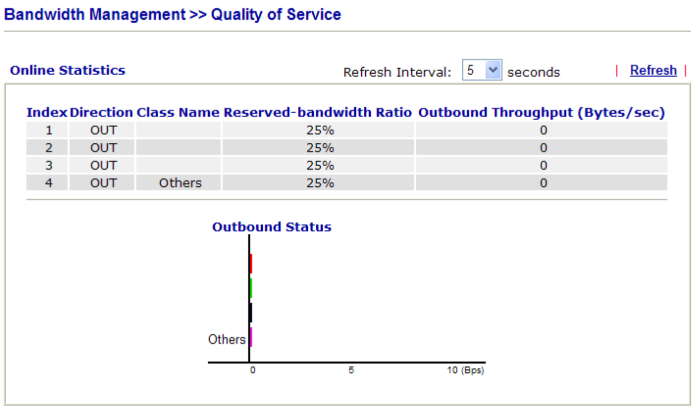
Reserved Bandwidth Ratio It is reserved for the group index in the form of ratio of **reserved bandwidth to upstream speed** and **reserved bandwidth to downstream speed**.

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

Outbound TCP ACK Prioritize The difference in bandwidth between download and upload are great in ADSL2+ environment. For the download speed might be impacted by the uploading TCP ACK, you can check this box to push ACK of upload faster to speed the network traffic.

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

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



Bandwidth Management >> Quality of Service

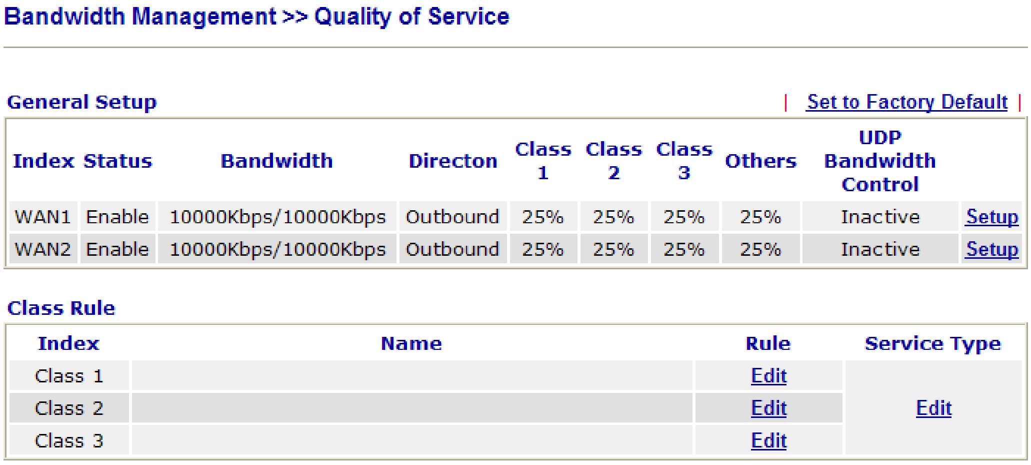
Online Statistics

Refresh Interval: 5 seconds | Refresh |

Index	Direction	Class Name	Reserved-bandwidth Ratio	Outbound Throughput (Bytes/sec)
1	OUT		25%	0
2	OUT		25%	0
3	OUT		25%	0
4	OUT	Others	25%	0

Edit the Class Rule for QoS

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



Bandwidth Management >> Quality of Service

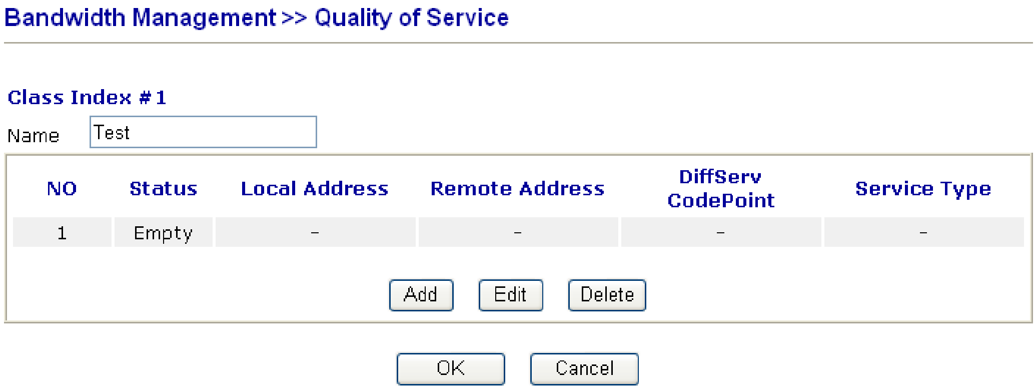
General Setup | Set to Factory Default |

Index	Status	Bandwidth	Directon	Class 1	Class 2	Class 3	Others	UDP Bandwidth Control	
WAN1	Enable	10000Kbps/10000Kbps	Outbound	25%	25%	25%	25%	Inactive	Setup
WAN2	Enable	10000Kbps/10000Kbps	Outbound	25%	25%	25%	25%	Inactive	Setup

Class Rule

Index	Name	Rule	Service Type
Class 1		Edit	Edit
Class 2		Edit	
Class 3		Edit	

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



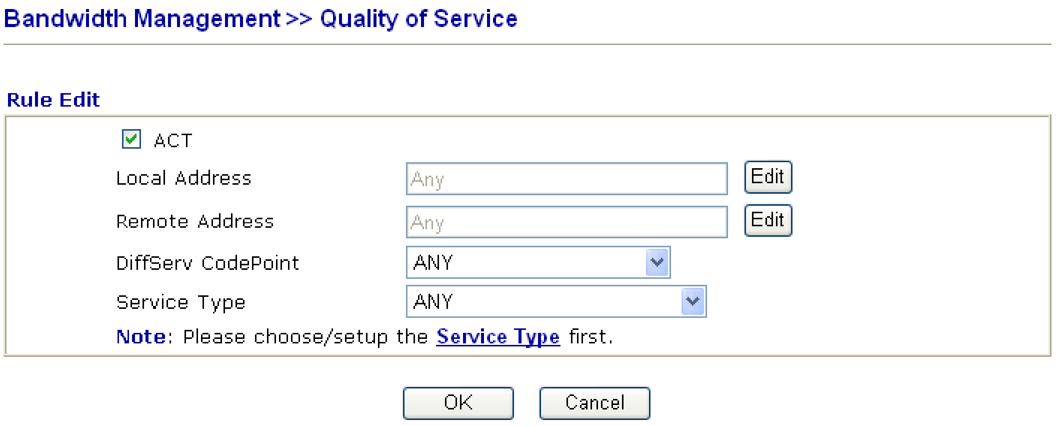
Bandwidth Management >> Quality of Service

Class Index #1

Name Test

NO	Status	Local Address	Remote Address	DiffServ CodePoint	Service Type
1	Empty	-	-	-	-

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



Bandwidth Management >> Quality of Service

Rule Edit

☑ ACT

Local Address	Any	Edit
Remote Address	Any	Edit
DiffServ CodePoint	ANY	
Service Type	ANY	

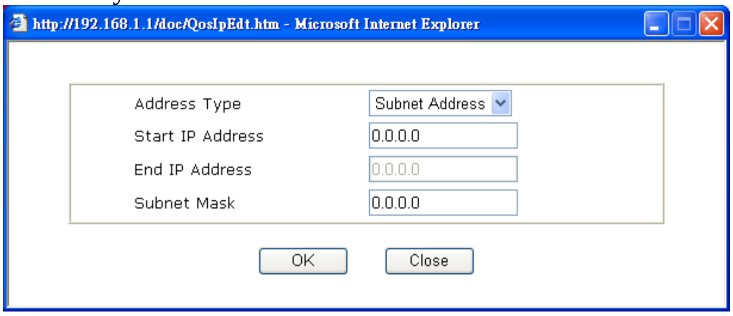
Note: Please choose/setup the Service Type first.

ACT Check this box to invoke these settings.

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

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

Edit It allows you to edit source address information.



http://192.168.1.1/doc/QosIpEdt.htm - Microsoft Internet Explorer

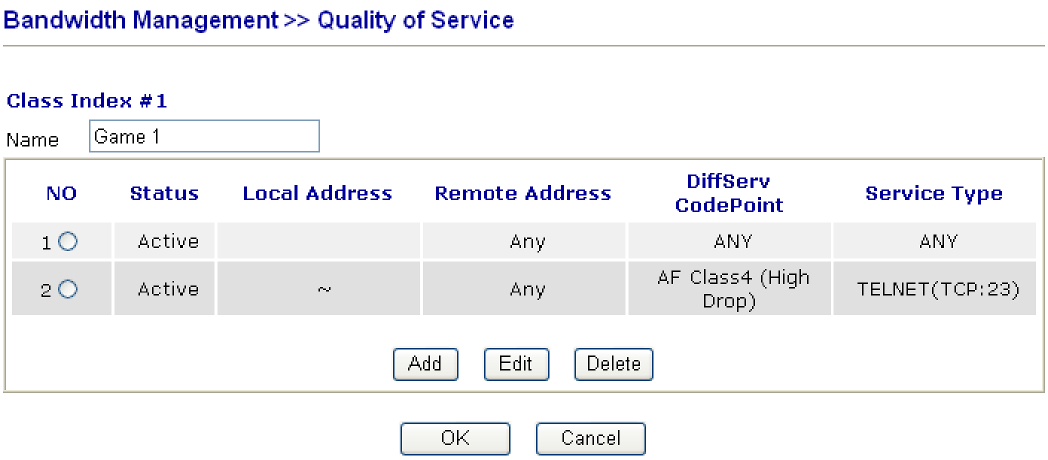
Address Type	Subnet Address
Start IP Address	0.0.0.0
End IP Address	0.0.0.0
Subnet Mask	0.0.0.0

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.


Bandwidth Management >> Quality of Service

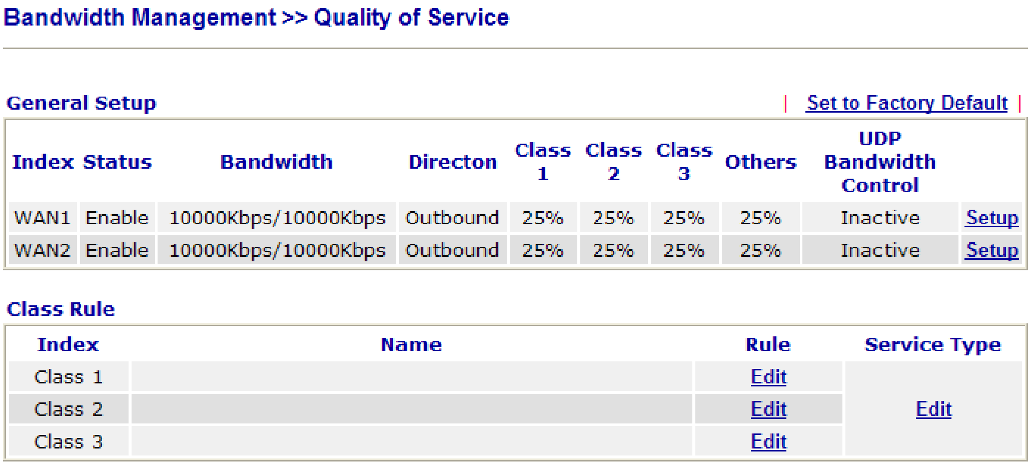
Class Index #1

Name Game 1

NO	Status	Local Address	Remote Address	DiffServ CodePoint	Service Type
1 ○	Active		Any	ANY	ANY
2 ○	Active	~	Any	AF Class4 (High Drop)	TELNET(TCP:23)

Edit the Service Type for Class Rule

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


Bandwidth Management >> Quality of Service

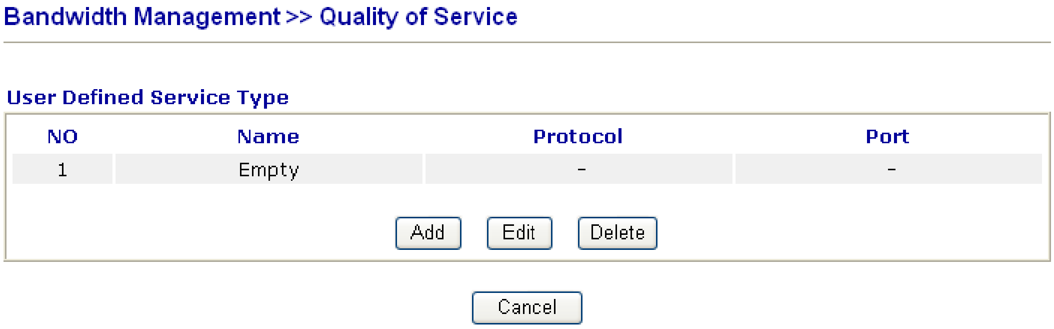
General Setup | Set to Factory Default |

Index	Status	Bandwidth	Directon	Class 1	Class 2	Class 3	Others	UDP Bandwidth Control	
WAN1	Enable	10000Kbps/10000Kbps	Outbound	25%	25%	25%	25%	Inactive	Setup
WAN2	Enable	10000Kbps/10000Kbps	Outbound	25%	25%	25%	25%	Inactive	Setup

Class Rule

Index	Name	Rule	Service Type
Class 1		Edit	Edit
Class 2		Edit	
Class 3		Edit	

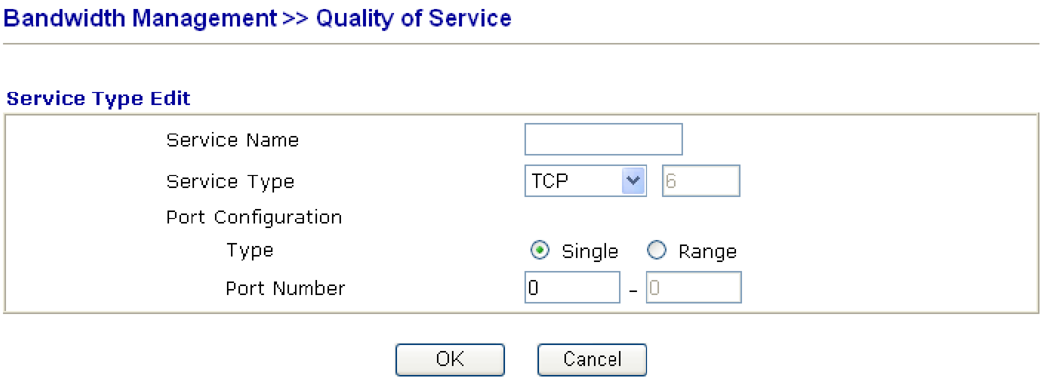
After you click the **Edit** link, you will see the following page.


Bandwidth Management >> Quality of Service

User Defined Service Type

NO	Name	Protocol	Port
1	Empty	-	-

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



Bandwidth Management >> Quality of Service

Service Type Edit

Service Name	
Service Type	TCP 6
Port Configuration	
Type	● Single ○ Range
Port Number	0 - 0

Service Name Type in a new service for your request.

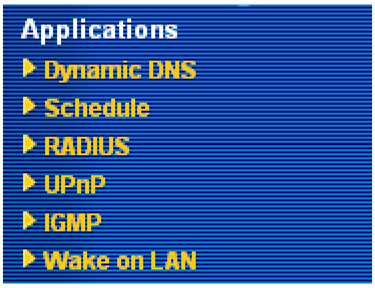
Service Type Choose the type (TCP, UDP or TCP/UDP) for the new service.

Port Configuration Click **Single** or **Range** 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

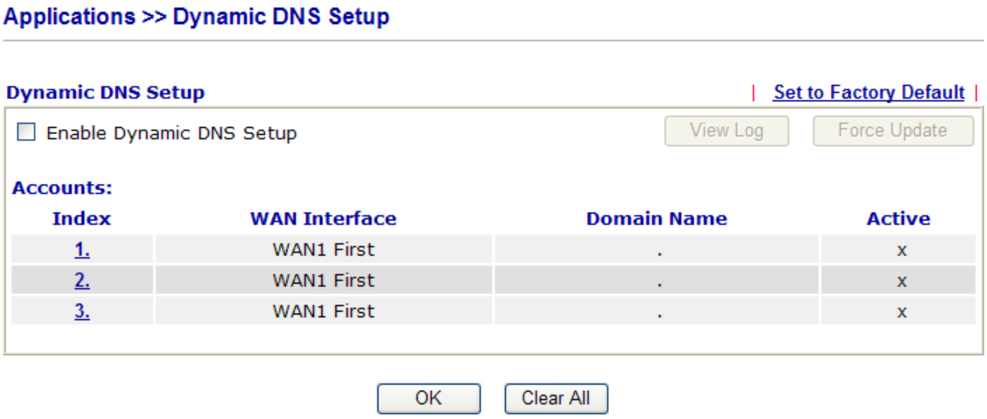
The ISP often provides you with a dynamic IP address when you connect to the Internet via your ISP. It means that the public IP address assigned to your router changes each time you access the Internet. The Dynamic DNS feature lets you assign a domain name to a dynamic WAN IP address. It allows the router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



□ Enable Dynamic DNS Setup

Accounts:

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

Set to Factory Default	Clear all profiles and recover to factory settings.
Enable Dynamic DNS Setup	Check this box to enable DDNS function.
Index	Click the number below Index to access into the setting page of DDNS setup to set account(s).
WAN Interface	Display current WAN interface used for accessing Internet.

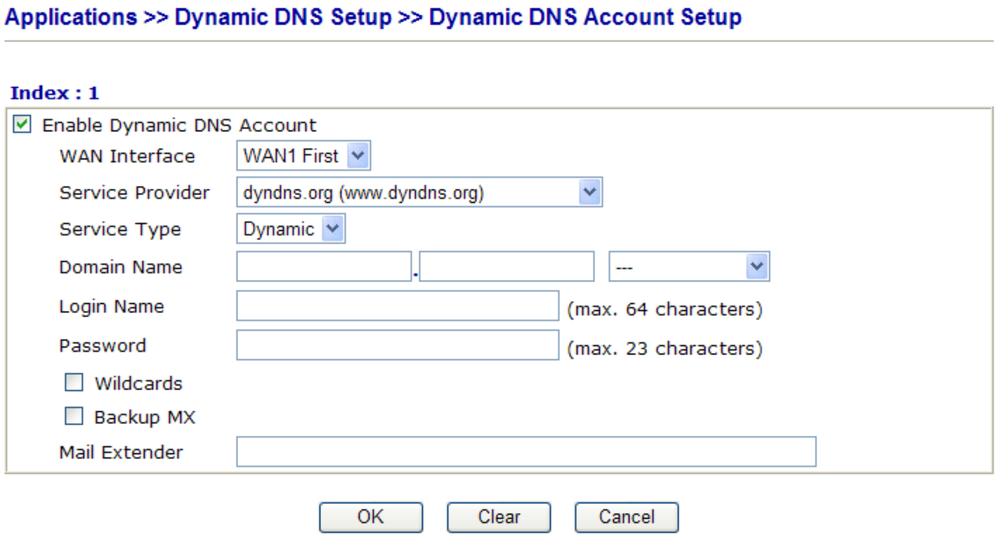
Domain Name Display the domain name that you set on the setting page of DDNS setup.

Active Display if this account is active or inactive.

View Log Display DDNS log status.

Force Update Force the router updates its information to DDNS server.

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



Applications >> Dynamic DNS Setup >> Dynamic DNS Account Setup

Index : 1

☑ Enable Dynamic DNS Account

WAN Interface: WAN1 First

Service Provider: dyndns.org (www.dyndns.org)

Service Type: Dynamic

Domain Name: . ---

Login Name: (max. 64 characters)

Password: (max. 23 characters)

□ Wildcards

□ Backup MX

Mail Extender

Enable Dynamic DNS Account Check this box to enable the current account. If you did check the box, you will see a check mark appeared on the Active column of the previous web page in step 2).

WAN Interface Select the WAN interface order to apply settings here.

Service Provider Select the service provider for the DDNS account.

Service Type Select a service type (Dynamic, Custom 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.

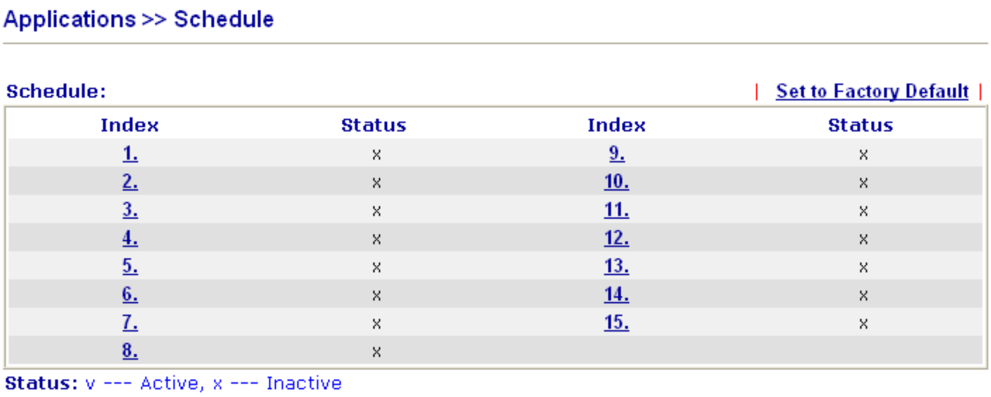
4. Click **OK** button to activate the settings. You will see your setting has been saved.

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.



Applications >> Schedule

Schedule: | Set to Factory Default |

Index	Status	Index	Status
1.	x	9.	x
2.	x	10.	x
3.	x	11.	x
4.	x	12.	x
5.	x	13.	x
6.	x	14.	x
7.	x	15.	x
8.	x		

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

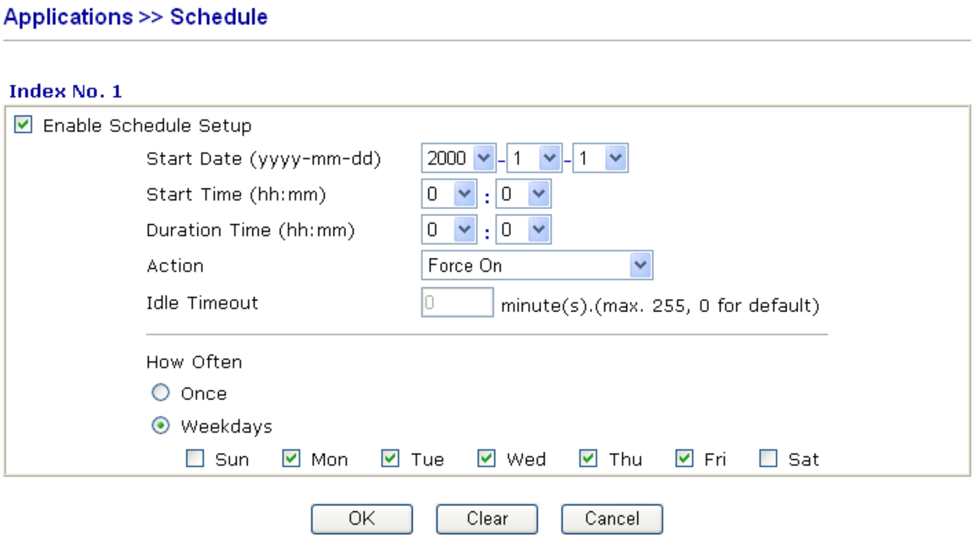
Set to Factory Default Clear all profiles and recover to factory settings.

Index Click the number below Index to access into the setting page of schedule.

Status Display if this schedule setting is active or inactive.

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

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



Applications >> Schedule

Index No. 1

☑ Enable Schedule Setup

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

Start Time (hh:mm) 0 : 0

Duration Time (hh:mm) 0 : 0

Action Force On

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

How Often

○ Once

● Weekdays

□ Sun ☑ Mon ☑ Tue ☑ Wed ☑ Thu ☑ Fri □ Sat

Enable Schedule Setup Check to enable the schedule.

Start Date (yyyy-mm-dd) Specify the starting date of the schedule.

Start Time (hh:mm) Specify the starting time of the schedule.

Duration Time (hh:mm) Specify the duration (or period) for the schedule.

Action Specify which action Call Schedule should apply during the period of the schedule.
Force On -Force the connection to be always on.
Force Down -Force the connection to be always down.
Enable Dial-On-Demand -Specify the connection to be dial-on-demand and the value of idle timeout should be specified in **Idle Timeout** field.
Disable Dial-On-Demand -Specify the connection to be up when it has traffic on the line. Once there is no traffic over idle timeout, the connection will be down and never up again during the schedule.

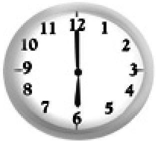
Idle Timeout Specify the duration (or period) for the schedule.
How often -Specify how often the schedule will be applied
Once -The schedule will be applied just once
Weekdays -Specify which days in one week should perform the schedule.

Example

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

Office Hour:

(Force On)



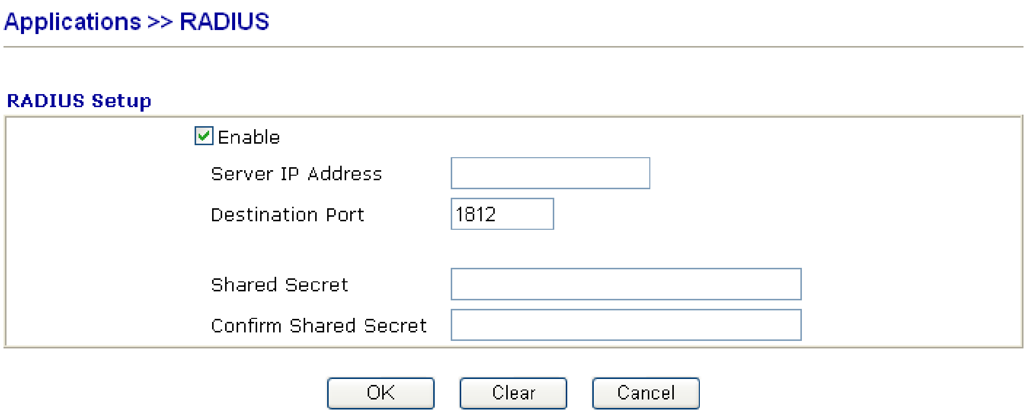
Mon - Sun **9:00 am** **to** **6:00 pm**

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

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 or a wireless station and the RADIUS server in performing mutual authentication. It enables centralized remote access authentication for network management.



Applications >> RADIUS

RADIUS Setup

☑ Enable

Server IP Address

Destination Port 1812

Shared Secret

Confirm Shared Secret

Enable Check to enable RADIUS client feature

Server IP Address Enter the IP address of RADIUS server

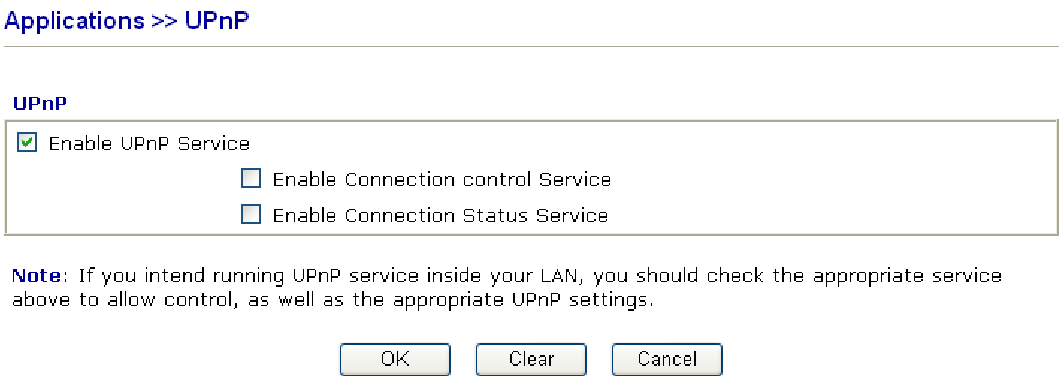
Destination Port The UDP port number that the RADIUS server is using. The default value is 1812, based on RFC 2138.

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.



Applications >> UPnP

UPnP

☑ Enable UPnP Service

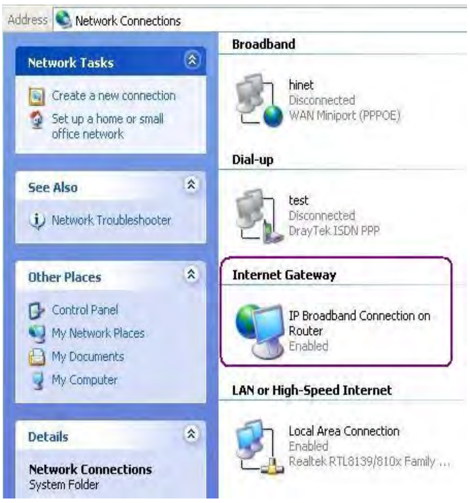
☐ Enable Connection control Service

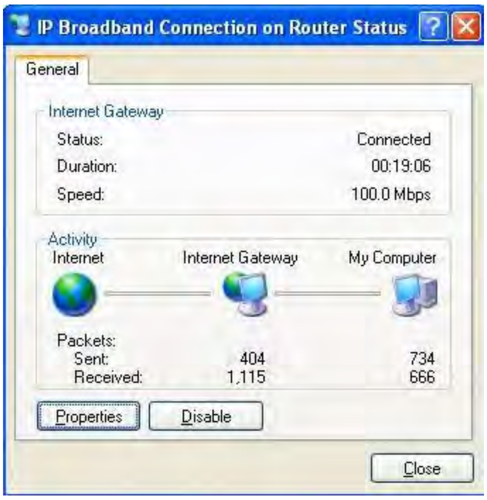
☐ Enable Connection Status Service

Note: If you intend running UPnP service inside your LAN, you should check the appropriate service above to allow control, as well as the appropriate UPnP settings.

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.





IP Broadband Connection on Router Status

General

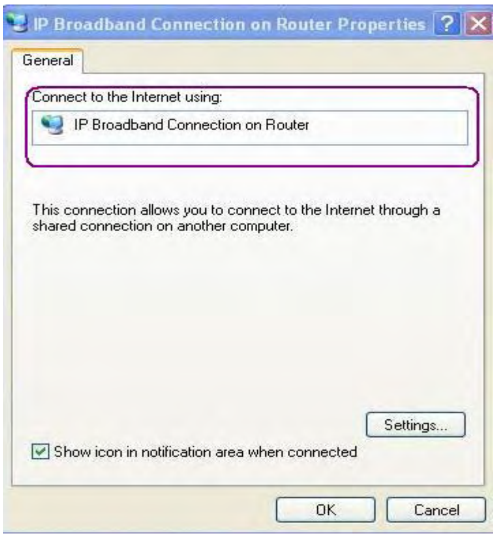
Internet Gateway

Status:	Connected
Duration:	00:19:06
Speed:	100.0 Mbps

Activity

	Internet	Internet Gateway	My Computer
Packets:			
Sent:		404	734
Received:		1,115	666

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.



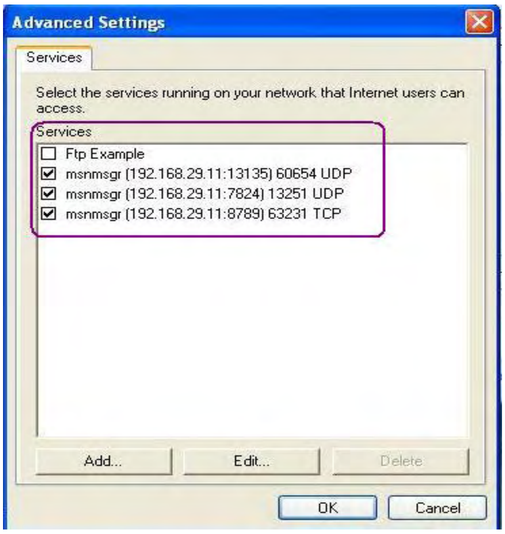
IP Broadband Connection on Router Properties

Connect to the Internet using:

IP Broadband Connection on Router

This connection allows you to connect to the Internet through a shared connection on another computer.

☑ Show icon in notification area when connected



Advanced Settings

Select the services running on your network that Internet users can access.

Services

□ Ftp Example
☑ msnmsgr (192.168.29.11:13135) 60654 UDP
☑ msnmsgr (192.168.29.11:7824) 13251 UDP
☑ msnmsgr (192.168.29.11:8789) 63231 TCP

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

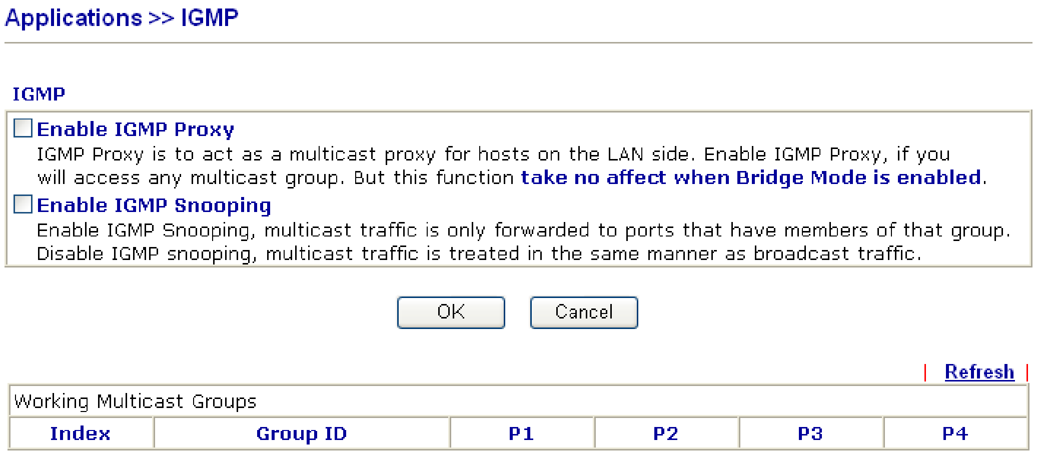
Activating the UPnP function on your network may incur some security threats. You should consider carefully these risks before activating the UPnP function.

- 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.



Applications >> IGMP

IGMP

☐ Enable IGMP Proxy
IGMP Proxy is to act as a multicast proxy for hosts on the LAN side. Enable IGMP Proxy, if you will access any multicast group. But this function **take no affect when Bridge Mode is enabled**.

☐ Enable IGMP Snooping
Enable IGMP Snooping, multicast traffic is only forwarded to ports that have members of that group. Disable IGMP snooping, multicast traffic is treated in the same manner as broadcast traffic.

Working Multicast Groups

Index	Group ID	P1	P2	P3	P4

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

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

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

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

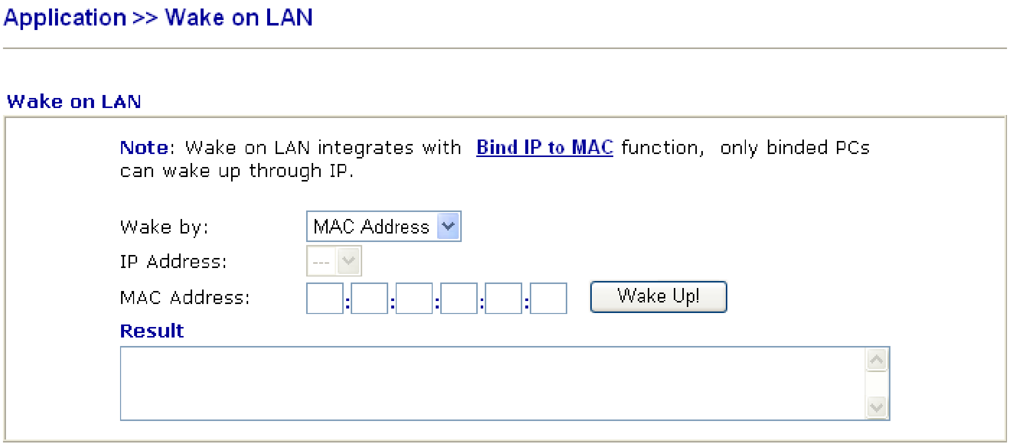
Refresh Click this link to renew the working multicast group status.

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

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.



Application >> Wake on LAN

Wake on LAN

Note: Wake on LAN integrates with Bind IP to MAC function, only binded PCs can wake up through IP.

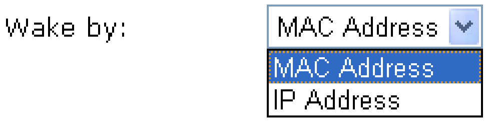
Wake by: MAC Address

IP Address: ---

MAC Address: : : : : :

Result

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

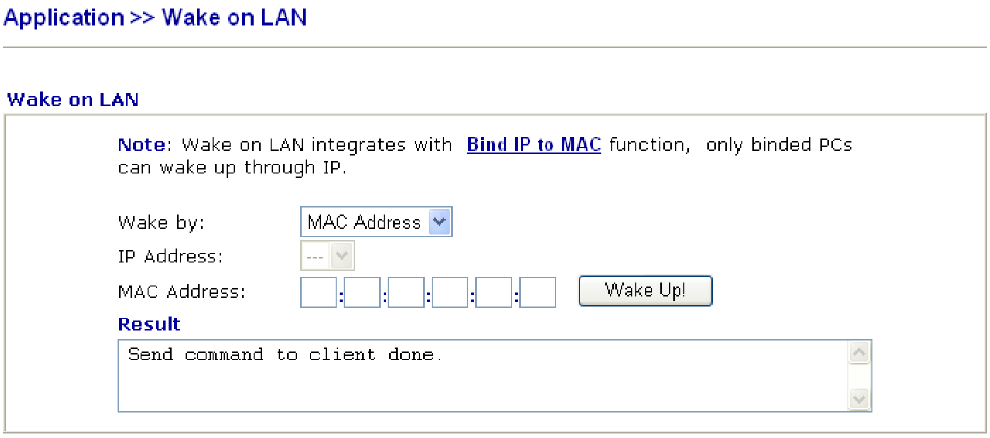


Wake by: MAC Address

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.



Application >> Wake on LAN

Wake on LAN

Note: Wake on LAN integrates with Bind IP to MAC function, only binded PCs can wake up through IP.

Wake by: MAC Address

IP Address: ---

MAC Address: : : : : :

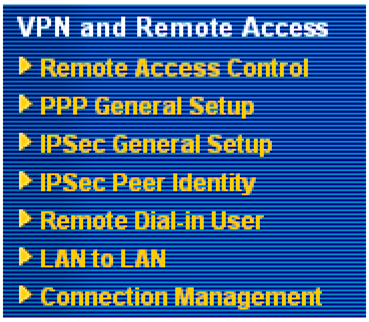
Result

```
Send command to client done.
```

5.9 VPN and Remote Access

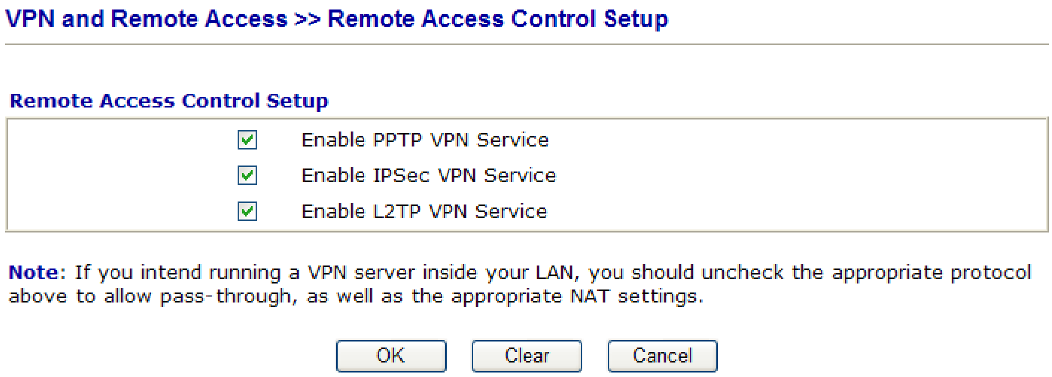
A Virtual Private Network (VPN) is the extension of a private network that encompasses links across shared or public networks like the Internet. In short, by VPN technology, you can send data between two computers across a shared or public network in a manner that emulates the properties of a point-to-point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



VPN and Remote Access >> Remote Access Control Setup

Remote Access Control Setup

☑ Enable PPTP VPN Service

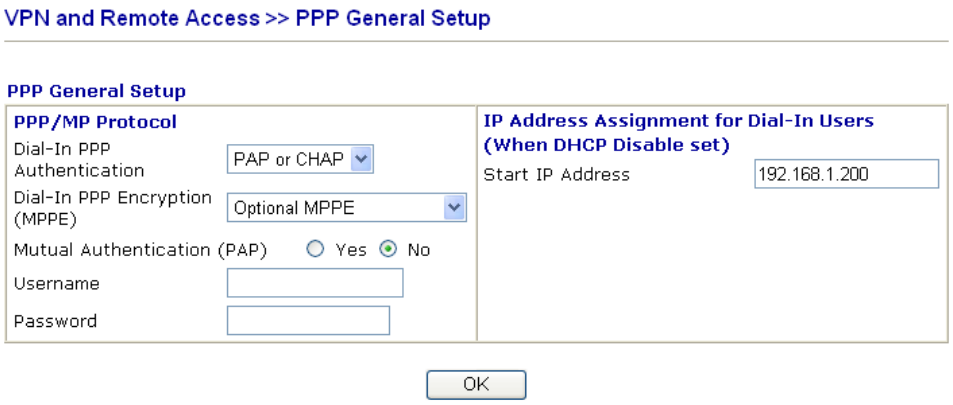
☑ Enable IPSec VPN Service

☑ Enable L2TP VPN Service

Note: If you intend running a VPN server inside your LAN, you should uncheck the appropriate protocol above to allow pass-through, as well as the appropriate NAT settings.

5.9.2 PPP General Setup

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



VPN and Remote Access >> PPP General Setup

PPP General Setup

PPP/MP Protocol

Dial-In PPP Authentication: PAP or CHAP

Dial-In PPP Encryption (MPPE): Optional MPPE

Mutual Authentication (PAP): ○ Yes ● No

Username:

Password:

IP Address Assignment for Dial-In Users (When DHCP Disable set)

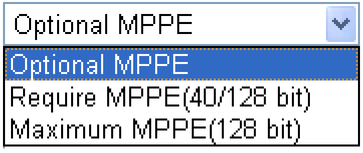
Start IP Address: 192.168.1.200

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.

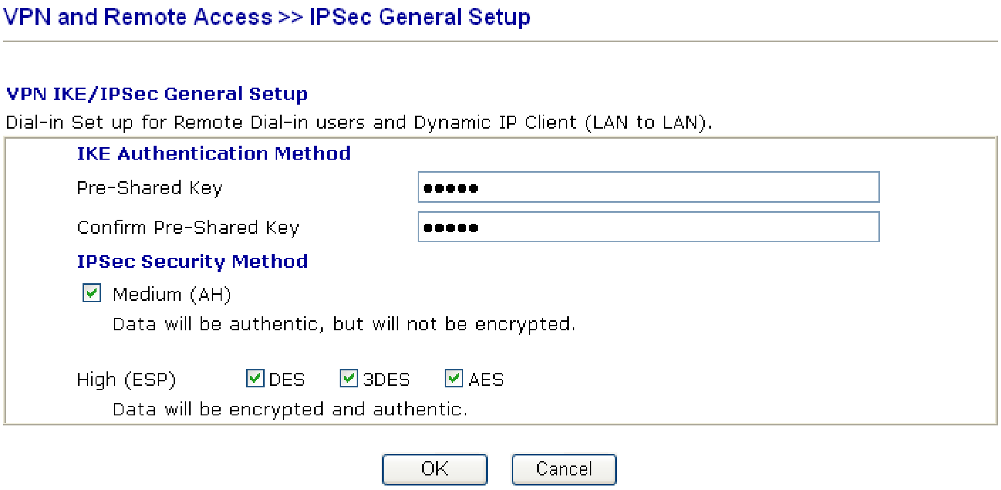
There are two phases of IPSec.

- 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.



VPN and Remote Access >> IPSec General Setup

VPN IKE/IPSec General Setup

Dial-in Set up for Remote Dial-in users and Dynamic IP Client (LAN to LAN).

IKE Authentication Method

Pre-Shared Key: ●●●●●

Confirm Pre-Shared Key: ●●●●●

IPSec Security Method

☑ Medium (AH)

Data will be authentic, but will not be encrypted.

High (ESP) ☑ DES ☑ 3DES ☑ AES

Data will be encrypted and authentic.

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

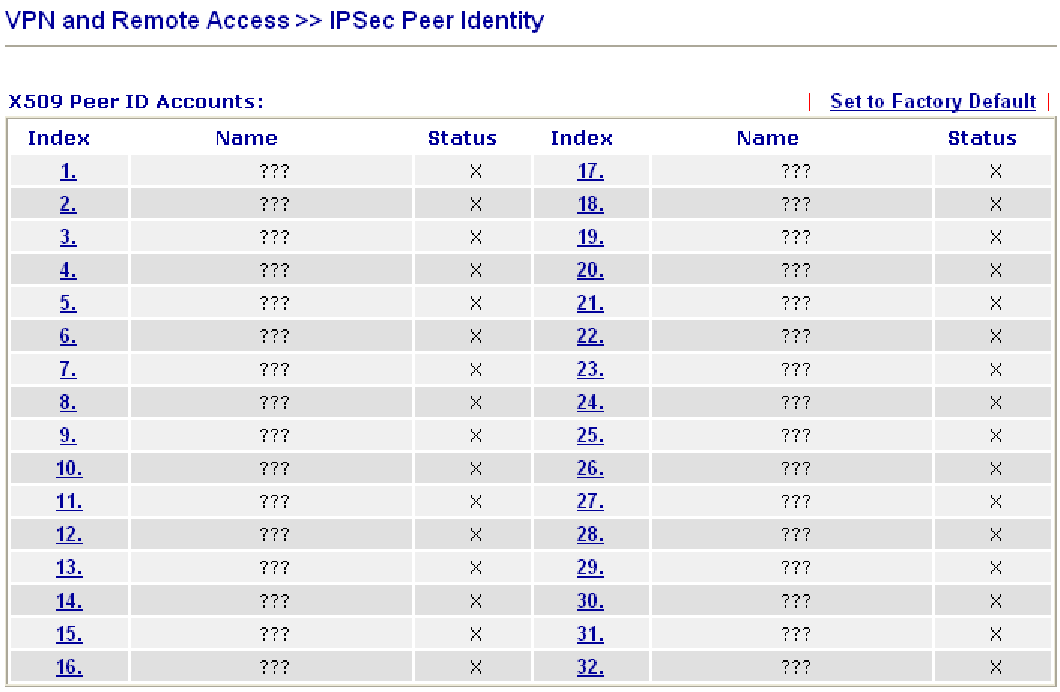
Pre-Shared Key -Currently only support Pre-Shared Key

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.



VPN and Remote Access >> IPSec Peer Identity

X509 Peer ID Accounts: | Set to Factory Default |

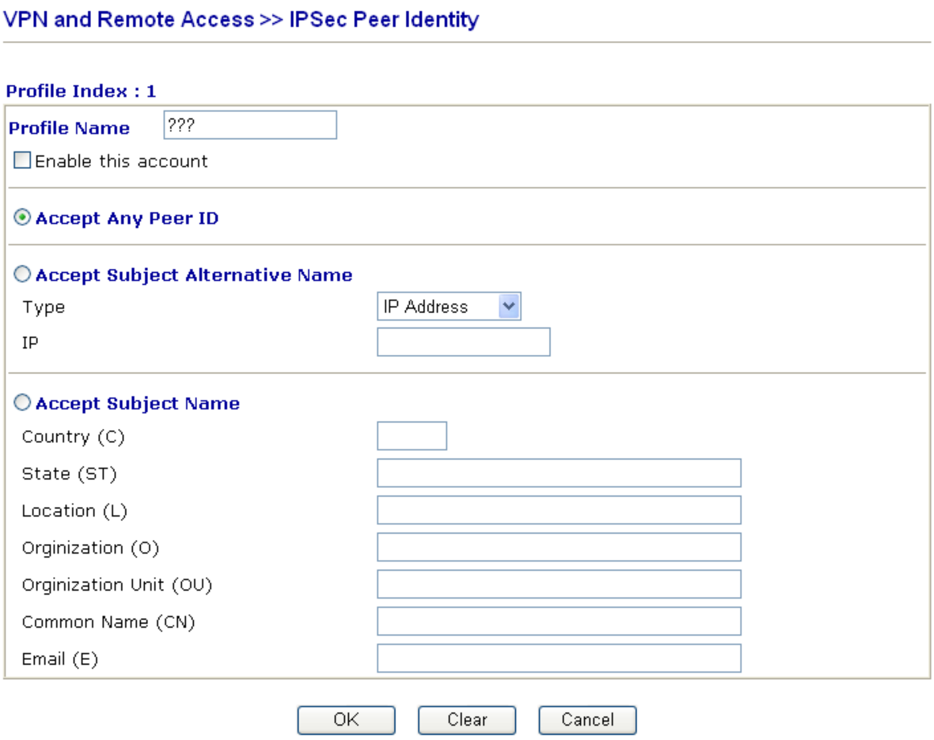
Index	Name	Status	Index	Name	Status
1.	???	×	17.	???	×
2.	???	×	18.	???	×
3.	???	×	19.	???	×
4.	???	×	20.	???	×
5.	???	×	21.	???	×
6.	???	×	22.	???	×
7.	???	×	23.	???	×
8.	???	×	24.	???	×
9.	???	×	25.	???	×
10.	???	×	26.	???	×
11.	???	×	27.	???	×
12.	???	×	28.	???	×
13.	???	×	29.	???	×
14.	???	×	30.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

Set to Factory Default Click it to clear all indexes.

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

Name Display the profile name of that index.

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



VPN and Remote Access >> IPSec Peer Identity

Profile Index : 1

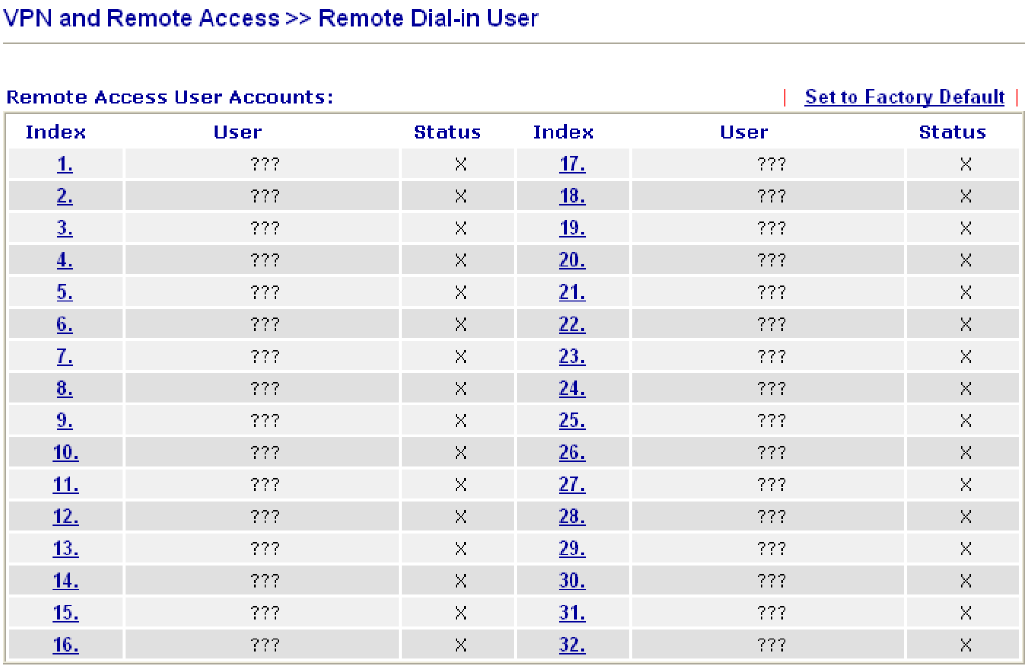
Profile Name	???
□ Enable this account	
● Accept Any Peer ID	
○ Accept Subject Alternative Name	
Type	IP Address
IP	
○ Accept Subject Name	
Country (C)	
State (ST)	
Location (L)	
Orginization (O)	
Orginization Unit (OU)	
Common Name (CN)	
Email (E)	

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

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.



VPN and Remote Access >> Remote Dial-in User

Remote Access User Accounts: | Set to Factory Default |

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

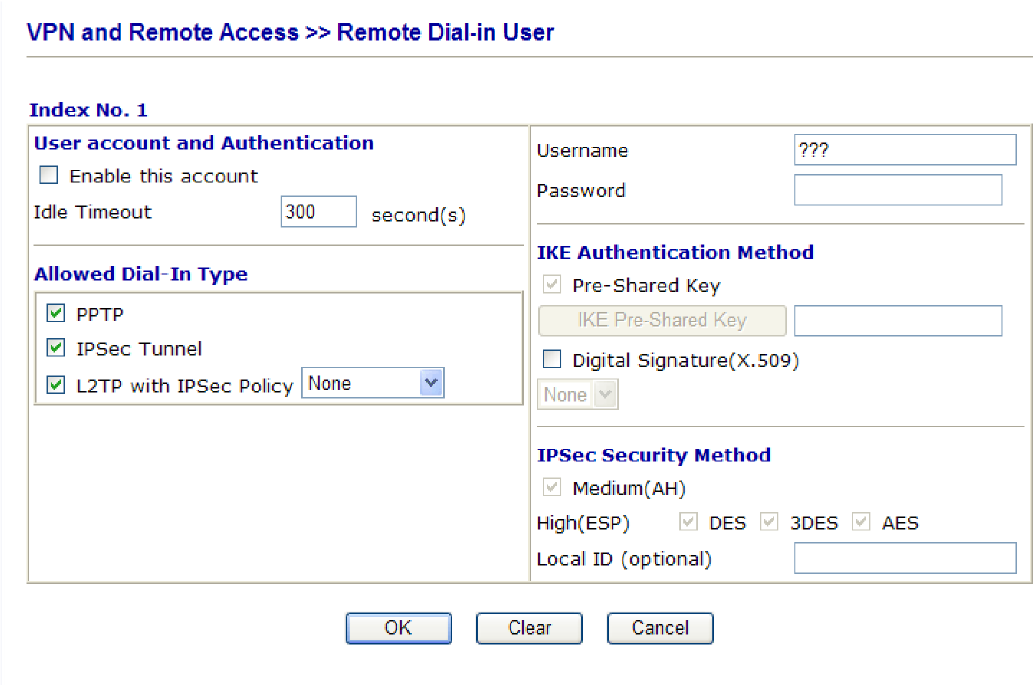
Set to Factory Default Click to clear all indexes.

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.



VPN and Remote Access >> Remote Dial-in User

Index No. 1

User account and Authentication

☐ Enable this account

Idle Timeout 300 second(s)

Allowed Dial-In Type

☑ PPTP

☑ IPSec Tunnel

☑ L2TP with IPSec Policy None

Username ???

Password

IKE Authentication Method

☑ Pre-Shared Key

IKE Pre-Shared Key

☐ Digital Signature(X.509)

None

IPSec Security Method

☑ Medium(AH)

High(ESP) ☑ DES ☑ 3DES ☑ AES

Local ID (optional)

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.

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

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

L2TP Allow the remote dial-in user to make a L2TP VPN connection through the Internet. You can select to use L2TP alone or with IPSec. Select from below:
None - Do not apply the IPSec policy. Accordingly, the VPN connection employed the L2TP without IPSec policy can be viewed as one pure L2TP connection.
Nice to Have - Apply the IPSec policy first, if it is applicable during negotiation. Otherwise, the dial-in VPN connection becomes one pure L2TP connection.
Must -Specify the IPSec policy to be definitely applied on the L2TP connection.

User Name This field is applicable when you select PPTP or L2TP with or without IPSec policy above.

Password This field is applicable when you select PPTP or L2TP with or without IPSec policy above.

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

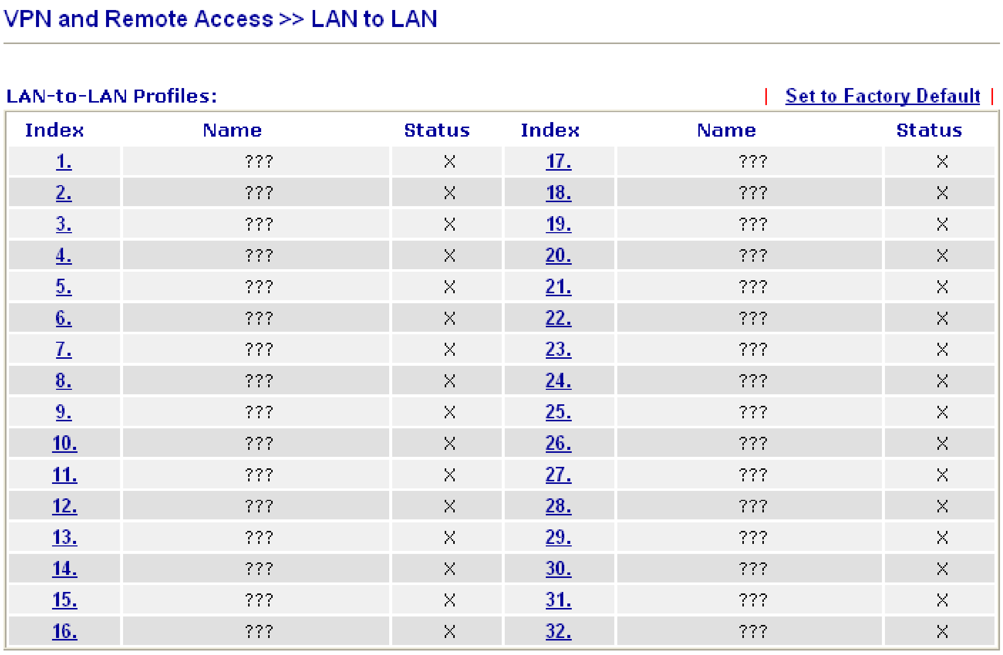
IPSec Security Method

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 2 VPN tunnels and provides 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.	???	×	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

Click to clear all indexes.

Name

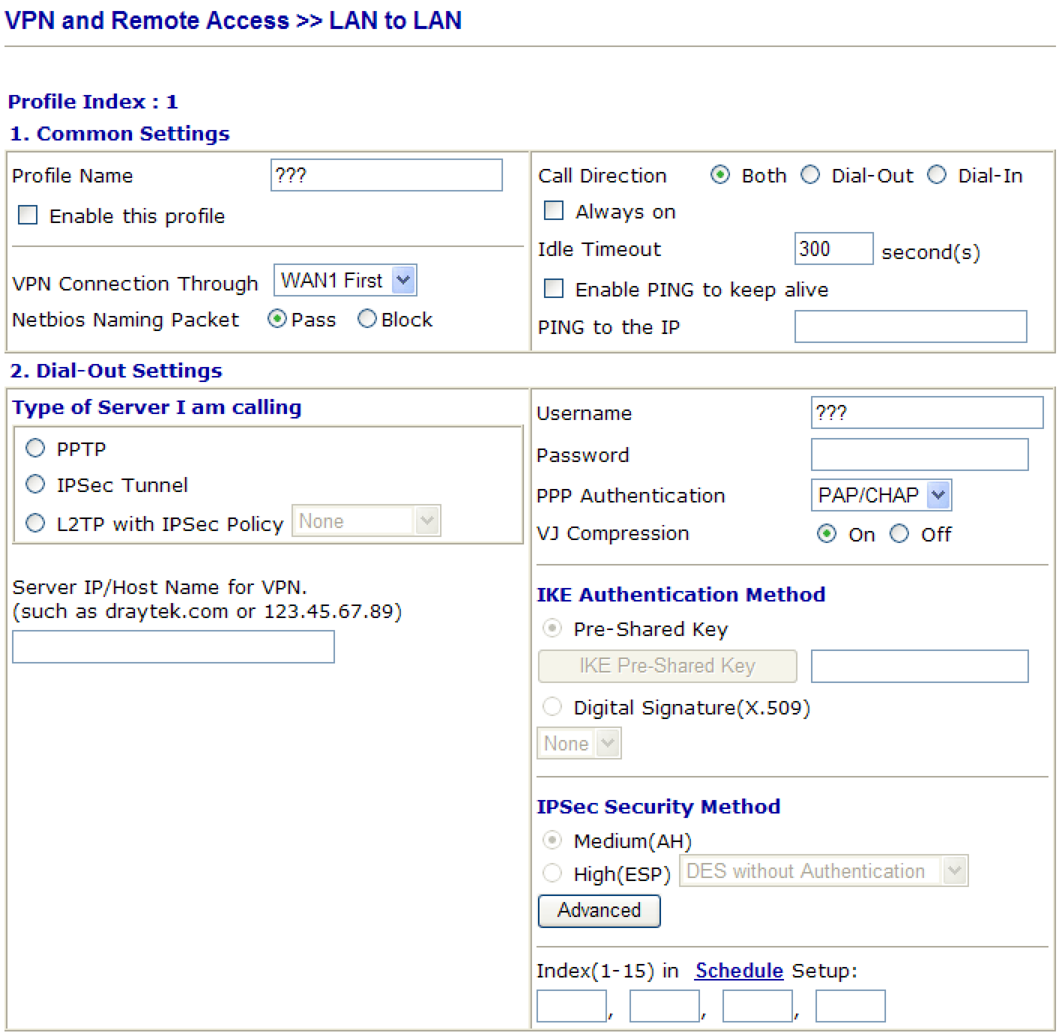
Indicate the name of the LAN-to-LAN profile. The symbol **???** represents that the profile is empty.

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.



VPN and Remote Access >> LAN to LAN

Profile Index : 1

1. Common Settings

Profile Name: ???

□ Enable this profile

VPN Connection Through: WAN1 First

Netbios Naming Packet: ● Pass ○ Block

Call Direction: ● Both ○ Dial-Out ○ Dial-In

□ Always on

Idle Timeout: 300 second(s)

□ Enable PING to keep alive

PING to the IP:

2. Dial-Out Settings

Type of Server I am calling

○ PPTP

○ IPSec Tunnel

○ L2TP with IPSec Policy: None

Server IP/Host Name for VPN.
(such as draytek.com or 123.45.67.89)

Username: ???

Password:

PPP Authentication: PAP/CHAP

VJ Compression: ● On ○ Off

IKE Authentication Method

● Pre-Shared Key

IKE Pre-Shared Key

○ Digital Signature(X.509)

None

IPSec Security Method

● Medium(AH)

○ High(ESP): DES without Authentication

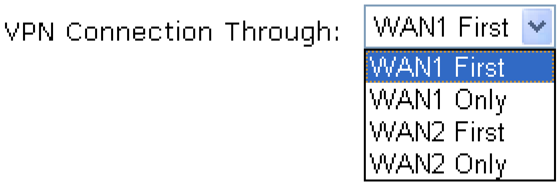
Advanced

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

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

Enable this profile Check here to activate this profile.

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



VPN Connection Through: WAN1 First

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

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

Netbios Naming Packet

Pass – click it to have an inquiry for data transmission between the hosts located on both sides of VPN Tunnel while connecting.
Block – When there is conflict occurred between the hosts on both sides of VPN Tunnel in connecting, such function can block data transmission of Netbios Naming Packet inside the tunnel.

Call Direction

Specify the allowed call direction of this LAN-to-LAN profile.
Both:-initiator/responder
Dial-Out- initiator only
Dial-In- responder only.

Always On or Idle Timeout

Always On-Check to enable router always keep VPN connection.
Idle Timeout: The default value is 300 seconds. If the connection has been idled over the value, the router will drop the connection.

Enable PING to keep alive

This function is to help the router to determine the status of IPSec VPN connection, especially useful in the case of abnormal VPN IPSec tunnel disruption. For details, please refer to the note below. Check to enable the transmission of PING packets to a specified IP address.

PING to the IP

Enter the IP address of the remote host that located at the other-end of the VPN tunnel.

> **Enable PING to Keep Alive** is used to handle abnormal IPSec VPN connection disruption. It will help to provide the state of a VPN connection for router's judgment of redial.
>
> Normally, if any one of VPN peers wants to disconnect the connection, it should follow a serial of packet exchange procedure to inform each other. However, if the remote peer disconnect without notice, Vigor router will by no where to know this situation. To resolve this dilemma, by continuously sending PING packets to the remote host, the Vigor router can know the true existence of this VPN connection and react accordingly. This is independent of DPD (dead peer detection).

PPTP

Build a PPTP VPN connection to the server through the Internet. You should set the identity like User Name and Password below for the authentication of remote server.

IPSec Tunnel

Build an IPSec VPN connection to the server through Internet.

L2TP with …

Build a L2TP VPN connection through the Internet. You can select to use L2TP alone or with IPSec. Select from below:
None: Do not apply the IPSec policy. Accordingly, the VPN connection employed the L2TP without IPSec policy can be viewed as one pure L2TP connection.

Nice to Have: Apply the IPSec policy first, if it is applicable during negotiation. Otherwise, the dial-out VPN connection becomes one pure L2TP connection.
Must: Specify the IPSec policy to be definitely applied on the L2TP connection.

User Name

This field is applicable when you select PPTP or L2TP with or without IPSec policy above.

Password

This field is applicable when you select PPTP or L2TP with or without IPSec policy above.

PPP Authentication

This field is applicable when you select 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.

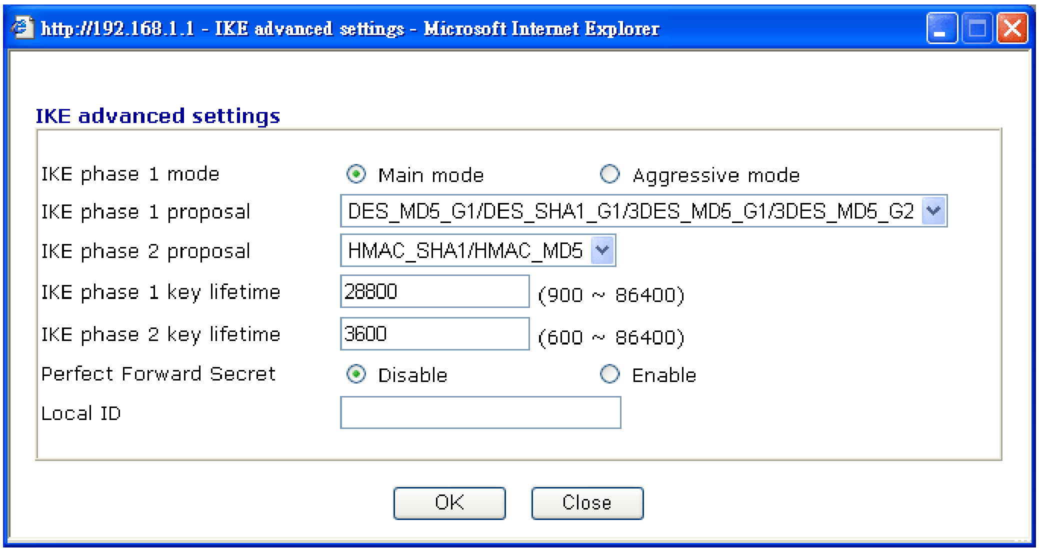
Medium

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:



http://192.168.1.1 - IKE advanced settings - Microsoft Internet Explorer

IKE advanced settings

IKE phase 1 mode	● Main mode	○ Aggressive mode
IKE phase 1 proposal	DES_MD5_G1/DES_SHA1_G1/3DES_MD5_G1/3DES_MD5_G2	
IKE phase 2 proposal	HMAC_SHA1/HMAC_MD5	
IKE phase 1 key lifetime	28800	(900 ~ 86400)
IKE phase 2 key lifetime	3600	(600 ~ 86400)
Perfect Forward Secret	● Disable	○ Enable
Local ID		

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.

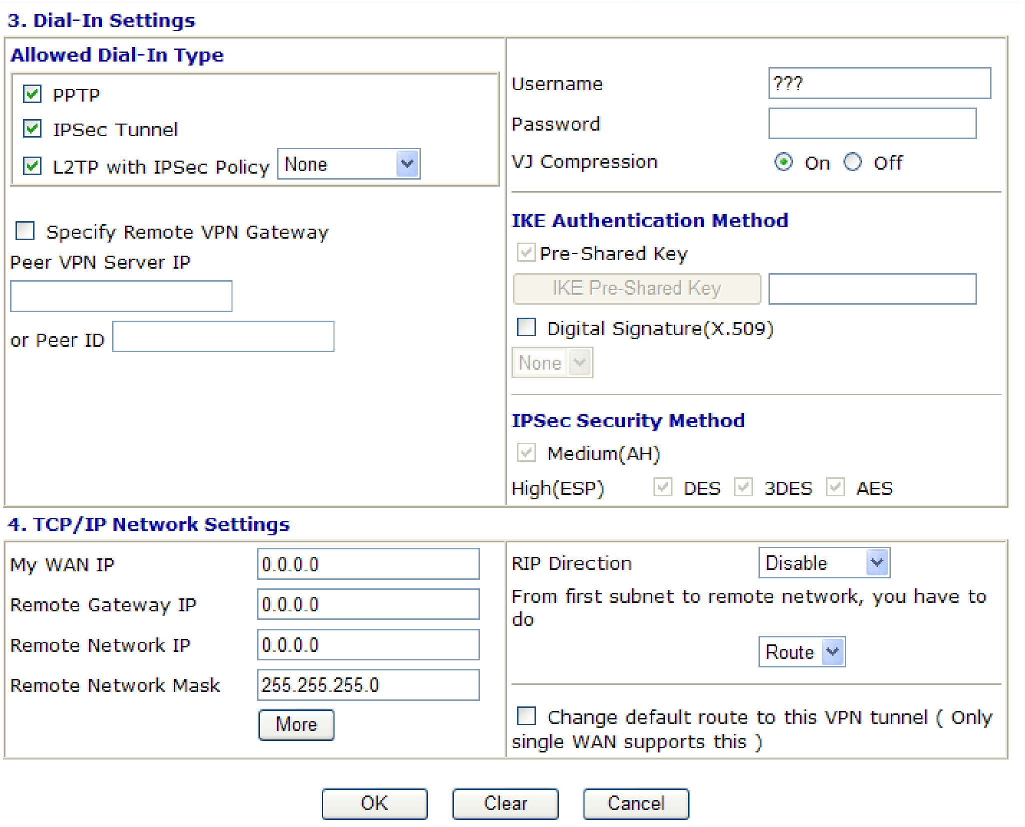
IKE phase 2 proposal-To propose the local available algorithms to the VPN peers, and get its feedback to find a match. Three combinations are available for both modes. We suggest you select the combination that covers the most algorithms.

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.



3. Dial-In Settings

Allowed Dial-In Type

☑ PPTP

☑ IPSec Tunnel

☑ L2TP with IPSec Policy: None

□ Specify Remote VPN Gateway

Peer VPN Server IP:

or Peer ID:

Username: ???

Password:

VJ Compression: ● On ○ Off

IKE Authentication Method

☑ Pre-Shared Key

IKE Pre-Shared Key:

□ Digital Signature(X.509): None

IPSec Security Method

☑ Medium(AH)

High(ESP) ☑ DES ☑ 3DES ☑ AES

4. TCP/IP Network Settings

My WAN IP: 0.0.0.0

Remote Gateway IP: 0.0.0.0

Remote Network IP: 0.0.0.0

Remote Network Mask: 255.255.255.0

RIP Direction: Disable

From first subnet to remote network, you have to do: Route

□ Change default route to this VPN tunnel (Only single WAN supports this)

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.

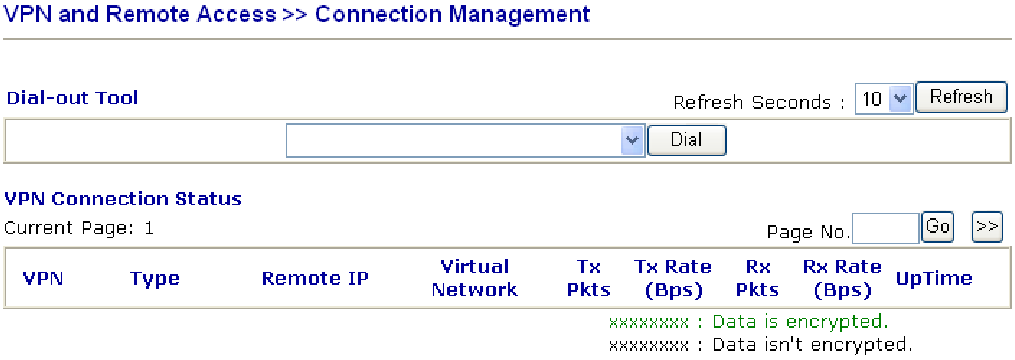
RIP Direction

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.



VPN and Remote Access >> Connection Management

Dial-out Tool

Refresh Seconds : 10

VPN Connection Status

Current Page: 1

Page No.

VPN	Type	Remote IP	Virtual Network	Tx Pkts	Tx Rate (Bps)	Rx Pkts	Rx Rate (Bps)	UpTime

xxxxxxxx : Data is encrypted.

xxxxxxxx : Data isn't encrypted.

Dial	Click this button to execute dial out function.
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.

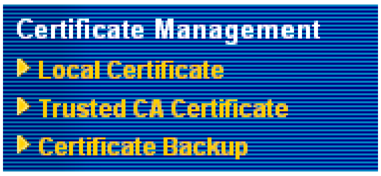
5.10 Certificate Management

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.

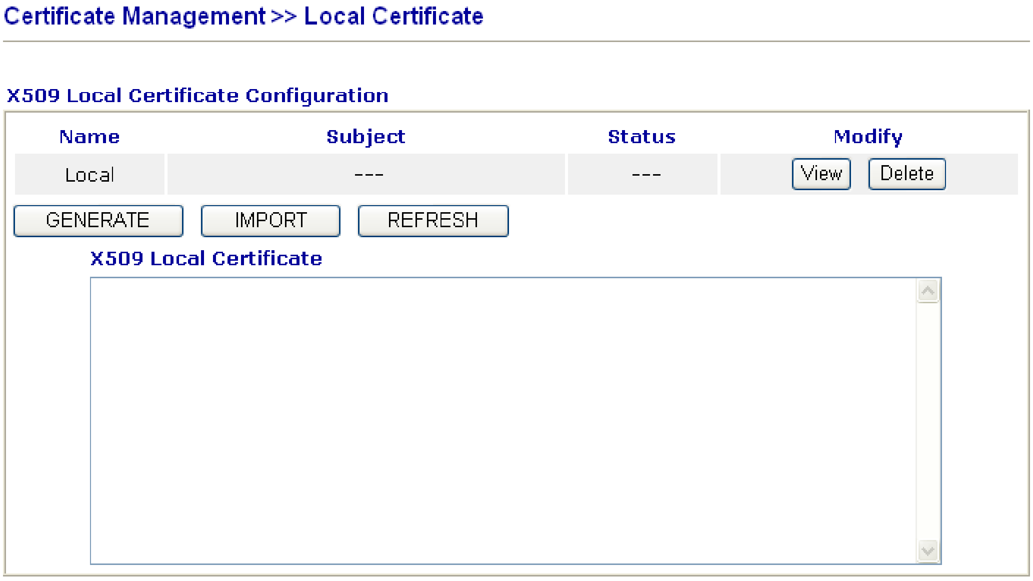
Any entity wants to utilize digital certificates should first request a certificate issued by a CA server. It should also retrieve certificates of other trusted CA servers so it can authenticate the peer with certificates issued by those trusted CA servers.

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.



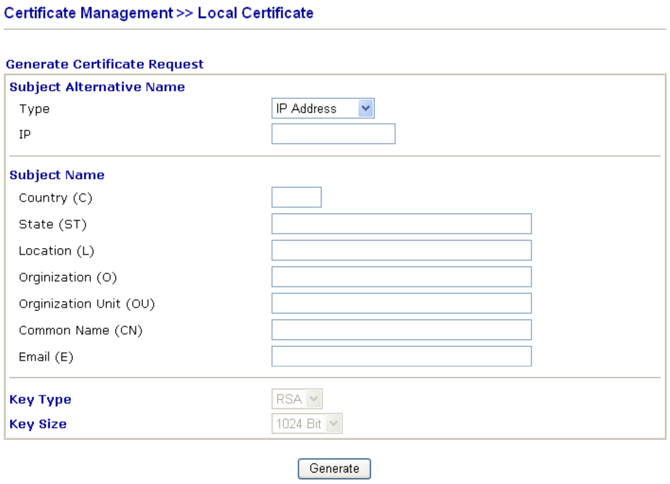
5.10.1 Local Certificate


Certificate Management >> Local Certificate

X509 Local Certificate Configuration

Name	Subject	Status	Modify
Local	---	---	View Delete

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



Certificate Management >> Local Certificate

Generate Certificate Request

Subject Alternative Name

Type	IP Address
IP	

Subject Name

Country (C)	
State (ST)	
Location (L)	
Orginization (O)	
Orginization Unit (OU)	
Common Name (CN)	
Email (E)	

Key Type	RSA
Key Size	1024 Bit

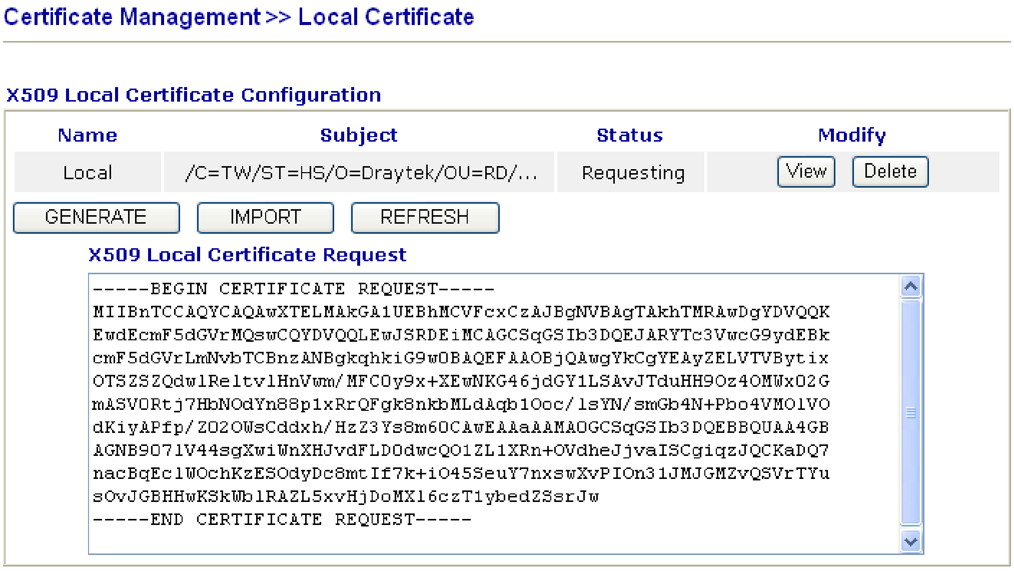
Type in all the information that the window request. Then click **Generate** again.

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:



Certificate Management >> Local Certificate

X509 Local Certificate Configuration

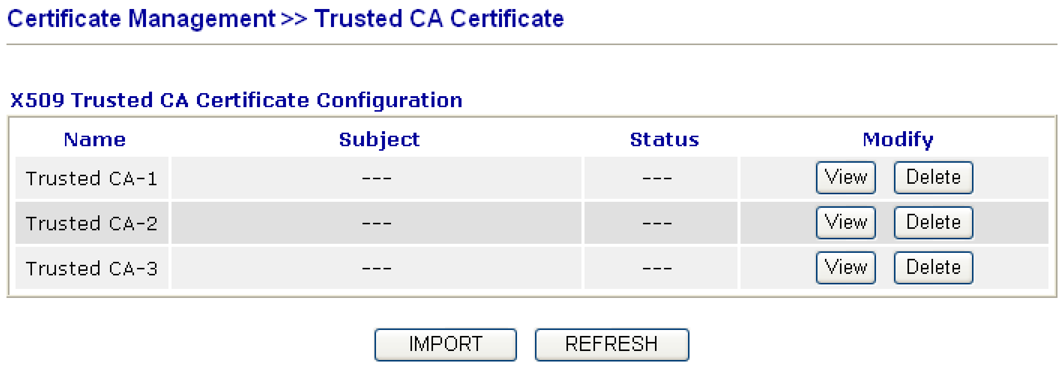
Name	Subject	Status	Modify
Local	/C=TW/ST=HS/O=Draytek/OU=RD/...	Requesting	View Delete

X509 Local Certificate Request

```
-----BEGIN CERTIFICATE REQUEST-----
MIIBnTCCAQYCAQAwXTELMAkGA1UEBhMCVFcxCzAJBgNVBAgTAkhTMRAwDgYDVQQK
EwdEcmF5dGVrMQswCQYDVQQLEwJSRDEiMCAGCSqGSIb3DQEJARYTc3VwcG9ydEBk
cmF5dGVrLmNvbTCBnzANBgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEAyZELVTVBytix
OTSZSZQdwlReltvlHnVwm/MFCOy9x+XEwNKG46jdGY1LSAvJTduHH9Oz4OMWxO2G
mASVORtj7HbNOdYn88p1xRrQFgk8nkbMLdAqb1Ooc/lsYN/smGb4N+Pbo4VMOlVO
dKiyAPfp/ZO2OWsCddxh/HzZ3Ys8m6OCAwEAAaAAMA0GCSqGSIb3DQEBBQUAA4GB
AGNB907lV44sgXwiWnXHJvdFLDOdwcQO1ZL1XRn+OVdheJjvaISCgiqzJQCKaDQ7
nacBqEclWOchKzESOdyDc8mtIf7k+iO45SeuY7nxswXvPIOn31JMJGMZvQSVrTYu
sOvJGBHHwKSkWblRAZL5xvHjDoMXl6czT1ybedZSsrJw
-----END CERTIFICATE REQUEST-----
```

5.10.2 Trusted CA Certificate

Trusted CA certificate lists three sets of trusted CA certificate.

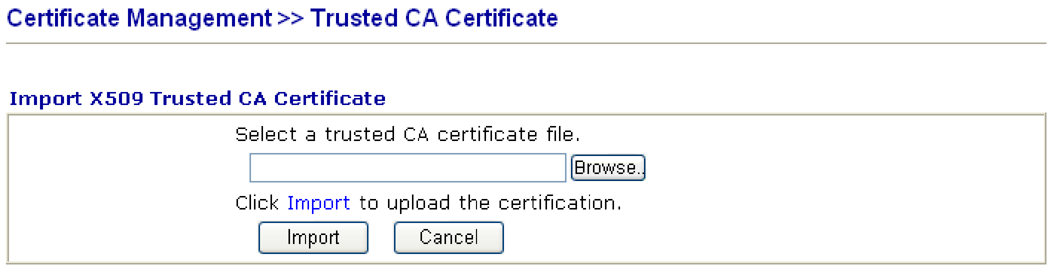


Certificate Management >> Trusted CA Certificate

X509 Trusted CA Certificate Configuration

Name	Subject	Status	Modify
Trusted CA-1	---	---	View Delete
Trusted CA-2	---	---	View Delete
Trusted CA-3	---	---	View Delete

To import a pre-saved trusted CA certificate, please click **IMPORT** to open the following window. Use **Browse…** to find out the saved text file. Then click **Import**. The one you imported will be listed on the Trusted CA Certificate window. Then click **Import** to use the pre-saved file.



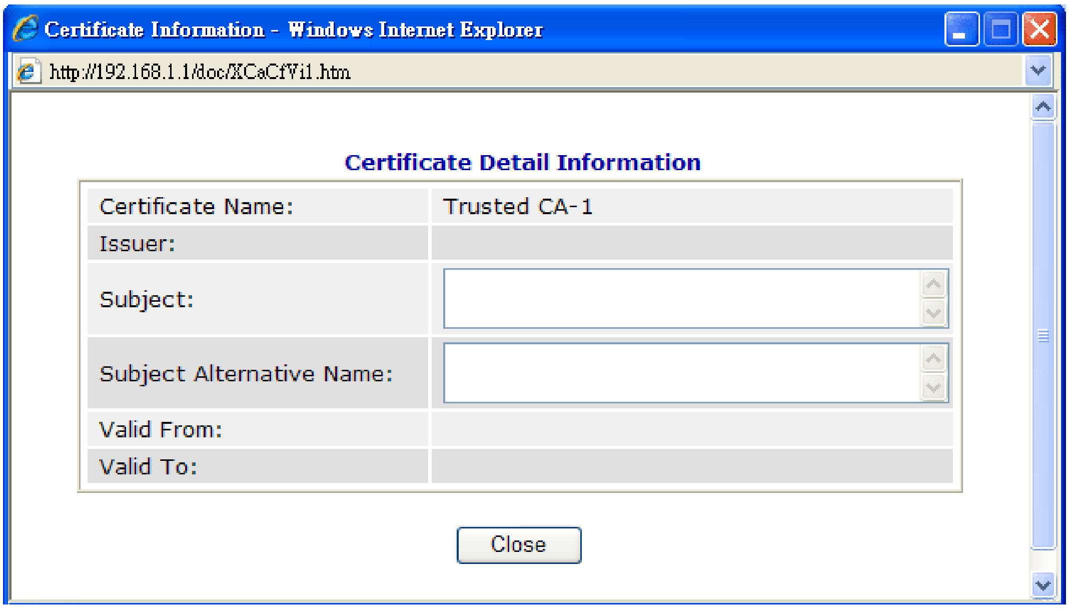
Certificate Management >> Trusted CA Certificate

Import X509 Trusted CA Certificate

Select a trusted CA certificate file.

Click Import to upload the certification.

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



Certificate Information - Windows Internet Explorer

http://192.168.1.1/doc/XCaCfVi1.htm

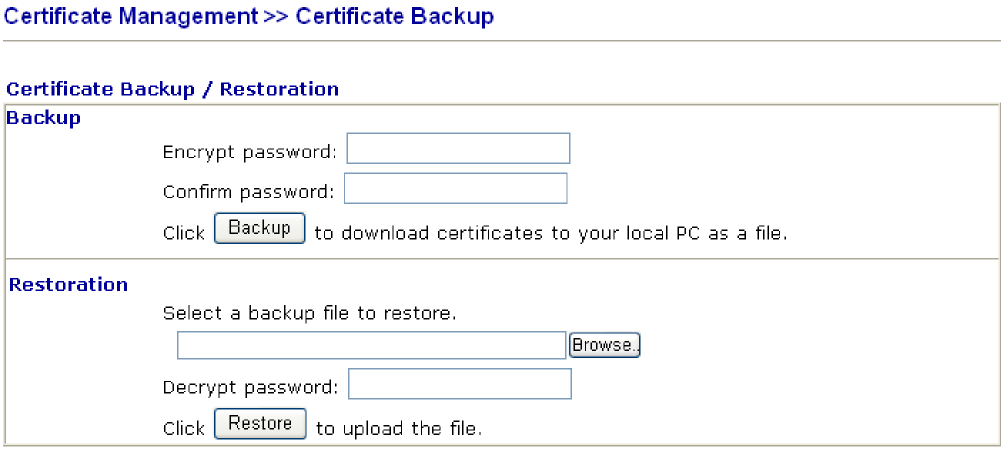
Certificate Detail Information

Certificate Name:	Trusted CA-1
Issuer:	
Subject:	
Subject Alternative Name:	
Valid From:	
Valid To:	

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.



Certificate Management >> Certificate Backup

Certificate Backup / Restoration

Backup

Encrypt password:

Confirm password:

Click Backup to download certificates to your local PC as a file.

Restoration

Select a backup file to restore.

Browse...

Decrypt password:

Click Restore to upload the file.

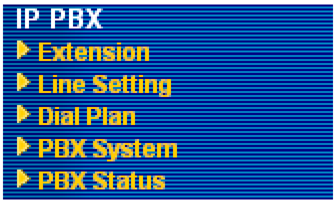
5.11 IP PBX

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 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.

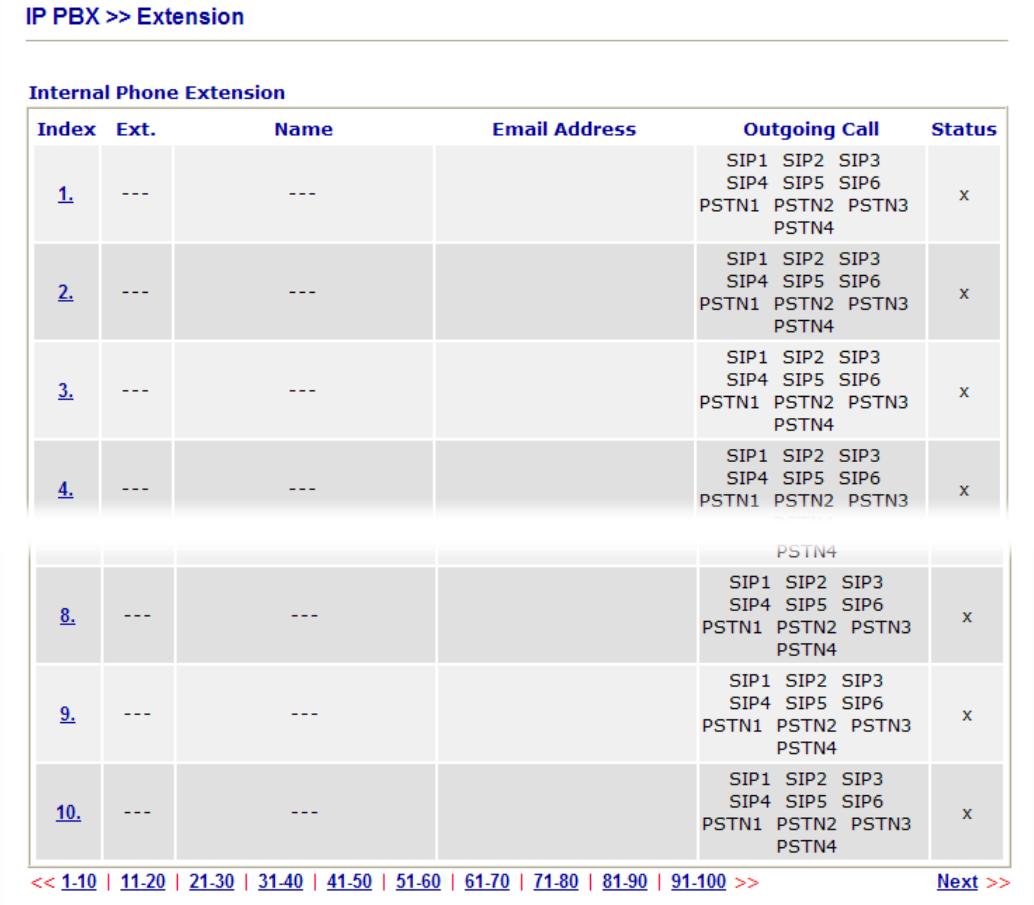
This menu can assist users to configure most of settings in IP PBX.

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.



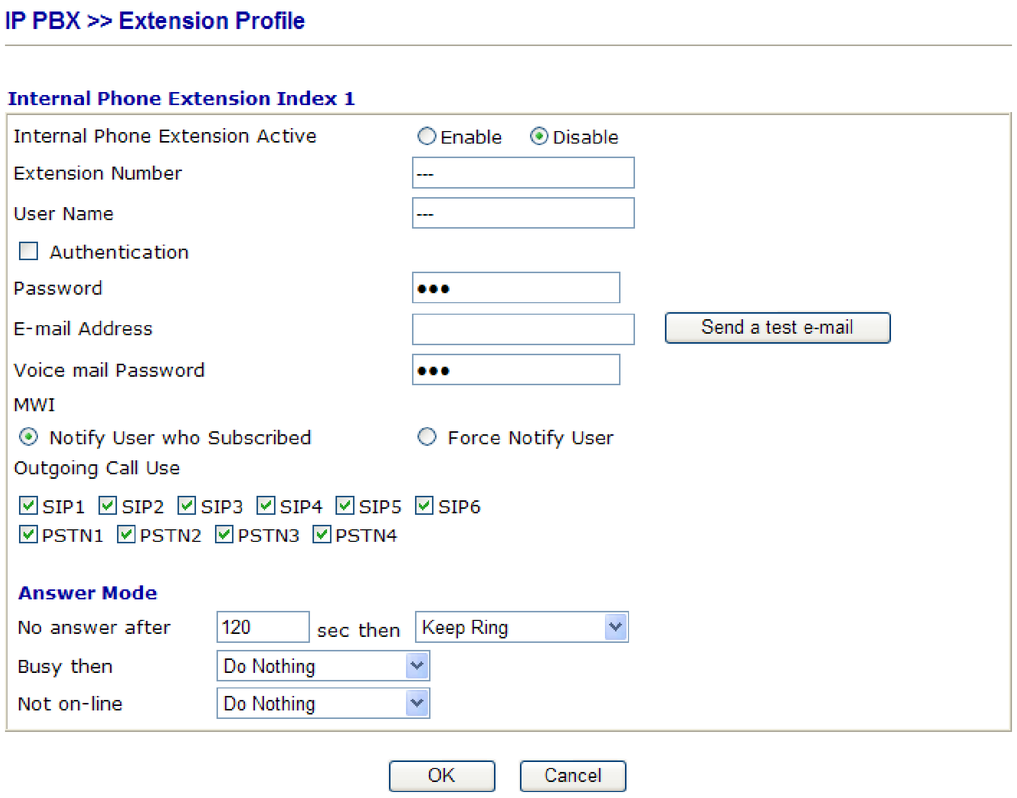
IP PBX >> Extension

Internal Phone Extension

Index	Ext.	Name	Email Address	Outgoing Call	Status
1.	---	---		SIP1 SIP2 SIP3 SIP4 SIP5 SIP6 PSTN1 PSTN2 PSTN3 PSTN4	x
2.	---	---		SIP1 SIP2 SIP3 SIP4 SIP5 SIP6 PSTN1 PSTN2 PSTN3 PSTN4	x
3.	---	---		SIP1 SIP2 SIP3 SIP4 SIP5 SIP6 PSTN1 PSTN2 PSTN3 PSTN4	x
4.	---	---		SIP1 SIP2 SIP3 SIP4 SIP5 SIP6 PSTN1 PSTN2 PSTN3	x
				PSTN4	
8.	---	---		SIP1 SIP2 SIP3 SIP4 SIP5 SIP6 PSTN1 PSTN2 PSTN3 PSTN4	x
9.	---	---		SIP1 SIP2 SIP3 SIP4 SIP5 SIP6 PSTN1 PSTN2 PSTN3 PSTN4	x
10.	---	---		SIP1 SIP2 SIP3 SIP4 SIP5 SIP6 PSTN1 PSTN2 PSTN3 PSTN4	x

<< 1-10 | 11-20 | 21-30 | 31-40 | 41-50 | 51-60 | 61-70 | 71-80 | 81-90 | 91-100 >> Next >>

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



IP PBX >> Extension Profile

Internal Phone Extension Index 1

Internal Phone Extension Active ○ Enable ● Disable

Extension Number: ---

User Name: ---

□ Authentication

Password: ●●●

E-mail Address:

Voice mail Password: ●●●

MWI

● Notify User who Subscribed ○ Force Notify User

Outgoing Call Use

☑ SIP1 ☑ SIP2 ☑ SIP3 ☑ SIP4 ☑ SIP5 ☑ SIP6

☑ PSTN1 ☑ PSTN2 ☑ PSTN3 ☑ PSTN4

Answer Mode

No answer after 120 sec then Keep Ring

Busy then Do Nothing

Not on-line Do Nothing

Internal Phone Extension Active
Click **Enable** to invoke such profile.

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.

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.

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 automatically. The IPPBX will deliver “NOTIFY” message to the users if there is a new message or the user registers on IPPBX again.

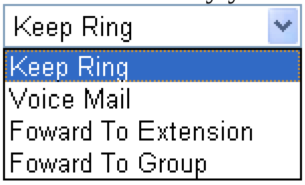
Outgoing Call Use

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.

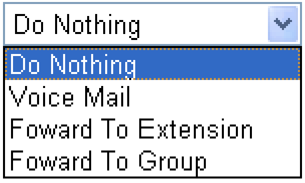
Answer Mode

Specify the way to process incoming phone calls.

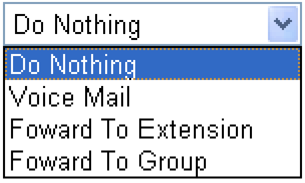
No answer after ….. – When the incoming phone call is not picked up, it will be processed by keeping, forwarding to certain extension or group. Please specify the waiting time and determine the way you want to process.



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

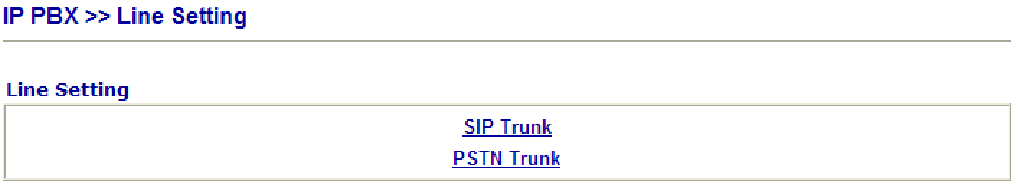


Not on-line – When this extension number is not online, you can forward the incoming phone call to other extension number of group.



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.



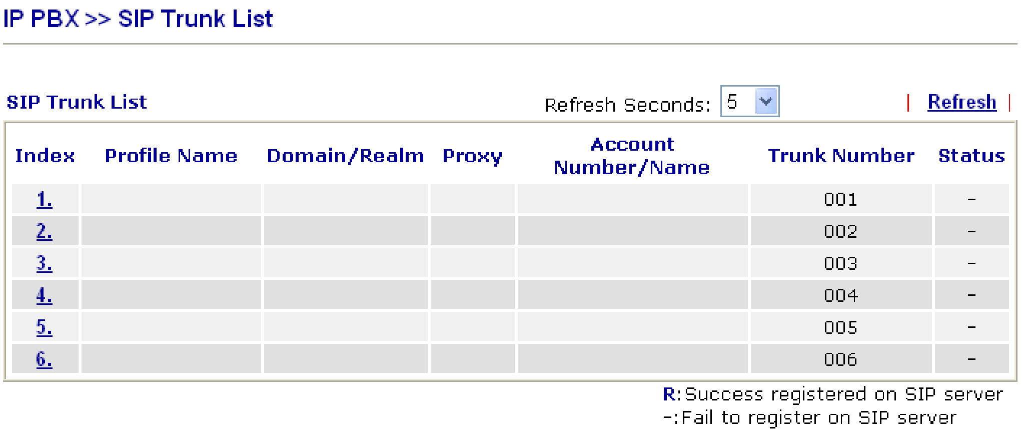
IP PBX >> Line Setting

Line Setting

SIP Trunk
PSTN Trunk

5.11.2.1 SIP Trunk

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



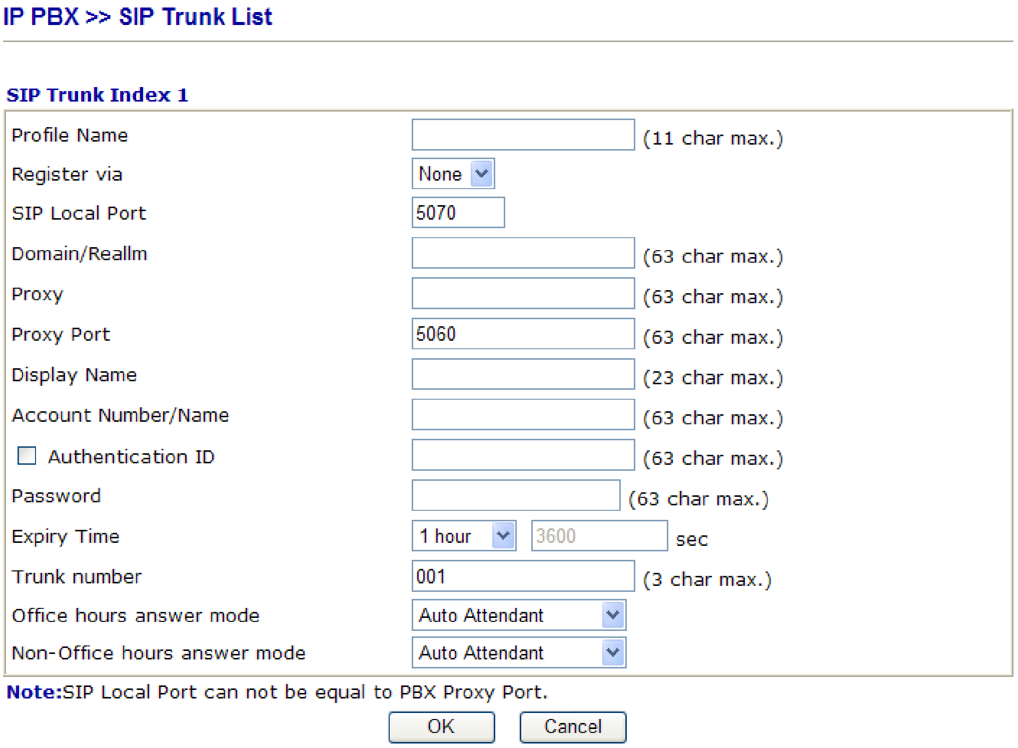
IP PBX >> SIP Trunk List

SIP Trunk List   Refresh Seconds: 5 | Refresh |

Index	Profile Name	Domain/Realm	Proxy	Account Number/Name	Trunk Number	Status
1.					001	-
2.					002	-
3.					003	-
4.					004	-
5.					005	-
6.					006	-

R:Success registered on SIP server
-:Fail to register on SIP server

Please click any number under Index to set detailed configuration.



IP PBX >> SIP Trunk List

SIP Trunk Index 1

Profile Name		(11 char max.)
Register via	None	
SIP Local Port	5070	
Domain/Reallm		(63 char max.)
Proxy		(63 char max.)
Proxy Port	5060	(63 char max.)
Display Name		(23 char max.)
Account Number/Name		(63 char max.)
□ Authentication ID		(63 char max.)
Password		(63 char max.)
Expiry Time	1 hour 3600	sec
Trunk number	001	(3 char max.)
Office hours answer mode	Auto Attendant	
Non-Office hours answer mode	Auto Attendant	

Note:SIP Local Port can not be equal to PBX Proxy Port.

OK   Cancel

Profile Name Assign a name for this profile for identifying. You can type similar name with the domain. For example, if the domain name is *draytel.org*, then you might set *draytel-1* in this field.

Register via If you want to make VoIP call without register personal information, please choose **None** and check the box to achieve the goal. Some SIP server allows user to use VoIP function without registering. Choosing **Auto** is recommended.

SIP Port Set the port number for sending/receiving SIP message for building a session. The default value is **6060.** Your peer must set the same value in his/her Registrar.

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

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

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 @..

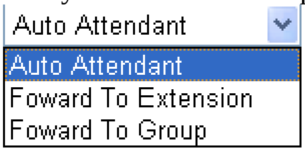
Authentication ID Check the box to invoke this function and enter the name or number used for SIP Authorization with SIP Registrar. If this setting value is the same as Account Name, it is not necessary for you to check the box and set any value in this field.

Password The password provided to you when you registered with a SIP service.

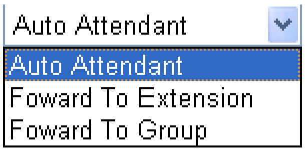
Expiry Time It is the time duration that your SIP Registrar server keeps your registration record. Before the time expires, the router will send another register request to SIP Registrar again.

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.

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.

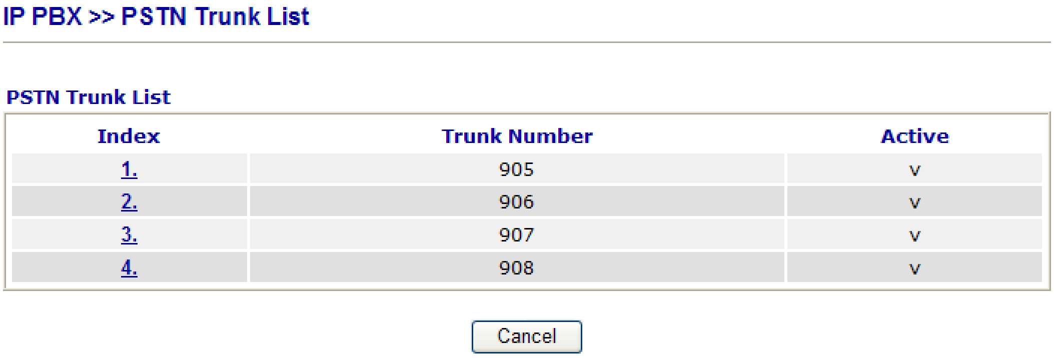


Non-office hours answer mode Set the answering mode for such outside line in non-office time. You can specify it with Auto Attendant (AA), or forward it to any Extension or Group directly.



5.11.2.2 PSTN Trunk

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

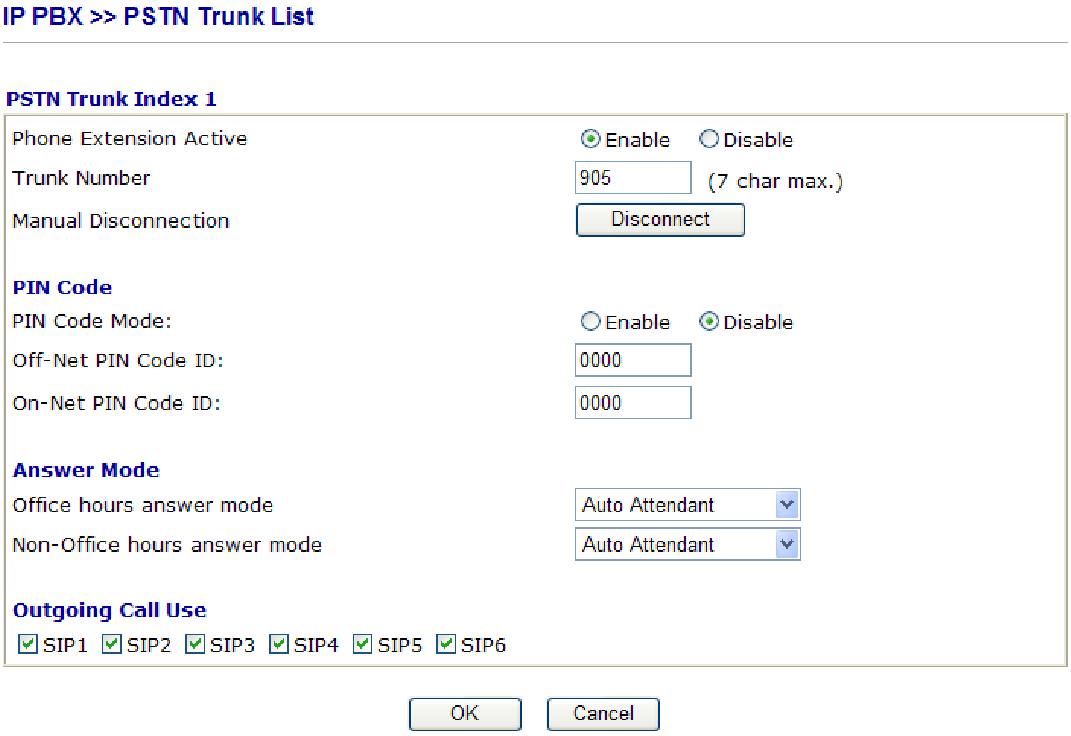


IP PBX >> PSTN Trunk List

PSTN Trunk List

Index	Trunk Number	Active
1.	905	v
2.	906	v
3.	907	v
4.	908	v

Please click any number under Index to set detailed configuration.



IP PBX >> PSTN Trunk List

PSTN Trunk Index 1

Phone Extension Active	● Enable ○ Disable
Trunk Number	905 (7 char max.)
Manual Disconnection	Disconnect

PIN Code

PIN Code Mode:	○ Enable ● Disable
Off-Net PIN Code ID:	0000
On-Net PIN Code ID:	0000

Answer Mode

Office hours answer mode	Auto Attendant
Non-Office hours answer mode	Auto Attendant

Outgoing Call Use

☑ SIP1 ☑ SIP2 ☑ SIP3 ☑ SIP4 ☑ SIP5 ☑ SIP6

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.

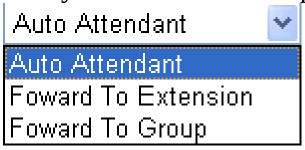
Manual Disconnection To disconnect the PSTN trunk, simply click the **Disconnect** button. The PSTN phone call will be disconnected immediately.

PIN Code Mode Click **Enable** to invoke this setting.

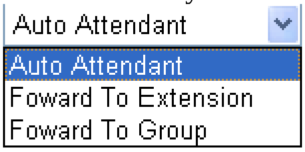
Off-Net PIN Code ID Type the PIN code number to make off-net call to PSTN trunk.

On-Net PIN Code ID 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.

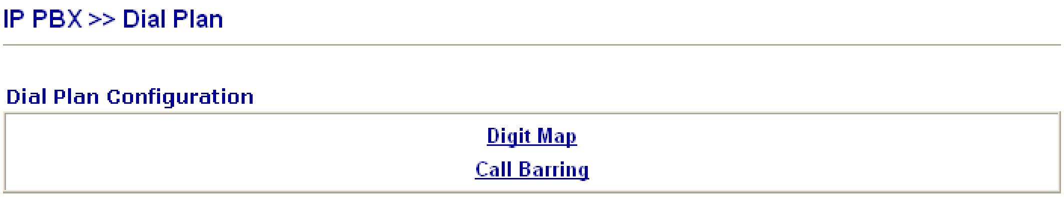


Non-office hours answer mode Set the answering mode for such outside line in non-office time. You can specify it with Auto Attendant (AA), or forward it to any Extension or Group directly.



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

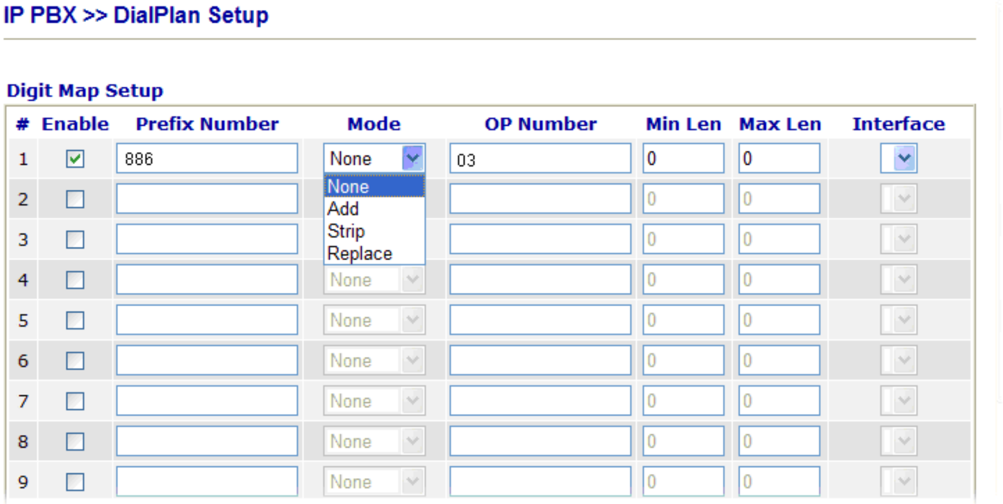


IP PBX >> Dial Plan

Dial Plan Configuration

5.11.3.1 Digit Map

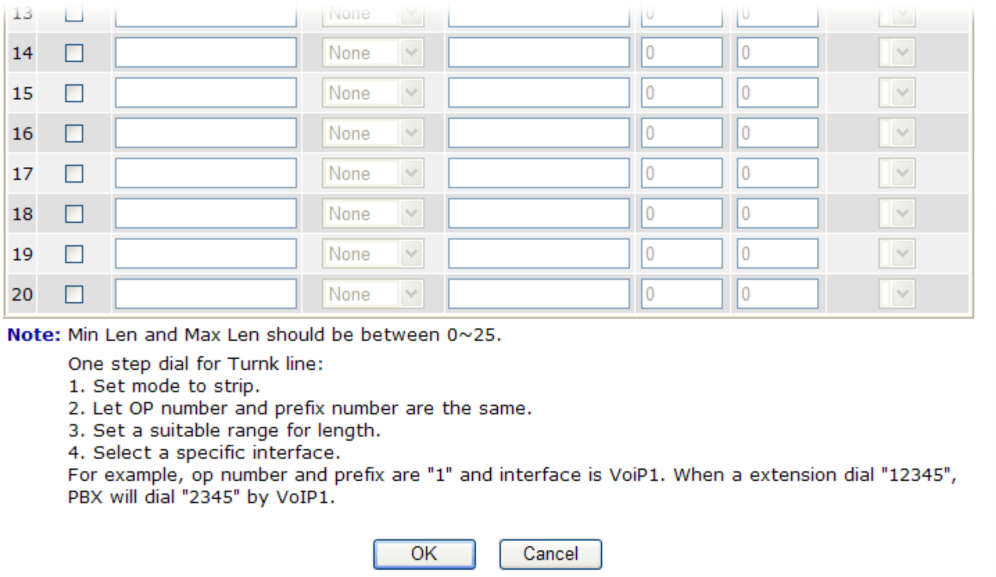
For the convenience of user, this page allows users to edit prefix number for the SIP account with adding number, stripping number or replacing number. It is used to help user having a quick and easy way to dial out through VoIP interface.



IP PBX >> DialPlan Setup

Digit Map Setup

#	Enable	Prefix Number	Mode	OP Number	Min Len	Max Len	Interface
1	☑	886	None	03	0	0	
2	□				0	0	
3	□				0	0	
4	□		None		0	0	
5	□		None		0	0	
6	□		None		0	0	
7	□		None		0	0	
8	□		None		0	0	
9	□		None		0	0	



13	□		None		0	0	
14	□		None		0	0	
15	□		None		0	0	
16	□		None		0	0	
17	□		None		0	0	
18	□		None		0	0	
19	□		None		0	0	
20	□		None		0	0	

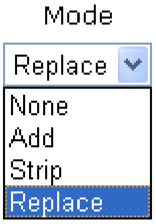
Note: Min Len and Max Len should be between 0~25.

One step dial for Turnk line:
1. Set mode to strip.
2. Let OP number and prefix number are the same.
3. Set a suitable range for length.
4. Select a specific interface.
For example, op number and prefix are "1" and interface is VoiP1. When a extension dial "12345", PBX will dial "2345" by VoIP1.

Enable Check this box to invoke this setting.

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

Mode **None** - No action.
Add - When you choose this mode, the OP number will be added with the prefix number for calling out through the specific VoIP interface.
Strip - When you choose this mode, the OP number will be deleted by the prefix number for calling out through the specific VoIP interface. For 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. For example, if the OP number is set with 03, it will be replaced by 8863 (prefix number). 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.

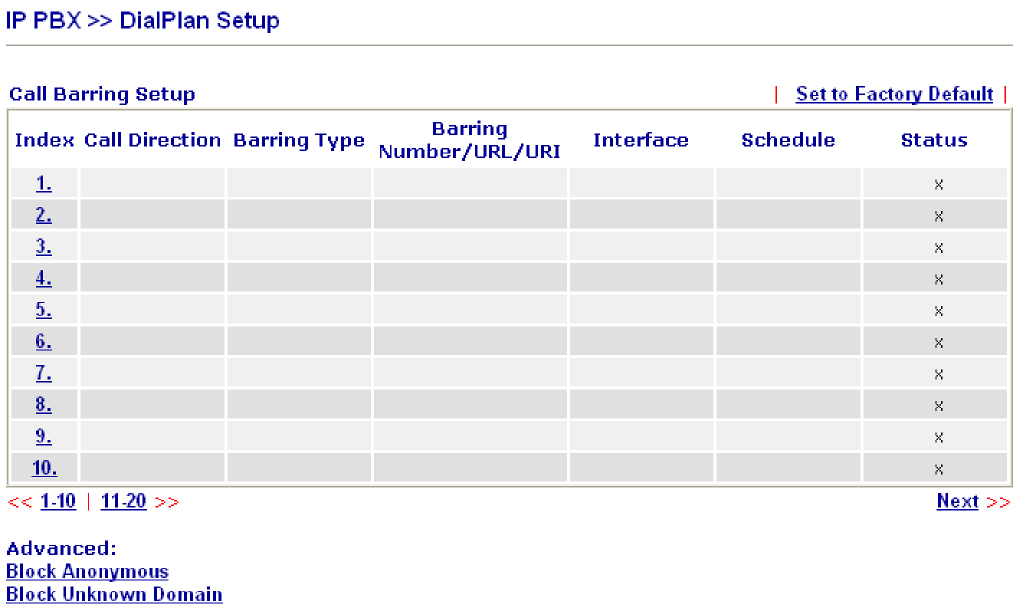
Min Len Set the minimal length of the dial number for applying the prefix number settings. Take the above picture (Prefix Table Setup web page) as an example, if the dial number is between 7 and 9, that number can apply the prefix number settings here.

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

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

5.11.3.2 Call Barring

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



IP PBX >> DialPlan Setup

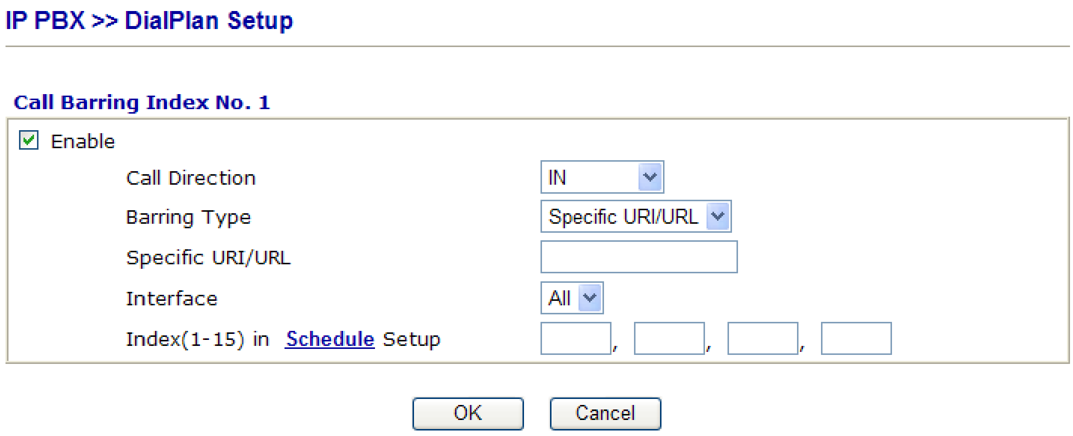
Call Barring Setup | Set to Factory Default |

Index	Call Direction	Barring Type	Barring Number/URL/URI	Interface	Schedule	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 >>

Advanced:
Block Anonymous
Block Unknown Domain

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



IP PBX >> DialPlan Setup

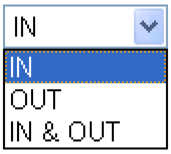
Call Barring Index No. 1

☑ Enable

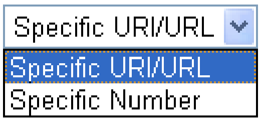
Call Direction	IN
Barring Type	Specific URI/URL
Specific URI/URL	
Interface	All
Index(1-15) in Schedule Setup	, , ,

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.



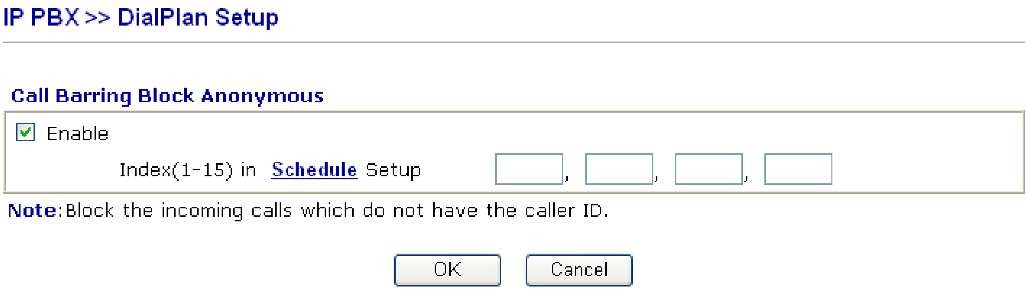
Specific Number/Specific URI/URL This field will be changed based on the type you selected for barring Type. Please type numbers or URI/URL

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

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.



IP PBX >> DialPlan Setup

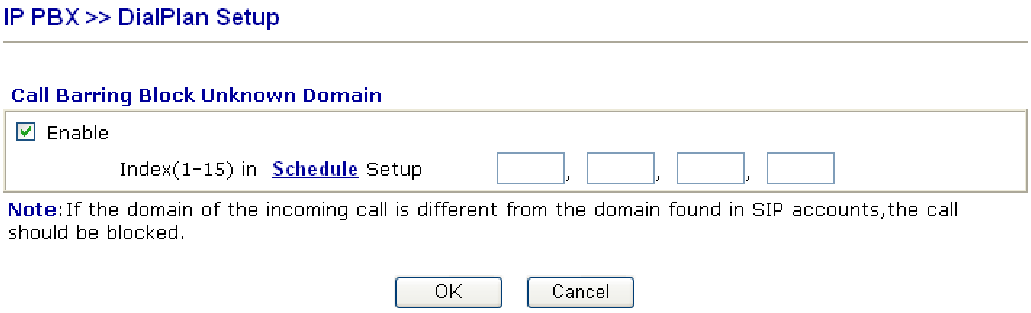
Call Barring Block Anonymous

☑ Enable

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

Note: Block the incoming calls which do not have the caller ID.

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.



IP PBX >> DialPlan Setup

Call Barring Block Unknown Domain

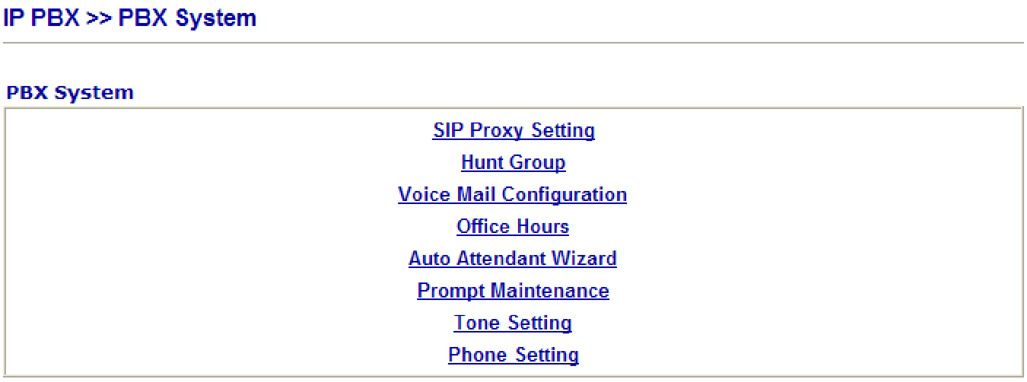
☑ Enable

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

Note: If the domain of the incoming call is different from the domain found in SIP accounts,the call should be blocked.

5.11.4 PBX System

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



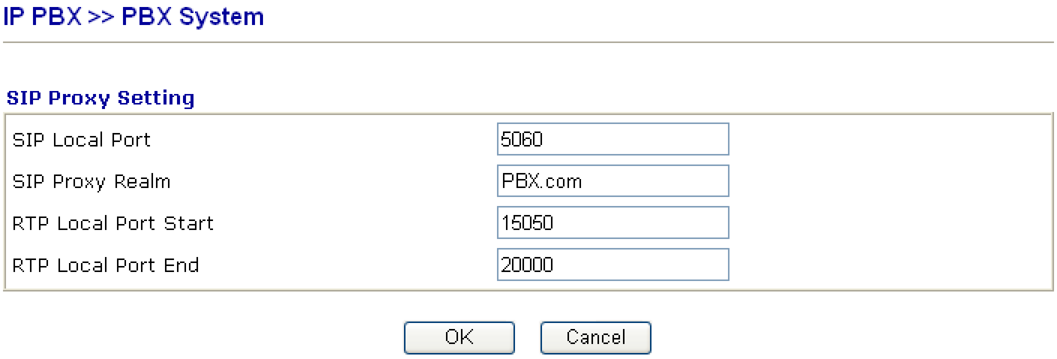
IP PBX >> PBX System

PBX System

SIP Proxy Setting
Hunt Group
Voice Mail Configuration
Office Hours
Auto Attendant Wizard
Prompt Maintenance
Tone Setting
Phone Setting

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.



IP PBX >> PBX System

SIP Proxy Setting

SIP Local Port	5060
SIP Proxy Realm	PBX.com
RTP Local Port Start	15050
RTP Local Port End	20000

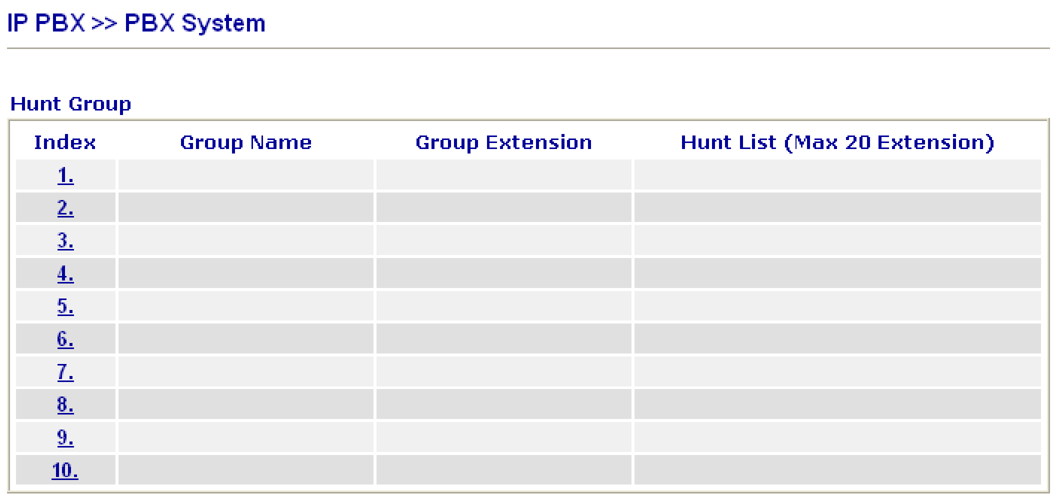
SIP Local Port Set a port number as SIP local port. The default setting is 5060.

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

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

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.



IP PBX >> PBX System

Hunt Group

Index	Group Name	Group Extension	Hunt List (Max 20 Extension)
1.			
2.			
3.			
4.			
5.			
6.			
7.			
8.			
9.			
10.			

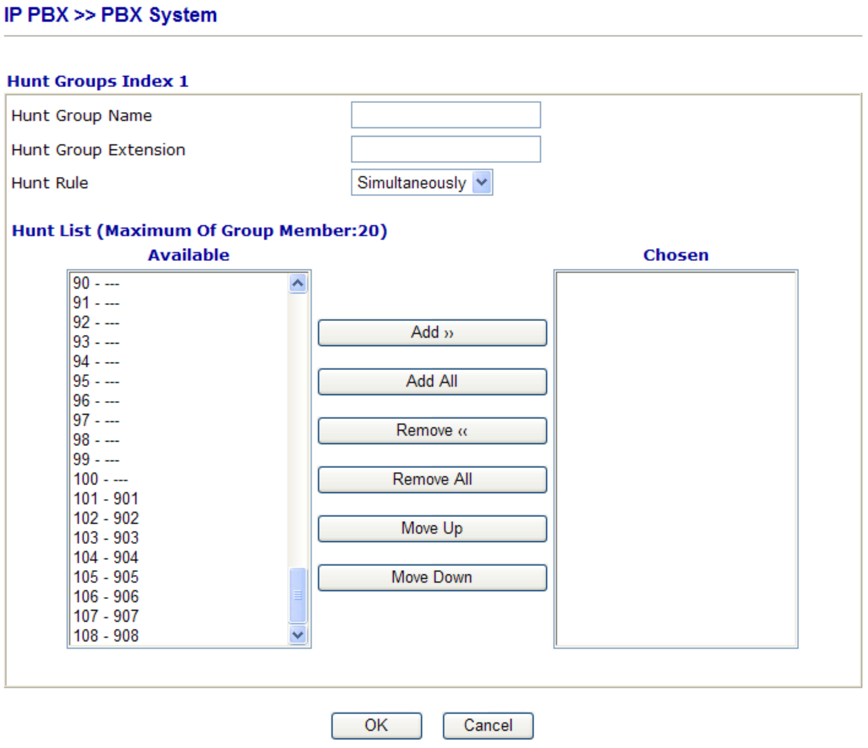
Index You can set 10 groups for using in different conditions. Simply click the number under Index to specify detailed information.

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.



IP PBX >> PBX System

Hunt Groups Index 1

Hunt Group Name	
Hunt Group Extension	
Hunt Rule	Simultaneously

Hunt List (Maximum Of Group Member:20)

Available

90 - ---
91 - ---
92 - ---
93 - ---
94 - ---
95 - ---
96 - ---
97 - ---
98 - ---
99 - ---
100 - ---
101 - 901
102 - 902
103 - 903
104 - 904
105 - 905
106 - 906
107 - 907
108 - 908

Chosen

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.

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.

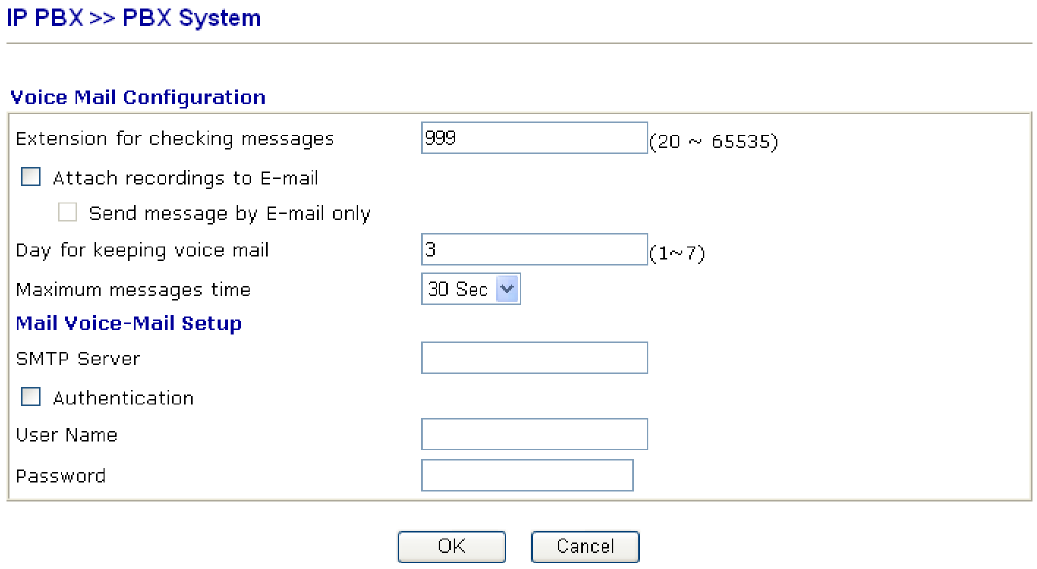
Remove All Click this button to clear all of the selections in Chosen area.

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.



IP PBX >> PBX System

Voice Mail Configuration

Extension for checking messages	999 (20 ~ 65535)
□ Attach recordings to E-mail	
□ Send message by E-mail only	
Day for keeping voice mail	3 (1~7)
Maximum messages time	30 Sec
Mail Voice-Mail Setup	
SMTP Server	
□ Authentication	
User Name	
Password	

Extension for checking messages The number specified here is used for the user to listen personal voice mail from IP PBX device.

Attach recordings to e-mail IP PBX can send the voice mail to the specified e-mail address for the incoming call if you check this box.
Send message through E-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.

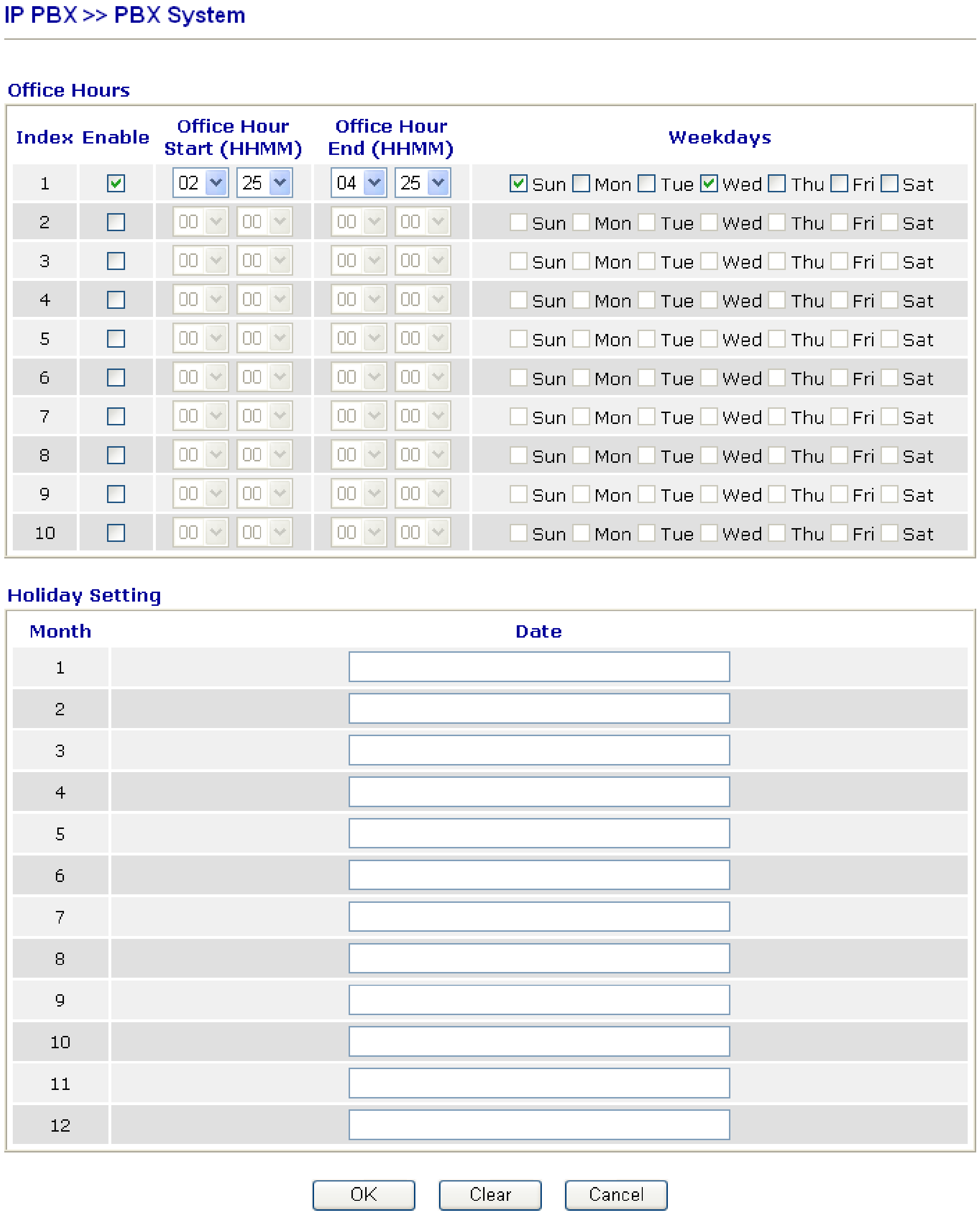
Authentication Check this box to authenticate the mail server.

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).



IP PBX >> PBX System

Office Hours

Index	Enable	Office Hour Start (HHMM)	Office Hour End (HHMM)	Weekdays
1	☑	02 25	04 25	☑ Sun ☐ Mon ☐ Tue ☑ Wed ☐ Thu ☐ Fri ☐ Sat
2	☐	00 00	00 00	☐ Sun ☐ Mon ☐ Tue ☐ Wed ☐ Thu ☐ Fri ☐ Sat
3	☐	00 00	00 00	☐ Sun ☐ Mon ☐ Tue ☐ Wed ☐ Thu ☐ Fri ☐ Sat
4	☐	00 00	00 00	☐ Sun ☐ Mon ☐ Tue ☐ Wed ☐ Thu ☐ Fri ☐ Sat
5	☐	00 00	00 00	☐ Sun ☐ Mon ☐ Tue ☐ Wed ☐ Thu ☐ Fri ☐ Sat
6	☐	00 00	00 00	☐ Sun ☐ Mon ☐ Tue ☐ Wed ☐ Thu ☐ Fri ☐ Sat
7	☐	00 00	00 00	☐ Sun ☐ Mon ☐ Tue ☐ Wed ☐ Thu ☐ Fri ☐ Sat
8	☐	00 00	00 00	☐ Sun ☐ Mon ☐ Tue ☐ Wed ☐ Thu ☐ Fri ☐ Sat
9	☐	00 00	00 00	☐ Sun ☐ Mon ☐ Tue ☐ Wed ☐ Thu ☐ Fri ☐ Sat
10	☐	00 00	00 00	☐ Sun ☐ Mon ☐ Tue ☐ Wed ☐ Thu ☐ Fri ☐ Sat

Holiday Setting

Month	Date
1	
2	
3	
4	
5	
6	
7	
8	
9	
10	
11	
12	

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

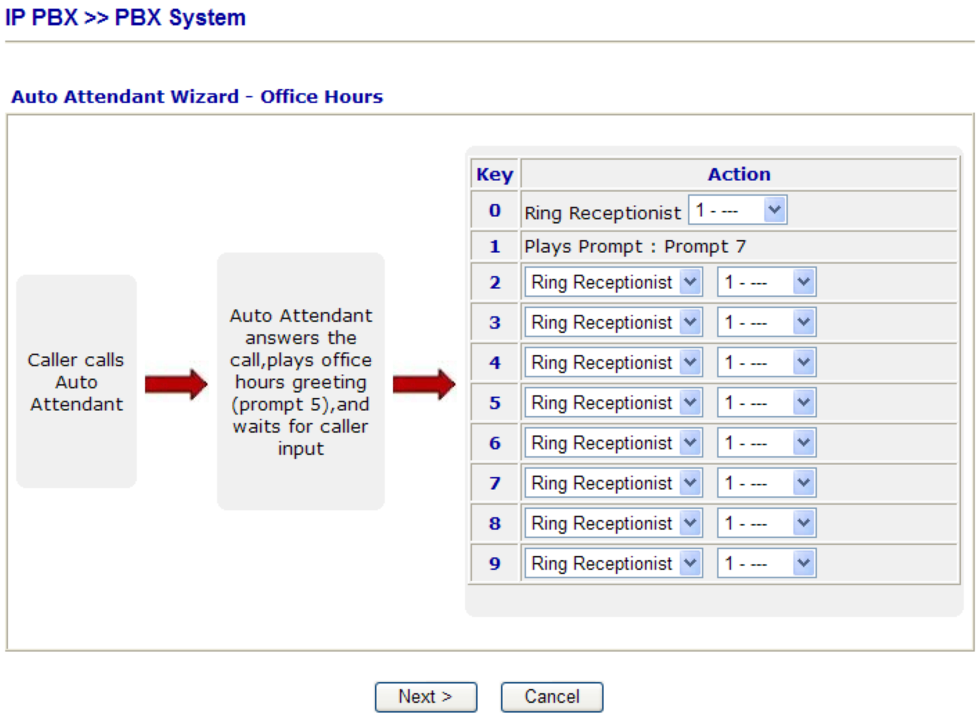
Office Hour End Use the drop down menu to choose the time as the ending point.

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.



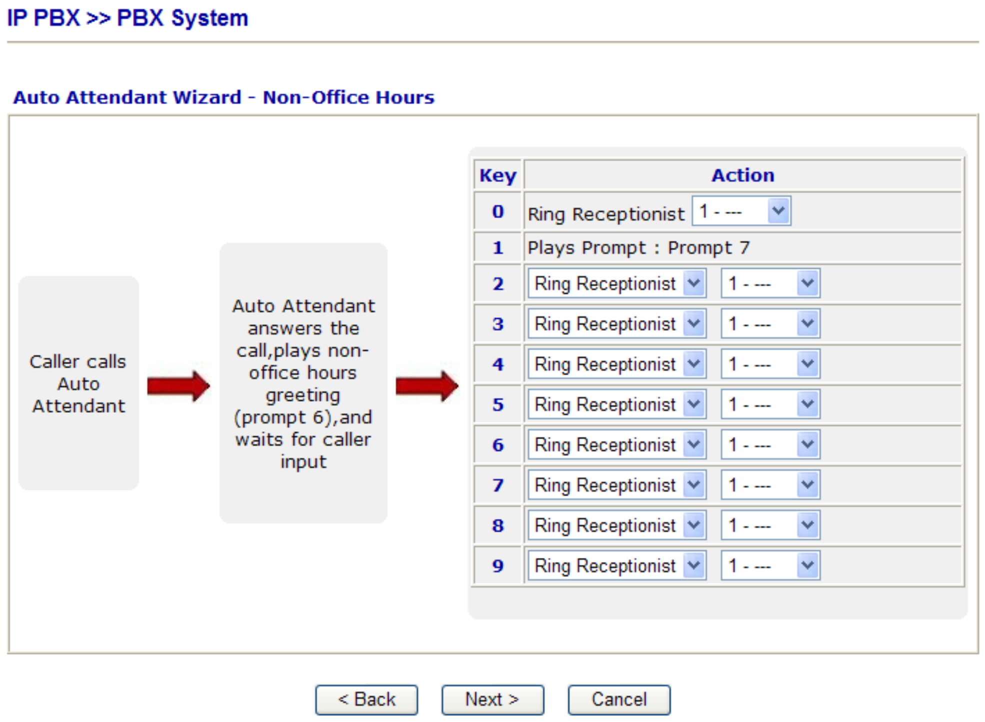
IP PBX >> PBX System

Auto Attendant Wizard - Office Hours

Caller calls Auto Attendant → Auto Attendant answers the call,plays office hours greeting (prompt 5),and waits for caller input →

Key	Action	
0	Ring Receptionist 1 - ---	
1	Plays Prompt : Prompt 7	
2	Ring Receptionist	1 - ---
3	Ring Receptionist	1 - ---
4	Ring Receptionist	1 - ---
5	Ring Receptionist	1 - ---
6	Ring Receptionist	1 - ---
7	Ring Receptionist	1 - ---
8	Ring Receptionist	1 - ---
9	Ring Receptionist	1 - ---

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



IP PBX >> PBX System

Auto Attendant Wizard - Non-Office Hours

Caller calls Auto Attendant → Auto Attendant answers the call,plays non-office hours greeting (prompt 6),and waits for caller input →

Key	Action	
0	Ring Receptionist 1 - ---	
1	Plays Prompt : Prompt 7	
2	Ring Receptionist	1 - ---
3	Ring Receptionist	1 - ---
4	Ring Receptionist	1 - ---
5	Ring Receptionist	1 - ---
6	Ring Receptionist	1 - ---
7	Ring Receptionist	1 - ---
8	Ring Receptionist	1 - ---
9	Ring Receptionist	1 - ---

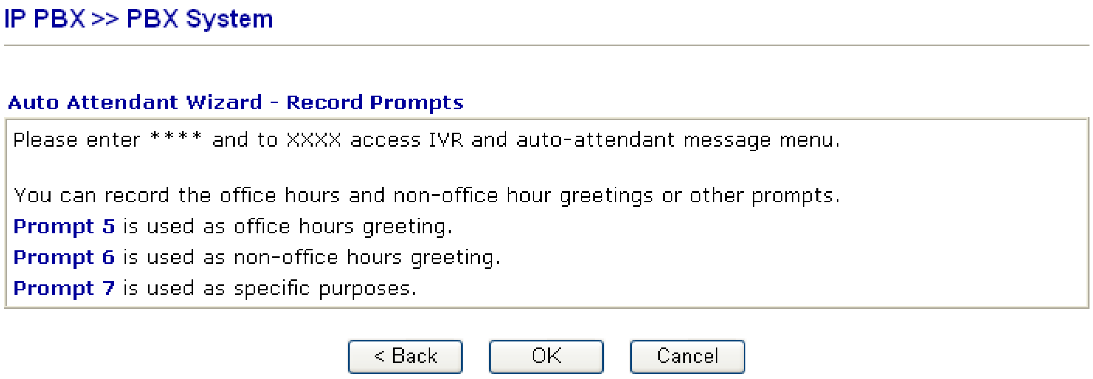
Ring Receptionist Only the extension number selected here will ring.

Plays Prompt Audio file will be played automatically.

Key 2-9 Drop down menu 1 contains **Ring Receptionist** /**Plays Prompt**/**Ring Hunt Group**.
Drop down menu 2 contains extension name (ex. Tom, Mike)

or [Prompt 1~ Prompt 10, audio files] or [Group Name (ex. Sales, RD2)]. It will be changed according to drop down menu 1.

Finally, the following window will appear.



IP PBX >> PBX System

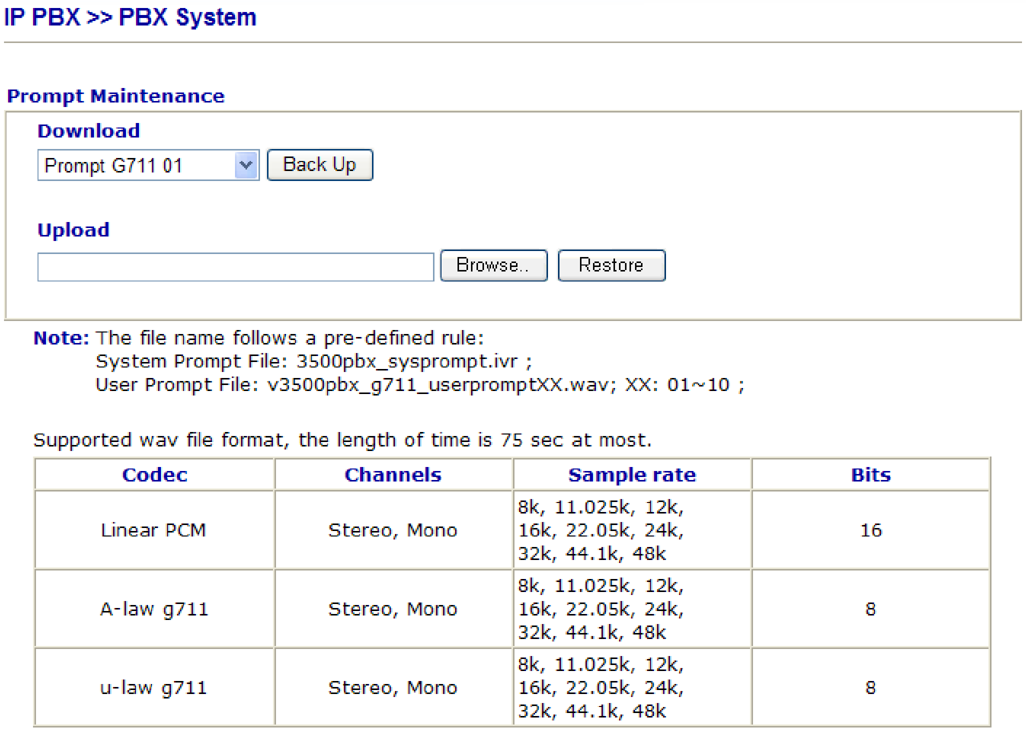
Auto Attendant Wizard - Record Prompts

Please enter **** and to XXXX access IVR and auto-attendant message menu.

You can record the office hours and non-office hour greetings or other prompts.
Prompt 5 is used as office hours greeting.
Prompt 6 is used as non-office hours greeting.
Prompt 7 is used as specific purposes.

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.



IP PBX >> PBX System

Prompt Maintenance

Download

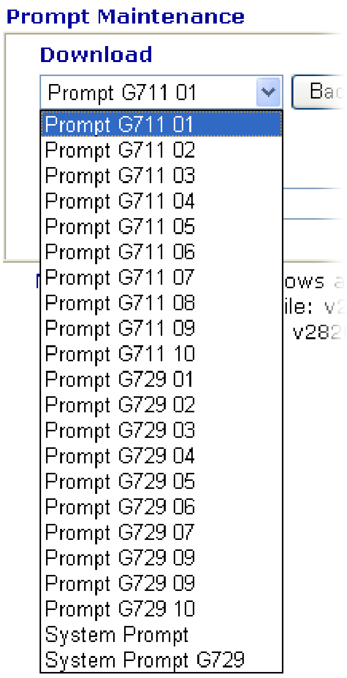
Upload

Note: The file name follows a pre-defined rule:
System Prompt File: 3500pbx_sysprompt.ivr ;
User Prompt File: v3500pbx_g711_userpromptXX.wav; XX: 01~10 ;

Supported wav file format, the length of time is 75 sec at most.

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:

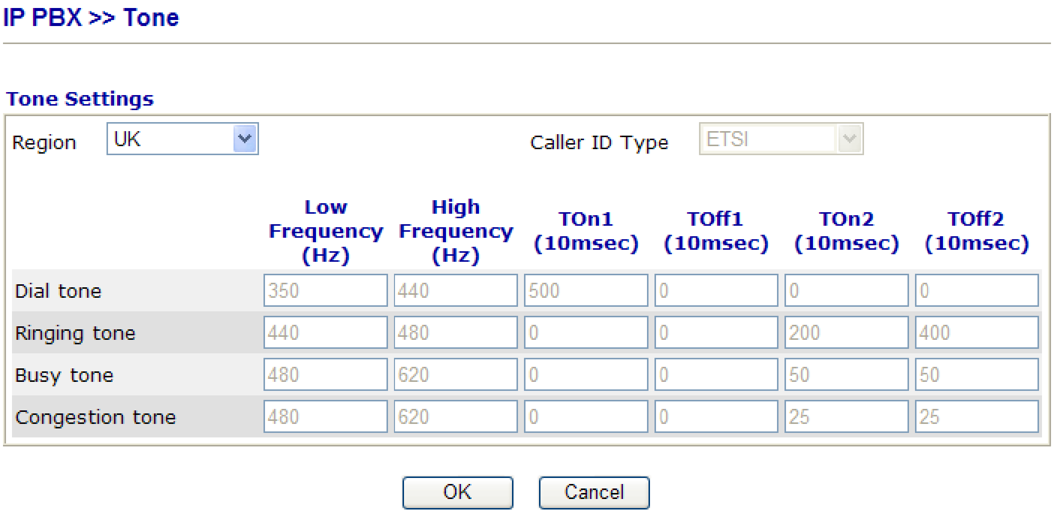
1. Please use *DOS-BOX FTP client* (Windows built-in FTP client utility) to login VigorIPPBX FTP server.
2. Press Enter to pass authentication.
3. Type **put v3510_g729_userprompt.ivr**.
4. Wait for a while. The message of **226 user prompts G.729 file has been uploaded successfully** will appear.
5.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


IP PBX >> Tone

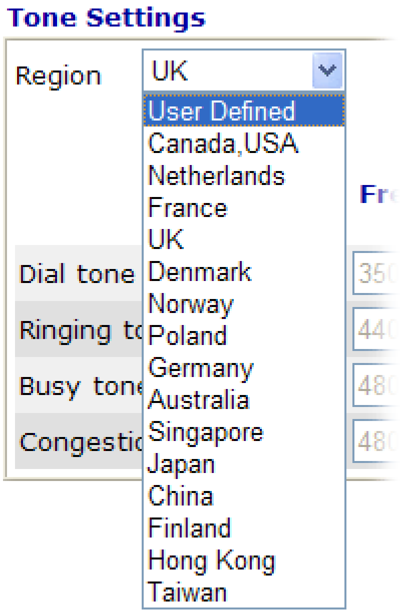
Tone Settings

Region: UK

Caller ID Type: ETSI

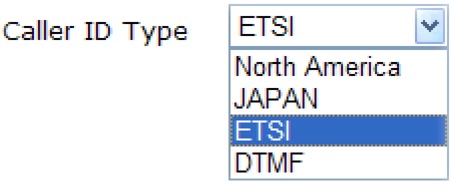
	Low Frequency (Hz)	High Frequency (Hz)	TOn1 (10msec)	TOff1 (10msec)	TOn2 (10msec)	TOff2 (10msec)
Dial tone	350	440	500	0	0	0
Ringing tone	440	480	0	0	200	400
Busy tone	480	620	0	0	50	50
Congestion tone	480	620	0	0	25	25

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.

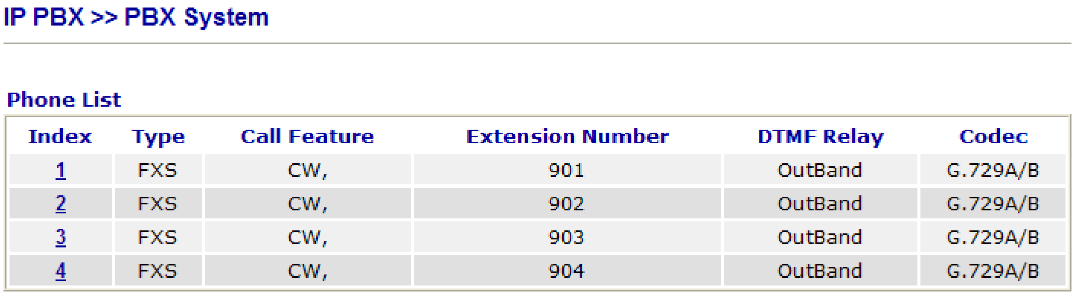
Caller ID Type Select the caller ID type for setting Dial tone, Ringing tone, Busy tone and Congestion tone respectively.



Caller ID Type: ETSI

5.11.4.8 Phone Setting

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

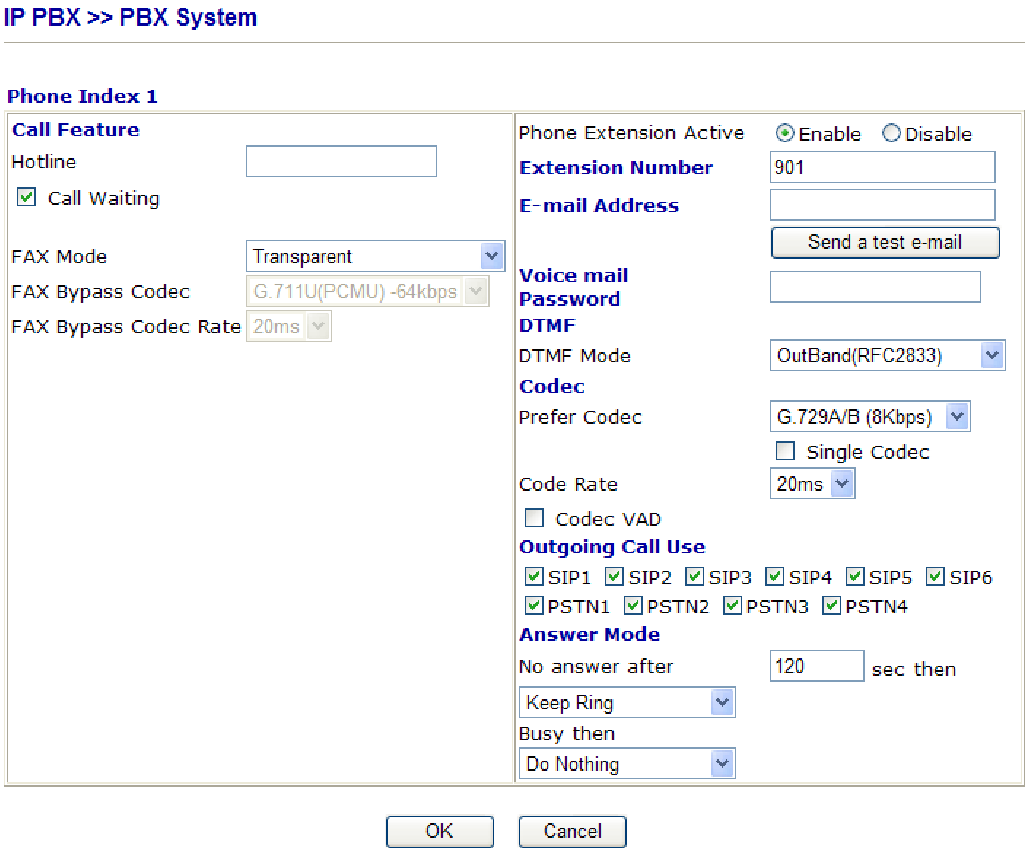


IP PBX >> PBX System

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.



IP PBX >> PBX System

Phone Index 1

Call Feature

Hotline:

☑ Call Waiting

FAX Mode: Transparent

FAX Bypass Codec: G.711U(PCMU) -64kbps

FAX Bypass Codec Rate: 20ms

Phone Extension Active: ● Enable ○ Disable

Extension Number: 901

E-mail Address:

Voice mail Password:

DTMF

DTMF Mode: OutBand(RFC2833)

Codec

Prefer Codec: G.729A/B (8Kbps)

□ Single Codec

Code Rate: 20ms

□ Codec VAD

Outgoing Call Use

☑ SIP1 ☑ SIP2 ☑ SIP3 ☑ SIP4 ☑ SIP5 ☑ SIP6

☑ PSTN1 ☑ PSTN2 ☑ PSTN3 ☑ PSTN4

Answer Mode

No answer after 120 sec then

Keep Ring

Busy then

Do Nothing

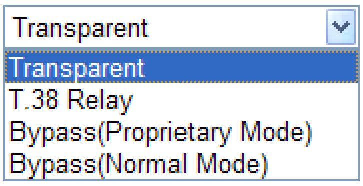
Hotline Check the box to enable it. Type in the SIP URL in the field for dialing automatically when you pick up the phone set.

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

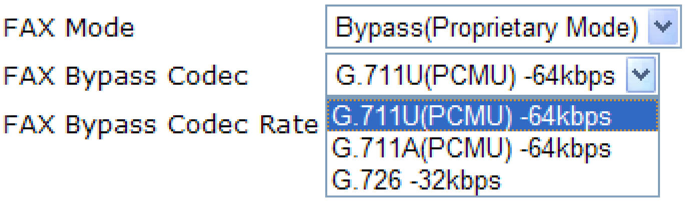
The FAX function mode. There are several options:


Transparent

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).

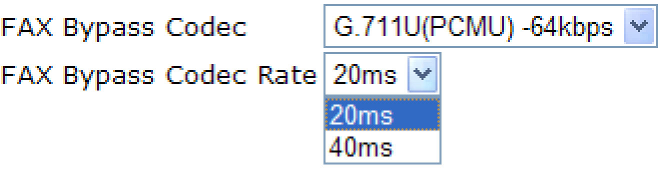
FAX Bypass Codec

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


FAX Mode Bypass(Proprietary Mode)
FAX Bypass Codec G.711U(PCMU) -64kbps
FAX Bypass Codec Rate

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.


FAX Bypass Codec G.711U(PCMU) -64kbps
FAX Bypass Codec Rate 20ms

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.

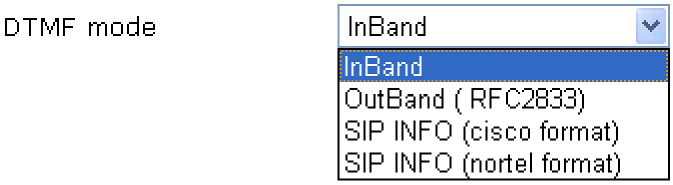
DTMF

DTMF 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.

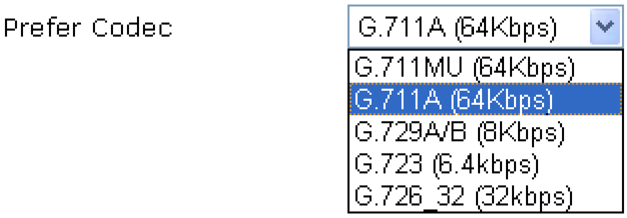
SIP INFO- Choose this one then the Vigor will capture the DTMF tone and transfer it into SIP form. Then it will be sent to the remote end with SIP message.


DTMF mode: InBand

Codec

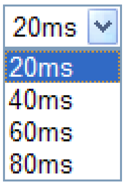
Prefer Codec - Select one of five codecs as the default for your VoIP calls. The codec used for each call will be negotiated with the peer party before each session, and so may not be your default choice. The default codec is G.729A/B; it occupies little bandwidth while maintaining good voice quality.

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.


Prefer Codec: G.711A (64Kbps)

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.


20ms

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

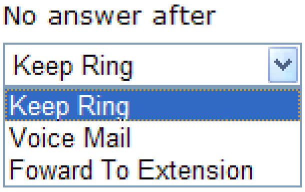
There are several outside lines (SIP accounts) for you to specify for such extension. Please check the one(s) you want.

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.

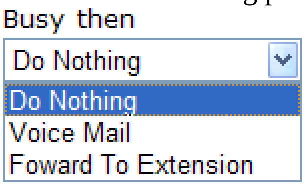


No answer after

Keep Ring

Keep Ring
Voice Mail
Foward To Extension

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

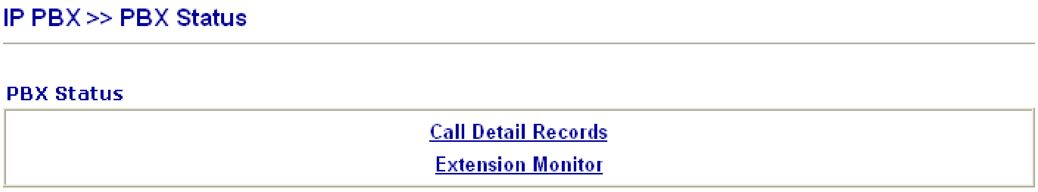


Busy then

Do Nothing

Do Nothing
Voice Mail
Foward To Extension

5.11.5 PBX Status



IP PBX >> PBX Status

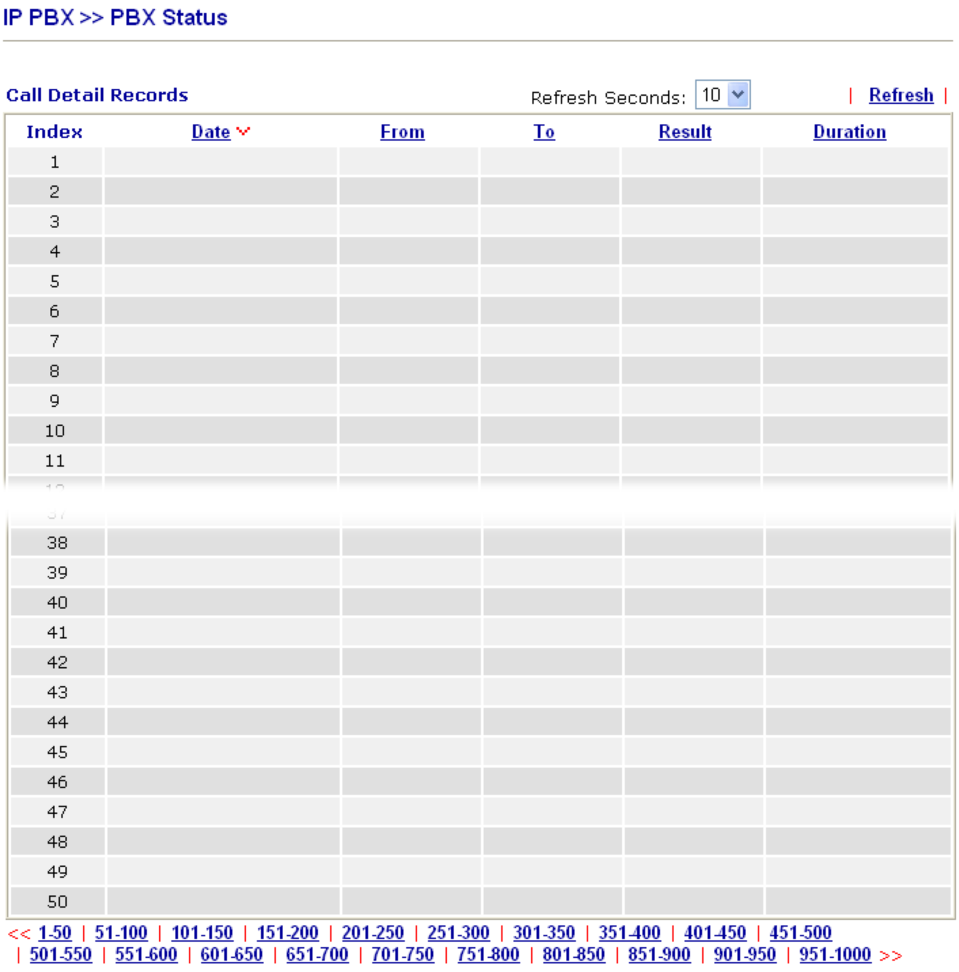
PBX Status

Call Detail Records

Extension Monitor

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.



IP PBX >> PBX Status

Call Detail Records   Refresh Seconds: 10 | Refresh |

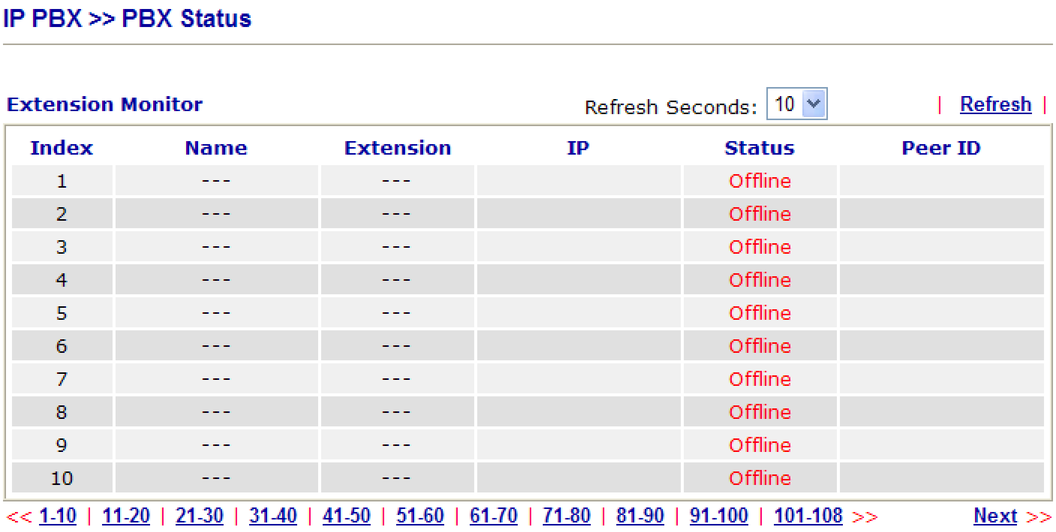
Index	Date ⌄	From	To	Result	Duration
1					
2					
3					
4					
5					
6					
7					
8					
9					
10					
11					
38					
39					
40					
41					
42					
43					
44					
45					
46					
47					
48					
49					
50					

<< 1-50 | 51-100 | 101-150 | 151-200 | 201-250 | 251-300 | 301-350 | 351-400 | 401-450 | 451-500 | 501-550 | 551-600 | 601-650 | 651-700 | 701-750 | 751-800 | 801-850 | 851-900 | 901-950 | 951-1000 >>

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.



IP PBX >> PBX Status

Extension Monitor

Refresh Seconds: 10

| Refresh |

Index	Name	Extension	IP	Status	Peer ID
1	---	---		Offline	
2	---	---		Offline	
3	---	---		Offline	
4	---	---		Offline	
5	---	---		Offline	
6	---	---		Offline	
7	---	---		Offline	
8	---	---		Offline	
9	---	---		Offline	
10	---	---		Offline	

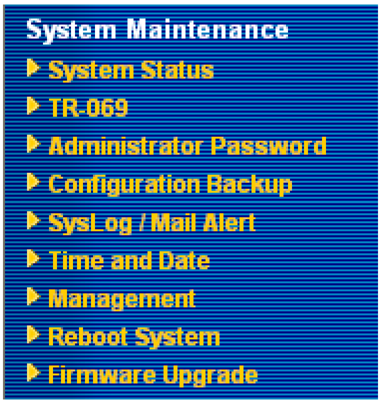
<< 1-10 | 11-20 | 21-30 | 31-40 | 41-50 | 51-60 | 61-70 | 71-80 | 81-90 | 91-100 | 101-108 >> Next >>

Refresh Click it to reload the page.

5.12 System Maintenance

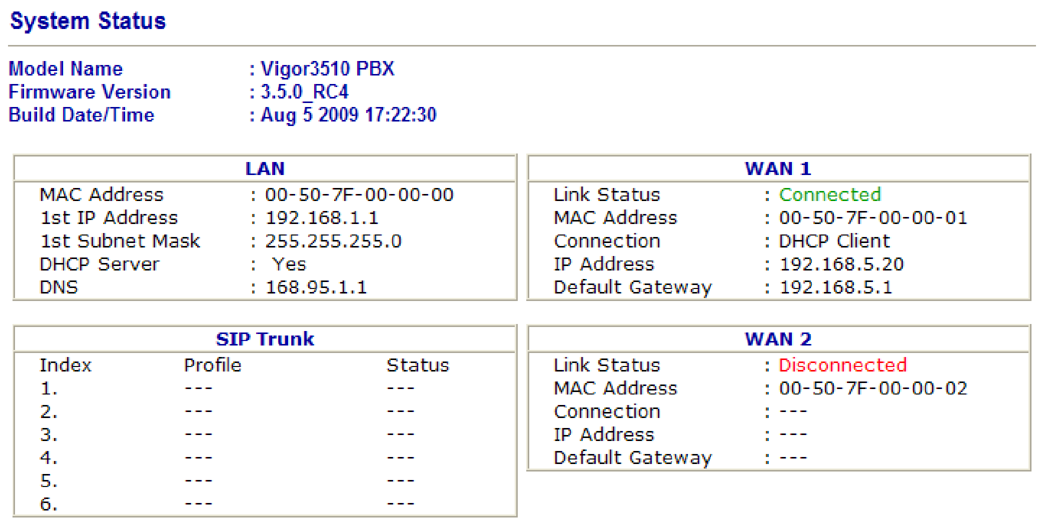
For the system setup, there are several items that you have to know the way of configuration: Status, Administrator Password, Configuration Backup, Syslog, Time setup, Reboot System, Firmware Upgrade.

Below shows the menu items for System Maintenance.



5.12.1 System Status

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



System Status

Model Name : Vigor3510 PBX
Firmware Version : 3.5.0_RC4
Build Date/Time : Aug 5 2009 17:22:30

LAN	
MAC Address	: 00-50-7F-00-00-00
1st IP Address	: 192.168.1.1
1st Subnet Mask	: 255.255.255.0
DHCP Server	: Yes
DNS	: 168.95.1.1

WAN 1	
Link Status	: Connected
MAC Address	: 00-50-7F-00-00-01
Connection	: DHCP Client
IP Address	: 192.168.5.20
Default Gateway	: 192.168.5.1

SIP Trunk

Index	Profile	Status
1.	---	---
2.	---	---
3.	---	---
4.	---	---
5.	---	---
6.	---	---

WAN 2	
Link Status	: Disconnected
MAC Address	: 00-50-7F-00-00-02
Connection	: ---
IP Address	: ---
Default Gateway	: ---

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.

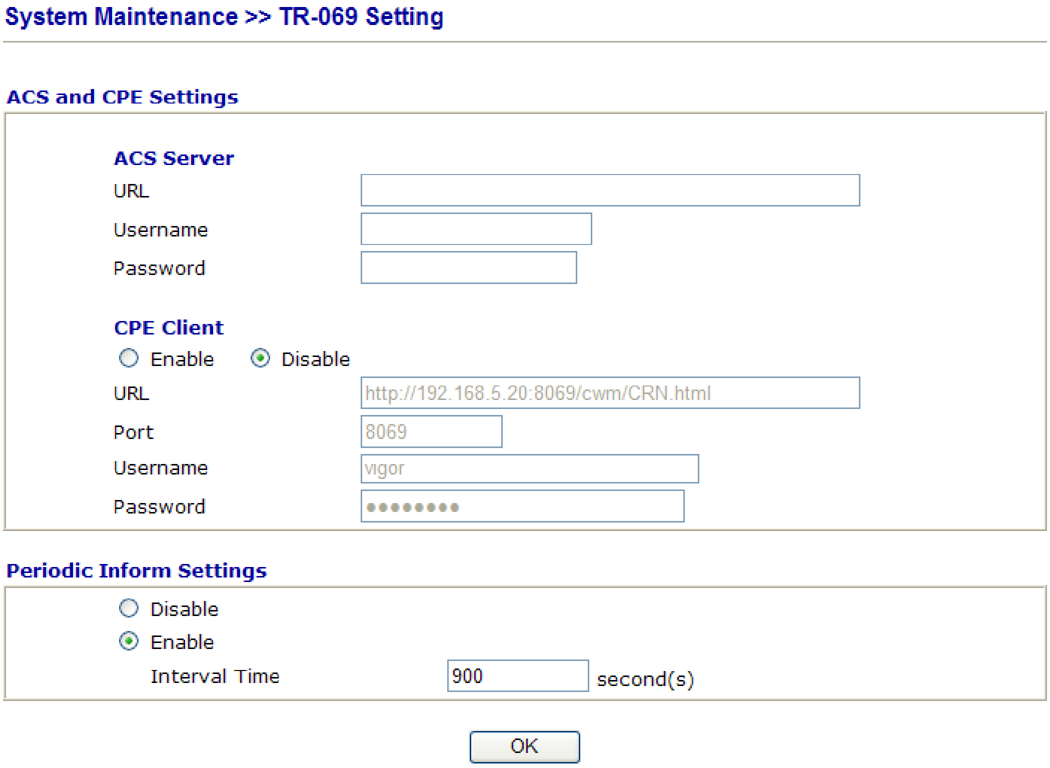
Default Gateway Display the assigned IP address of the default gateway.

SIP Trunk-------

Index/Profile/Status Display current status for SIP profiles.

5.12.2 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.



System Maintenance >> TR-069 Setting

ACS and CPE Settings

ACS Server

URL

Username

Password

CPE Client

○ Enable ● Disable

URL http://192.168.5.20:8069/cwm/CRN.html

Port 8069

Username vigor

Password ●●●●●●●●

Periodic Inform Settings

○ Disable

● Enable

Interval Time 900 second(s)

ACS Server

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

CPE Client

It is not necessary for you to type them. Such information is useful for Auto Configuration Server.

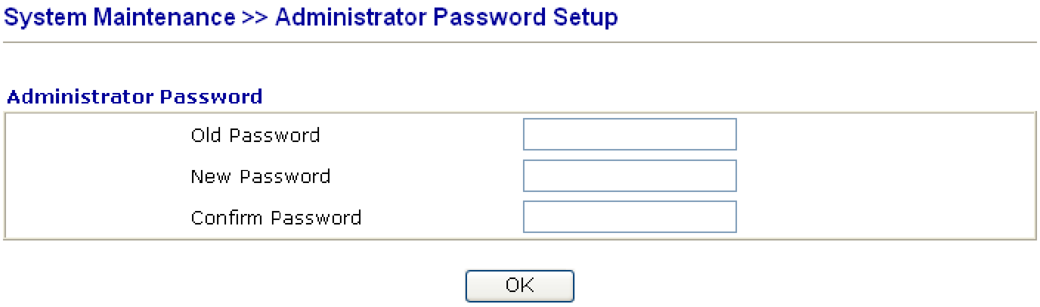
Enable/Disable – Sometimes, port conflict might be occurred. To solve such problem, you might want to change port number for CPE. Please click Enable and change the port number.

Periodic Inform Settings

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

5.12.3 Administrator Password

This page allows you to set new password.



System Maintenance >> Administrator Password Setup

Administrator Password

Old Password	
New Password	
Confirm 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.

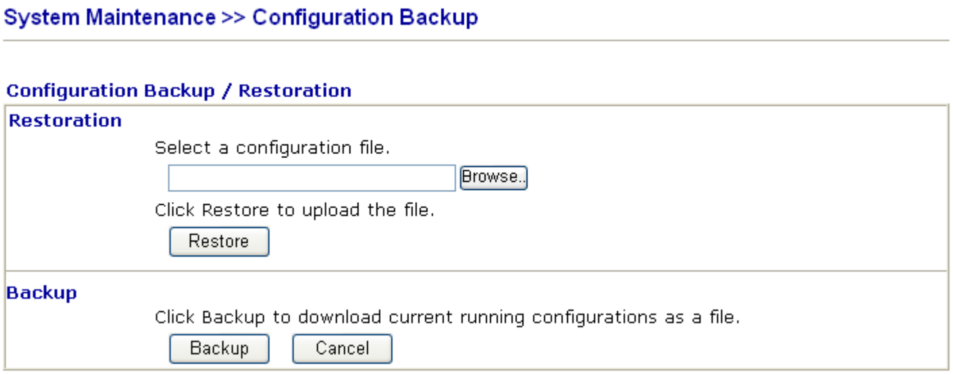
When you click OK, the login window will appear. Please use the new password to access into the web configurator again.

5.12.4 Configuration Backup

Backup the Configuration

Follow the steps below to backup your configuration.

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



System Maintenance >> Configuration Backup

Configuration Backup / Restoration

Restoration

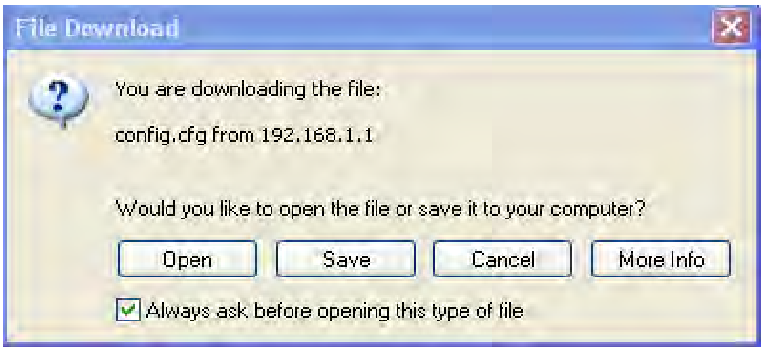
Select a configuration file.

Click Restore to upload the file.

Backup

Click Backup to download current running configurations as a file.

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


File Download

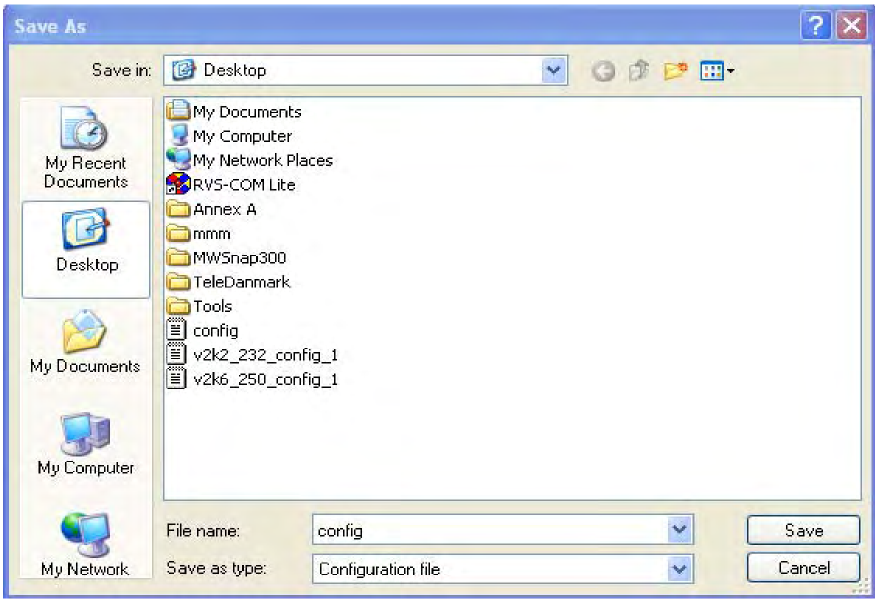
You are downloading the file:

config.cfg from 192.168.1.1

Would you like to open the file or save it to your computer?

☑ Always ask before opening this type of file

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


Save As

Save in: Desktop

File name: config

Save as type: Configuration file

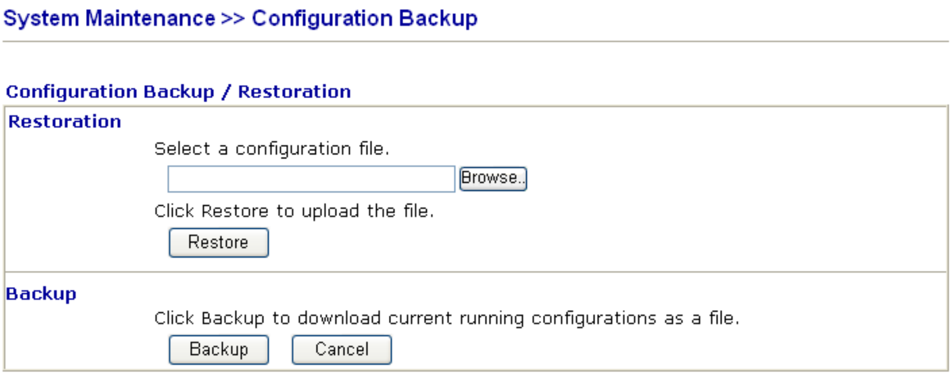
4. Click **Save** button, the configuration will download automatically to your computer as a file named **config.cfg**.

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

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

Restore Configuration

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



System Maintenance >> Configuration Backup

Configuration Backup / Restoration

Restoration

Select a configuration file.

Browse..

Click Restore to upload the file.

Restore

Backup

Click Backup to download current running configurations as a file.

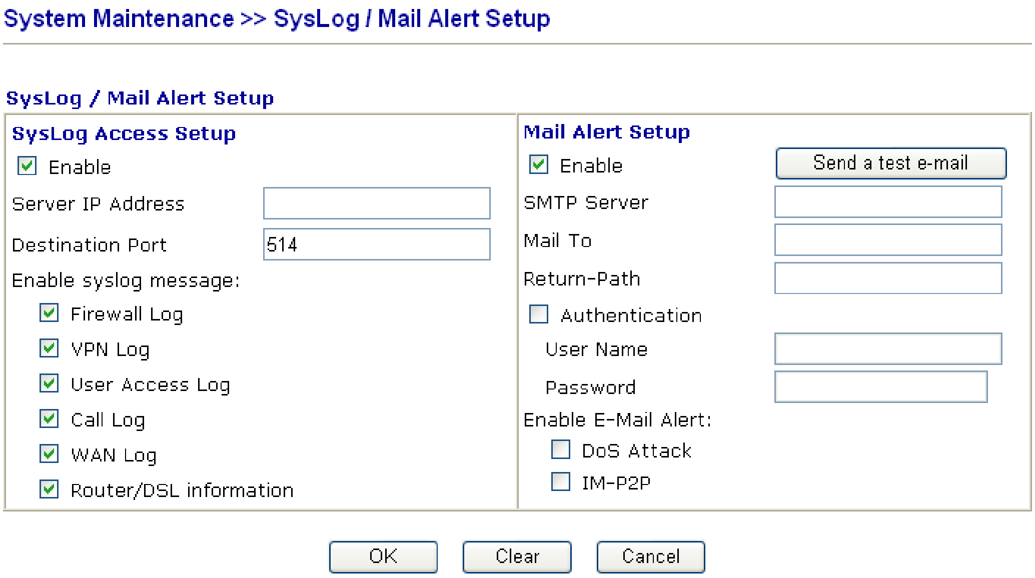
Backup Cancel

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

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

5.12.5 Syslog/Mail Alert

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



System Maintenance >> SysLog / Mail Alert Setup

SysLog / Mail Alert Setup

SysLog Access Setup

☑ Enable

Server IP Address

Destination Port 514

Enable syslog message:

☑ Firewall Log

☑ VPN Log

☑ User Access Log

☑ Call Log

☑ WAN Log

☑ Router/DSL information

Mail Alert Setup

☑ Enable

Send a test e-mail

SMTP Server

Mail To

Return-Path

□ Authentication

User Name

Password

Enable E-Mail Alert:

□ DoS Attack

□ IM-P2P

OK Clear Cancel

Enable (Syslog Access…)	Check “**Enable**” to activate function of syslog.
Syslog Server IP	The IP address of the Syslog server.
Destination Port	Assign a port for the Syslog protocol.
Enable syslog message	Check the box listed on this web page to send the corresponding message of firewall, VPN, User Access, Call, WAN, Router/DSL information to Syslog.
Enable (Alert Setup…)	Check “**Enable**” to activate function of mail alert.
Send a test e-mail	Make a simple test for the e-mail address specified in this page. Please assign the mail address first and click this button to execute a test for verify the mail address is available or not.
SMTP Server	The IP address of the SMTP server.

Mail To Assign a mail address for sending mails out.

Return-Path Assign an e-mail address of another mailbox to accept all returned messages if fatal problems occur at the recipient mailbox.
The e-mail address typed here also acts as the Sender address while Vigor sends out the alert e-mails.

Authentication Check this box to activate this function while using e-mail application.

User Name Type the user name for authentication.

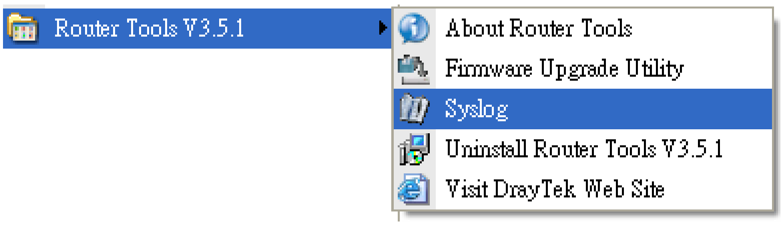
Password Type the password for authentication.

Enable E-mail Alert Check the box to send alert message to the e-mail box while the modem detecting the item(s) you specify here.

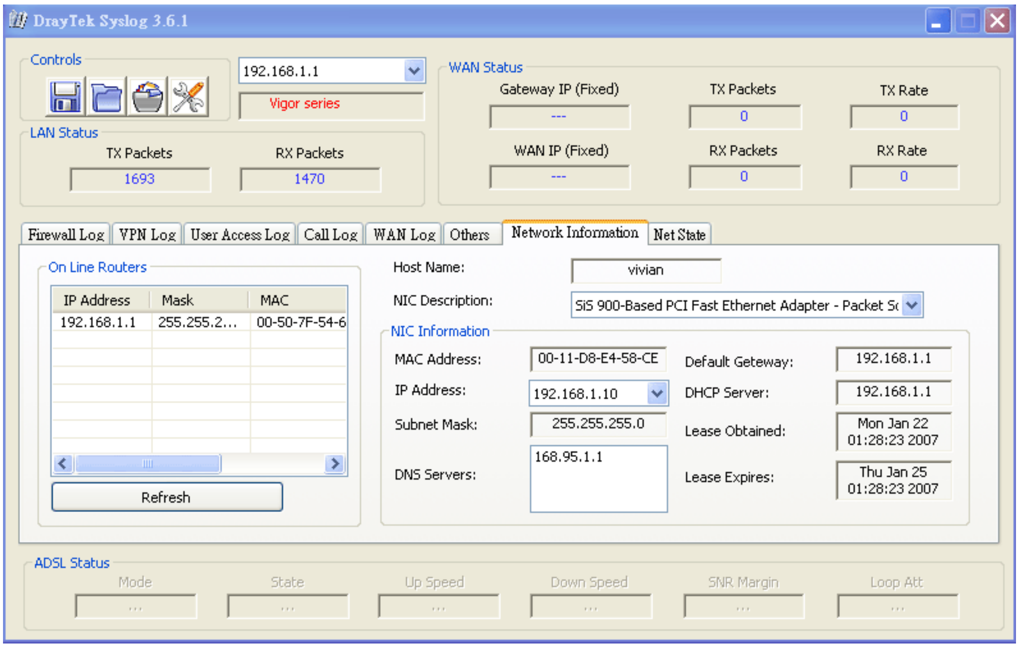
Click **OK** to save these settings.

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.


DrayTek Syslog 3.6.1

Controls: 192.168.1.1 — Vigor series

LAN Status: TX Packets 1693; RX Packets 1470

WAN Status: Gateway IP (Fixed) ---; TX Packets 0; TX Rate 0; WAN IP (Fixed) ---; RX Packets 0; RX Rate 0

On Line Routers

IP Address	Mask	MAC
192.168.1.1	255.255.2...	00-50-7F-54-6

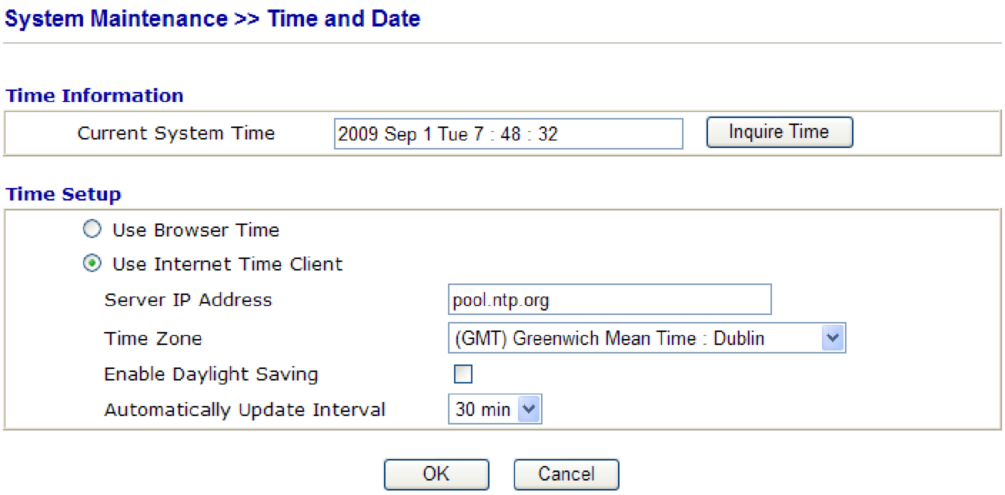
Host Name: vivian
NIC Description: SiS 900-Based PCI Fast Ethernet Adapter - Packet Sc

NIC Information
MAC Address: 00-11-D8-E4-58-CE
IP Address: 192.168.1.10
Subnet Mask: 255.255.255.0
DNS Servers: 168.95.1.1
Default Geteway: 192.168.1.1
DHCP Server: 192.168.1.1
Lease Obtained: Mon Jan 22 01:28:23 2007
Lease Expires: Thu Jan 25 01:28:23 2007

ADSL Status: Mode ...; State ...; Up Speed ...; Down Speed ...; SNR Margin ...; Loop Att ...

5.12.6 Time and Date

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



System Maintenance >> Time and Date

Time Information

Current System Time	2009 Sep 1 Tue 7 : 48 : 32	Inquire Time

Time Setup

○ Use Browser Time

● Use Internet Time Client

Server IP Address	pool.ntp.org
Time Zone	(GMT) Greenwich Mean Time : Dublin
Enable Daylight Saving	□
Automatically Update Interval	30 min

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.

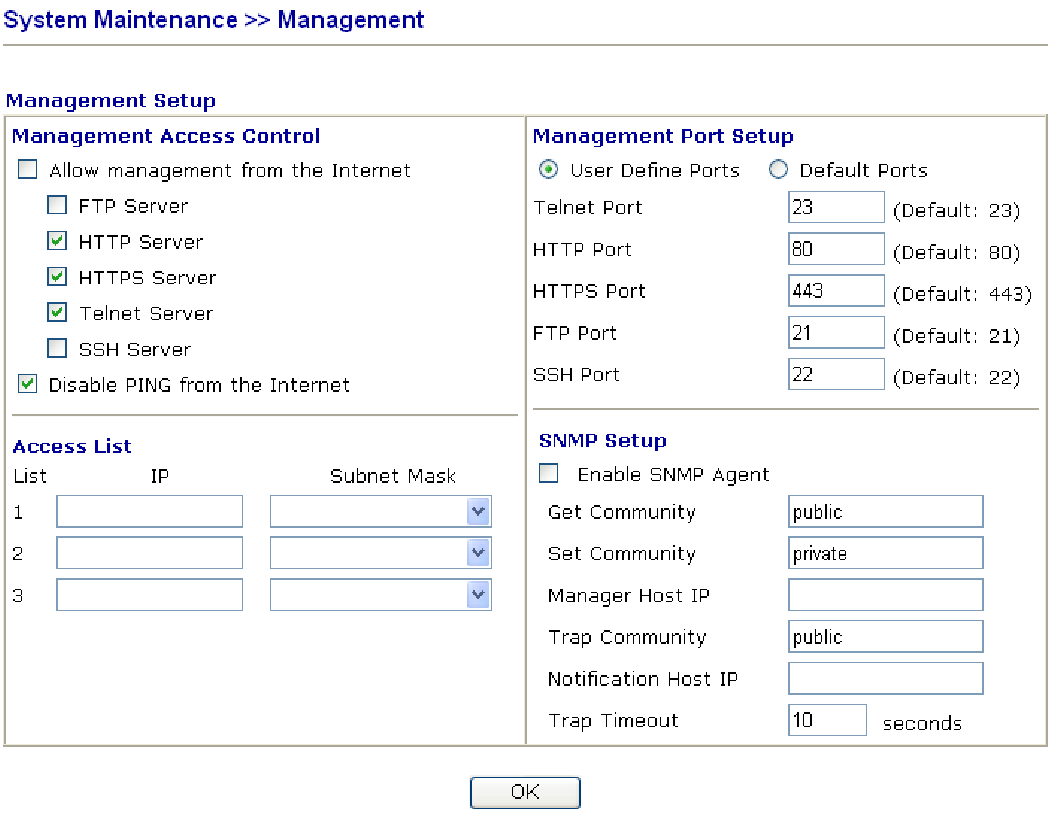
Time Zone Select the time zone where the router is located.

Automatically Update Interval Select a time interval for updating from the NTP server.

Click **OK** to save these settings.

5.12.7 Management

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



System Maintenance >> Management

Management Setup

Management Access Control

□ Allow management from the Internet
□ FTP Server
☑ HTTP Server
☑ HTTPS Server
☑ Telnet Server
□ SSH Server
☑ Disable PING from the Internet

Access List

List	IP	Subnet Mask
1		
2		
3		

Management Port Setup

● User Define Ports ○ Default Ports

Telnet Port	23	(Default: 23)
HTTP Port	80	(Default: 80)
HTTPS Port	443	(Default: 443)
FTP Port	21	(Default: 21)
SSH Port	22	(Default: 22)

SNMP Setup

□ Enable SNMP Agent

Get Community	public
Set Community	private
Manager Host IP	
Trap Community	public
Notification Host IP	
Trap Timeout	10 seconds

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.

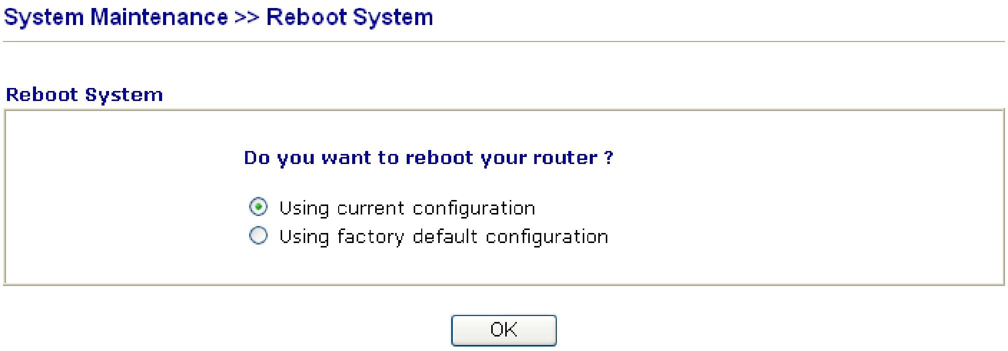
Trap Community Set trap community by typing a proper name. The default setting is **public.**

Notification Host IP Set the IP address of the host that will receive the trap community.

Trap Timeout The default setting is 10 seconds.

5.12.8 Reboot System

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



System Maintenance >> Reboot System

Reboot System

Do you want to reboot your router ?

● Using current configuration

○ Using factory default configuration

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

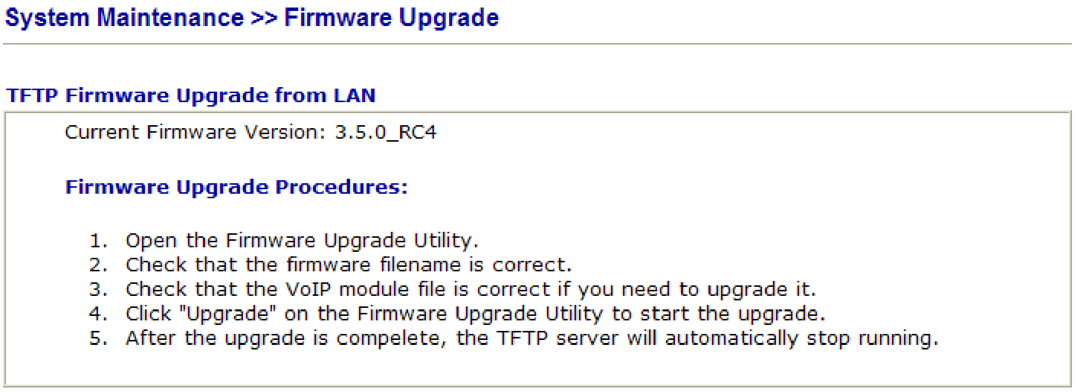
> **Note:** When the system pops up Reboot System web page after you configure web settings, please click **OK** to reboot your router for ensuring normal operation and preventing unexpected errors of the router in the future.

5.12.9 Firmware Upgrade

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

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

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



System Maintenance >> Firmware Upgrade

TFTP Firmware Upgrade from LAN

Current Firmware Version: 3.5.0_RC4

Firmware Upgrade Procedures:

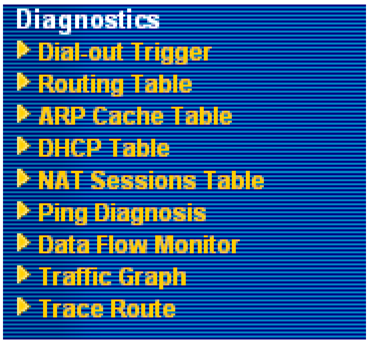
1. Open the Firmware Upgrade Utility.
2. Check that the firmware filename is correct.
3. Check that the VoIP module file is correct if you need to upgrade it.
4. Click "Upgrade" on the Firmware Upgrade Utility to start the upgrade.
5. After the upgrade is compelete, the TFTP server will automatically stop running.

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

5.13 Diagnostics

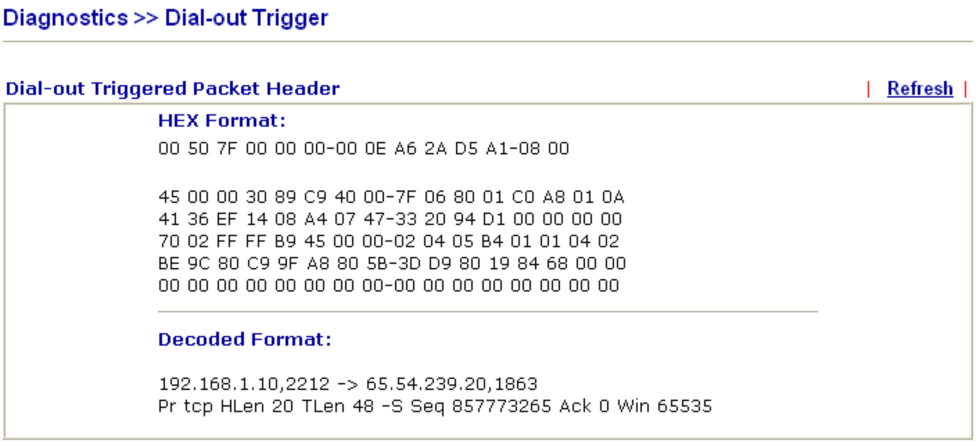
Diagnostic Tools provide a useful way to **view** or **diagnose** the status of your Vigor router.

Below shows the menu items for Diagnostics.



5.13.1 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.



Dial-out Triggered Packet Header

HEX Format:

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

45 00 00 30 89 C9 40 00-7F 06 80 01 C0 A8 01 0A
41 36 EF 14 08 A4 07 47-33 20 94 D1 00 00 00 00
70 02 FF FF B9 45 00 00-02 04 05 B4 01 01 04 02
BE 9C 80 C9 9F A8 80 5B-3D D9 80 19 84 68 00 00
00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00
```

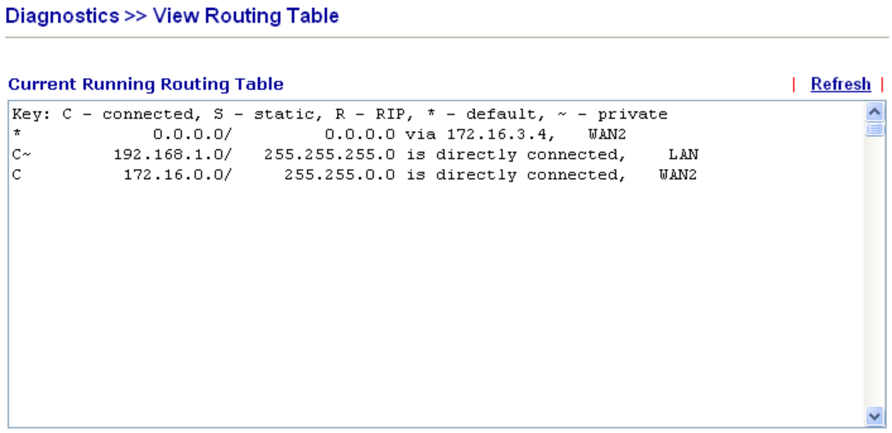
Decoded Format:

```
192.168.1.10,2212 -> 65.54.239.20,1863
Pr tcp HLen 20 TLen 48 -S Seq 857773265 Ack 0 Win 65535
```

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.

5.13.2 Routing Table

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



Diagnostics >> View Routing Table

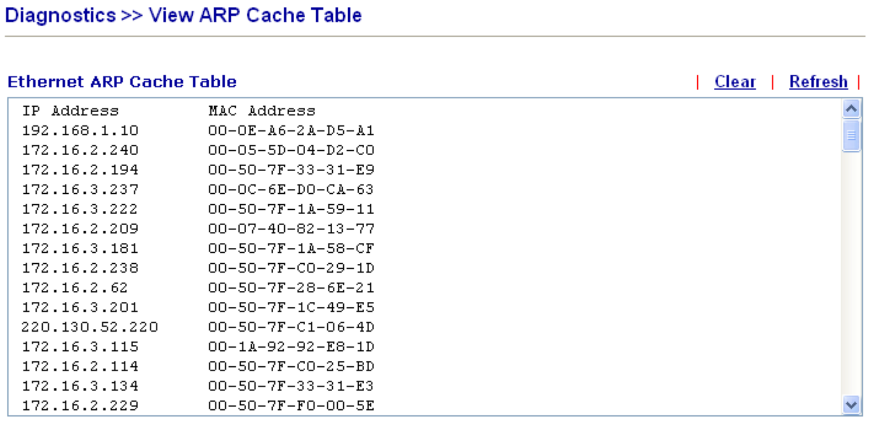
Current Running Routing Table | Refresh |

```
Key: C - connected, S - static, R - RIP, * - default, ~ - private
*              0.0.0.0/          0.0.0.0 via 172.16.3.4,    WAN2
C~         192.168.1.0/   255.255.255.0 is directly connected,     LAN
C           172.16.0.0/     255.255.0.0 is directly connected,    WAN2
```

Refresh Click it to reload the page.

5.13.3 ARP Cache Table

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



Diagnostics >> View ARP Cache Table

Ethernet ARP Cache Table | Clear | Refresh |

```
IP Address          MAC Address
192.168.1.10        00-0E-A6-2A-D5-A1
172.16.2.240        00-05-5D-04-D2-C0
172.16.2.194        00-50-7F-33-31-E9
172.16.3.237        00-0C-6E-D0-CA-63
172.16.3.222        00-50-7F-1A-59-11
172.16.2.209        00-07-40-82-13-77
172.16.3.181        00-50-7F-1A-58-CF
172.16.2.238        00-50-7F-C0-29-1D
172.16.2.62         00-50-7F-28-6E-21
172.16.3.201        00-50-7F-1C-49-E5
220.130.52.220      00-50-7F-C1-06-4D
172.16.3.115        00-1A-92-92-E8-1D
172.16.2.114        00-50-7F-C0-25-BD
172.16.3.134        00-50-7F-33-31-E3
172.16.2.229        00-50-7F-F0-00-5E
```

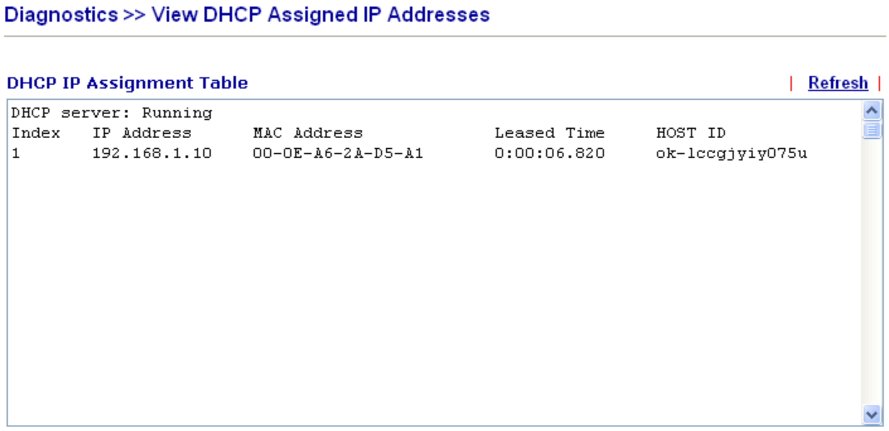
Refresh Click it to reload the page.

Clear Click it to clear the whole table.

5.13.4 DHCP Table

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

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



Diagnostics >> View DHCP Assigned IP Addresses

DHCP IP Assignment Table | Refresh |

```
DHCP server: Running
Index   IP Address      MAC Address             Leased Time     HOST ID
1       192.168.1.10    00-0E-A6-2A-D5-A1       0:00:06.820     ok-lccgjyiy075u
```

Index It displays the connection item number.

IP Address It displays the IP address assigned by this router for specified PC.

MAC Address It displays the MAC address for the specified PC that DHCP assigned IP address for it.

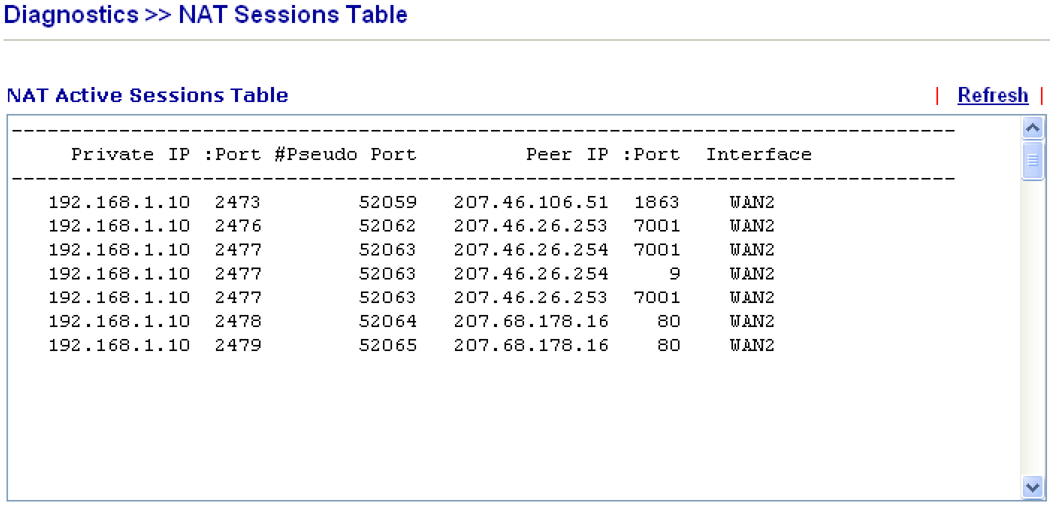
Leased Time It displays the leased time of the specified PC.

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

Refresh Click it to reload the page.

5.13.5 NAT Sessions Table

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



Diagnostics >> NAT Sessions Table

NAT Active Sessions Table | Refresh |

```
--------------------------------------------------------------------------------
     Private IP :Port #Pseudo Port          Peer IP :Port  Interface
--------------------------------------------------------------------------------
   192.168.1.10  2473        52059  207.46.106.51  1863     WAN2
   192.168.1.10  2476        52062  207.46.26.253  7001     WAN2
   192.168.1.10  2477        52063  207.46.26.254  7001     WAN2
   192.168.1.10  2477        52063  207.46.26.254     9     WAN2
   192.168.1.10  2477        52063  207.46.26.253  7001     WAN2
   192.168.1.10  2478        52064  207.68.178.16    80     WAN2
   192.168.1.10  2479        52065  207.68.178.16    80     WAN2
```

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.

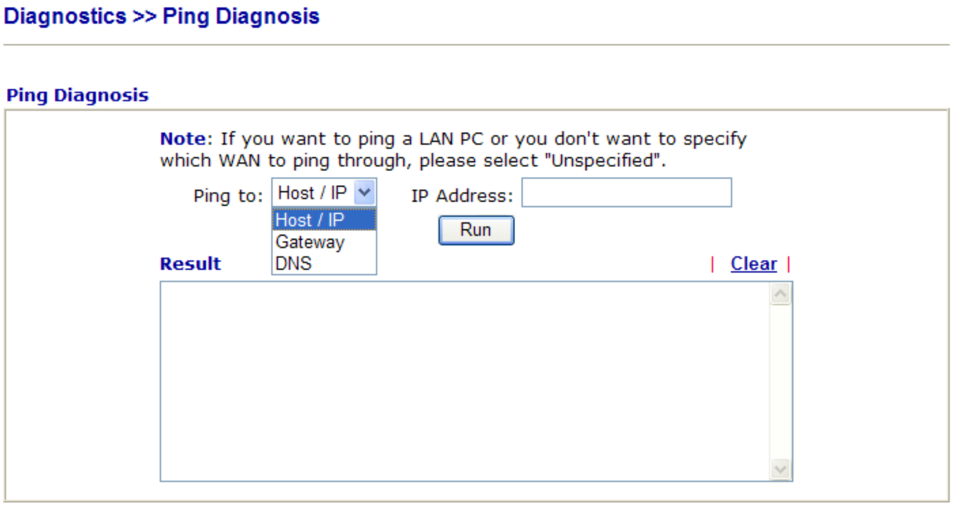
Peer IP:Port It indicates the destination IP address and port of remote host.

Interface It displays the representing number for different interface.

Refresh Click it to reload the page.

5.13.6 Ping Diagnosis

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



Diagnostics >> Ping Diagnosis

Ping Diagnosis

Note: If you want to ping a LAN PC or you don't want to specify which WAN to ping through, please select "Unspecified".

Ping to: Host / IP

IP Address:

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.

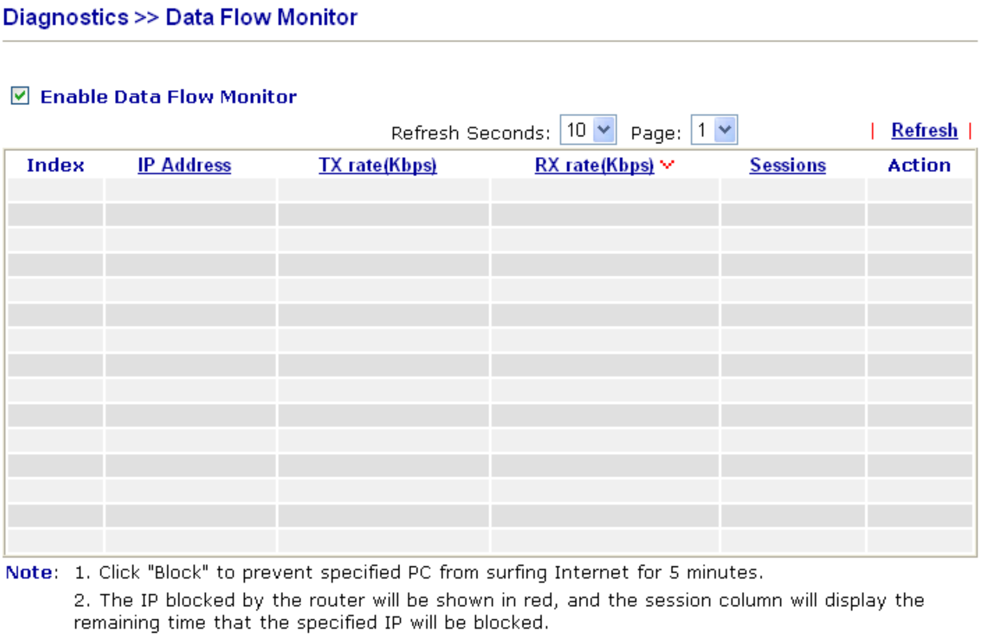
Run Click this button to start the ping work. The result will be displayed on the screen.

Clear Click this link to remove the result on the window.

5.13.7 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.



Diagnostics >> Data Flow Monitor

☑ Enable Data Flow Monitor

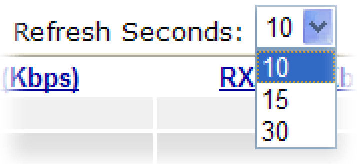
Refresh Seconds: 10 Page: 1 | Refresh |

Index	IP Address	TX rate(Kbps)	RX rate(Kbps)	Sessions	Action

Note: 1. Click "Block" to prevent specified PC from surfing Internet for 5 minutes.
2. The IP blocked by the router will be shown in red, and the session column will display the remaining time that the specified IP will be blocked.

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 Seconds: 10

Refresh Click this link to refresh this page manually.

Index Display the number of the data flow.

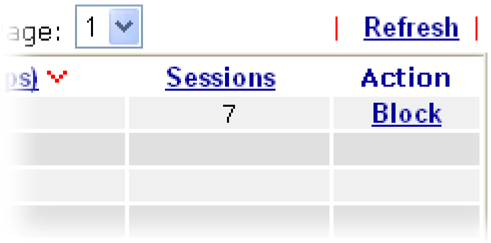
IP Address Display the IP address of the monitored device.

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.

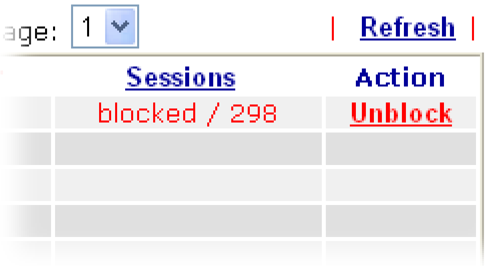
Action **Block -** can prevent specified PC accessing into Internet within 5 minutes.



age: 1 | Refresh |

ps)	Sessions	Action
	7	Block

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

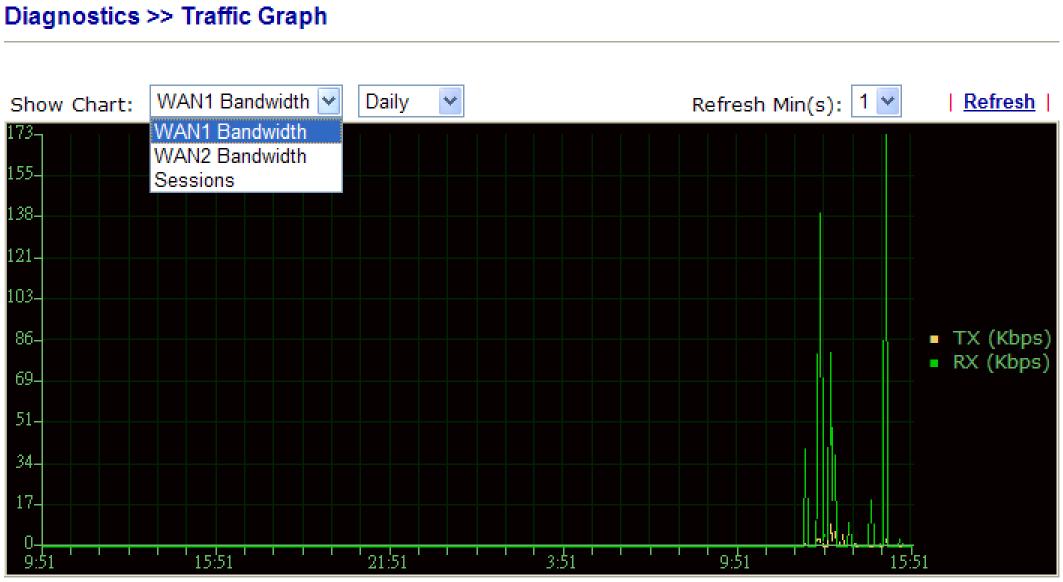


age: 1 | Refresh |

	Sessions	Action
	blocked / 298	Unblock

5.13.8 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.

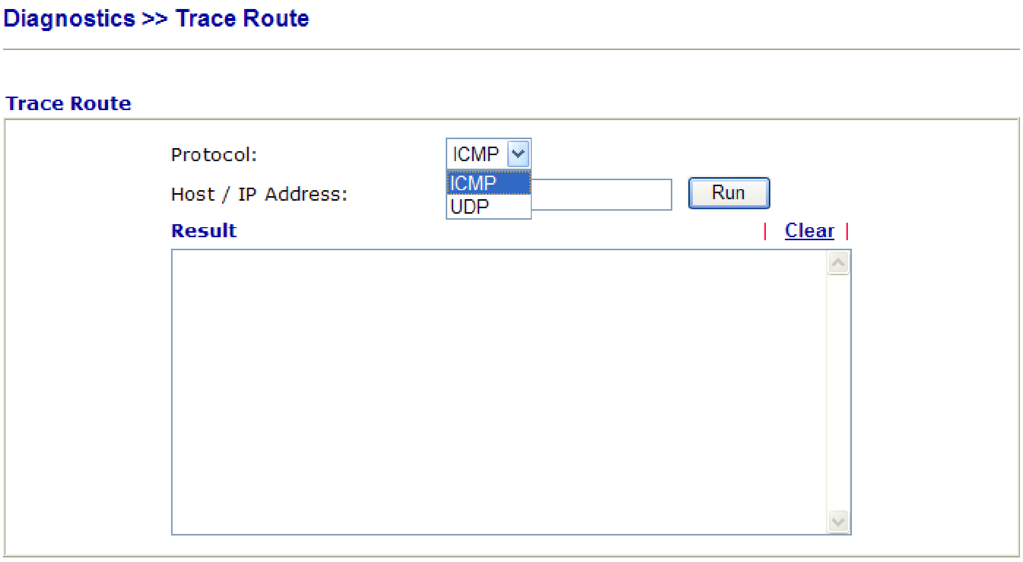


Diagnostics >> Traffic Graph

Show Chart: WAN1 Bandwidth Daily Refresh Min(s): 1 | Refresh |

5.13.9 Trace Route

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



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.

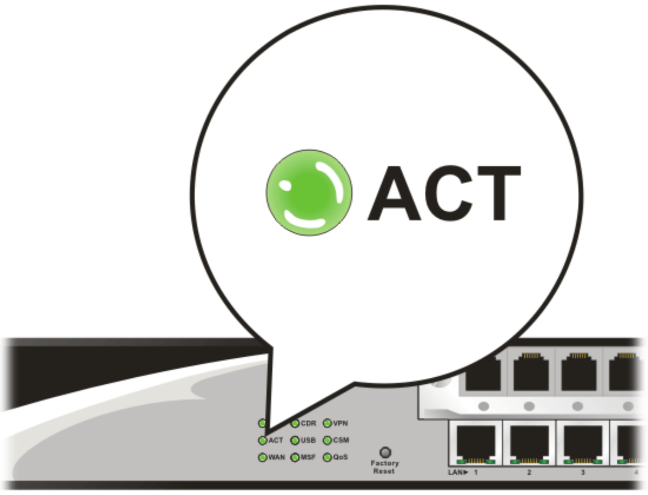
- Checking if the hardware status is OK or not.
- Checking if the network connection settings on your computer are OK or not.
- Pinging the router from your computer.
- Checking if the ISP settings are OK or not.
- Backing to factory default setting if necessary.

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



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

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

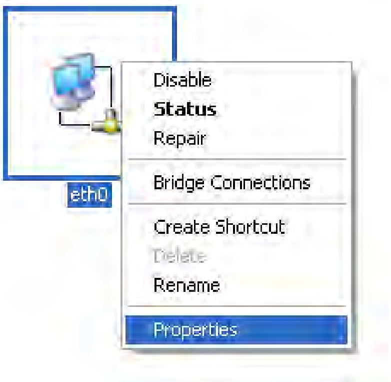
Sometimes the link failure occurs due to the wrong network connection settings. After trying the above section, if the link is stilled failed, please do the steps listed below to make sure the network connection settings is OK.

For Windows

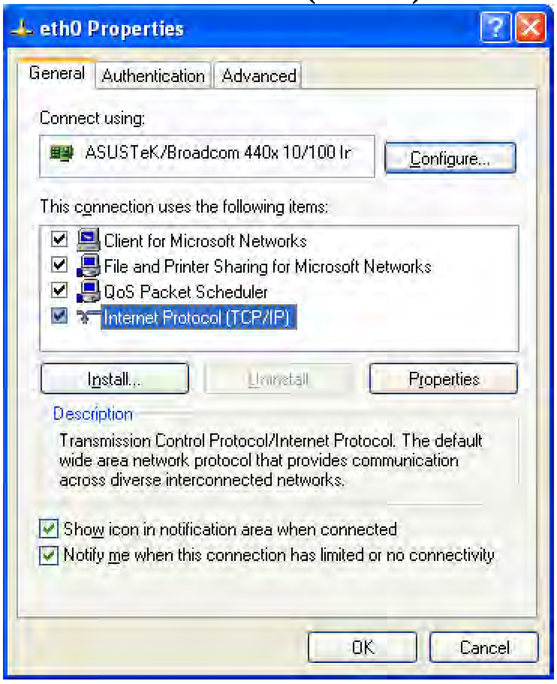
The example is based on Windows XP. As to the examples for other operation systems, please refer to the similar steps or find support notes in **www.draytek.com**.

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**.



eth0 Properties

General | Authentication | Advanced

Connect using:

ASUSTeK/Broadcom 440x 10/100 Ir [Configure...]

This connection uses the following items:

☑ Client for Microsoft Networks
☑ File and Printer Sharing for Microsoft Networks
☑ QoS Packet Scheduler
☑ Internet Protocol (TCP/IP)

[Install...] [Uninstall] [Properties]

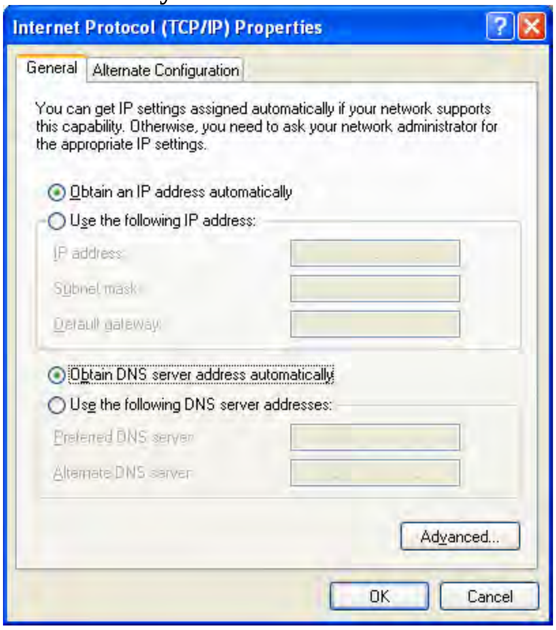
Description

Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

☑ Show icon in notification area when connected
☑ Notify me when this connection has limited or no connectivity

[OK] [Cancel]

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



Internet Protocol (TCP/IP) Properties

General | Alternate Configuration

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

● Obtain an IP address automatically

○ Use the following IP address:

IP address:

Subnet mask:

Default gateway:

● Obtain DNS server address automatically

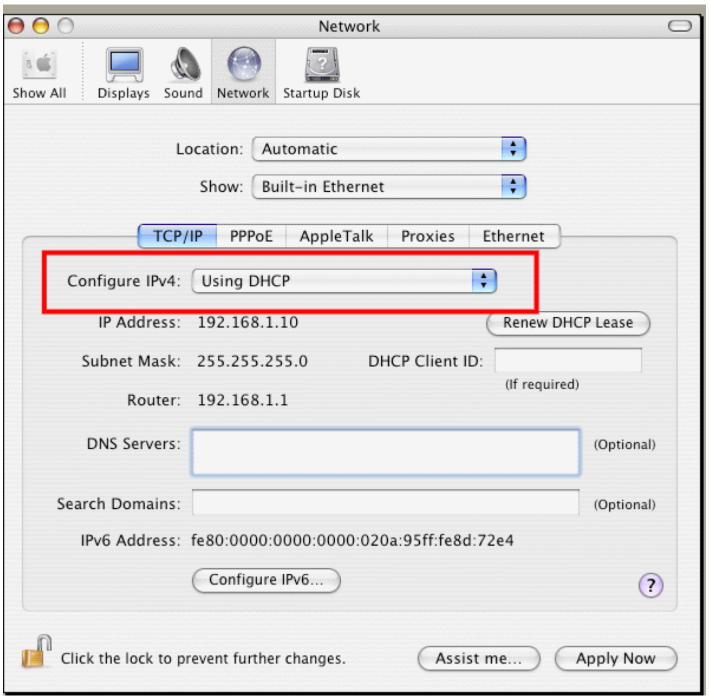
○ Use the following DNS server addresses:

Preferred DNS server:

Alternate DNS server:

For MacOs

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



Location: Automatic

Show: Built-in Ethernet

TCP/IP | PPPoE | AppleTalk | Proxies | Ethernet

Configure IPv4: Using DHCP

IP Address: 192.168.1.10

Subnet Mask: 255.255.255.0

DHCP Client ID: (If required)

Router: 192.168.1.1

DNS Servers: (Optional)

Search Domains: (Optional)

IPv6 Address: fe80:0000:0000:0000:020a:95ff:fe8d:72e4

Click the lock to prevent further changes.

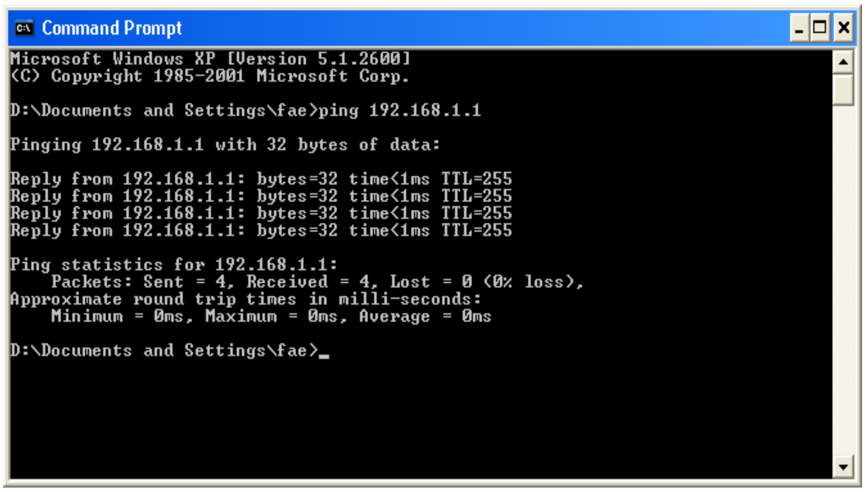
6.3 Pinging the Router from Your Computer

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). The DOS command dialog will appear.

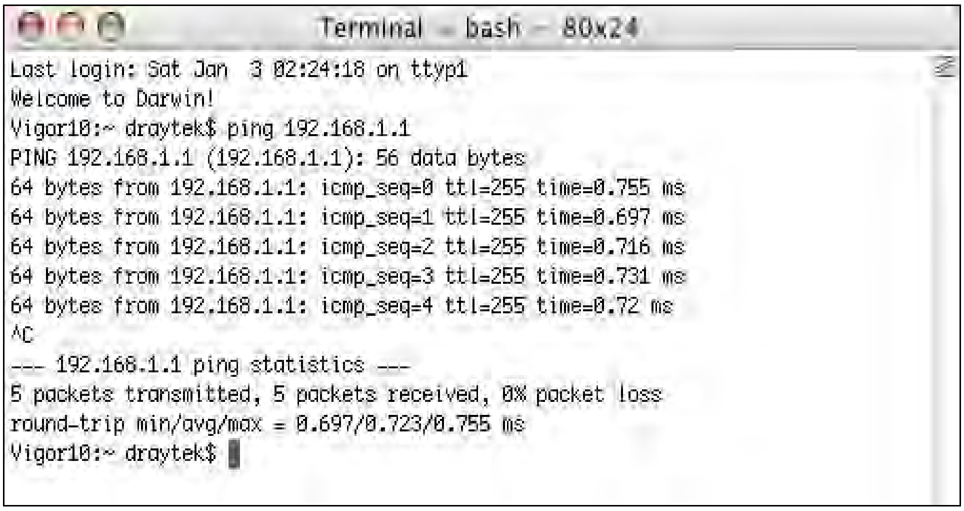


```
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

D:\Documents and Settings\fae>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:

Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

D:\Documents and Settings\fae>_
```

3. Type ping 192.168.1.1 and press [Enter]. If the link is OK, the line of **“Reply from 192.168.1.1:bytes=32 time<1ms TTL=255”** will appear.
4. If the line does not appear, please check the IP address setting of your computer.

For MacOs (Terminal)

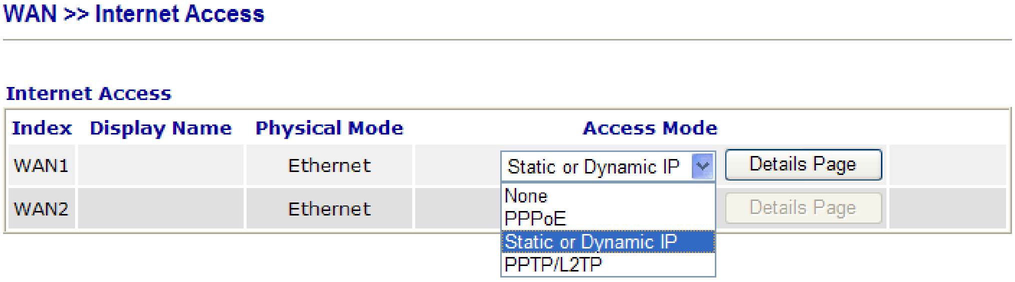
1. Double click on the current used MacOs on the desktop.
2. Open the **Application** folder and get into **Utilities**.
3. Double click **Terminal**. The Terminal window will appear.
4. Type **ping 192.168.1.1** and press [Enter]. If the link is OK, the line of **“64 bytes from 192.168.1.1: icmp_seq=0 ttl=255 time=xxxx ms**” will appear.



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

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.



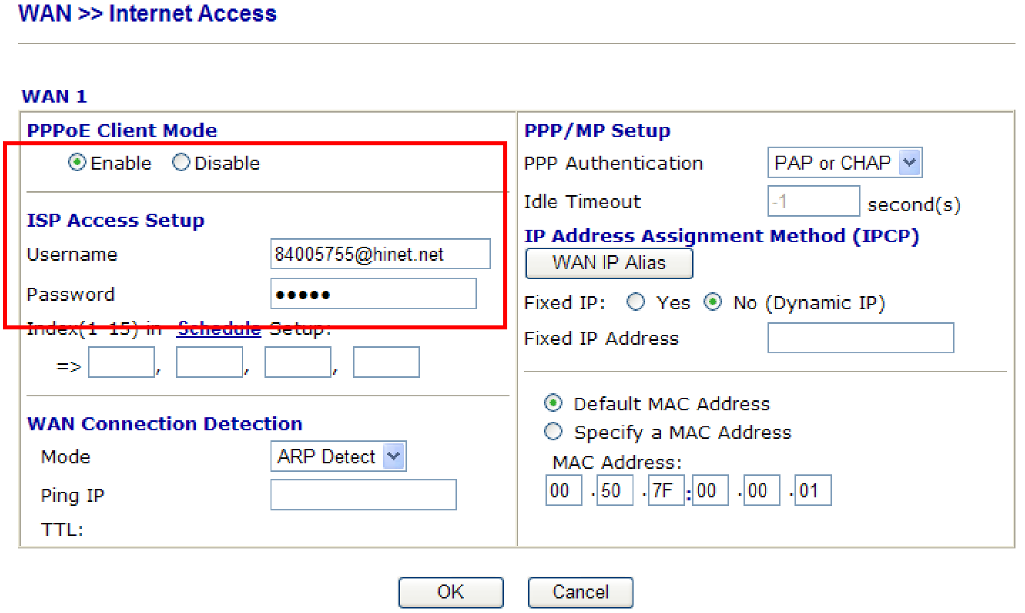
WAN >> Internet Access

Internet Access

Index	Display Name	Physical Mode	Access Mode	
WAN1		Ethernet	Static or Dynamic IP	Details Page
WAN2		Ethernet		Details Page

For PPPoE Users

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



WAN >> Internet Access

WAN 1

PPPoE Client Mode

● Enable ○ Disable

ISP Access Setup

Username: 84005755@hinet.net

Password: •••••

Index(1-15) in Schedule Setup:

=> , , ,

WAN Connection Detection

Mode: ARP Detect

Ping IP:

TTL:

PPP/MP Setup

PPP Authentication: PAP or CHAP

Idle Timeout: -1 second(s)

IP Address Assignment Method (IPCP)

WAN IP Alias

Fixed IP: ○ Yes ● No (Dynamic IP)

Fixed IP Address:

● Default MAC Address

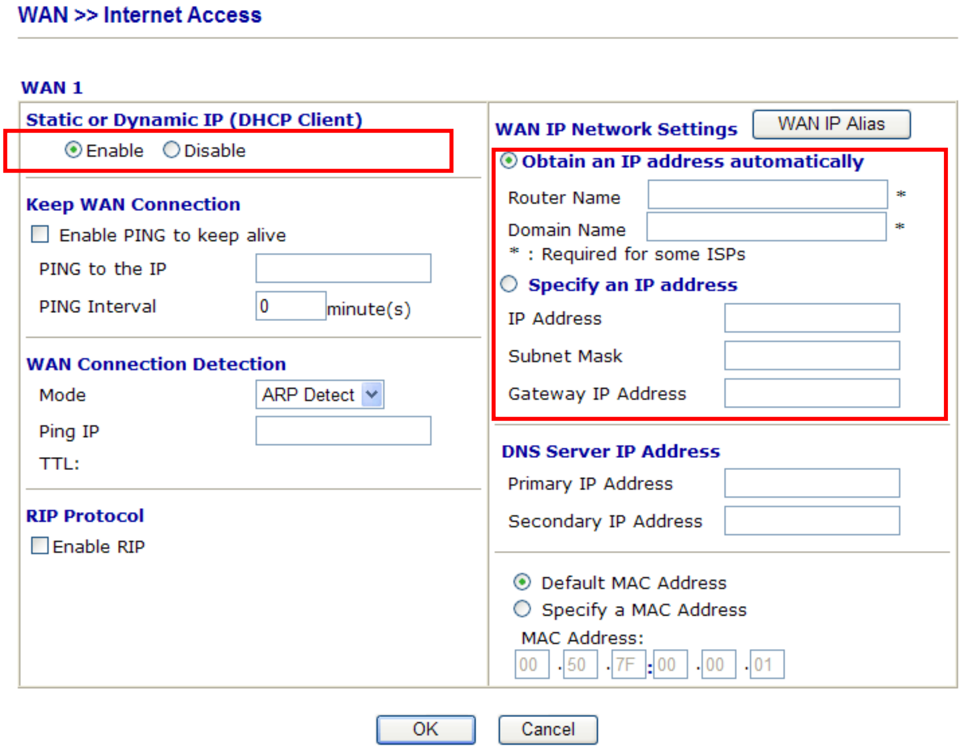
○ Specify a MAC Address

MAC Address: 00 .50 .7F :00 .00 .01

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**.



WAN >> Internet Access

WAN 1

Static or Dynamic IP (DHCP Client)
● Enable ○ Disable

Keep WAN Connection
□ Enable PING to keep alive
PING to the IP
PING Interval 0 minute(s)

WAN Connection Detection
Mode ARP Detect
Ping IP
TTL:

RIP Protocol
□ Enable RIP

WAN IP Network Settings [WAN IP Alias]
● Obtain an IP address automatically
Router Name *
Domain Name *
* : Required for some ISPs
○ Specify an IP address
IP Address
Subnet Mask
Gateway IP Address

DNS Server IP Address
Primary IP Address
Secondary IP Address

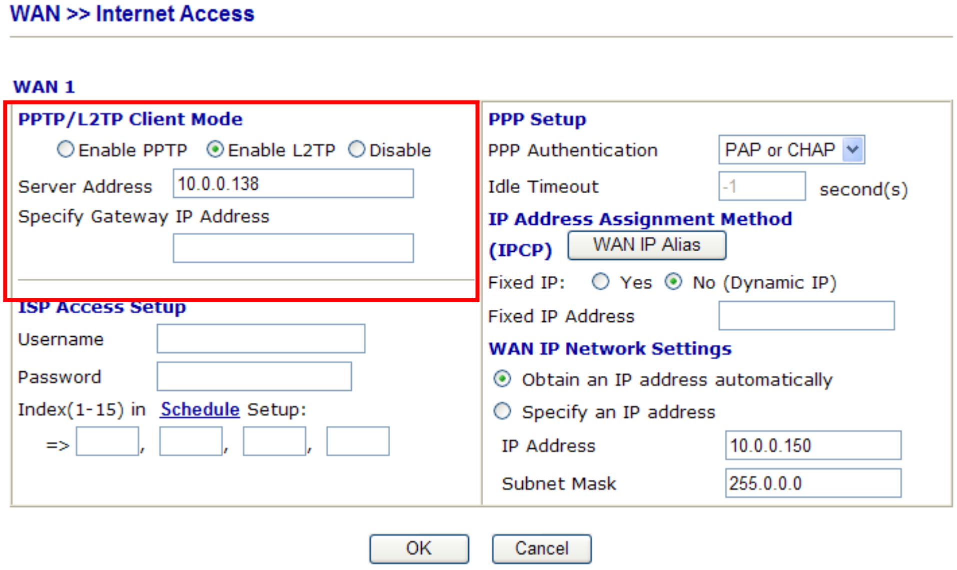
● Default MAC Address
○ Specify a MAC Address
MAC Address:
00 . 50 . 7F : 00 . 00 . 01

[OK] [Cancel]

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).



WAN >> Internet Access

WAN 1

PPTP/L2TP Client Mode
○ Enable PPTP ● Enable L2TP ○ Disable
Server Address 10.0.0.138
Specify Gateway IP Address

ISP Access Setup
Username
Password
Index(1-15) in Schedule Setup:
=> , , ,

PPP Setup
PPP Authentication PAP or CHAP
Idle Timeout -1 second(s)
IP Address Assignment Method (IPCP) [WAN IP Alias]
Fixed IP: ○ Yes ● No (Dynamic IP)
Fixed IP Address
WAN IP Network Settings
● Obtain an IP address automatically
○ Specify an IP address
IP Address 10.0.0.150
Subnet Mask 255.0.0.0

[OK] [Cancel]

6.5 Backing to Factory Default Setting If Necessary

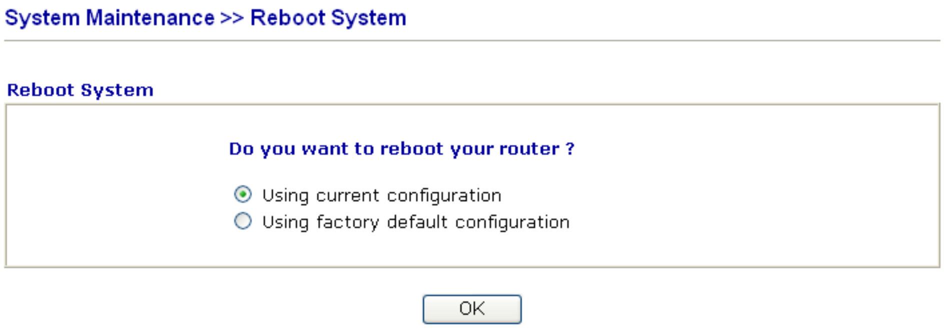
Sometimes, a wrong connection can be improved by returning to the default settings. Try to reset the router by software or hardware.

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.



System Maintenance >> Reboot System

Reboot System

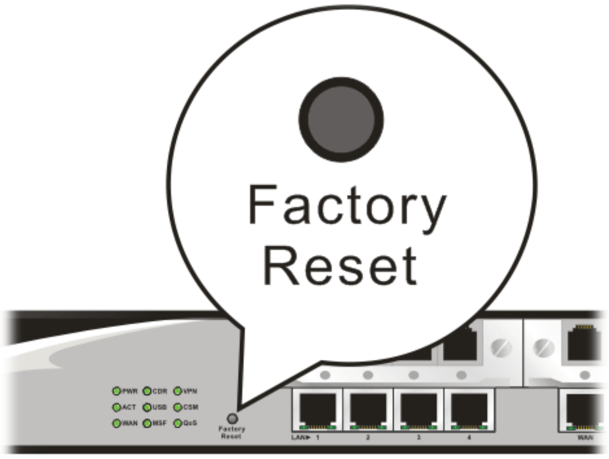
Do you want to reboot your router ?

● Using current configuration
○ Using factory default configuration

OK

Hardware Reset

While the router is running (ACT LED blinking), press the **Factory Reset** button and hold for more than 5 seconds. When you see the **ACT** LED blinks rapidly, please release the button. Then, the router will restart with the default configuration.



After restore the factory default setting, you can configure the settings for the router again to fit your personal request.

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.

This page is left blank.

Appendix: Hardware Specifications

Temperature	Operating : 0°C ~ 45°C
	Storage : -25°C ~ 70°C
Humidity	10% ~ 90% (non-condensing)
Max. Power Consumption	10 Watt
Dimension	L241 * W165 * H44 (mm)
Power	DC 12V ~ 15V