DrayTek

Vigor2900 Series Security Router User's Guide

Version: 2.0

Date: 2006/1/16

Table of Contents

1 Preface

Targeting requirement for residential, SOHO (Small Office and Home Office) and business users, the Vigor2900 series provides exceptional bandwidth for Internet access.

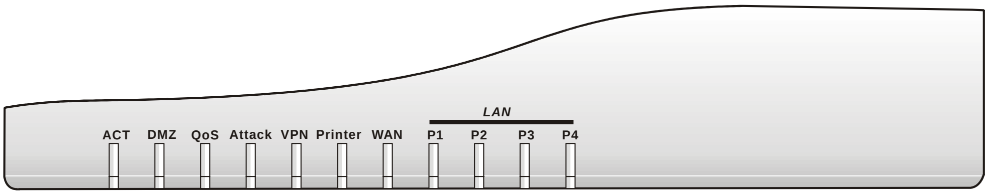
To secure your network, the Vigor2900 series provides an advanced firewall with advanced features, such as NAT with multi VPN pass-through, Stateful Packet Inspection (SPI) to offer network reliability by detecting and prohibiting malicious penetrating packets, user-configurable web filtering for parental control against network abuse etc.

Vigor2900 series is embedded with an 802.11g compliant wireless module which provides wireless LAN access with data rate as much as (up to 54Mbps for Vigor2900G/VG/VGi only). As for data privacy of wireless network, the Vigor2900 series can encode all transmissions data with standard WEP and industrial strength WPA2 (IEEE 802.11i) encryption. Additional features include Wireless Client List and MAC Address Control for maintaining control over user's authorization in your network, and Hidden SSID for being invisible to outside intruders scanning.

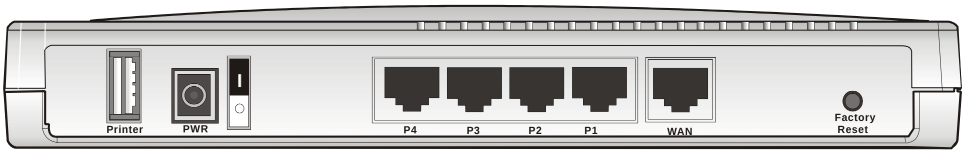
1.1 LED Indicators and Connectors

The displays of LED indicators and connectors for the routers are different slightly.

1.1.1 Front and Rear View for Vigor2900

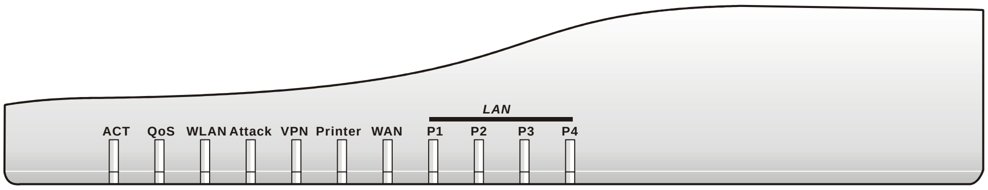


LED	Status	Explanation
ACT (Activity)	Blinking	The router is powered on and running properly.
DMZ	On	DMZ Host is specified in certain site.
QoS	On	The QoS function is active.
Attack	On	DoS Defense function is active.
	Blinking	An attack is detected.
VPN	On	The VPN tunnel is launched.
Printer	On	The USB interface printer is ready.
WAN	Orange	A normal 10Mbps WAN link is ready.
	Green	A normal 100Mbps WAN link is ready.
	Blinking	Ethernet packets are transmitting.
LAN (1, 2, 3, 4)	Orange	A normal 10Mbps connection is through its corresponding port.
	Green	A normal 100Mbps connection is through its corresponding port.
	Blinking	Ethernet packets are transmitting.

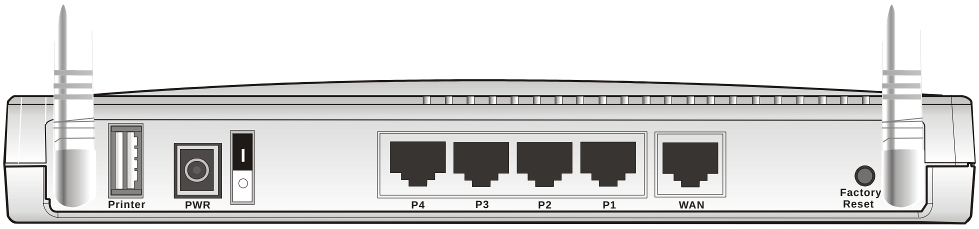


Interface	Description
Printer	Connecter for a USB printer.
PWR	Connecter for a power adapter.
0/1	Power Switch.
P1 – P4	Connecter for local networked devices.
WAN	Connecter for remote networked devices.
Factory Reset	Restore the default settings. Usage: Turn on the router (ACT LED is blinking). Press 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.

1.1.2 Front and Rear View for Vigor2900G

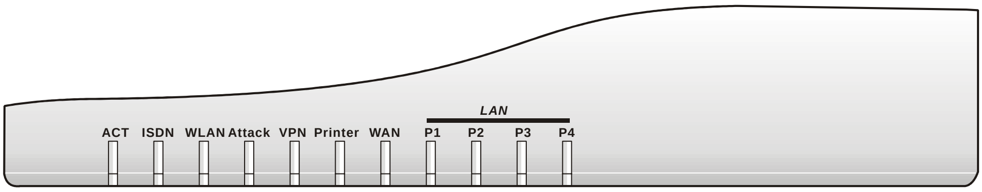


LED	Status	Explanation
ACT (Activity)	Blinking	The router is powered on and running properly.
QoS	On	The QoS function is active.
WLAN	On	The wireless LAN function is enabled.
	Blinking	Ethernet packets are transmitting over wireless LAN.
Attack	On	DoS Defense function is active.
	Blinking	An attack is detected.
VPN	On	The VPN tunnel is launched.
Printer	On	The USB interface printer is ready.
WAN	Orange	A normal 10Mbps WAN link is ready.
	Green	A normal 100Mbps WAN link is ready.
	Blinking	Ethernet packets are transmitting.
LAN (1, 2, 3, 4)	Orange	A normal 10Mbps connection is through its corresponding port.
	Green	A normal 100Mbps connection is through its corresponding port.
	Blinking	Ethernet packets are transmitting.

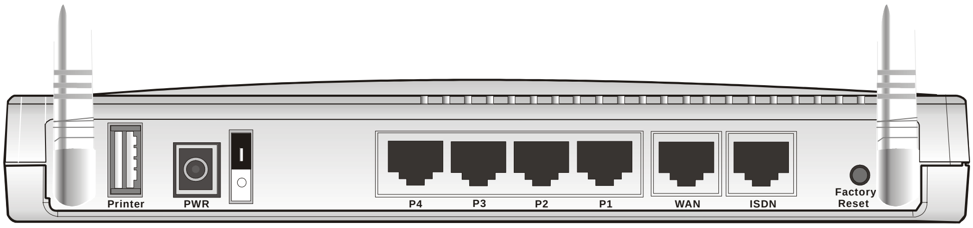


Interface	Description
Printer	Connecter for a USB printer.
PWR	Connecter for a power adapter.
0/1	Power Switch.
P1 – P4	Connecter for local networked devices.
WAN	Connecter for remote networked devices.
Factory Reset	Restore the default settings. Usage: Turn on the router (ACT LED is blinking). Press 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.

1.1.3 Front and Rear View for Vigor2900Gi

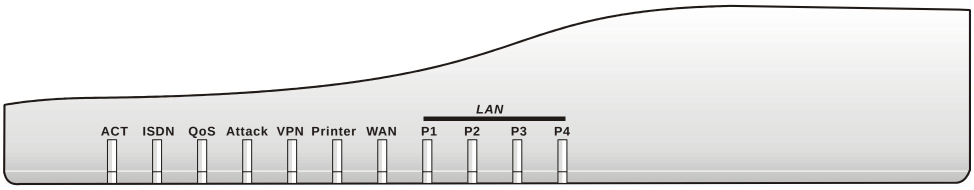


LED	Status	Explanation
ACT (Activity)	Blinking	The router is powered on and running properly.
ISDN	On	The ISDN network is correctly setup.
	Blinking	A successful remote connection on the ISDN BRI B1/B2 channel.
WLAN	On	The wireless LAN function is enabled.
	Blinking	Ethernet packets are transmitting over wireless LAN.
Attack	On	DoS Defense function is active.
	Blinking	An attack is detected.
VPN	On	The VPN tunnel is launched.
Printer	On	The USB interface printer is ready.
WAN	Orange	A normal 10Mbps WAN link is ready.
	Green	A normal 100Mbps WAN link is ready.
	Blinking	Ethernet packets are transmitting.
LAN (1, 2, 3, 4)	Orange	A normal 10Mbps connection is through its corresponding port.
	Green	A normal 100Mbps connection is through its corresponding port.
	Blinking	Ethernet packets are transmitting.

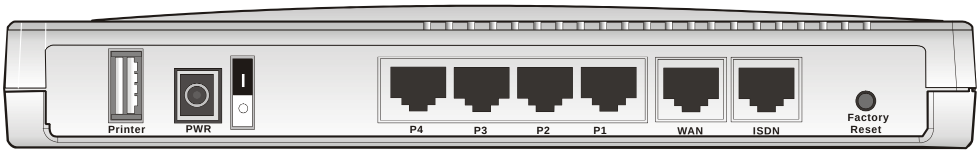


Interface	Description
Printer	Connecter for a USB printer.
PWR	Connecter for a power adapter.
0/1	Power Switch.
P1 – P4	Connecter for local networked devices.
WAN	Connecter for remote networked devices.
ISDN	Connecter for NT1 (or NT1+) box provided by ISDN service provider.
Factory Reset	Restore the 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.

1.1.4 Front and Rear View for Vigor2900i

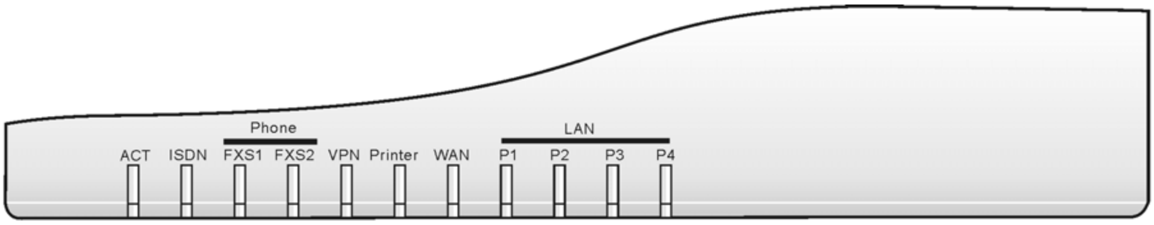


LED	Status	Explanation
ACT (Activity)	Blinking	The router is powered on and running properly.
ISDN	On	The ISDN network is correctly setup.
	Blinking	A successful remote connection on the ISDN BRI B1/B2 channel.
QoS	On	The QoS function is active.
Attack	On	DoS Defense function is active.
	Blinking	An attack is detected.
VPN	On	The VPN tunnel is launched.
Printer	On	The USB interface printer is ready.
WAN	Orange	A normal 10Mbps WAN link is ready.
	Green	A normal 100Mbps WAN link is ready.
	Blinking	Ethernet packets are transmitting.
LAN (1, 2, 3, 4)	Orange	A normal 10Mbps connection is through its corresponding port.
	Green	A normal 100Mbps connection is through its corresponding port.
	Blinking	Ethernet packets are transmitting.

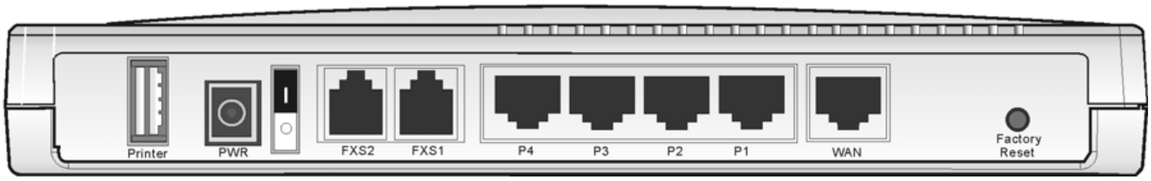


Interface	Description
Printer	Connecter for a USB printer.
PWR	Connecter for a power adapter.
0/1	Power Switch.
P1 – P4	Connecter for local networked devices.
WAN	Connecter for remote networked devices.
ISDN	Connect for NT1 (or NT1+) box provided by ISDN service provider.
Factory Reset	Restore the default 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.

1.1.5 Front and Rear View for Vigor2900V

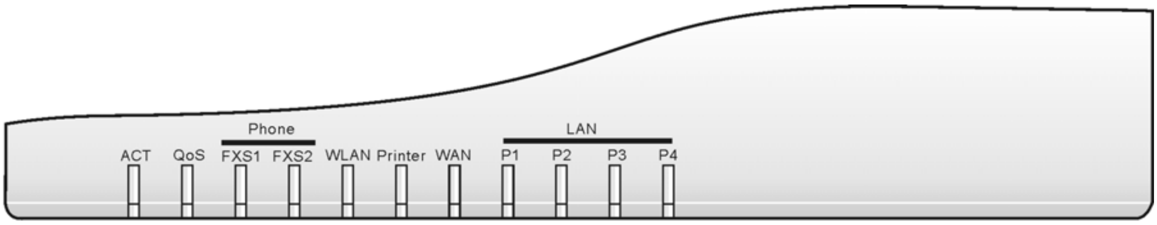


LED	Status	Explanation
ACT (Activity)	Blinking	The router is powered on and running properly.
QoS	On	The QoS function is active.
Phone (FXS1, FXS2)	On	The phone is off hook (the handset of phone is hanging).
	Blinking	A phone call is incoming.
VPN	On	The VPN tunnel is launched.
Printer	On	The USB interface printer is ready.
WAN	Orange	A normal 10Mbps WAN link is ready.
	Green	A normal 100Mbps WAN link is ready.
	Blinking	Ethernet packets are transmitting.
LAN (1, 2, 3, 4)	Orange	A normal 10Mbps connection is through its corresponding port.
	Green	A normal 100Mbps connection is through its corresponding port.
	Blinking	Ethernet packets are transmitting.

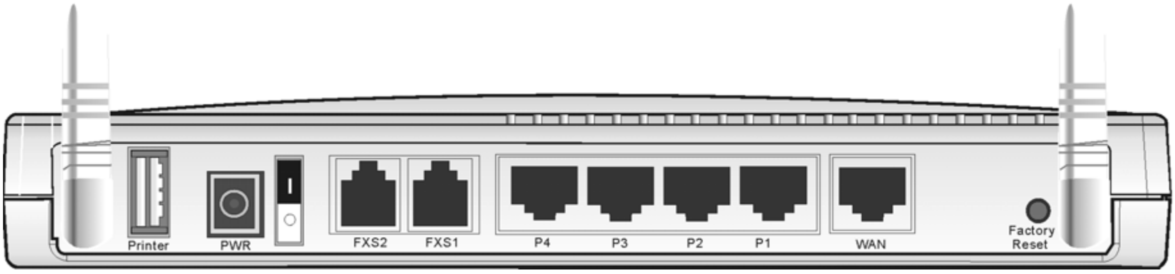


Interface	Description
Printer	Connecter for a USB printer.
PWR	Connecter for a power adapter.
0/1	Power Switch.
FXS 2 - 1	Connecter of analog phone for VoIP communication.
P1 – P4	Connecter for local networked devices.
WAN	Connecter for remote networked devices.
Factory Reset	Restore the default settings. 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.

1.1.6 Front and Rear View for Vigor2900VG

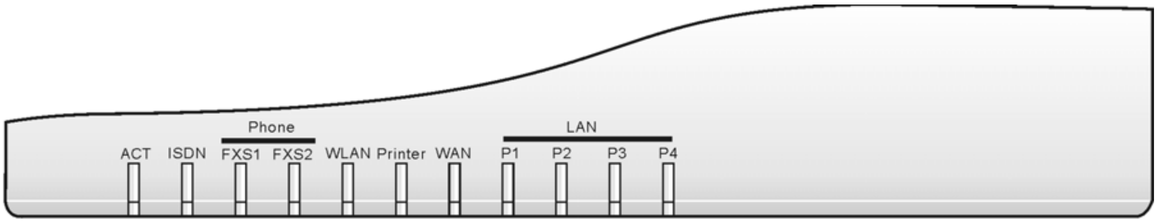


LED	Status	Explanation
ACT (Activity)	Blinking	The router is powered on and running properly.
QoS	On	The QoS function is active.
Phone (FXS1, FXS2)	On	The phone is off hook (the handset of phone is hanging).
	Blinking	A phone call is incoming.
WLAN	On	The wireless LAN function is enabled.
	Blinking	Ethernet packets are transmitting over wireless LAN.
Printer	On	The USB interface printer is ready.
WAN	Orange	A normal 10Mbps WAN link is ready.
	Green	A normal 100Mbps WAN link is ready.
	Blinking	Ethernet packets are transmitting.
LAN (1, 2, 3, 4)	Orange	A normal 10Mbps connection is through its corresponding port.
	Green	A normal 100Mbps connection is through its corresponding port.
	Blinking	Ethernet packets are transmitting.

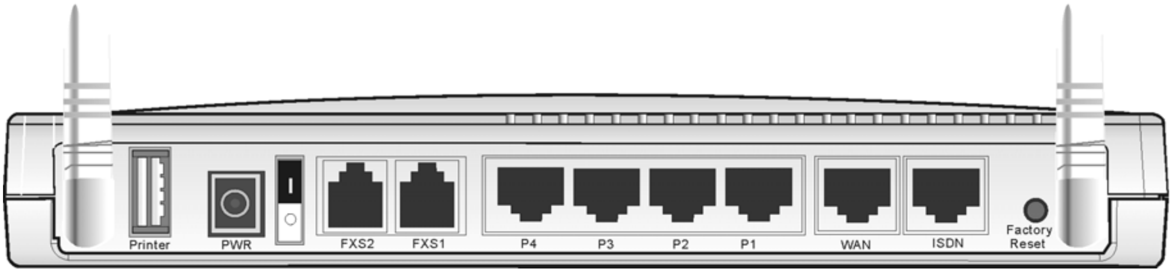


Interface	Description
Printer	Connecter for a USB printer.
PWR	Connecter for a power adapter.
0/1	Power Switch.
FXS 2 - 1	Connecter of analog phone for VoIP communication.
P1 – P4	Connecter for local networked devices.
WAN	Connecter for remote networked devices.
Factory Reset	Restore the default settings. 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.

1.1.7 Front and Rear View for Vigor2900VGi

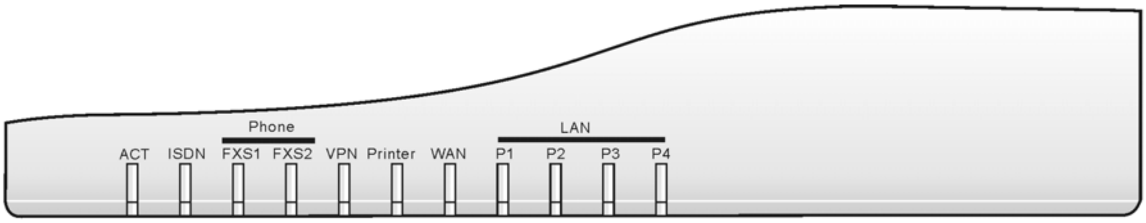


LED	Status	Explanation
ACT (Activity)	Blinking	The router is powered on and running properly.
ISDN	On	The ISDN network is correctly setup.
	Blinking	A successful remote connection on the ISDN BRI B1/B2 channel.
Phone (FXS1, FXS2)	On	The phone is off hook (the handset of phone is hanging).
	Blinking	A phone call is incoming.
WLAN	On	The wireless LAN function is enabled.
	Blinking	Ethernet packets are transmitting over wireless LAN.
Printer	On	The USB interface printer is ready.
WAN	Orange	A normal 10Mbps WAN link is ready.
	Green	A normal 100Mbps WAN link is ready.
	Blinking	Ethernet packets are transmitting.
LAN (1, 2, 3, 4)	Orange	A normal 10Mbps connection is through its corresponding port.
	Green	A normal 100Mbps connection is through its corresponding port.
	Blinking	Ethernet packets are transmitting.

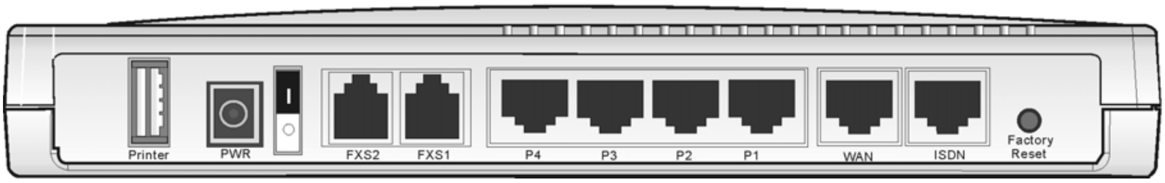


Interface	Description
Printer	Connecter for a USB printer.
PWR	Connecter for a power adapter.
0/1	Power Switch.
FXS 2 - 1	Connecter of analog phone for VoIP communication.
P1 – P4	Connecter for local networked devices.
WAN	Connecter for remote networked devices.
Factory Reset	Restore the default settings. 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.

1.1.8 Front and Rear View for Vigor2900Vi



LED	Status	Explanation
ACT (Activity)	Blinking	The router is powered on and running properly.
ISDN	On	The ISDN network is correctly setup.
	Blinking	A successful remote connection on the ISDN BRI B1/B2 channel.
Phone (FXS1, FXS2)	On	The phone is off hook (the handset of phone is hanging).
	Blinking	A phone call is incoming.
VPN	On	The VPN tunnel is launched.
Printer	On	The USB interface printer is ready.
WAN	Orange	A normal 10Mbps WAN link is ready.
	Green	A normal 100Mbps WAN link is ready.
	Blinking	Ethernet packets are transmitting.
LAN (1, 2, 3, 4)	Orange	A normal 10Mbps connection is through its corresponding port.
	Green	A normal 100Mbps connection is through its corresponding port.
	Blinking	Ethernet packets are transmitting.



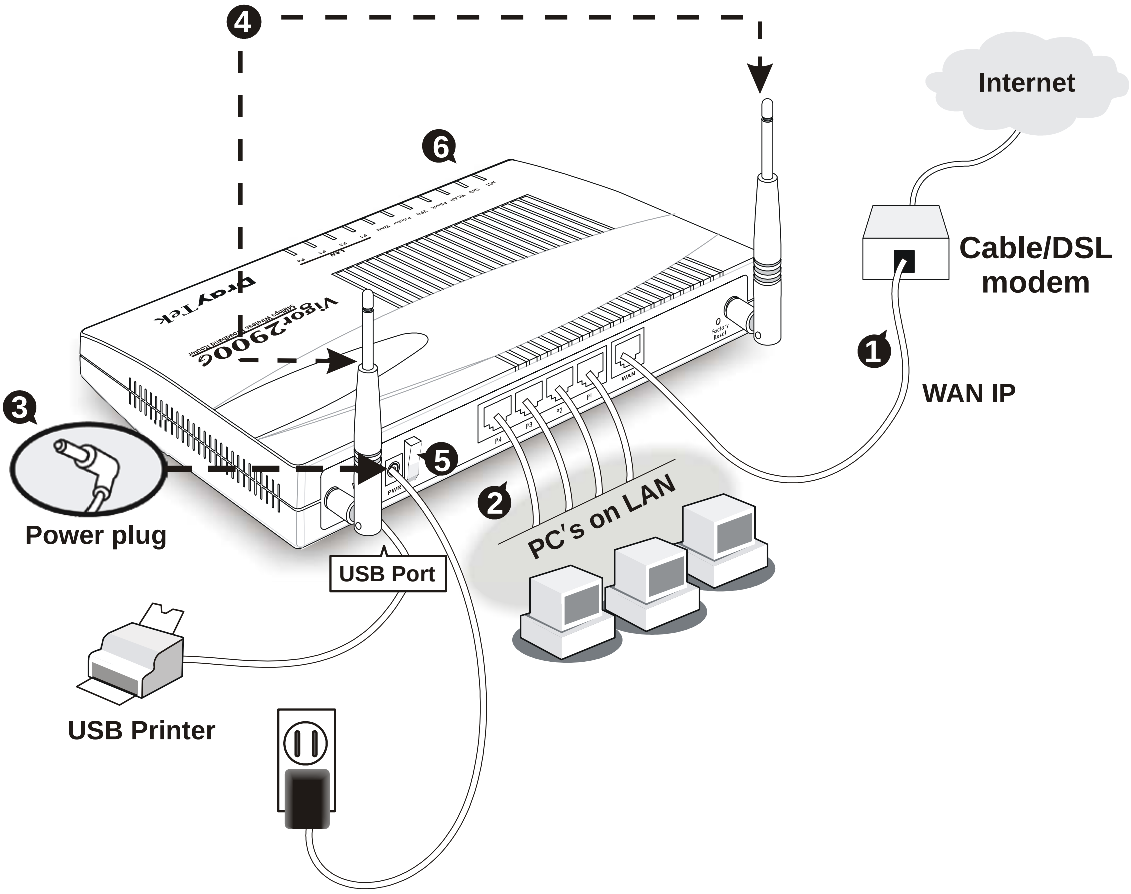
Interface	Description
Printer	Connecter for a USB printer.
PWR	Connecter for a power adapter.
0/1	Power Switch.
FXS 2 - 1	Connecter of analog phone for VoIP communication.
P1 – P4	Connecter for local networked devices.
WAN	Connecter for remote networked devices.
Factory Reset	Restore the default settings. 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.

1.2 Hardware Installation

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

1. Connect this device to a router with an Ethernet cable.
2. Connect one port of 4-port switch to your computer with a RJ-45 cable. This device allows you to connect 4 PCs directly.
3. Connect one end of the power cord to the power port of this device. Connect the other end to the wall outlet of electricity.
4. Connect detachable antennas to the router for Vigor2900 Series.
5. Power on the router.
6. Check the **ACT** and **WAN**, **LAN** LEDs to assure network connections.

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



2 Configuring Basic Settings

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

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

2.1 Changing Password

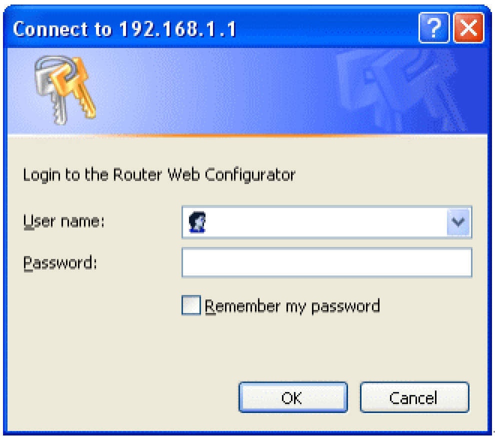
For security reasons, it is strongly recommend that you set the administrator password for the router. During the first setup, the router requires no password. If no password is configured, the router will be open to any user in the LAN or the Internet, and users can log into the router unlimitedly and change the settings.

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

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

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

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



Connect to 192.168.1.1

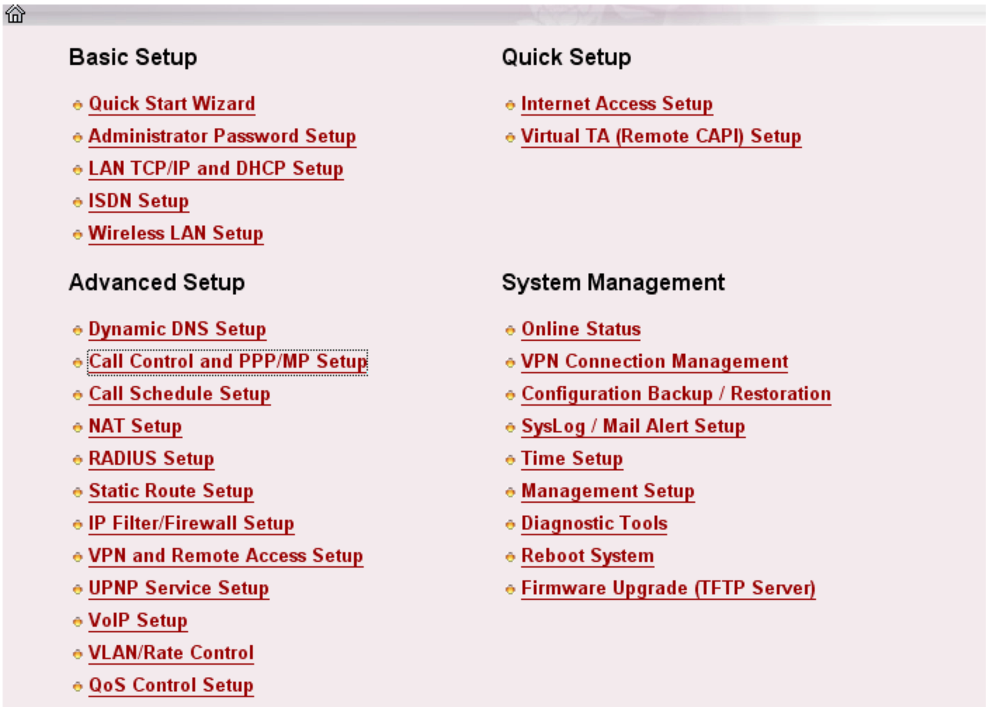
Login to the Router Web Configurator

User name:

Password:

□ Remember my password

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



Basic Setup

- Quick Start Wizard
- Administrator Password Setup
- LAN TCP/IP and DHCP Setup
- ISDN Setup
- Wireless LAN Setup

Quick Setup

- Internet Access Setup
- Virtual TA (Remote CAPI) Setup

Advanced Setup

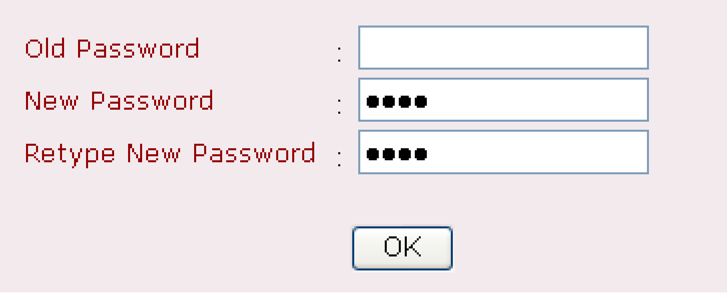
- Dynamic DNS Setup
- Call Control and PPP/MP Setup
- Call Schedule Setup
- NAT Setup
- RADIUS Setup
- Static Route Setup
- IP Filter/Firewall Setup
- VPN and Remote Access Setup
- UPNP Service Setup
- VoIP Setup
- VLAN/Rate Control
- QoS Control Setup

System Management

- Online Status
- VPN Connection Management
- Configuration Backup / Restoration
- SysLog / Mail Alert Setup
- Time Setup
- Management Setup
- Diagnostic Tools
- Reboot System
- Firmware Upgrade (TFTP Server)

Notice: Some of the settings might not appear as above, because the home page will change slightly according to the features that your router has.

4. Click **Administrator Password Setup** from the **Basic Setup** group.



Old Password :

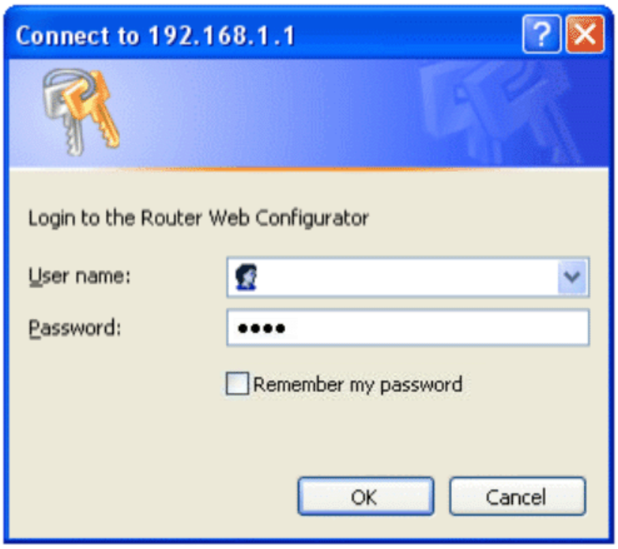
New Password : ●●●●

Retype New Password : ●●●●

OK

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

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



Connect to 192.168.1.1

Login to the Router Web Configurator

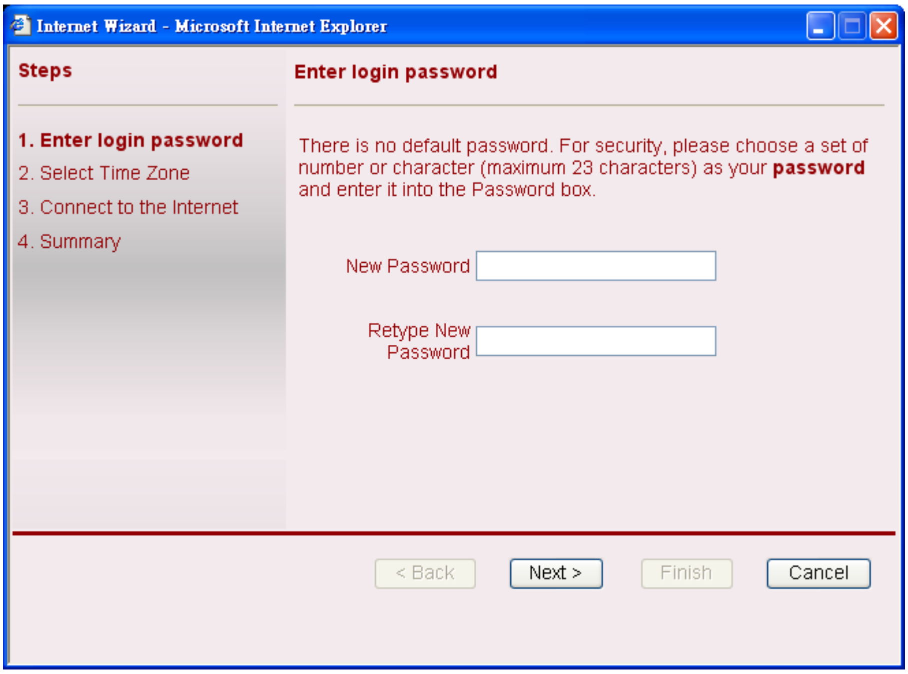
User name:

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.



Internet Wizard - Microsoft Internet Explorer

Steps

1. Enter login password
2. Select Time Zone
3. Connect to the Internet
4. Summary

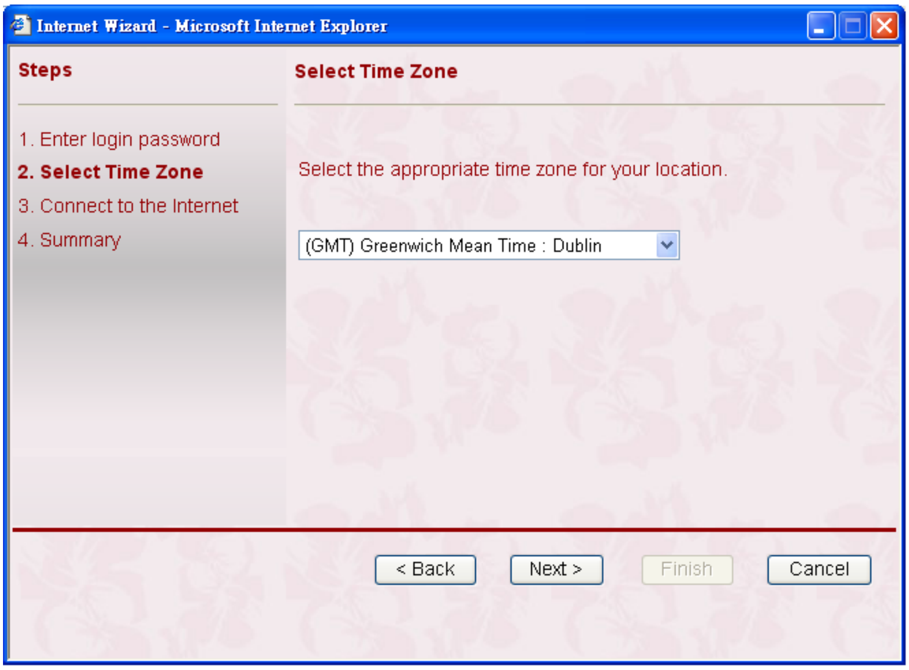
Enter login password

There is no default password. For security, please choose a set of number or character (maximum 23 characters) as your **password** and enter it into the Password box.

New Password

Retype New Password

After typing the password, please click **Next**. The following screen will appear.



Select Time Zone

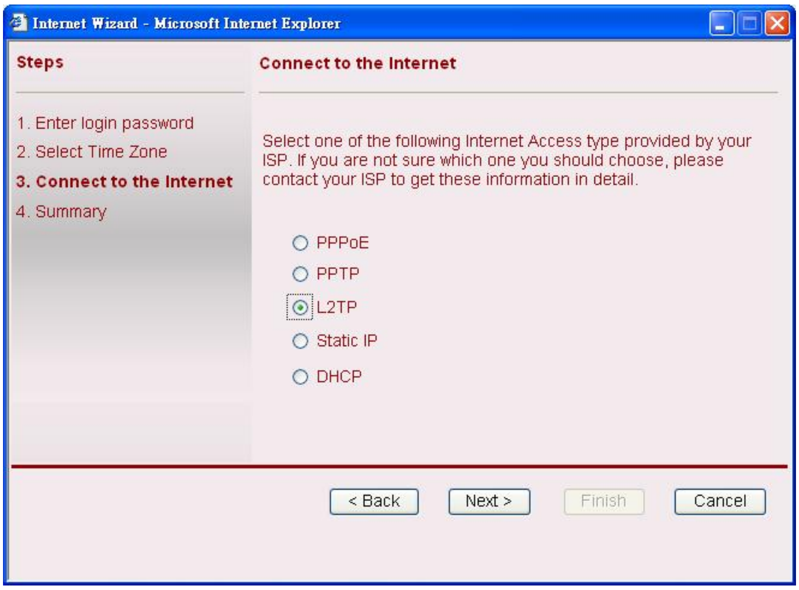
Select the appropriate time zone for your location.

(GMT) Greenwich Mean Time : Dublin

Please select the appropriate time zone for the router. Then, click **Next**.

2.2.1 Selecting Protocol

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.



Connect to the Internet

Select one of the following Internet Access type provided by your ISP. If you are not sure which one you should choose, please contact your ISP to get these information in detail.

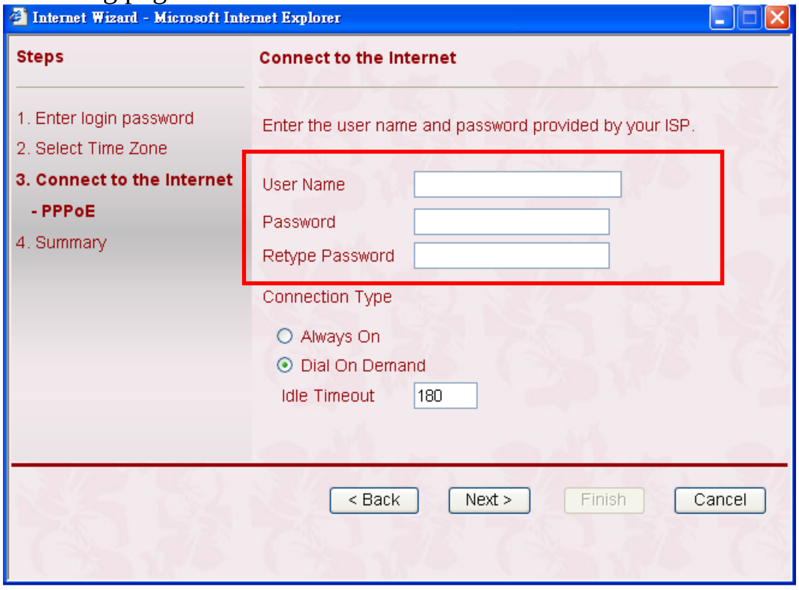
○ PPPoE
○ PPTP
● L2TP
○ Static IP
○ DHCP

2.2.2 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. And the PPPoA stands for Point-to-Point Protocol over ATM. PPPoA uses the PPP dial-up protocol with ATM as the transport.

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:



Internet Wizard - Microsoft Internet Explorer

Connect to the Internet

Enter the user name and password provided by your ISP.

User Name

Password

Retype Password

Connection Type

○ Always On

● Dial On Demand

Idle Timeout 180

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

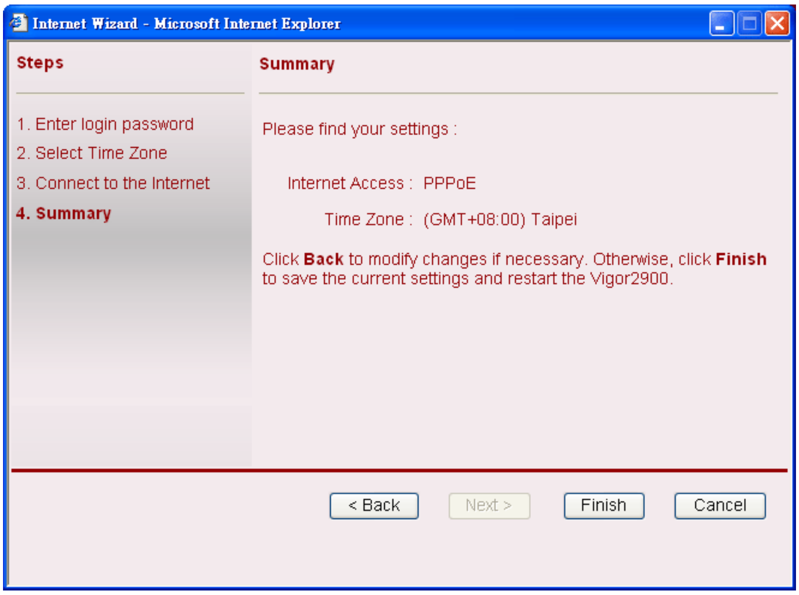
Password Assign a valid password provided by the ISP.

Retype Password Retype the password.

Always On Check this box to allow the router connecting to Internet forever.

Idle Timeout Type in the value (unit is second) as the idle timeout of the connection. When the time is expired, the internet connection will be dropped immediately.

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



Internet Wizard - Microsoft Internet Explorer

Summary

Please find your settings :

Internet Access : PPPoE

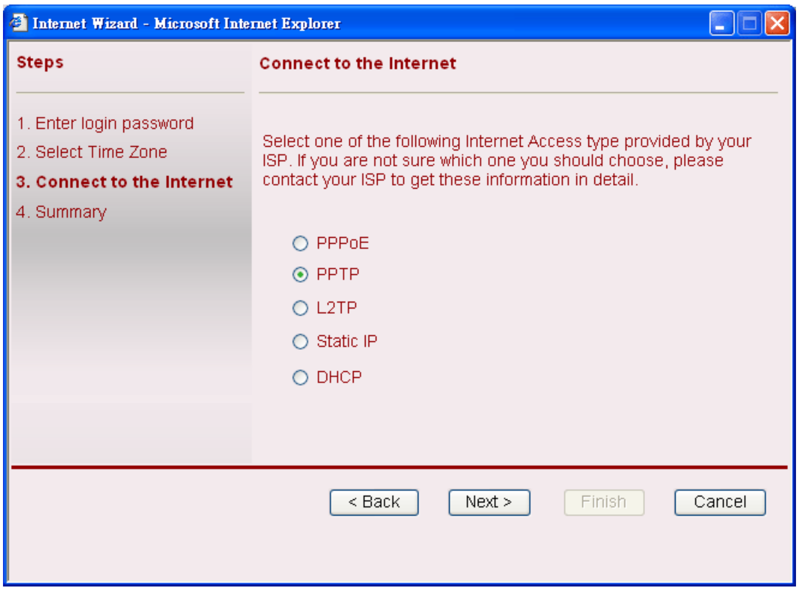
Time Zone : (GMT+08:00) Taipei

Click **Back** to modify changes if necessary. Otherwise, click **Finish** to save the current settings and restart the Vigor2900.

Click **Finish** to save current settings and restart the router.

2.2.3 PPTP

For PPTP connection, please click **PPTP** as the protocol.



Internet Wizard - Microsoft Internet Explorer

Steps

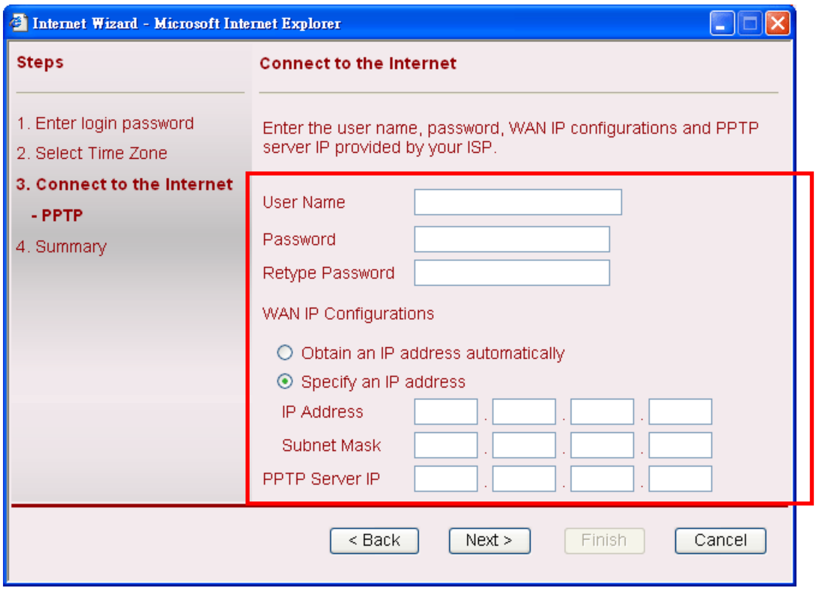
1. Enter login password
2. Select Time Zone
3. **Connect to the Internet**
4. Summary

Connect to the Internet

Select one of the following Internet Access type provided by your ISP. If you are not sure which one you should choose, please contact your ISP to get these information in detail.

○ PPPoE
● PPTP
○ L2TP
○ Static IP
○ DHCP

Click **Next** to see the following page.



Internet Wizard - Microsoft Internet Explorer

Steps

1. Enter login password
2. Select Time Zone
3. **Connect to the Internet**
   - PPTP
4. Summary

Connect to the Internet

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

User Name

Password

Retype Password

WAN IP Configurations

○ Obtain an IP address automatically
● Specify an IP address

IP Address . . .

Subnet Mask . . .

PPTP Server IP . . .

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

Password Assign a valid password provided by the ISP.

Retype Password Retype the password.

Obtain an IP address automatically Click this selection to get the IP address from the router automatically.

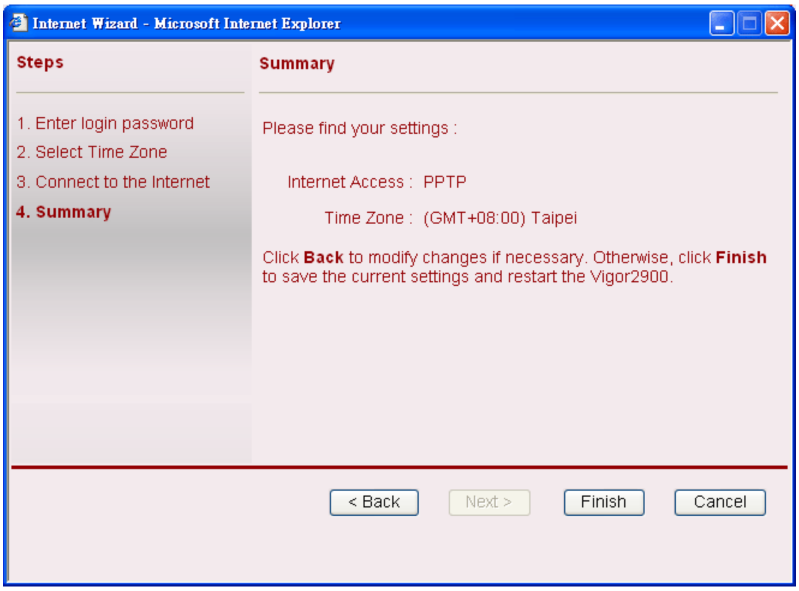
Specify an IP address Click this selection to specify an IP address and subnet mask manually.

IP Address Type a specific IP address for PPTP connection mode that obtained from ISP.

Subnet Mask Type the subnet mask.

PPTP Server IP Specify the IP address of the PPTP Server.

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



Please find your settings :

Internet Access : PPTP

Time Zone : (GMT+08:00) Taipei

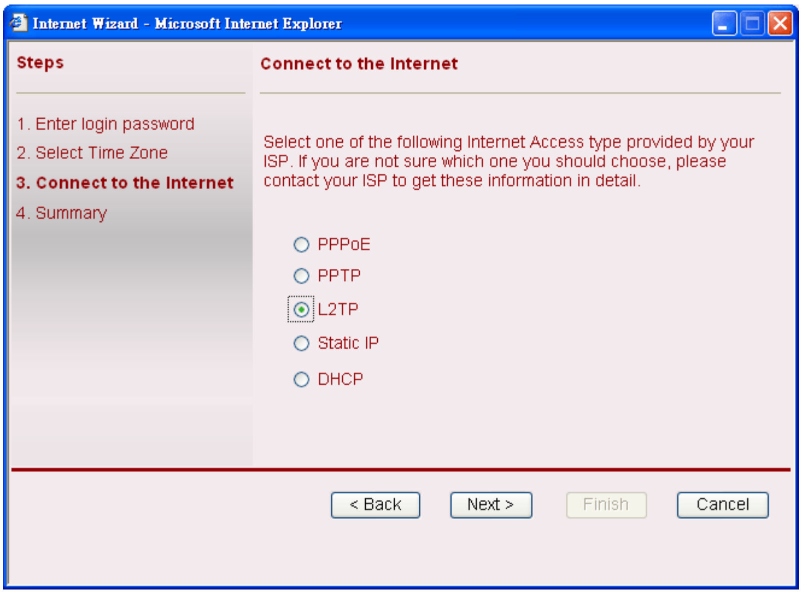
Click **Back** to modify changes if necessary. Otherwise, click **Finish** to save the current settings and restart the Vigor2900.

Click **Finish** to save current settings and restart the router.

2.2.4 L2TP

Note: This setting is available only for ***Vigor 2900, Vigor 2900G, Vigor 2900Gi*** and ***Vigor 2900i***.

Click **L2TP** as the protocol.



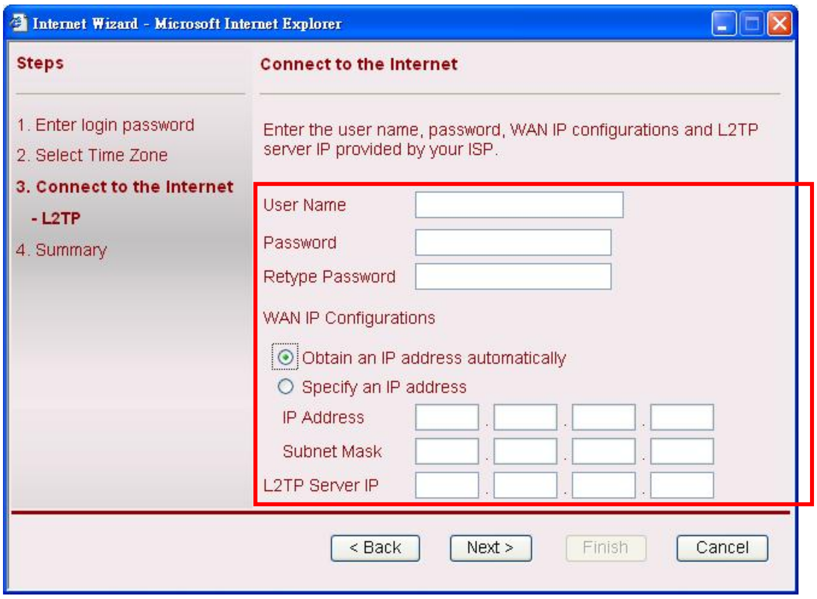
Internet Wizard - Microsoft Internet Explorer
Steps
1. Enter login password
2. Select Time Zone
3. Connect to the Internet
4. Summary

Connect to the Internet

Select one of the following Internet Access type provided by your ISP. If you are not sure which one you should choose, please contact your ISP to get these information in detail.

○ PPPoE
○ PPTP
● L2TP
○ Static IP
○ DHCP

Click **Next** to see the following page.



Internet Wizard - Microsoft Internet Explorer
Steps
1. Enter login password
2. Select Time Zone
3. Connect to the Internet
- L2TP
4. Summary

Connect to the Internet

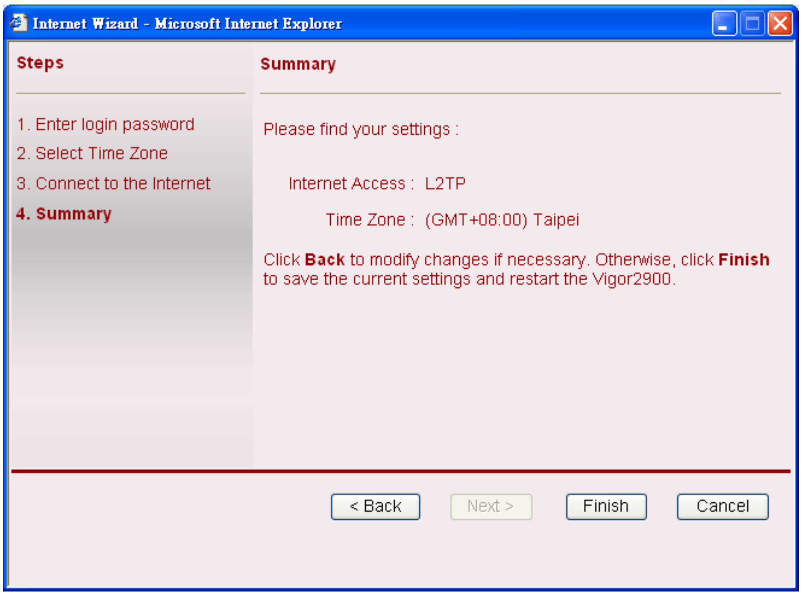
Enter the user name, password, WAN IP configurations and L2TP server IP provided by your ISP.

User Name
Password
Retype Password
WAN IP Configurations
● Obtain an IP address automatically
○ Specify an IP address
IP Address . . .
Subnet Mask . . .
L2TP Server IP . . .

User Name	Assign a specific valid user name provided by the ISP.
Password	Assign a valid password provided by the ISP.
Retype Password	Retype the password.
Obtain an IP address automatically	Click this selection to get the IP address from the router automatically.
Specify an IP address	Click this selection to specify an IP address and subnet mask manually.
IP Address	Type a specific IP address for PPTP connection mode that obtained from ISP.

Subnet Mask	Type the subnet mask.
PPTP Server IP	Specify the IP address of the PPTP Server.

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



Summary

Please find your settings :

Internet Access : L2TP

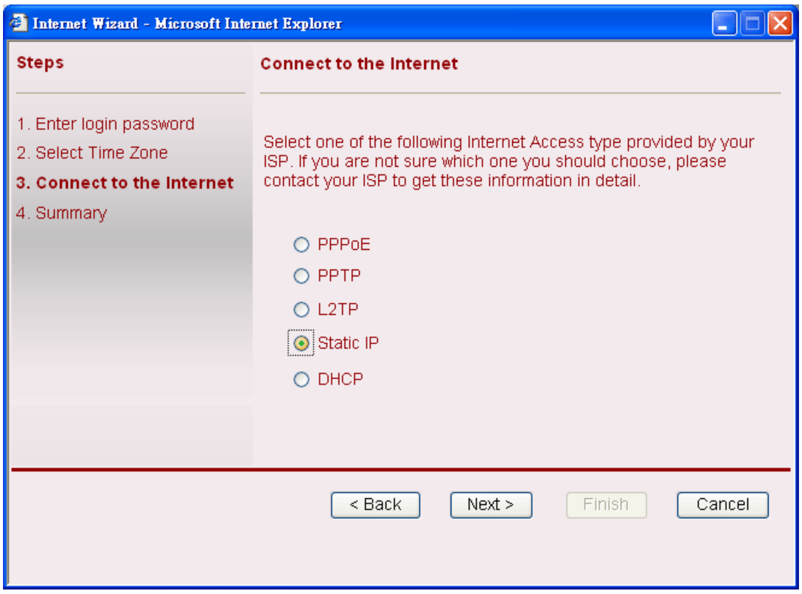
Time Zone : (GMT+08:00) Taipei

Click **Back** to modify changes if necessary. Otherwise, click **Finish** to save the current settings and restart the Vigor2900.

Click **Finish** to save current settings and restart the router.

2.2.5 Static IP

Click **Static IP** as the protocol.

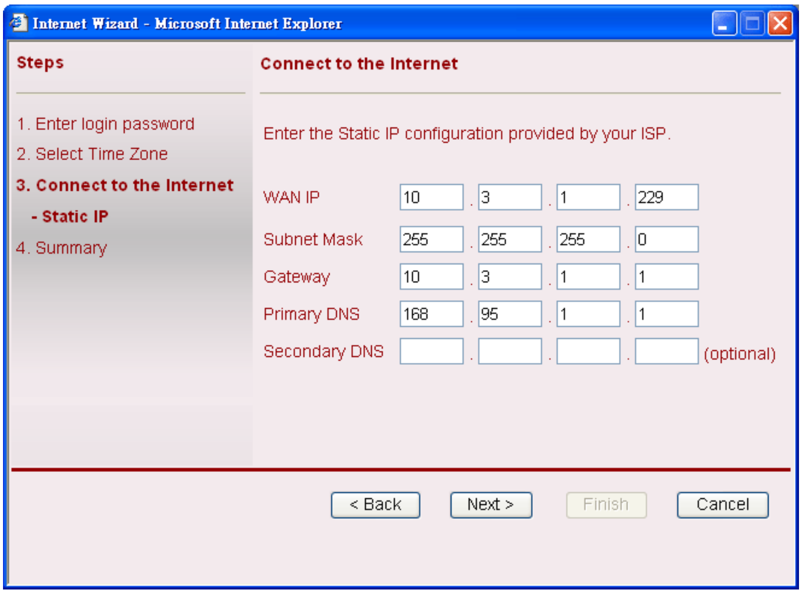


Connect to the Internet

Select one of the following Internet Access type provided by your ISP. If you are not sure which one you should choose, please contact your ISP to get these information in detail.

○ PPPoE
○ PPTP
○ L2TP
● Static IP
○ DHCP

Click **Next** to see the following page.



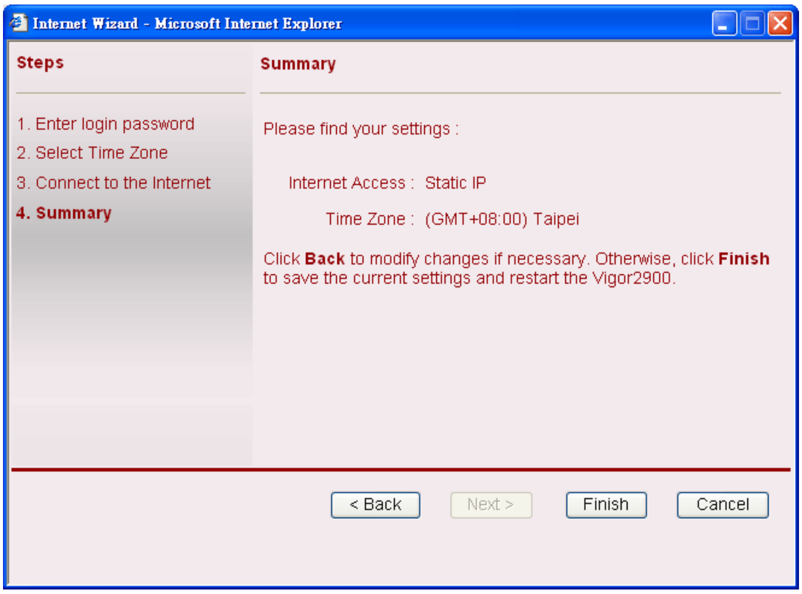
Connect to the Internet

Enter the Static IP configuration provided by your ISP.

WAN IP	10	3	1	229	
Subnet Mask	255	255	255	0	
Gateway	10	3	1	1	
Primary DNS	168	95	1	1	
Secondary DNS					(optional)

WAN IP	Type the WAN IP address that obtained from ISP.
Subnet Mask	Type the subnet mask obtained from ISP.
Gateway	Type the gateway address obtained from ISP.
Primary DNS	Type the IP address as the primary DNS obtained from ISP.
Second DNS	Type the IP address as the secondary DNS.

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



Summary

Please find your settings :

Internet Access : Static IP

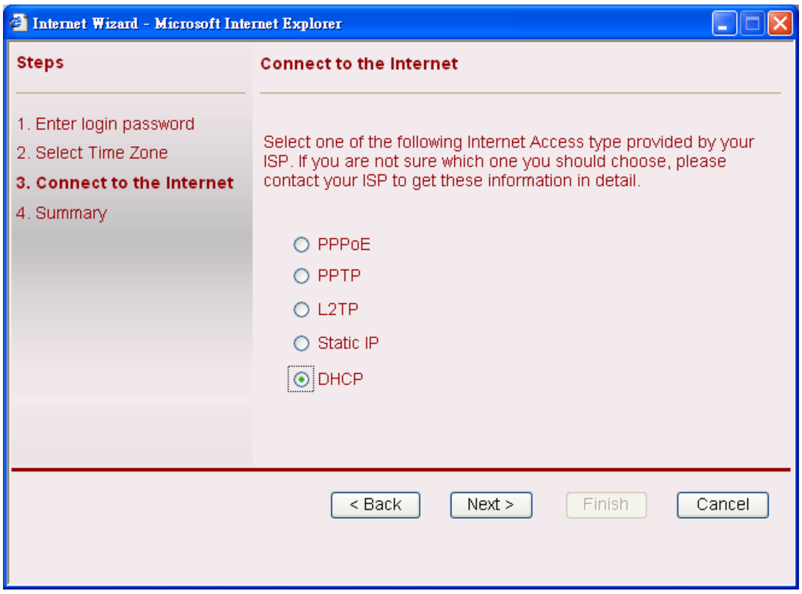
Time Zone : (GMT+08:00) Taipei

Click **Back** to modify changes if necessary. Otherwise, click **Finish** to save the current settings and restart the Vigor2900.

Click **Finish** to save current settings and restart the router.

2.2.6 DHCP

Click **DHCP** as the protocol.



Steps

1. Enter login password
2. Select Time Zone
3. **Connect to the Internet**
4. Summary

Connect to the Internet

Select one of the following Internet Access type provided by your ISP. If you are not sure which one you should choose, please contact your ISP to get these information in detail.

○ PPPoE

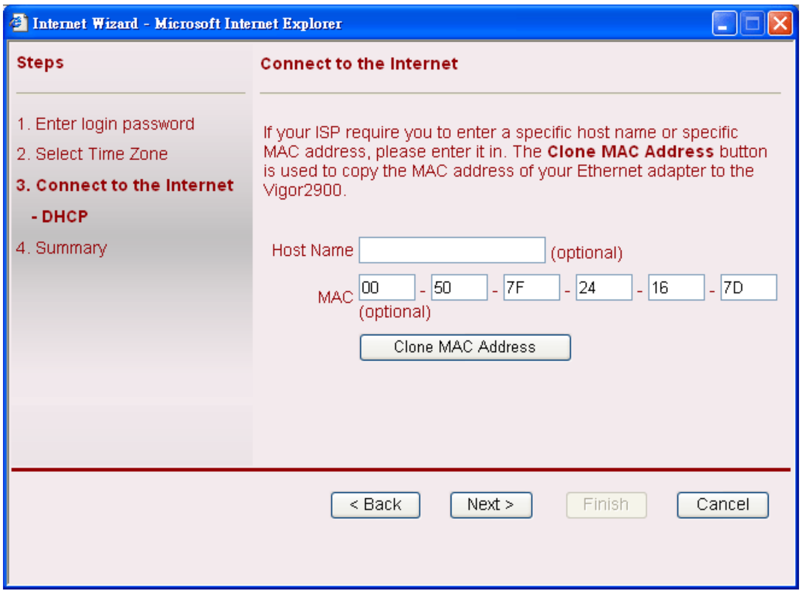
○ PPTP

○ L2TP

○ Static IP

● DHCP

Click **Next** to see the following page.



Steps

1. Enter login password
2. Select Time Zone
3. **Connect to the Internet**
   - DHCP
4. Summary

Connect to the Internet

If your ISP require you to enter a specific host name or specific MAC address, please enter it in. The **Clone MAC Address** button is used to copy the MAC address of your Ethernet adapter to the Vigor2900.

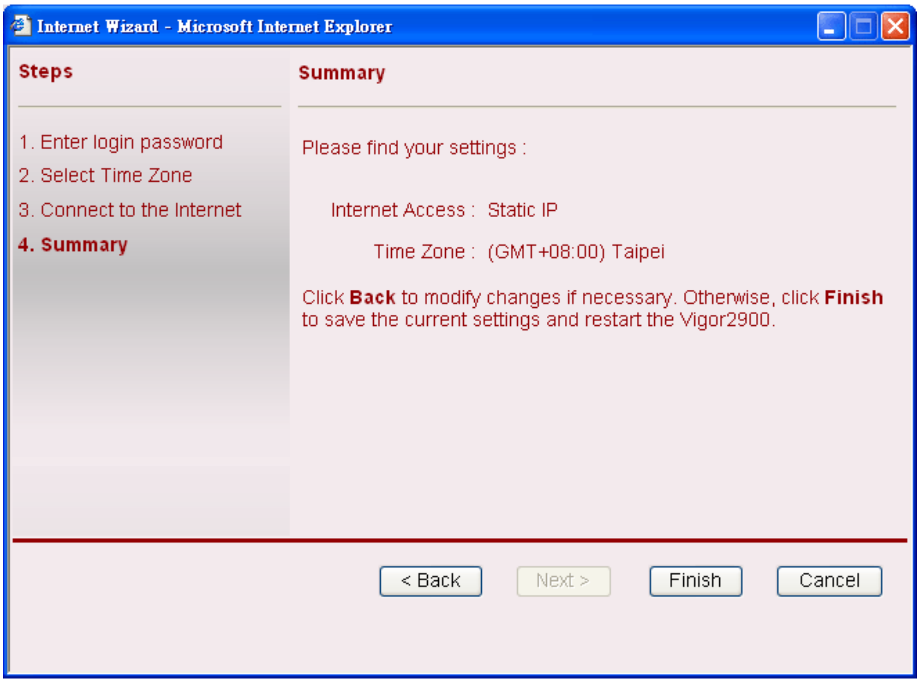
Host Name (optional)

MAC 00 - 50 - 7F - 24 - 16 - 7D (optional)

Host Name Specify the host name for the router.

MAC This is an optional setting. The router will detect the MAC address automatically. If not, click **Clone MAC Address** to obtain it.

Type in all the information that your ISP provides for this protocol. After finishing the settings in this page, click **Next** to see the following page.



Summary

Please find your settings :

Internet Access : Static IP

Time Zone : (GMT+08:00) Taipei

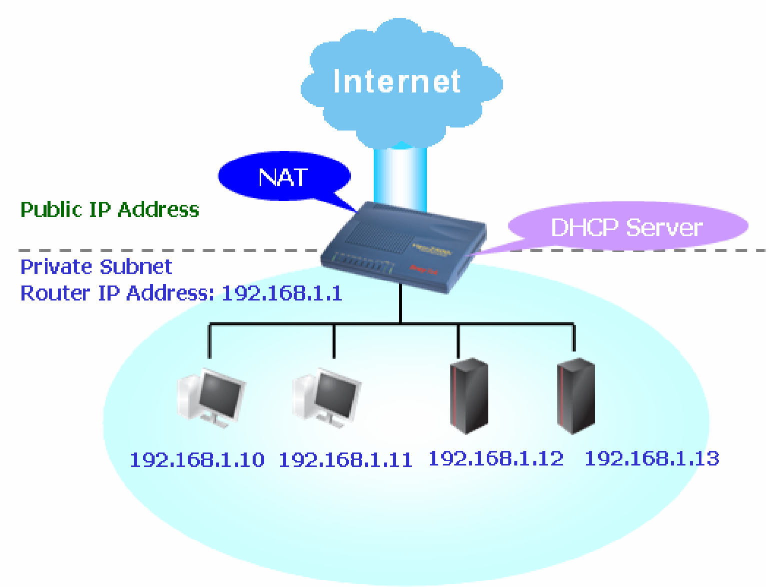
Click **Back** to modify changes if necessary. Otherwise, click **Finish** to save the current settings and restart the Vigor2900.

Click **Finish** to save current settings and restart the router.

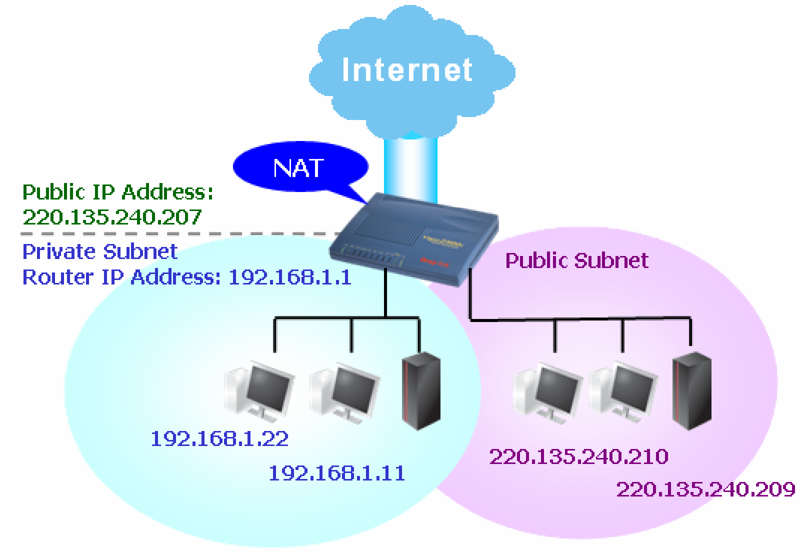
2.3 LAN TCP/IP and DHCP Server

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)

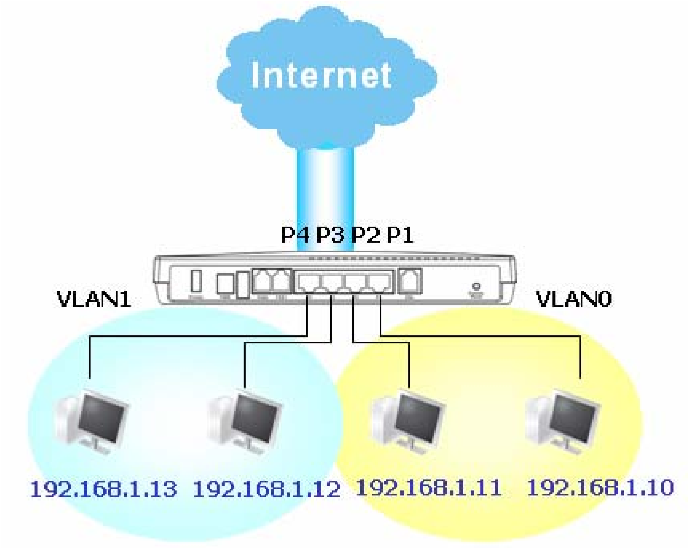
Vigor router will exchange routing information with neighboring routers using the RIP to accomplish IP routing. This allows users to change the information of the router such as IP address and the routers will automatically inform for each other.

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

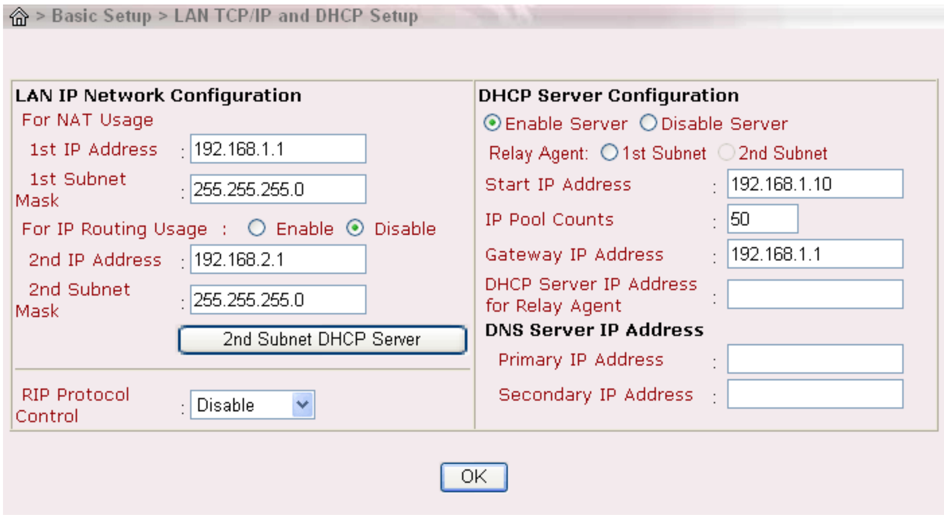
You can group local hosts by physical ports and create up to 4 virtual LANs. To manage the communication between different groups, please set up rules in Virtual LAN (VLAN) function and the rate of each.



Web Page Configuration

This page provides you the general settings for LAN.

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



> Basic Setup > LAN TCP/IP and DHCP Setup

LAN IP Network Configuration

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

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)

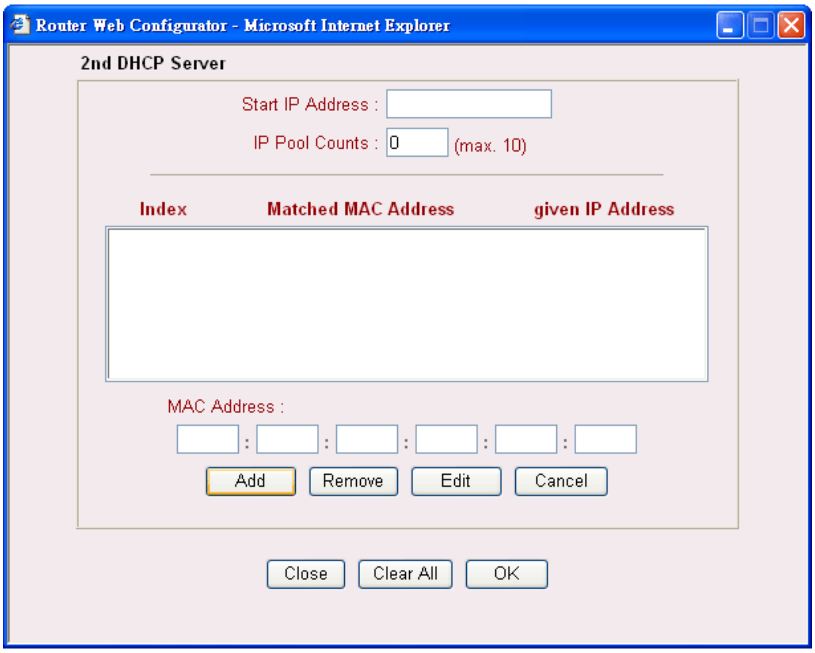
For IP Routing Usage Click **Enable** to invoke this function. The default setting is **Disable**.

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

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.



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 : : : : : :

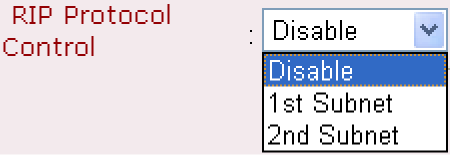
Start IP Address: Enter a value of the IP address pool for the DHCP server to start with when issuing IP addresses. If the 2nd IP address of your router is 220.135.240.1, the starting IP address must be 220.135.240.2 or greater, but smaller than 220.135.240.254.

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 220.135.240.4.

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.

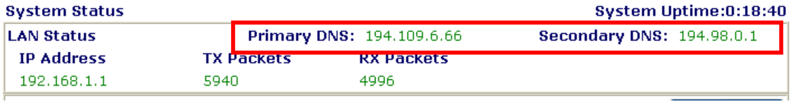
DNS Server Configuration

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.

Primary IP Address -You must specify a DNS server IP address here because your ISP should provide you with usually more than one DNS Server. If your ISP does not provide it, the router will automatically apply default DNS Server IP address: 194.109.6.66 to this field.

Secondary IP Address - You can specify secondary DNS server IP address here because your ISP often provides you more than one DNS Server. If your ISP does not provide it, the router will automatically apply default secondary DNS Server IP address: 194.98.0.1 to this field.

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



System Status System Uptime:0:18:40

LAN Status Primary DNS: 194.109.6.66 Secondary DNS: 194.98.0.1

IP Address	TX Packets	RX Packets
192.168.1.1	5940	4996

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.

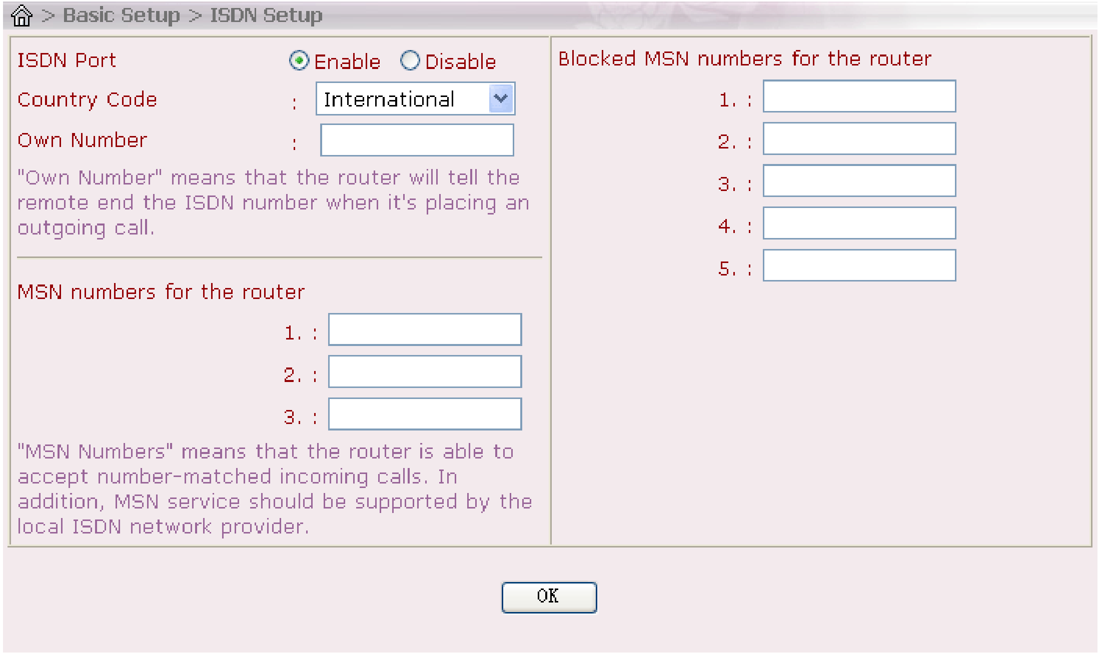
If the IP address of a domain name is already in the DNS cache, the router will resolve the domain name immediately. Otherwise, the router forwards the DNS query packet to the external DNS server by establishing a WAN (e.g. DSL/Cable) connection.

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.

2.4 ISDN Setup

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

Note: The following is available for **Vigor2900VGi/Vi** only.



> Basic Setup > ISDN Setup

ISDN Port ● Enable ○ Disable

Country Code : International

Own Number :

"Own Number" means that the router will tell the remote end the ISDN number when it's placing an outgoing call.

MSN numbers for the router

1. :

2. :

3. :

"MSN Numbers" means that the router is able to accept number-matched incoming calls. In addition, MSN service should be supported by the local ISDN network provider.

Blocked MSN numbers for the router

1. :

2. :

3. :

4. :

5. :

ISDN Port Click **Enable** to open the ISDN port and **Disable** to close it.

Country Code For proper operation on your local ISDN network, you should choose the correct country code.

Own Number Enter your ISDN number. Every outgoing call will carry the number to the receiver.

MSN Numbers for the Router **MSN Numbers** mean that the router is able to accept only number-matched incoming calls. In addition, MSN services should be supported by local ISDN network provider. The router provides three fields for MSN numbers. Note that MSN services must be acquired from your local telecommunication operators. By default, MSN function is disabled. If you leave the fields blank, all incoming calls will be accepted without number matching.

Blocked MSN Numbers for the router Enter the specified MSN number into the fields to prevent the router from dialing the specific MSN number.

For example, DrayTek provides the **Remote Activation** (refer to section 3.2) feature for the teleworkers who wish to dial in the head office over the ISDN. With this feature, teleworkers can make a phone call to the router at the head office and ask the router to dial up the ISP. As a result, the teleworkers can be authorized with their office accounts to utilize ISDN dial-up services and both sides can thus engage in secure communication over the LAN-to-LAN ISDN.

The ISDN interface of Vigor2900VGi and Vigor2900Vi routers supports the **VTA** (**Virtual Terminal Adapter,** please refer to section 2.8) feature. VTA is actually a "CAPI" software, which can simulate a real ISDN terminal adapter installed on your computer. You can install the CAPI-compliant software for dial-up networking, fax or voice applications depending on the functionality of the CAPI software you installed. To employ the VTA feature, please download the VTA drivers (available only to Windows 98SE/2000/XP) from http://www.draytek.com/english/support/download.php.

2.5 Wireless LAN Setup

Note: The following is available for **G** models only.

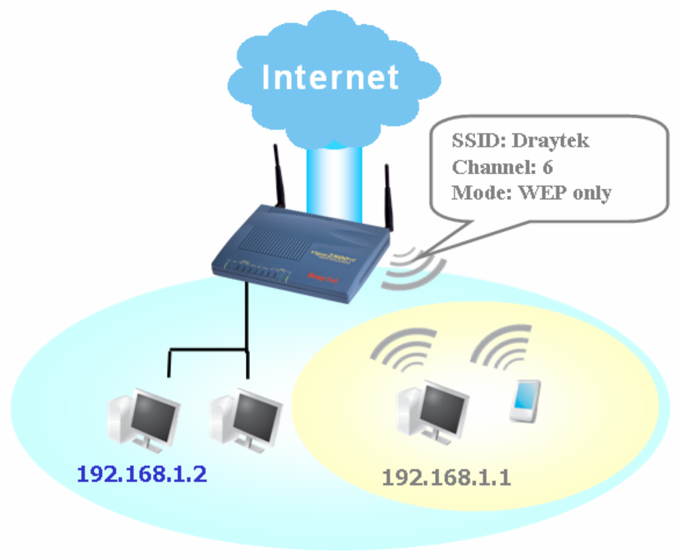
2.5.1 Basic Concepts

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

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

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

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



Security Overview

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

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

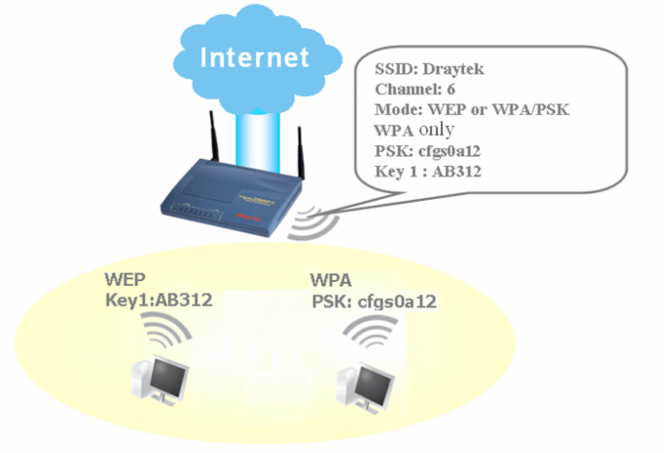
WEP (Wired Equivalent Privacy) is a legacy method to encrypt each frame transmitted via radio using either a 64-bit or128-bit key. Usually access point will preset a set of four keys and it will communicate with each station using only one out of the four keys.

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

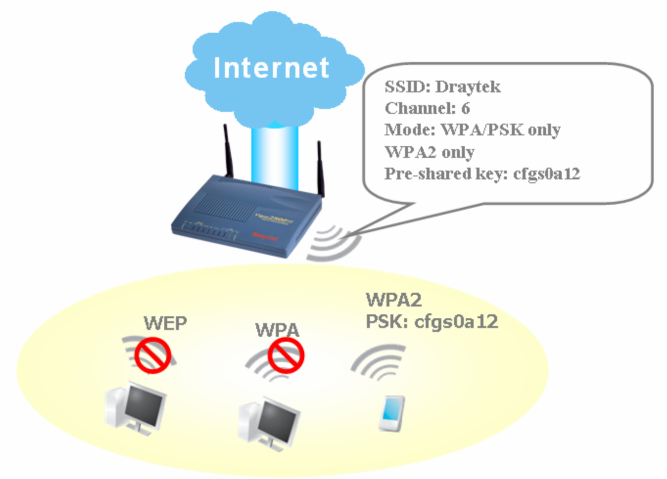
In WPA-Personal, a pre-defined key is used for encryption during data transmission. WPA applies Temporal Key Integrity Protocol (TKIP) for data encryption while WPA2 applies AES. The WPA-Enterprise combines not only encryption but also authentication.

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

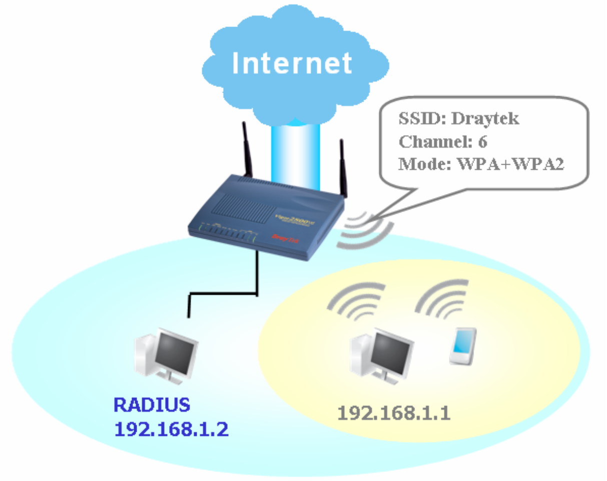
Example 1



Example 2



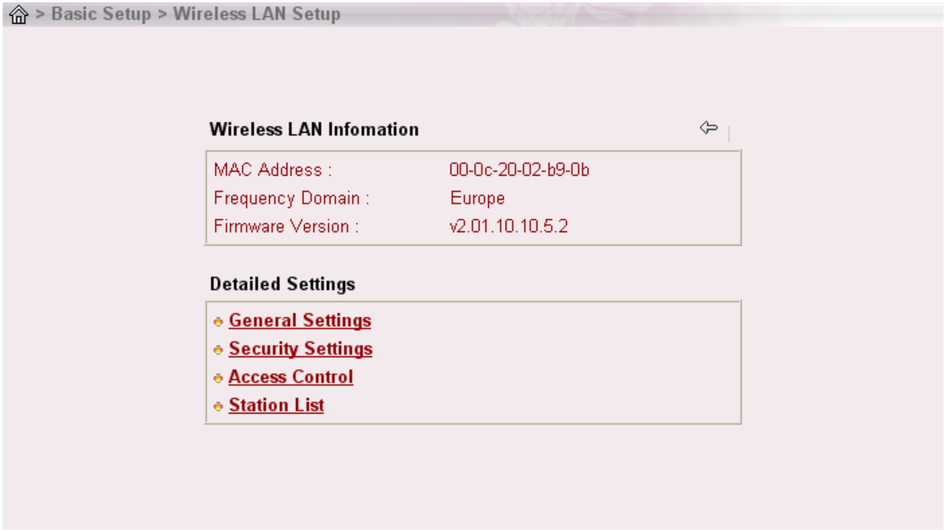
Example 3



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

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

Click **Wireless LAN Setup** from the **Basic Setup** group. You will see the following page.



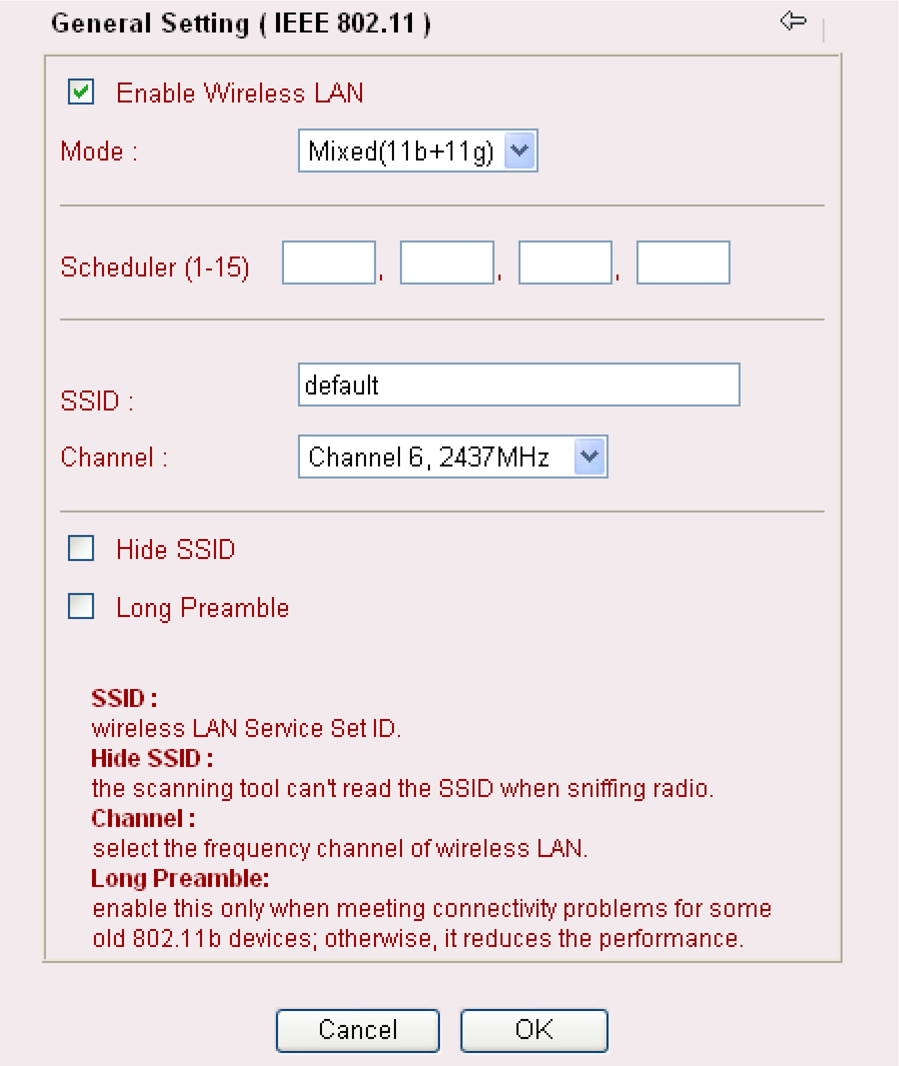
Wireless LAN Infomation

MAC Address :	00-0c-20-02-b9-0b
Frequency Domain :	Europe
Firmware Version :	v2.01.10.10.5.2

Detailed Settings

2.5.2 General Settings

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



General Setting (IEEE 802.11)

☑ Enable Wireless LAN

Mode : Mixed(11b+11g)

Scheduler (1-15) , , ,

SSID : default

Channel : Channel 6, 2437MHz

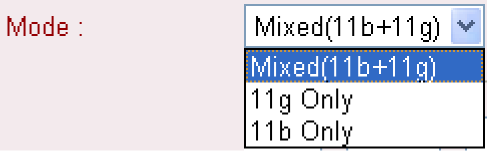
□ Hide SSID

□ Long Preamble

SSID :
wireless LAN Service Set ID.
Hide SSID :
the scanning tool can't read the SSID when sniffing radio.
Channel :
select the frequency channel of wireless LAN.
Long Preamble:
enable this only when meeting connectivity problems for some old 802.11b devices; otherwise, it reduces the performance.

Enable Wireless LAN Check the box to enable wireless function.

Mode Select an appropriate wireless mode.
Mixed (11b+11g) - The radio can support both IEEE802.11b and IEEE802.11g protocols simultaneously.
11g only - The radio only supports IEEE802.11g.
11b only - The radio only supports IEEE802.11b.



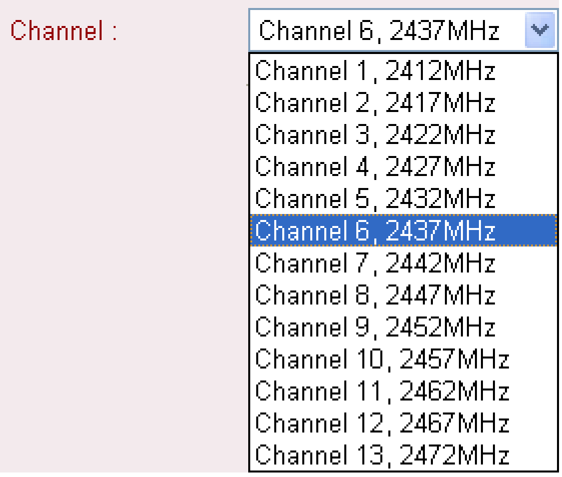
Scheduler (1-15) Set the wireless LAN to work at certain time interval only. You may choose up to 4 schedules out of the 15 schedules pre-defined in **Call Schedule Setup** in **Advanced Setup group** setup. The default setting of this filed is blank and the function will always work.

SSID The default SSID is "default". We suggest you change it to a particular name. It is the identification of the wireless

LAN. SSID can be any text numbers or various special characters.

Channel

The channel of frequency of the wireless LAN. The default channel is 6. You may switch channel if the selected channel is under serious interference.



Channel : Channel 6, 2437MHz

Hide SSID

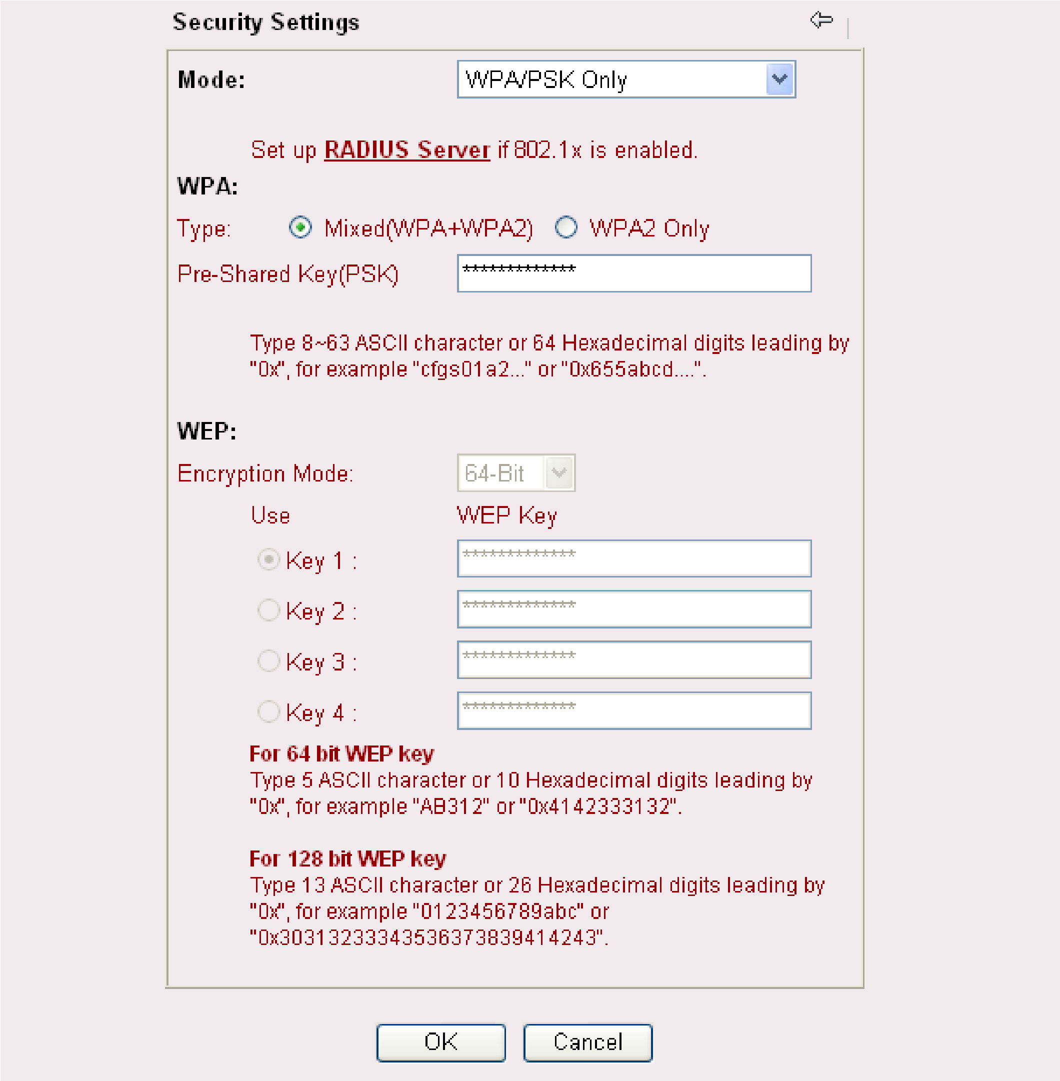
Check it to prevent from wireless sniffing and make it harder for unauthorized clients or STAs to join your wireless LAN. Depending on the wireless utility, the user may only see the information except SSID or just cannot see any thing about Vigor wireless router while site surveying.

Long Preamble

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

2.5.3 Security

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



Security Settings

Mode: WPA/PSK Only

Set up RADIUS Server if 802.1x is enabled.

WPA:

Type: ● Mixed(WPA+WPA2) ○ WPA2 Only

Pre-Shared Key(PSK) **************

Type 8~63 ASCII character or 64 Hexadecimal digits leading by "0x", for example "cfgs01a2..." or "0x655abcd....".

WEP:

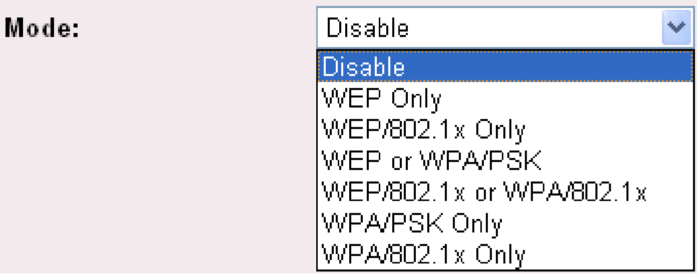
Encryption Mode: 64-Bit

Use	WEP Key
● Key 1 :	**************
○ Key 2 :	**************
○ Key 3 :	**************
○ Key 4 :	**************

For 64 bit WEP key
Type 5 ASCII character or 10 Hexadecimal digits leading by "0x", for example "AB312" or "0x4142333132".

For 128 bit WEP key
Type 13 ASCII character or 26 Hexadecimal digits leading by "0x", for example "0123456789abc" or "0x30313233343536373839414243".

Mode There are several modes provided for you to choose.



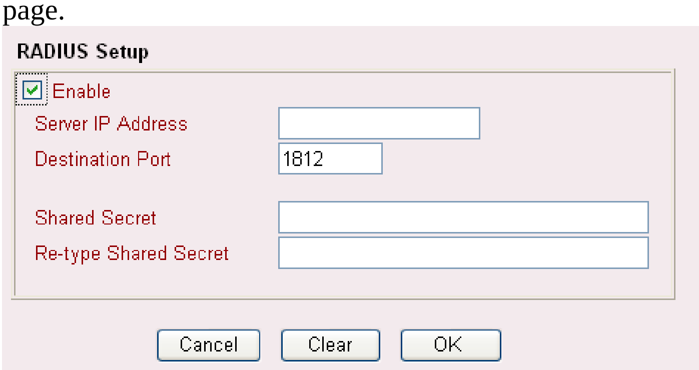
Mode: Disable

Disable - Turn off the encryption mechanism.
WEP Only - Accepts only WEP clients and the encryption key should be entered in WEP Key.
WEP/802.1x Only - Accept WEP clients with 802.1x authentication. Since the key will be auto-negotiated during authentication, the field of key setting below will be not available for input.
WEP or WPA/PSK - Accepts WEP and WPA clients with legal key accordingly. Only Mixed (WPA+WPA2) is

applicable if you select WPA/PSK.
WEP/802.1x or WPA/802.1x - Accept WEP or WPA clients with 802.1x authentication. Only Mixed(WPA+WPA2) is applicable if you select WPA/PSK. Since the key will be auto-negotiated during authentication, the field of key setting below will be not available for input.
WPA/PSK Only - Accepts WPA clients and the encryption key should be entered in PSK. Remember to select WPA type to define either Mixed or WPA2 only in the field below.
WPA/802.1x Only - Accept WPA clients with 802.1x authentication. Remember to select WPA type to define either Mixed or WPA2 only in the field below. Since the key will be auto-negotiated during authentication, the field of key setting below will be not available for input.

Radius Server

If you select **WEP/802.1x Only**, **WEP/802.1x or WPA/802.1x or WPA/802.1x Only** as the security mode, you have to set up RADIUS Server for using with those modes. Click the **Radius Server** link to open the following page.



RADIUS Setup

☑ Enable

Server IP Address:

Destination Port: 1812

Shared Secret:

Re-type Shared Secret:

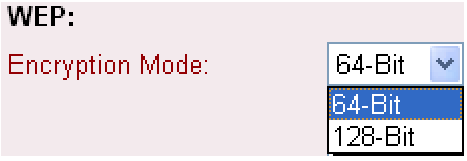
Check **Enable**. Type the IP address for the Radius server. Specify the destination port. The default setting is 1812. Then type the shared secret and confirm the key again. When you finish the settings, please click **OK** to leave the page and invoke the settings.

WPA

The WPA encrypts each frame transmitted from the radio using the key, which either PSK entered manually in this field below or automatically negotiated via 802.1x authentication.
Pre-Shared Key (PSK) - Enter **8~63** ASCII characters, such as 012345678.(or 64 Hexadecimal digits leading by 0x, such as "0x321253abcde...").

WEP

64-Bit - For 64 bits WEP key, enter **5** ASCII characters, such as 12345 (or 10 hexadecimal digitals leading by 0x, such as 0x4142434445.)
128-Bit - For 128 bits WEP key, enter **13** ASCII characters, such as ABCDEFGHIJKLM (or 26 hexadecimal digits leading by 0x, such as 0x4142434445464748494A4B4C4D).



WEP:

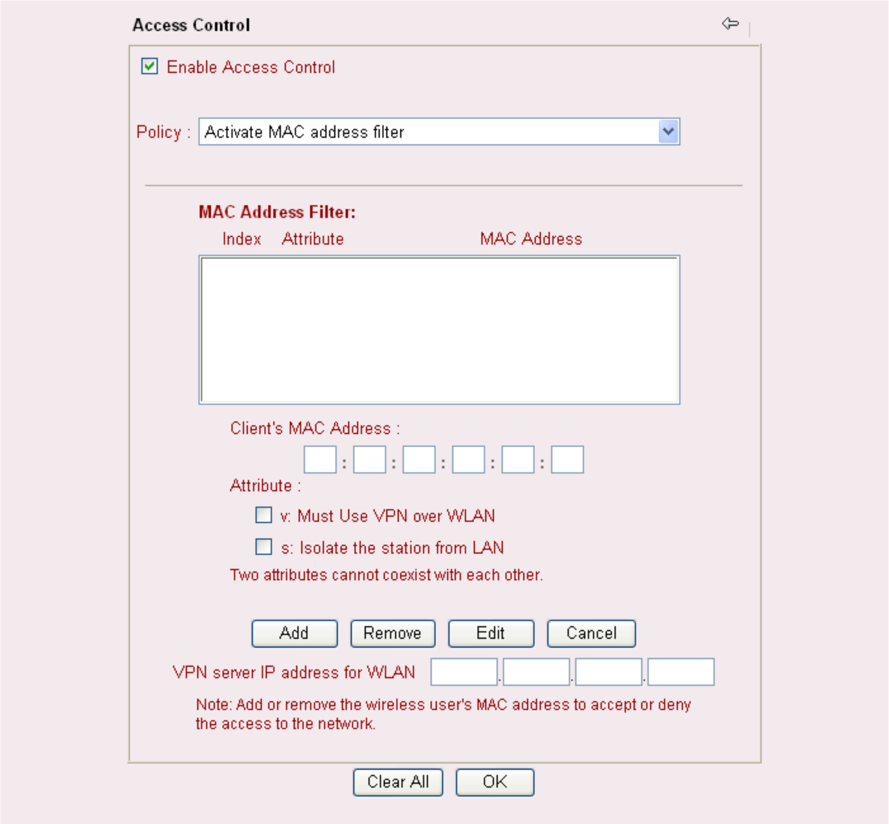
Encryption Mode: 64-Bit

64-Bit
128-Bit

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

2.5.4 Access Control

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



Access Control

☑ Enable Access Control

Policy : Activate MAC address filter

MAC Address Filter:

Index	Attribute	MAC Address

Client's MAC Address : □ : □ : □ : □ : □ : □

Attribute :

☐ v: Must Use VPN over WLAN

☐ s: Isolate the station from LAN

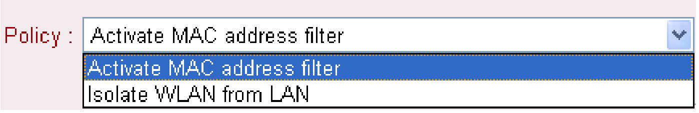
Two attributes cannot coexist with each other.

VPN server IP address for WLAN □ . □ . □ . □

Note: Add or remove the wireless user's MAC address to accept or deny the access to the network.

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

Policy Select to enable any one of the following policy. Choose **Activate MAC address filter** to type in the MAC addresses for other clients in the network manually. Choose **Isolate WLAN from LAN** will separate all the WLAN stations from LAN based on the MAC Address list.



Policy : Activate MAC address filter

Activate MAC address filter
Isolate WLAN from LAN

MAC Address Filter Display all MAC addresses that are edited before. Four buttons (Add, Remove,

Client's MAC Address - Manually enter the MAC address of wireless client.

Attribute — **v -** select to apply VPN to the connection of the wireless client of the MAC address.
s - select to isolate the wireless connection of the wireless client of the MAC address from LAN.

Add — Add a new MAC address into the list.

Remove — Delete the selected MAC address in the list.

Edit — Edit the selected MAC address in the list.

Cancel — Give up the access control set up.

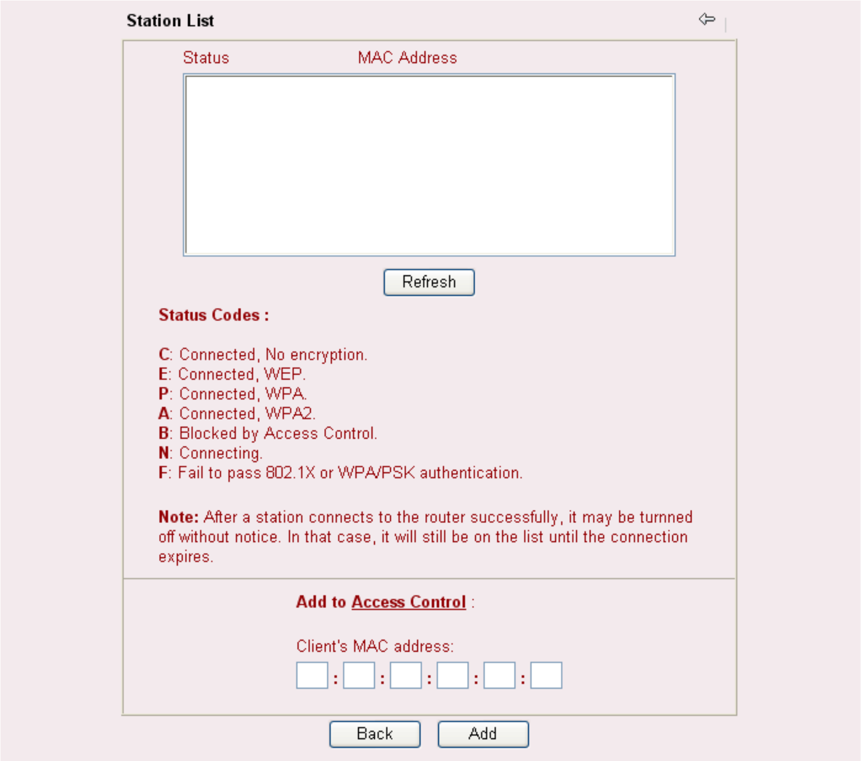
VPN server IP address for WLAN — It enables the construction of VPN tunnels(PPTP/L2TP/L2TP over IPSec) over Wireless LAN. For instance, you can adopt WEP plus VPN over WLAN to provide double protection mechanisms for data frames.

Clear All — Clean all entries in the MAC address list.

OK — Click it to save the access control list.

2.5.5 Station List

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



Station List

Status MAC Address

Refresh

Status Codes :

C: Connected, No encryption.
E: Connected, WEP.
P: Connected, WPA.
A: Connected, WPA2.
B: Blocked by Access Control.
N: Connecting.
F: Fail to pass 802.1X or WPA/PSK authentication.

Note: After a station connects to the router successfully, it may be turned off without notice. In that case, it will still be on the list until the connection expires.

Add to Access Control :

Client's MAC address: [ ] : [ ] : [ ] : [ ] : [ ] : [ ]

Back Add

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

Add — Click this button to add current selected MAC address into **Access Contro**l.

2.6 Internet Access Setup

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 **Quick Setup** group and click the **Internet Access Setup** link. This section will introduce some basic concepts of Internet and explain the connection modes in details.

2.6.1 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

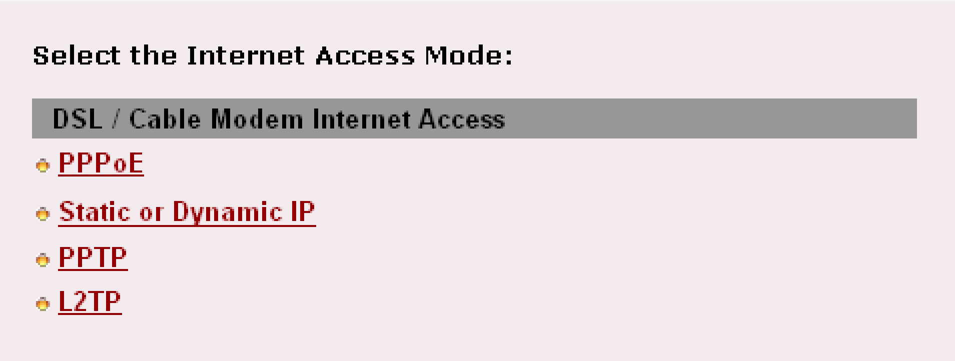
To acquire a public IP address from your ISP for Vigor router as a customer premises equipment, there are three common protocols: **Point to Point Protocol over Ethernet (PPPoE), PPPoA** and **MPoA**. **Multi-PVC** is provided for more advanced setup of the above.

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

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

In the **Quick Setup** field, you can configure the router for different connection types, such as ISDN, PPPoE, PPTP, Dynamic/Static IP or Broadband Access with ISDN dial backup. Note that the types of ISDN and Broadband Access with ISDN dial backup are available only to Vigor routers with the ISDN interface (e.g. Vigor2900VGi).

Click **Internet Access Setup** on the **Quick Setup** page. You will access the following page.

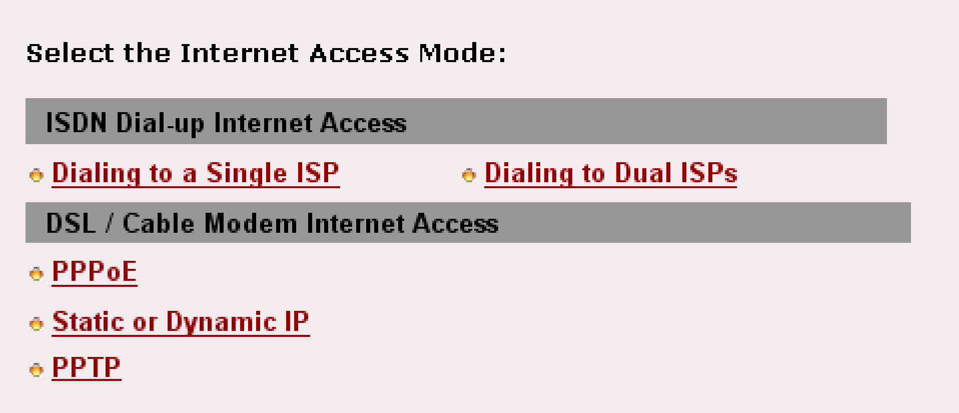


Select the Internet Access Mode:

DSL / Cable Modem Internet Access

- PPPoE
- Static or Dynamic IP
- PPTP
- L2TP

If your router supports ISDN function, you will get the following page with ISDN dial-up Internet Access.



Select the Internet Access Mode:

ISDN Dial-up Internet Access

- Dialing to a Single ISP
- Dialing to Dual ISPs

DSL / Cable Modem Internet Access

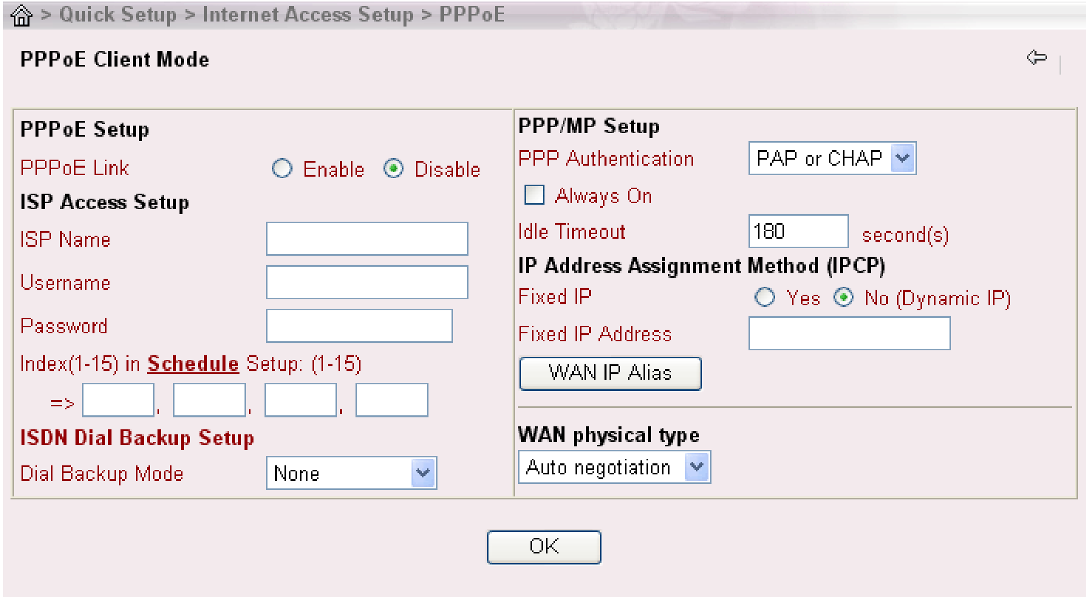
- PPPoE
- Static or Dynamic IP
- PPTP

The following sections will introduce the Internet Access Modes.

2.6.2 PPPoE

As a CPE device, Vigor router encapsulates the PPP session based for transport across the ADSL loop and your ISP's Digital Subscriber Line Access Multiplexer (DSLAM).

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



> Quick Setup > Internet Access Setup > PPPoE

PPPoE Client Mode

PPPoE Setup

PPPoE Link ○ Enable ● Disable

ISP Access Setup

ISP Name

Username

Password

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

=> , , ,

ISDN Dial Backup Setup

Dial Backup Mode: None

PPP/MP Setup

PPP Authentication: PAP or CHAP

□ Always On

Idle Timeout: 180 second(s)

IP Address Assignment Method (IPCP)

Fixed IP ○ Yes ● No (Dynamic IP)

Fixed IP Address

WAN physical type

Auto negotiation

PPPoE Link

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 Name

Type in the ISP Name provided by ISP in this field.

Username

Type in the username provided by ISP in this field.

Password

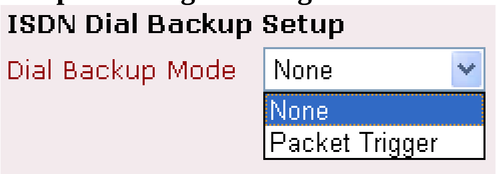
Type in the password provided by ISP in this field.

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.

ISDN Dial Backup Setup

This setting is available for the routers supporting ISDN function only. Before utilizing the ISDN dial backup feature, you must create a dial backup profile first. Please click **Internet Access Setup** > **Dialing to a Single ISP** to enter the backup profile.



ISDN Dial Backup Setup

Dial Backup Mode: None

Due to the absence of the ISDN interface in some models (e.g., Vigor2900V and Vigor2900VG), the ISDN dial backup feature and its associated setup options are not available to them. Please refer to the previous part for further information.

None - Disable the backup function.

Packet Trigger -The backup line is not on until a packet from a local host triggers the router to establish a connection.

PPP Authentication

Select **PAP only** or **PAP or CHAP** for PPP.

Always On

Check this box if you want the router keeping connecting to Internet forever.

Idle Timeout

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

Fixed IP

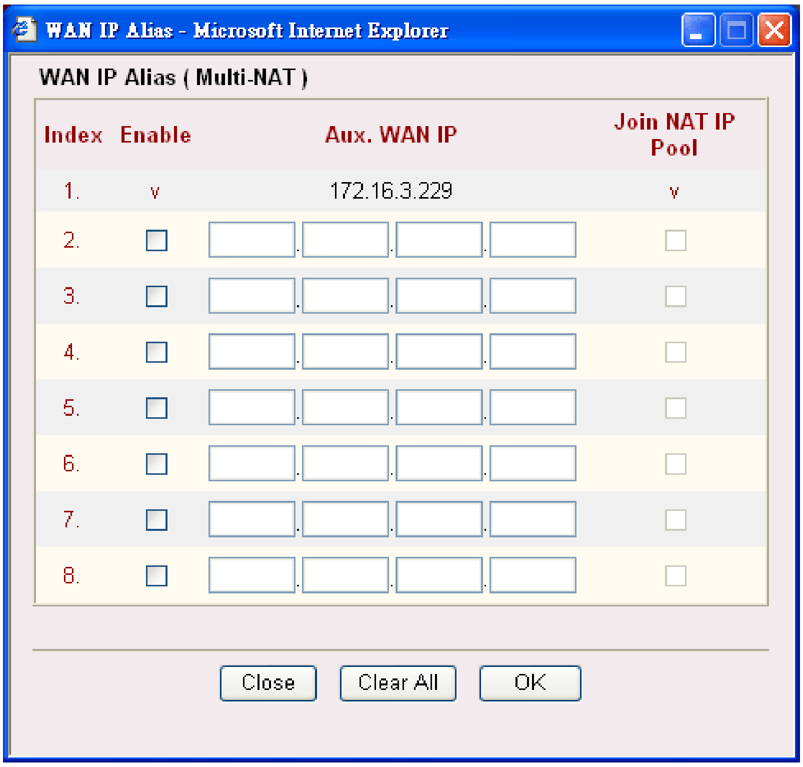
Usually ISP dynamically assigns IP address to you each time you connect to it and request. In some case, your ISP provides service to always assign you the same IP address whenever you request. In this case, you can fill in this IP address in the Fixed IP field. Please contact your ISP before you want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

Fixed IP Address

Type a fixed IP address.

WAN IP Alias

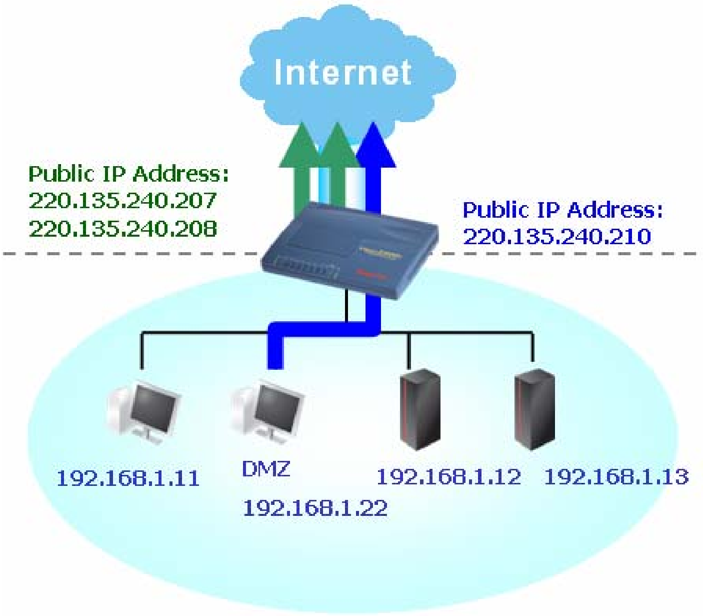
If you have multiple public IP addresses and would like to utilize them on the WAN interface, please use WAN IP Alias. You can set up to 8 public IP addresses other than the current one you are using.



WAN IP Alias (Multi-NAT)

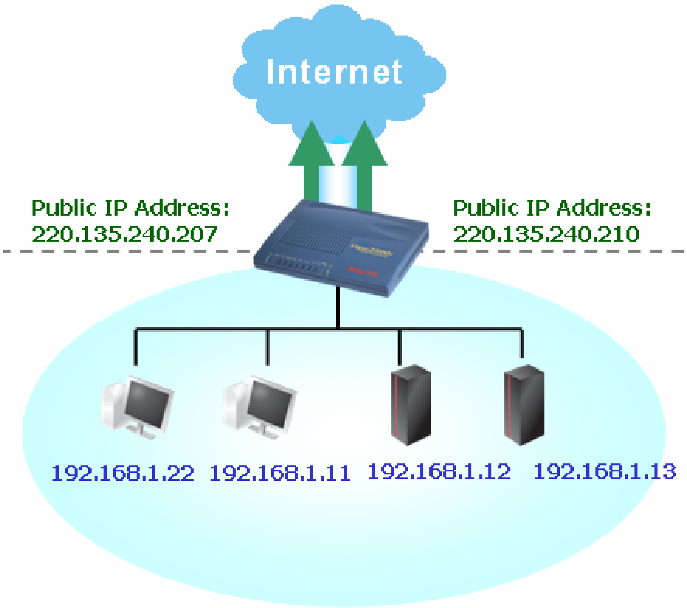
Index	Enable	Aux. WAN IP	Join NAT IP Pool
1.	v	172.16.3.229	v
2.	□	. . .	□
3.	□	. . .	□
4.	□	. . .	□
5.	□	. . .	□
6.	□	. . .	□
7.	□	. . .	□
8.	□	. . .	□

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

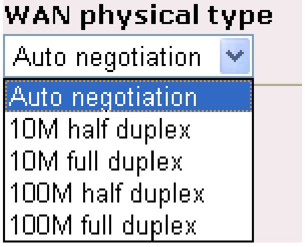


If you do not check **Join NAT IP Pool**, you can still use these public

IP addresses for other purpose, such as DMZ host, Open Ports.



WAN physical type Check and choose a proper type used for duplex between this device and other router that you want to communicate. Both sides should use the same physical type; otherwise, the connection might be failed due to inconsistent type. It is recommended for you to set Auto negotiation as the physical type.



WAN physical type

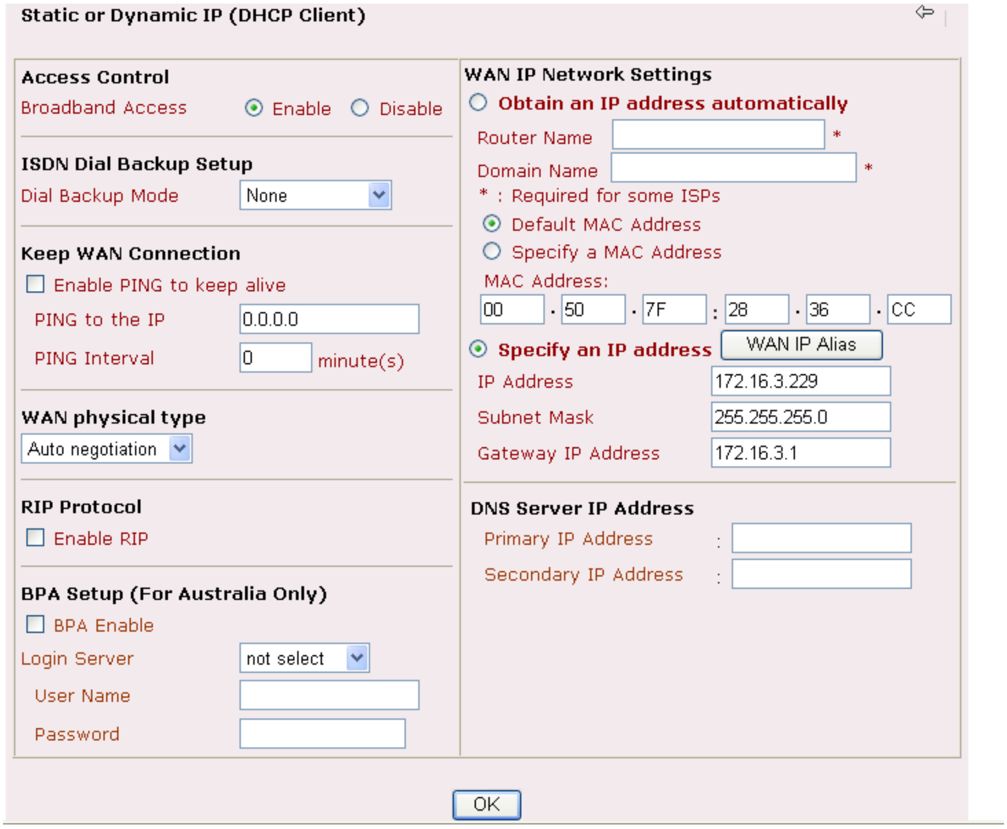
Auto negotiation

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

2.6.3 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 choose **Static or Dynamic IP** as the accessing protocol of the internet, please select **Internet Access Setup** on the **Quick Setup** page. **Next,** choose the **Static or Dynamic IP** link. The following web page will be shown.



Static or Dynamic IP (DHCP Client)

Access Control

Broadband Access ● Enable ○ Disable

ISDN Dial Backup Setup

Dial Backup Mode: None

Keep WAN Connection

□ Enable PING to keep alive

PING to the IP: 0.0.0.0

PING Interval: 0 minute(s)

WAN physical type: Auto negotiation

RIP Protocol

□ Enable RIP

BPA Setup (For Australia Only)

□ BPA Enable

Login Server: not select

User Name:

Password:

WAN IP Network Settings

○ Obtain an IP address automatically

Router Name: *

Domain Name: *

* : Required for some ISPs

● Default MAC Address

○ Specify a MAC Address

MAC Address: 00 . 50 . 7F : 28 . 36 . CC

● Specify an IP address

IP Address: 172.16.3.229

Subnet Mask: 255.255.255.0

Gateway IP Address: 172.16.3.1

DNS Server IP Address

Primary IP Address :

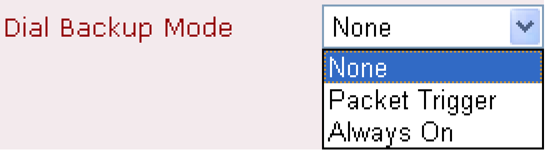
Secondary IP Address :

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.

ISDN Dial Backup Setup

This setting is available for the routers supporting ISDN function only. Before utilizing the ISDN dial backup feature, you must create a dial backup profile first. Please click **Internet Access Setup** > **Dialing to a Single ISP** to enter the backup profile.



Dial Backup Mode: None

Due to the absence of the ISDN interface in some models (e.g., Vigor2900V and Vigor2900VG), the ISDN dial backup feature and its associated setup options are not available to them. Please refer to the previous part for further information.

None - Disable the backup function.

Packet Trigger -The backup line is not on until a packet from a local host triggers the router to establish a connection.

Always On - If the broadband connection is no longer available, the backup line will be activated automatically and always on until the broadband connection is restored. We recommend you to enable this feature if you host a web server for your customers' access.

Keep WAN Connection

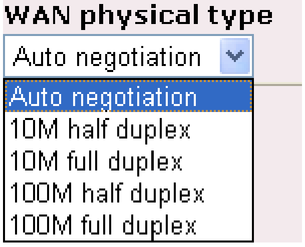
Normally, this function is designed for Dynamic IP environments because some ISPs will drop connections if there is no traffic within certain periods of time. Check **Enable PING to keep alive** box to activate this function.

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 physical type

Check and choose a proper type used for duplex between this device and other router that you want to communicate. Both sides should use the same physical type; otherwise, the connection might be failed due to inconsistent type. It is recommended for you to set Auto negotiation as the physical type.

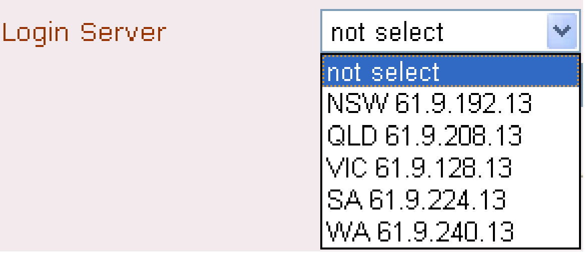

WAN physical type
Auto negotiation

RIP Protocol

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

BPA Setup

This setting is useful for Australia only.
BPA Enable - Check this box to activate this function.
Login Server - Select any one of the login server for your device.

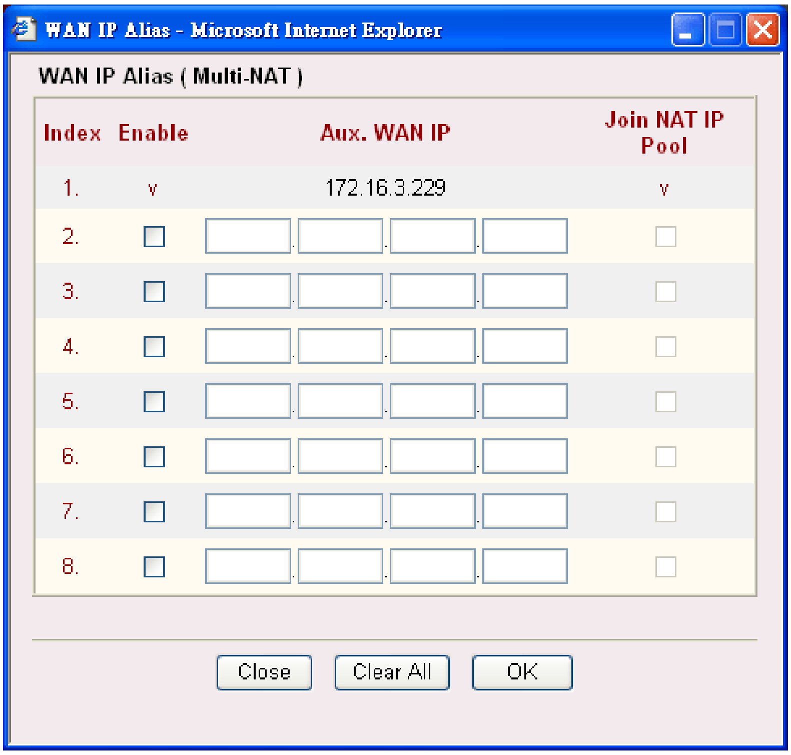

Login Server: not select

User Name - Type the user name obtained from ISP.
Password - Type the password obtained from ISP.

WAN IP Network Settings

This group allows you to obtain an IP address automatically and allows you type in IP address manually.

Obtain an IP address automatically – Click this button to obtain the IP address automatically 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.
Default MAC Address – Click this radio button to use default MAC address for the router.
Specify a MAC Address - Some Cable service providers specify a specific MAC address for access authentication. In such cases you need to click the **Specify a MAC Address** and enter the MAC address in the MAC Address field.
WAN IP 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.



WAN IP Alias (Multi-NAT)

Index	Enable	Aux. WAN IP	Join NAT IP Pool
1.	v	172.16.3.229	v
2.	□	. . .	□
3.	□	. . .	□
4.	□	. . .	□
5.	□	. . .	□
6.	□	. . .	□
7.	□	. . .	□
8.	□	. . .	□

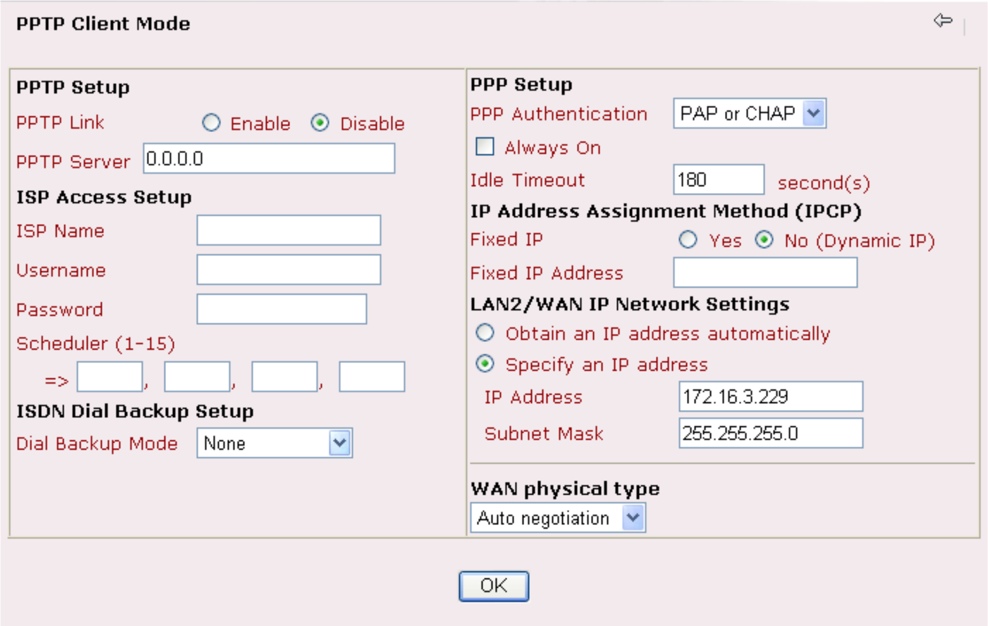
Specify an IP address – Click this radio button to specify some data if you want to use **Static IP** mode.
IP Address – Type the IP address.
Subnet Mask – Type the subnet mask.
Gateway IP Address – Type the gateway IP address.

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.

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

2.6.4 PPTP

To choose **PPTP** as the accessing protocol of the internet, please select **Internet Access Setup** on the **Quick Setup** page. **Next,** choose the **PPTP** link. The following web page will be shown.



PPTP Client Mode

PPTP Setup

PPTP Link ○ Enable ● Disable

PPTP Server 0.0.0.0

ISP Access Setup

ISP Name

Username

Password

Scheduler (1-15)

=> , , ,

ISDN Dial Backup Setup

Dial Backup Mode None

PPP Setup

PPP Authentication PAP or CHAP

□ Always On

Idle Timeout 180 second(s)

IP Address Assignment Method (IPCP)

Fixed IP ○ Yes ● No (Dynamic IP)

Fixed IP Address

LAN2/WAN IP Network Settings

○ Obtain an IP address automatically

● Specify an IP address

IP Address 172.16.3.229

Subnet Mask 255.255.255.0

WAN physical type

Auto negotiation

PPTP Setup

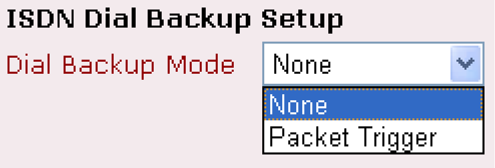
PPTP Link - Click **Enable** to enable a PPTP client to establish a tunnel to a DSL modem on the WAN interface.
PPTP Server - Specify the IP address of the PPTP server.

ISP Access Setup

ISP Name - Type in the ISP Name provided by ISP in this field.
Username -Type in the username provided by ISP in this field.
Password -Type in the password provided by ISP in this field.
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.

ISDN Dial Backup Setup

This setting is available for the routers supporting ISDN function only. Before utilizing the ISDN dial backup feature, you must create a dial backup profile first. Please click **Internet Access Setup** > **Dialing to a Single ISP** to enter the backup profile.



ISDN Dial Backup Setup

Dial Backup Mode None

.

Due to the absence of the ISDN interface in some models (e.g., Vigor2900V and Vigor2900VG), the ISDN dial backup feature and its associated setup options are not available to them. Please refer to the previous part for further information.
None - Disable the backup function.
Packet Trigger -The backup line is not on until a packet from a local host triggers the router to establish a connection.
Always On - If the broadband connection is no longer available, the backup line will be activated automatically and always on until the broadband connection is restored. We recommend you to enable this feature if you host a web server for your customers' access.

PPP Setup

PPP Authentication - Select **PAP only** or **PAP or CHAP** for PPP.
Always On -Check this box if you want the router keeping connecting to Internet forever.

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

IP Address 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.

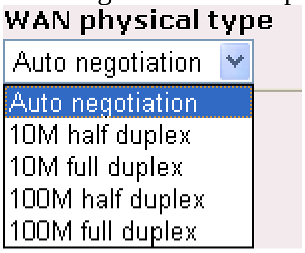
LAN2/WAN IP Network Settings

Obtain an IP address automatically – Click this button to obtain the IP address automatically.

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

WAN physical type

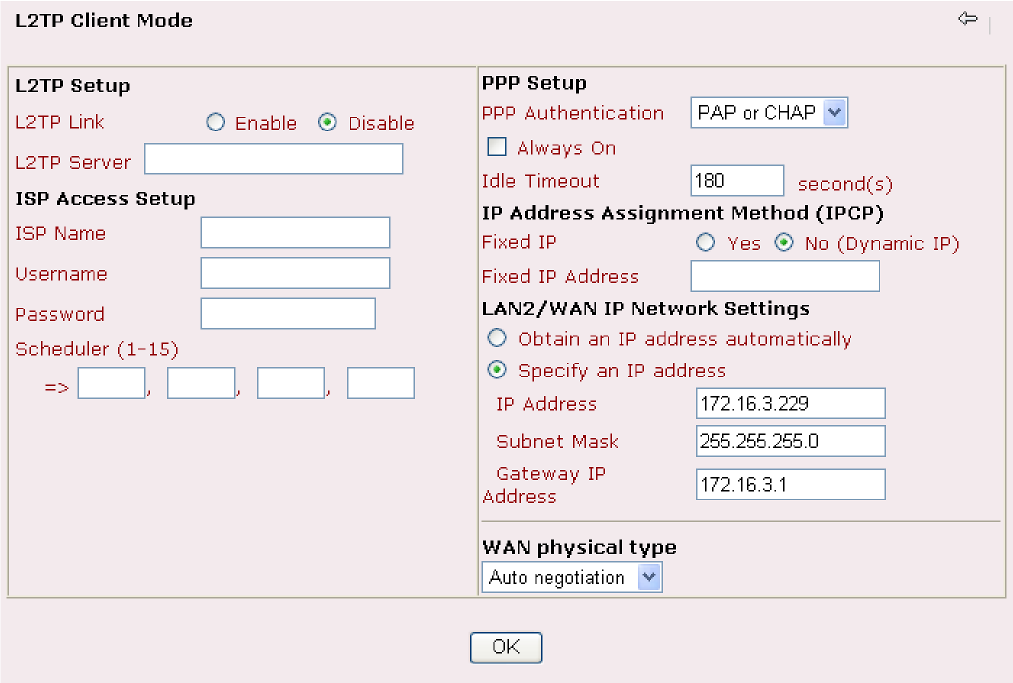
Check and choose a proper type used for duplex between this device and other router that you want to communicate. Both sides should use the same physical type; otherwise, the connection might be failed due to inconsistent type. It is recommended for you to set Auto negotiation as the physical type.



WAN physical type: Auto negotiation

2.6.5 L2TP

To choose **L2TP** as the accessing protocol of the internet, please select **Internet Access Setup** on the **Quick Setup** page. **Next,** choose the **L2TP** link. The following web page will be shown.



L2TP Client Mode

L2TP Setup

L2TP Link ○ Enable ● Disable

L2TP Server

ISP Access Setup

ISP Name

Username

Password

Scheduler (1-15)

=> , , ,

PPP Setup

PPP Authentication: PAP or CHAP

□ Always On

Idle Timeout: 180 second(s)

IP Address Assignment Method (IPCP)

Fixed IP ○ Yes ● No (Dynamic IP)

Fixed IP Address

LAN2/WAN IP Network Settings

○ Obtain an IP address automatically

● Specify an IP address

IP Address: 172.16.3.229

Subnet Mask: 255.255.255.0

Gateway IP Address: 172.16.3.1

WAN physical type: Auto negotiation

L2TP Setup

L2TP Link - Click **Enable** to enable a L2TP client to establish a tunnel to a DSL modem on the WAN interface.
L2TP Server - Specify the IP address of the L2TP server.

ISP Access Setup

ISP Name - Type in the ISP Name provided by ISP in this field.
Username -Type in the username provided by ISP in this field.
Password -Type in the password provided by ISP in this field.
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.
Always On -Check this box if you want the router keeping connecting to Internet forever.
Idle Timeout - Set the timeout for breaking down the Internet after passing through the time without any action.

IP Address 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.

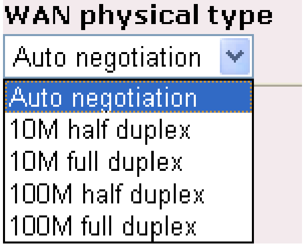
LAN2/WAN IP Network Settings

Obtain an IP address automatically – Click this button to obtain the IP address automatically.

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

WAN physical type

Check and choose a proper type used for duplex between this device and other router that you want to communicate. Both sides should use the same physical type; otherwise, the connection might be failed due to inconsistent type. It is recommended for you to set Auto negotiation as the physical type.



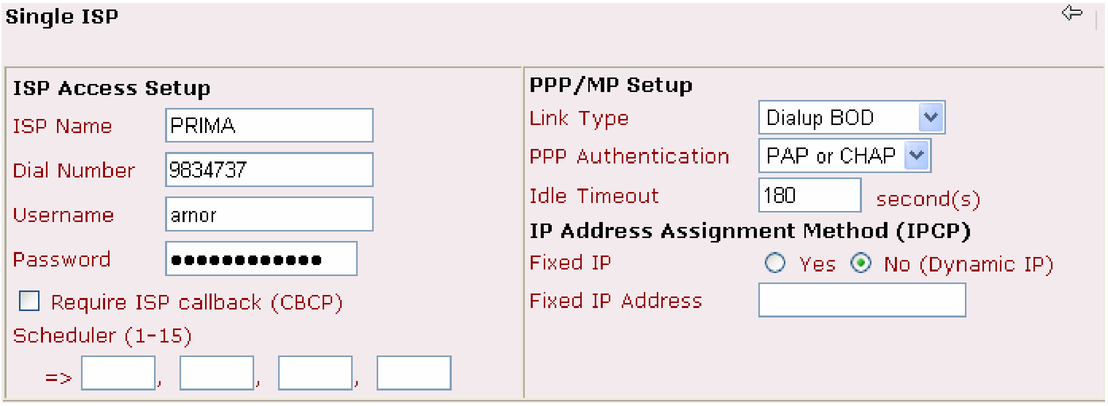
WAN physical type

Auto negotiation

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

2.6.6 Dialing to a Single ISP

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



Single ISP

ISP Access Setup

ISP Name	PRIMA
Dial Number	9834737
Username	arnor
Password	●●●●●●●●●●●●

□ Require ISP callback (CBCP)

Scheduler (1-15)

=> , , ,

PPP/MP Setup

Link Type	Dialup BOD
PPP Authentication	PAP or CHAP
Idle Timeout	180 second(s)

IP Address Assignment Method (IPCP)

Fixed IP	○ Yes ● No (Dynamic IP)
Fixed IP Address	

ISP Name Enter your ISP name.

Dial Number Enter the ISDN access number provided by your ISP.

Username Enter the username provided by your ISP.

Password Enter the password provided by your ISP.

Require ISP Callback (CBCP) If your ISP supports the callback function, check this box to activate the Callback Control Protocol during the PPP negotiation.

Scheduler (1-15) Enter the index of schedule profiles to control the Internet access according to the preconfigured schedules.

Link Type There are four link types: Link Disable, Dialup 64 Kbps, Dialup 128 Kbps, and Dialup BOD.
Link Disable - Disable the ISDN dial-out function.
Dialup 64Kbps - Use one ISDN B channel for Internet access.
Dialup 128Kbps - Use both ISDN B channels for Internet access.
Dialup BOD - BOD stands for bandwidth-on-demand. The router will use only one B channel in low traffic situations. Once the single B channel bandwidth is fully used, the other B channel will be activated automatically through the dialup. For more detailed BOD parameter settings, please refer to the **Advanced Setup** field > **Call Control and PPP/MP Setup**.

PPP Authentication **PAP Only -** Configure the PPP session to use the PAP protocol to negotiate the username and password with the ISP.
PAP or CHAP - Configure the PPP session to use the PAP or CHAP protocols to negotiate the username and password with the ISP.

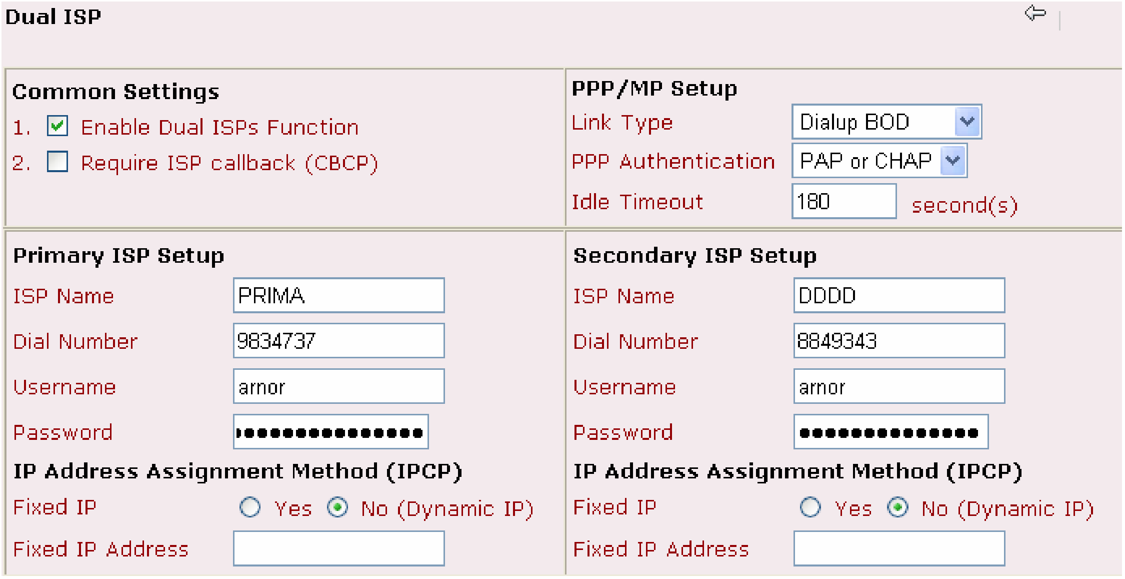
Idle Timeout Idle timeout means the router will be disconnect after being idle for a preset amount of time. The default is 180 seconds. If you set the time to 0, the ISDN connection to the ISP will always remain on.

Fixed IP In most environments, you should not change these settings as most ISPs provide a dynamic IP address for the router when it connects to the ISP. If your ISP provides a fixed IP address, check **Yes t**o invoke this function and enter the IP address in the field of **Fixed IP Address**.

Fixed IP Address Type the IP address.

2.6.7 Dialing to a Dual ISPs

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



Dual ISP

Common Settings

1. ☑ Enable Dual ISPs Function
2. □ Require ISP callback (CBCP)

PPP/MP Setup

Link Type	Dialup BOD
PPP Authentication	PAP or CHAP
Idle Timeout	180 second(s)

Primary ISP Setup

ISP Name	PRIMA
Dial Number	9834737
Username	arnor
Password	•••••••••••••••

IP Address Assignment Method (IPCP)

Fixed IP	○ Yes ● No (Dynamic IP)
Fixed IP Address	

Secondary ISP Setup

ISP Name	DDDD
Dial Number	8849343
Username	arnor
Password	•••••••••••••••

IP Address Assignment Method (IPCP)

Fixed IP	○ Yes ● No (Dynamic IP)
Fixed IP Address	

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

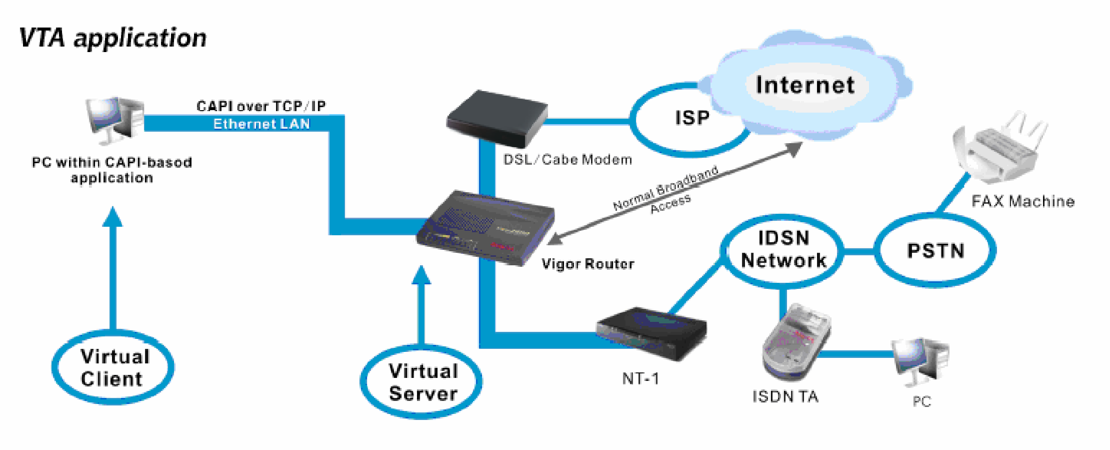
2.7 Virtual TA (Remote CAPI) Setup

Note: This setting is available for *i* models only.

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

- The Virtual TA client only supports Microsoft™ Windows 95 OSR2.1/98/98SE/Me/2000 platforms.

- The Virtual TA client only supports the CAPI 2.0 protocol and has no built-in FAX engine.
- One ISDN BRI interface has two B channels. The maximum number of active clients is also two.
- Before you configure the Virtual TA, you must set the correct country code.

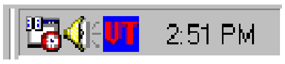


As depicted in the above application scenario, the Virtual TA client can make an outgoing call or accept an incoming call to/from a peer FAX machine or ISDN TA, etc.

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

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

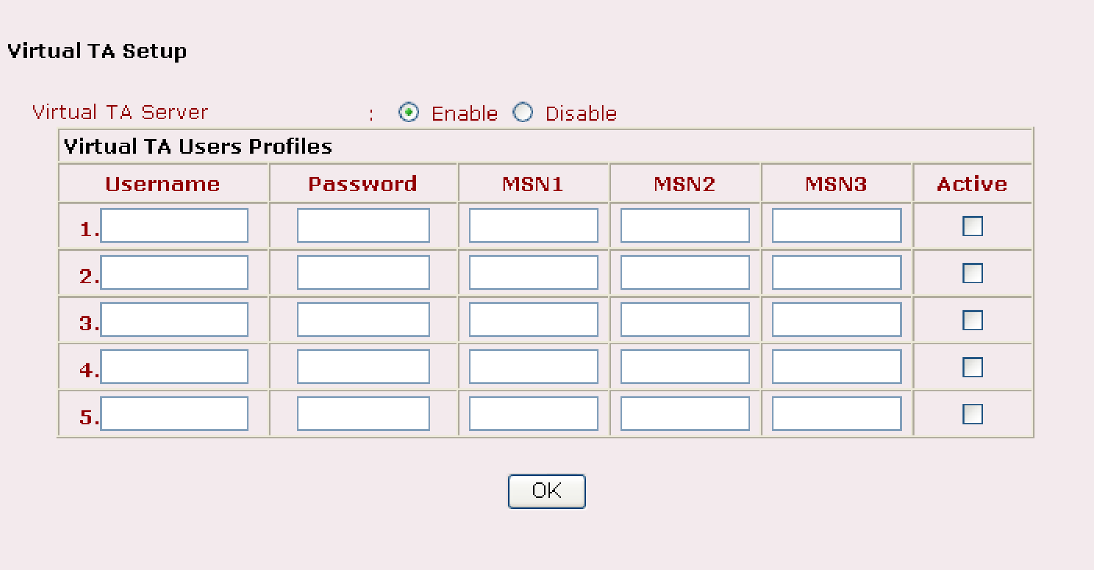
When the icon text is GREEN, the Virtual TA client is connected to the Virtual TA server and you can launch your CAPI-based software to use the client to access the router. Please read your software user guide for detailed configuration. If the icon text is RED, it means the client has lost the connection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



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

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

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



Virtual TA Setup

Virtual TA Server : ● Enable ○ Disable

Virtual TA Users Profiles

Username	Password	MSN1	MSN2	MSN3	Active
1.					□
2.					□
3.					□
4.					□
5.					□

Virtual TA Server **Enable:** Select it to activate the server.
Disable: Select it to deactivate the server. All Virtual TA applications will be terminated.

Username Enter the username of a specific client.

Password Enter the password of a specific client.

MSN1/ MSN2/MSN3 MSN stands for **Multiple Subscriber Number**. It means you can apply to more than one ISDN lines number over a single subscribed line. Note that the service must be acquired from your telecom. Specify the MSN numbers for a specific client. If you have no MSN services, leave this field blank.

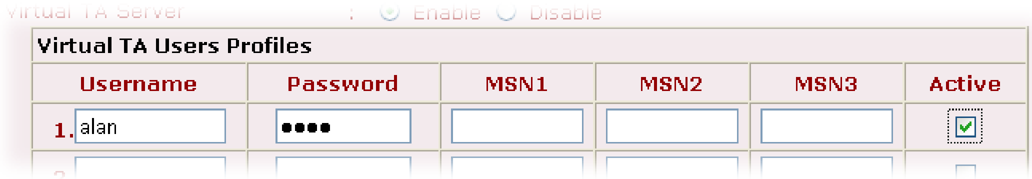
Active Check it to enable the client to access the server.

User Profile

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

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

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

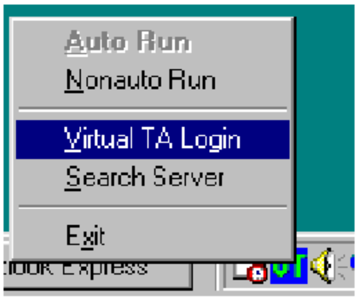


Virtual TA Server : ○ Enable ○ Disable

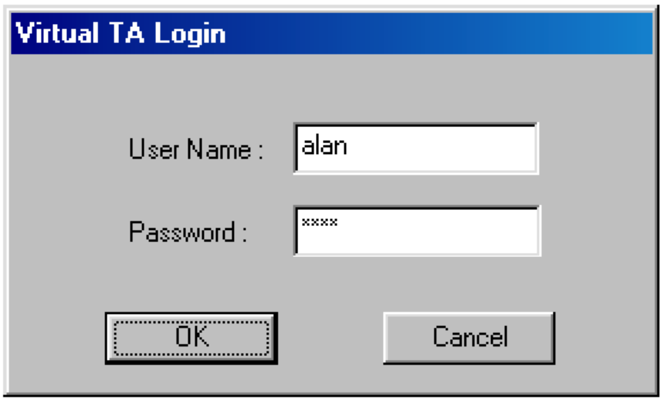
Virtual TA Users Profiles

Username	Password	MSN1	MSN2	MSN3	Active
1. alan	●●●●				☑

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



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



Virtual TA Login

User Name : alan

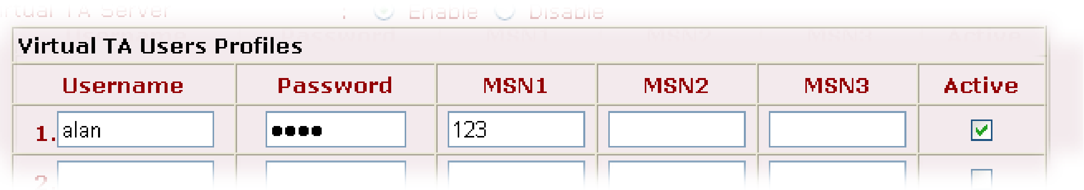
Password : ****

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

MSN Configuration

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

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



Virtual TA Users Profiles

	Username	Password	MSN1	MSN2	MSN3	Active
1.	alan	●●●●	123			☑

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

3 Advanced Web Configuration

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

3.1 Dynamic DNS Setup

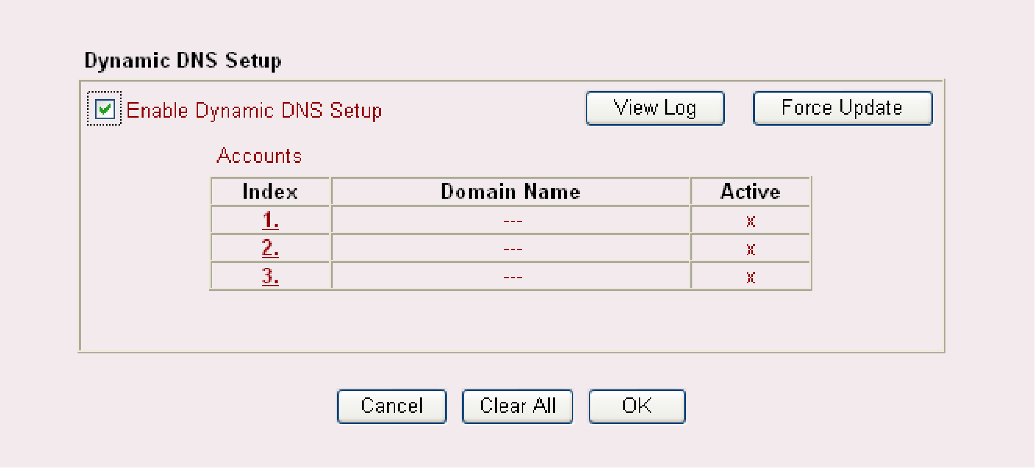
The ISP often provides you with a dynamic IP address when you connect to the Internet via your ISP. It means that the public IP address assigned to your router changes each time you access the Internet. The Dynamic DNS feature lets you assign a domain name to a dynamic WAN IP address. It allows the router 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 (e.g., hostname.dyndns.org), and an account with username: *test* and password: *test*.

2. Select **Dynamic DNS Setup** from the **Advanced Setup** group. The following page will appear.



Dynamic DNS Setup

☑ Enable Dynamic DNS Setup

Accounts

Index	Domain Name	Active
1.	---	x
2.	---	x
3.	---	x

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

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

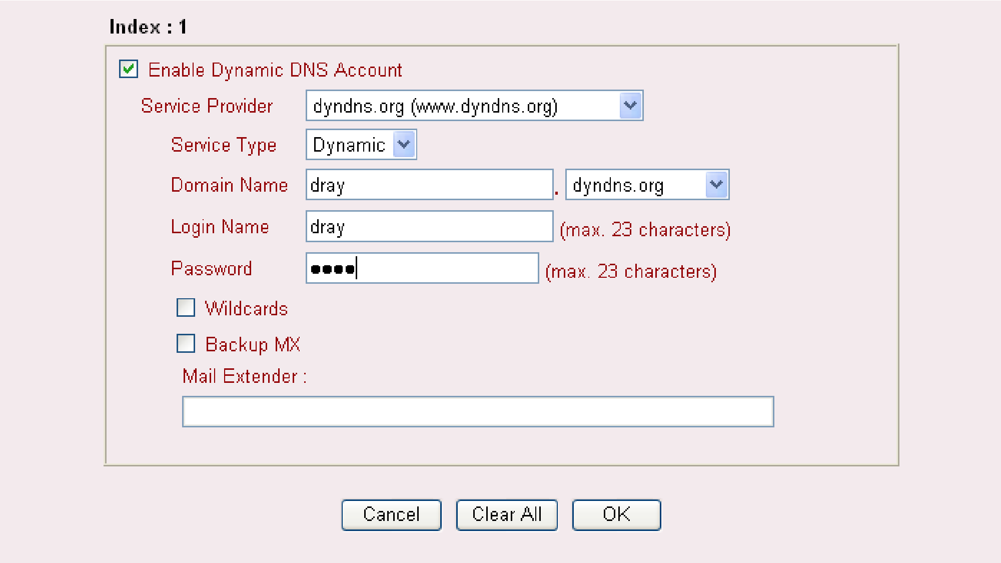
Domain Name Display the domain name that you set on the setting page of DDNS setup.

Active Display if this account is active or inactive.

View Log It opens another dialog and shows log for DDNS information.

Force Update Click this button to get the newest DDNS information.

3. Select Index number 1 to add an account for the router. Check Enable Dynamic DNS Account, and choose correct Service Provider: dyndns.org, type the registered hostname: *hostname* and domain name suffix: dyndns.org in the Domain Name block. The following two blocks should be typed your account Login Name: *test* and Password: *test*.



Index : 1

☑ Enable Dynamic DNS Account

Service Provider	dyndns.org (www.dyndns.org)
Service Type	Dynamic
Domain Name	dray . dyndns.org
Login Name	dray (max. 23 characters)
Password	•••• (max. 23 characters)

□ Wildcards

□ Backup MX

Mail Extender :

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

Service Provider Select the service provider for the DDNS account.

Service Type Select a service type (Dynamic, Custom, Static).

Domain Name Type in a domain name that you applied previously.

Login Name Type in the login name that you set for applying domain.

Password Type in the password that you set for applying domain.

Mail Extender Some DDNS Server might ask to provide additional information, e.g., e-mail address. Type in necessary e-mail address in this field in accordance with the DDNS server.

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

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

Disable the Function and Clear all Dynamic DNS Accounts

Uncheck **Enable Dynamic DNS Setup**, and press **Clear All** button to disable the function and clear all accounts from the router.

Delete a Dynamic DNS Account

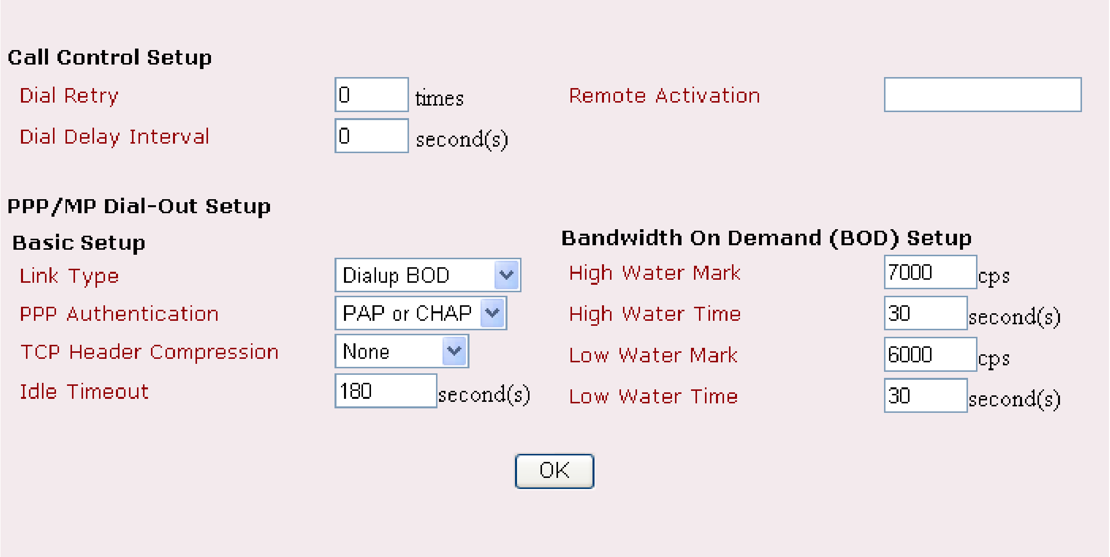
On the **Dynamic DNS Setup** page, click the **Index** number you want to delete and then press **Clear All** button to delete the account.

3.2 Call Control and PPP/MP Setup

Some applications require that the router (only for the *i* models) be remotely activated, or be able to dial up to the ISP via the ISDN interface. Vigor routers provide this feature which allows you to make a phone call to the router and then ask it to dial up to the ISP. Accordingly, you can access your remote network to retrieve resources. Of course, you should have a fixed IP address and expose some internal network resources to the outside world, such as FTP, WWW and so on.

Note: Call Control and PPP/MP are only available for the models of Vigor2900VGi and Vigor2900Vi equipped with the ISDN interface.

Click **Call Control and PPP/MP Setup** from **Advanced Setup** group.



Call Control Setup

Dial Retry: 0 times

Dial Delay Interval: 0 second(s)

Remote Activation:

PPP/MP Dial-Out Setup

Basic Setup

Link Type: Dialup BOD

PPP Authentication: PAP or CHAP

TCP Header Compression: None

Idle Timeout: 180 second(s)

Bandwidth On Demand (BOD) Setup

High Water Mark: 7000 cps

High Water Time: 30 second(s)

Low Water Mark: 6000 cps

Low Water Time: 30 second(s)

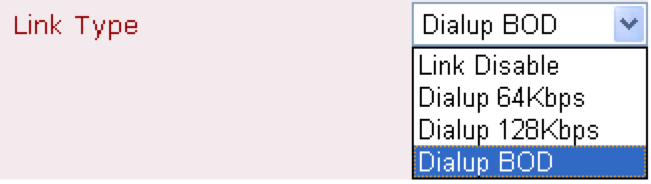
Note: Please set **Dialing to a Single ISP** first before configuring this web page.

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

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

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

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



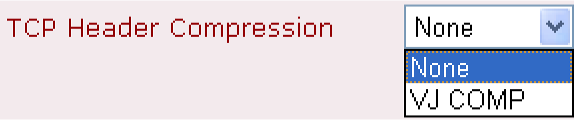
Link Type: Dialup BOD

PPP Authentication

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

TCP Header Compression

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



TCP Header Compression: None

Idle Timeout

Because our IDSN link type is "Dial On Demand", the connection will be initiated only when needed.

High Water Mark and High Water Time

BOD stands for bandwidth-on-demand for Multiple-Link PPP (ML-PPP or MP). **High Water Mark/ High Water Time/ Low Water Mark/Low Water Time** parameters are applied when you set the **Link Type** to **Dialup BOD**. The ISDN usually uses one B channel to access the Internet or remote network when you choose the Dialup BOD link type. The router will use the parameters here to decide on when you activate/drop the additional B channel. Note that **cps** (characters-per-second) measures the total link utilization.

These parameters specify the situation in which the second channel will be activated. With the first connected channel, if its utilization exceeds the High Water Mark and such a channel is being used over the High Water Time, the additional channel will be activated. Thus, the total link speed will be 128kbps (two B channels).

Low Water Mark and Low Water Time

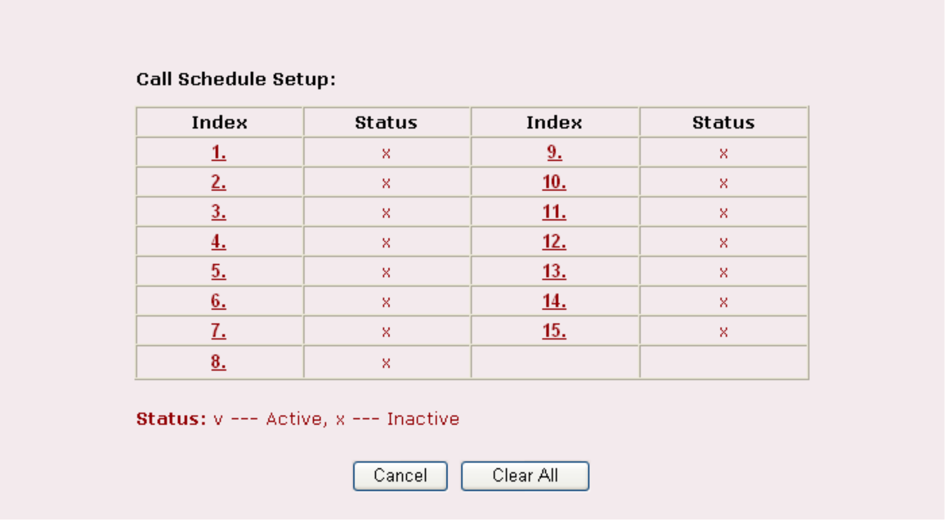
These parameters specify the situation in which the second channel will be dropped. In terms of the two B channels, if their utilization is under the Low Water Mark and these two channels are being used over the High Water Time, the additional channel will be dropped. As a result, the total link speed will be 64kbps (one B channel).

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

3.3 Call Schedule Setup

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 the **System Management** group, select **Time and Date** to open the time setup page, 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.



Call Schedule Setup:

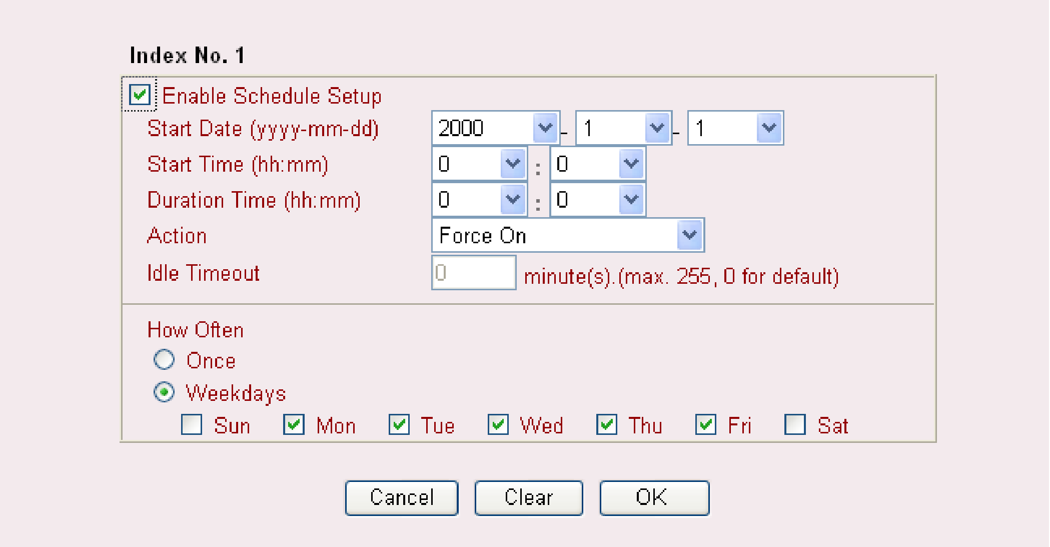
Index	Status	Index	Status
1.	x	9.	x
2.	x	10.	x
3.	x	11.	x
4.	x	12.	x
5.	x	13.	x
6.	x	14.	x
7.	x	15.	x
8.	x		

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

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.



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.

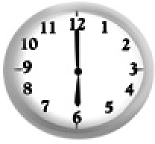
How often Specify how often the schedule will be applied.
Once -The schedule will be applied just once
Weekdays -Specify which days in one week should perform the schedule.

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 **Call Schedule 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.

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

3.4 NAT Setup

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.

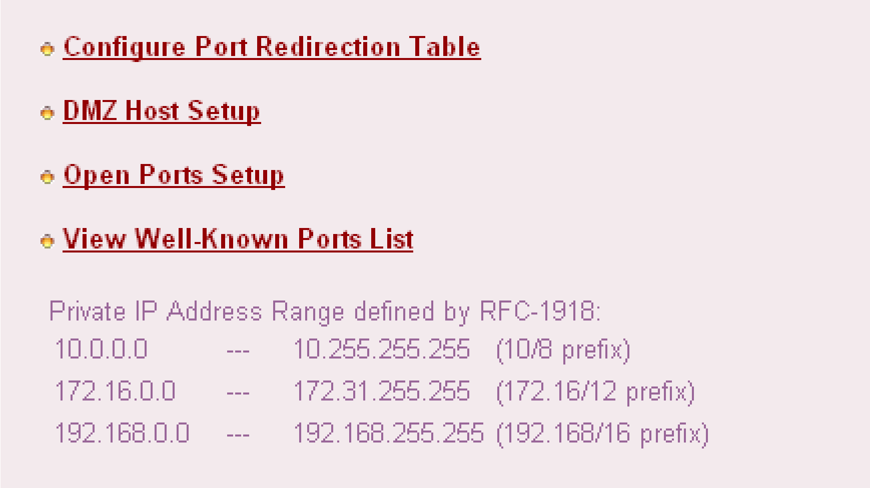
When the outgoing packets destined to some public server on the Internet reach the NAT router, the router will change its source address into the public IP address of the router, select the available public port, and then forward it. At the same time, the router shall list an entry in a table to memorize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

Click **NAT Setup** on the **Advanced Setup** page. The setting items for NAT will be shown as below.



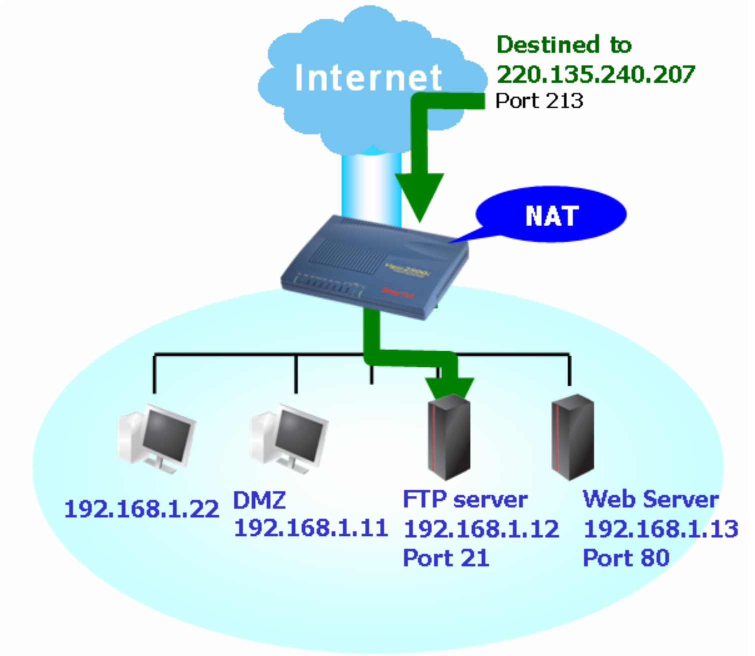
- Configure Port Redirection Table
- DMZ Host Setup
- Open Ports Setup
- View Well-Known Ports List

Private IP Address Range defined by RFC-1918:

10.0.0.0	---	10.255.255.255	(10/8 prefix)
172.16.0.0	---	172.31.255.255	(172.16/12 prefix)
192.168.0.0	---	192.168.255.255	(192.168/16 prefix)

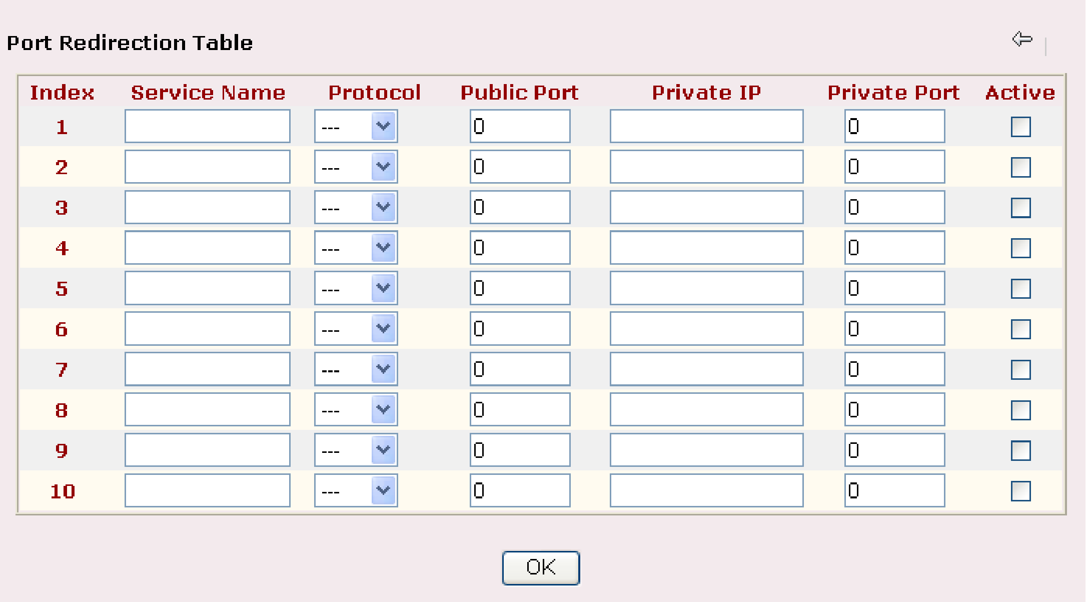
3.4.1 Configure Port Redirection Table

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



The port redirection can only apply to incoming traffic.

To use this function, please go to **NAT** page and choose **Port Redirection** web page. The **Port Redirection Table** provides 10 port-mapping entries for the internal hosts.



Port Redirection Table

Index	Service Name	Protocol	Public Port	Private IP	Private Port	Active
1		---	0		0	□
2		---	0		0	□
3		---	0		0	□
4		---	0		0	□
5		---	0		0	□
6		---	0		0	□
7		---	0		0	□
8		---	0		0	□
9		---	0		0	□
10		---	0		0	□

Service Name Enter the description of the specific network service.

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

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

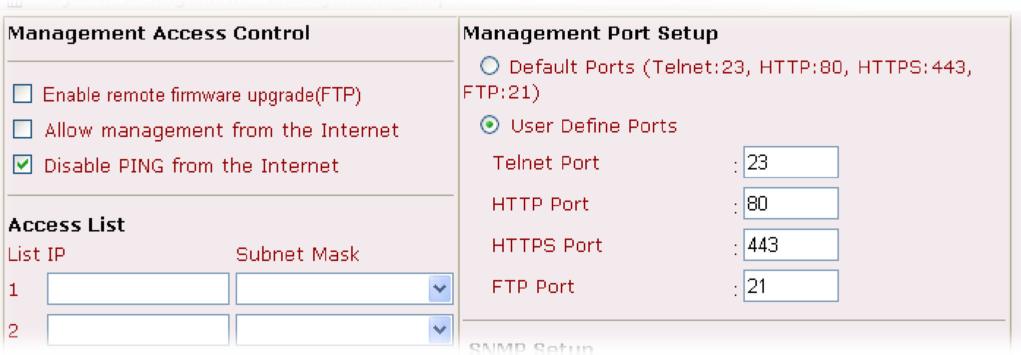
Private IP Specify the private IP address of the internal host providing the service.

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

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

Note that the router has its own built-in services (servers) such as Telnet, HTTP and FTP etc. Since the common port numbers of these services (servers) are all the same, you may need to reset the router 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 by the **Management Setup** in the **System Management** group. You then will access the admin screen of by suffixing the IP address with 8080, e.g., http://192.168.1.1:8080 instead of port 80.



Management Access Control

□ Enable remote firmware upgrade(FTP)

□ Allow management from the Internet

☑ Disable PING from the Internet

Access List

List IP		Subnet Mask
1		
2		

Management Port Setup

○ Default Ports (Telnet:23, HTTP:80, HTTPS:443, FTP:21)

● User Define Ports

Telnet Port : 23

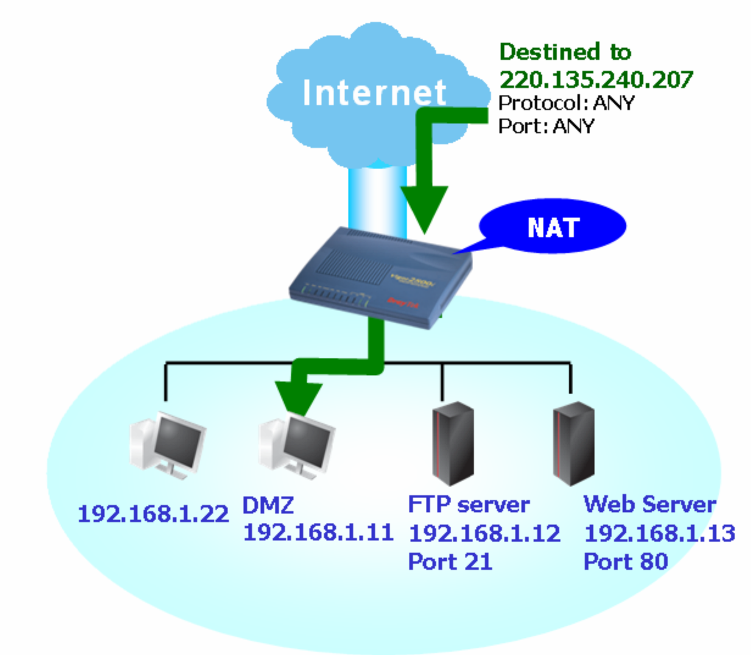
HTTP Port : 80

HTTPS Port : 443

FTP Port : 21

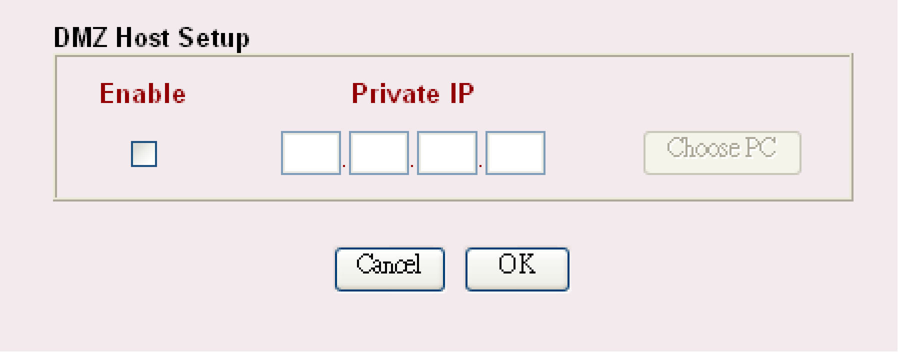
3.4.2 DMZ Host Setup

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.



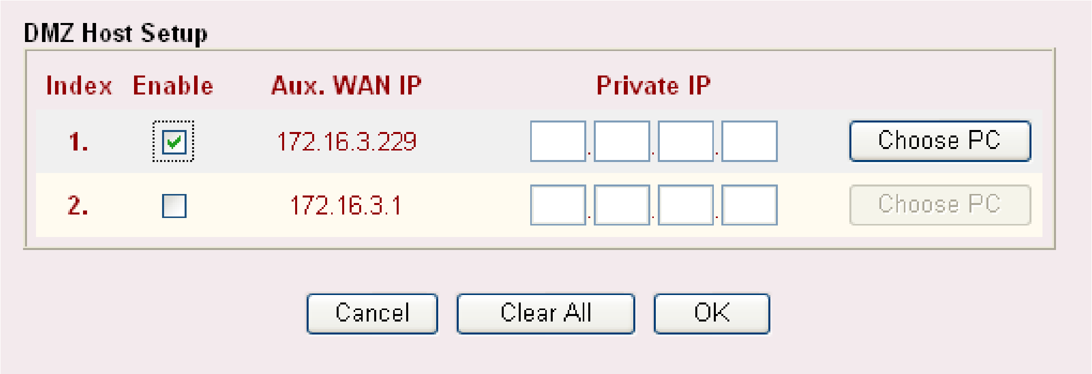
The inherent security properties of NAT are somewhat bypassed if you set up DMZ host. We suggest you to add additional filter rules or a secondary firewall.

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


DMZ Host Setup

Enable	Private IP	
□	___ . ___ . ___ . ___	Choose PC

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



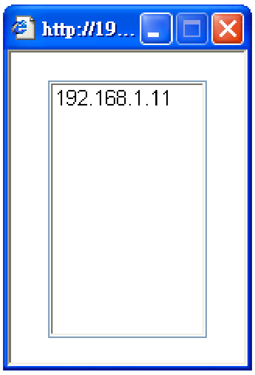
DMZ Host Setup

Index	Enable	Aux. WAN IP	Private IP	
1.	☑	172.16.3.229	. . .	Choose PC
2.	□	172.16.3.1	. . .	Choose PC

Enable Check to enable the DMZ Host function.

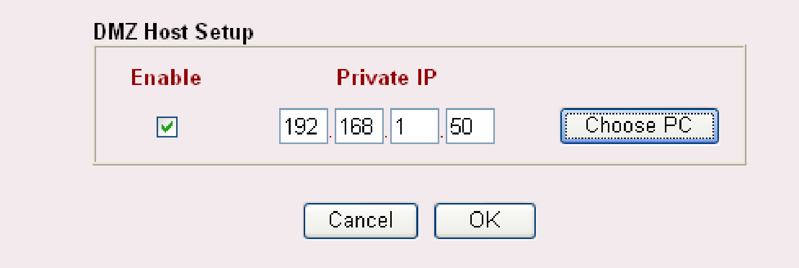
Private IP Enter the private IP address of the DMZ host, or click Choose PC to select one.

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.



192.168.1.11

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.



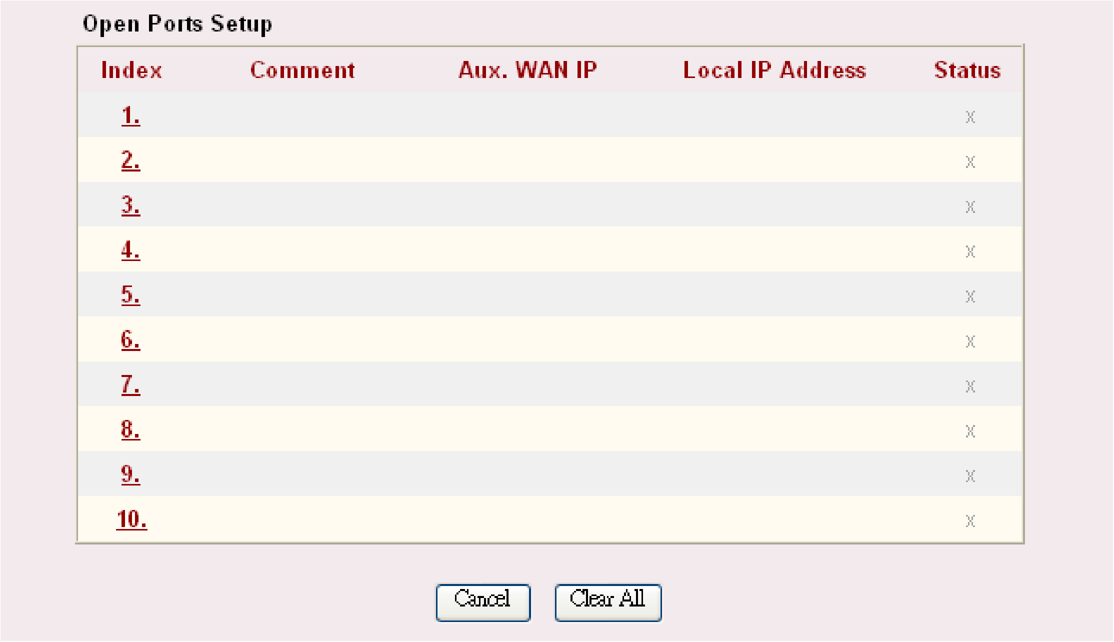
DMZ Host Setup

Enable	Private IP	
☑	192 . 168 . 1 . 50	Choose PC

3.4.3 Open Ports Setup

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:



Open Ports Setup

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

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

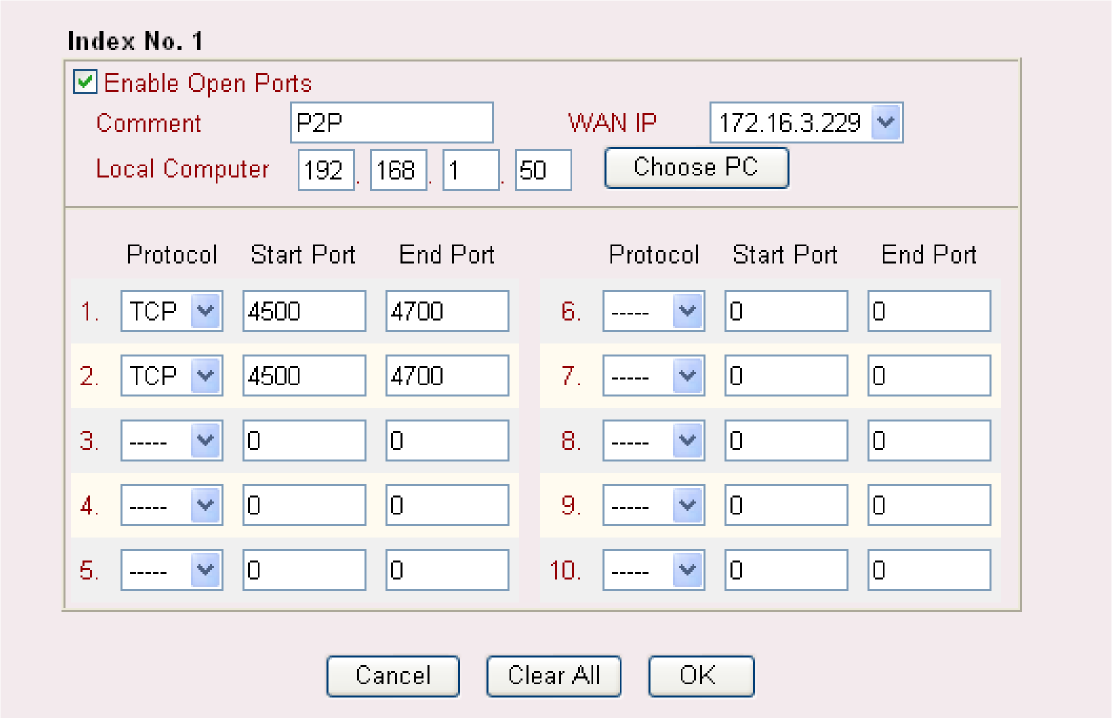
Comment Specify the name for the defined network service.

Aux. WAN IP Display the private IP address of the local host that you specify in WAN Alias. If you did not specify any IP address in WAN Alias, this item will not be shown.

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

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

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



Index No. 1

☑ Enable Open Ports

Comment: P2P

WAN IP: 172.16.3.229

Local Computer: 192 . 168 . 1 . 50

	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

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

Enable Open Ports Check to enable this entry.

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

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

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

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

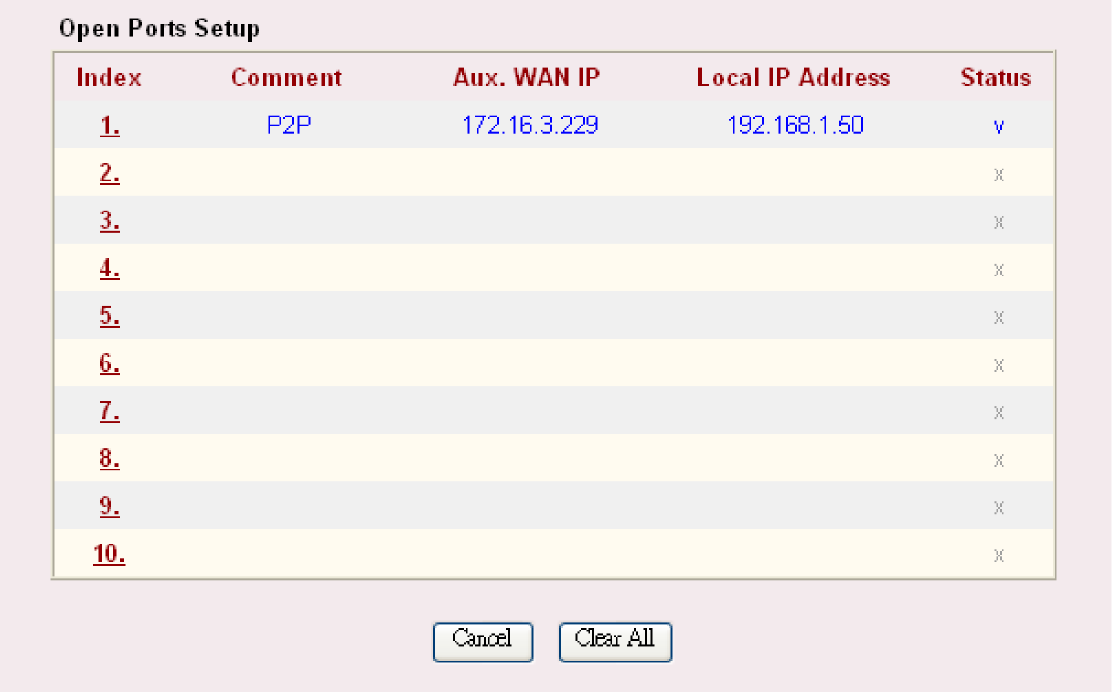
Start Port Specify the starting port number of the service offered by the local host.

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

Cancel Exit this page without saving any change.

Clear All Remove all the settings in this page.

OK Save all the settings and exit this page.

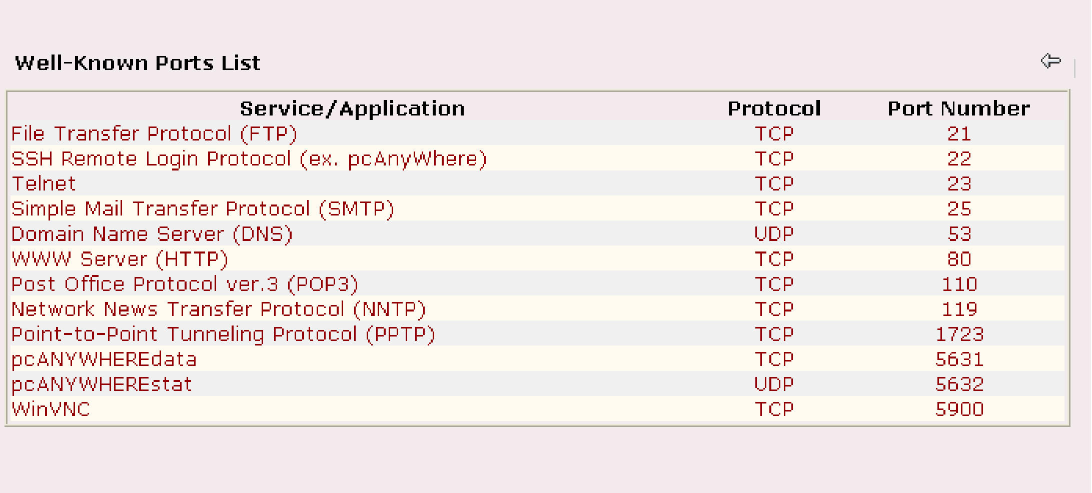


Open Ports Setup

Index	Comment	Aux. WAN IP	Local IP Address	Status
1.	P2P	172.16.3.229	192.168.1.50	v
2.				x
3.				x
4.				x
5.				x
6.				x
7.				x
8.				x
9.				x
10.				x

3.4.4 View Well-Known Ports List

There is a list providing some well-known port numbers of certain services/applications for your reference.

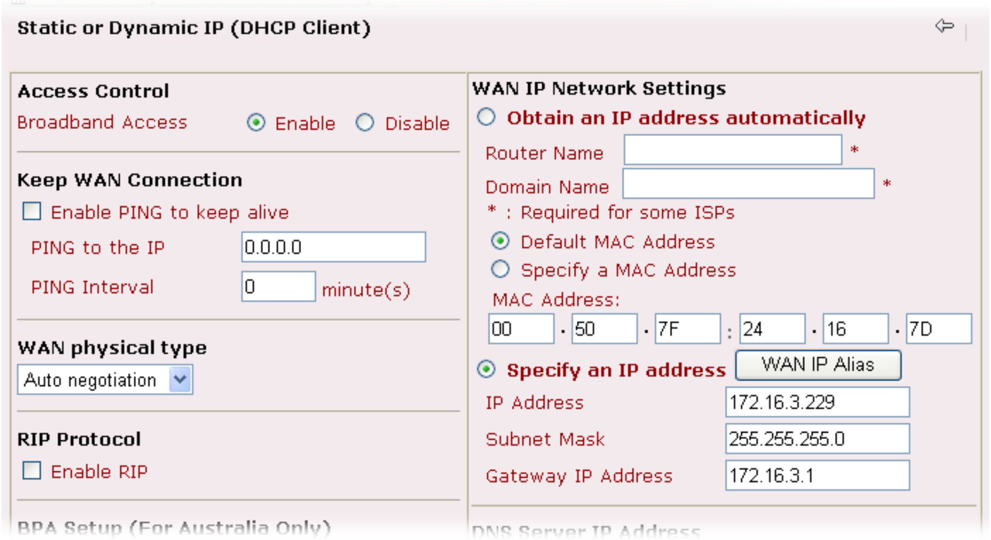


Well-Known Ports List

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

3.4.5 Multi-NAT Setup

If you have a group of static public IP addresses obtained from your ISP, you can use the Multi-NAT feature to set up multiple DMZ hosts or multiple hosts with open ports on your Vigor router. Click **Internet Access Setup** on the **Quick Setup** group of the main page. Next, click **Static or Dynamic IP**. The following screen will appear.



Static or Dynamic IP (DHCP Client)

Access Control

Broadband Access ● Enable ○ Disable

Keep WAN Connection

□ Enable PING to keep alive

PING to the IP 0.0.0.0

PING Interval 0 minute(s)

WAN physical type

Auto negotiation

RIP Protocol

□ Enable RIP

BPA Setup (For Australia Only)

WAN IP Network Settings

○ Obtain an IP address automatically

Router Name *

Domain Name *

* : Required for some ISPs

● Default MAC Address

○ Specify a MAC Address

MAC Address: 00 . 50 . 7F : 24 . 16 . 7D

● Specify an IP address

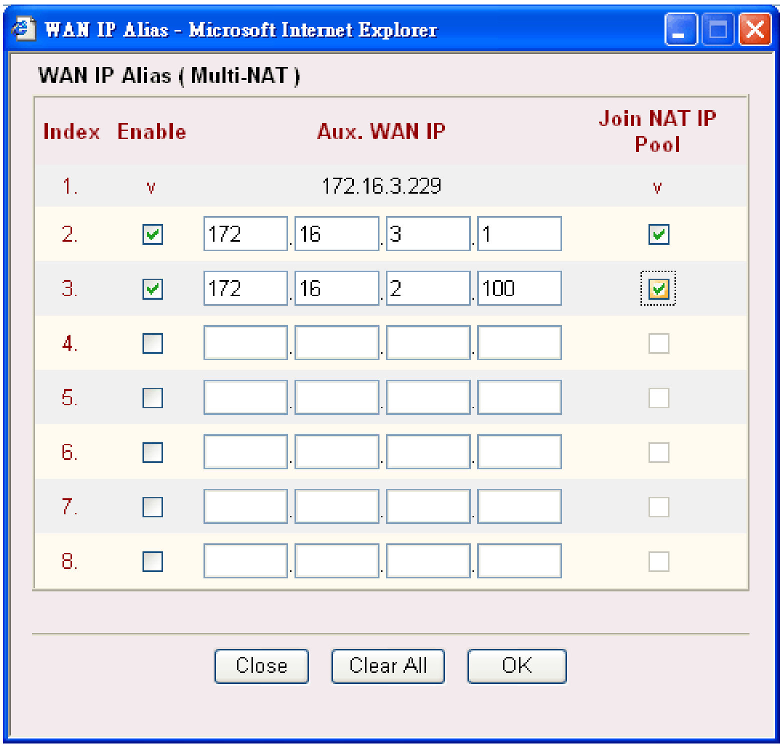
IP Address 172.16.3.229

Subnet Mask 255.255.255.0

Gateway IP Address 172.16.3.1

DNS Server IP Address

When you press the **WAN IP Alias** button, a window will show up for you to input other public IP addresses. The **Join NAT IP Pool** check box indicates that the local users can use this IP to connect to the Internet. If you do not chick this check box, this IP address will not be available to the local users.

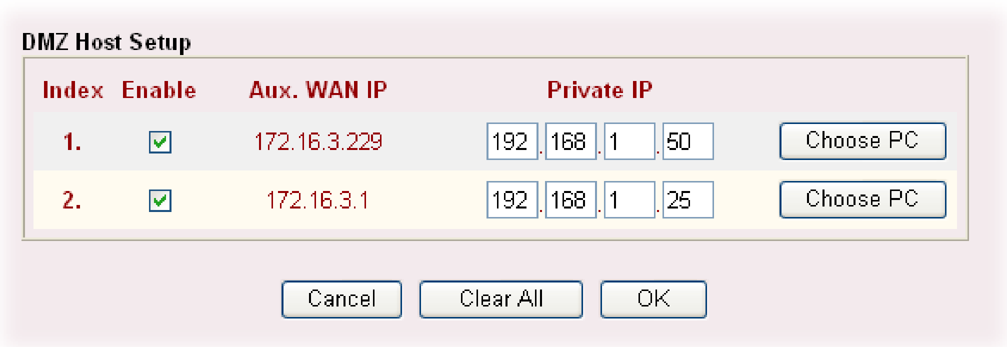


WAN IP Alias - Microsoft Internet Explorer

WAN IP Alias (Multi-NAT)

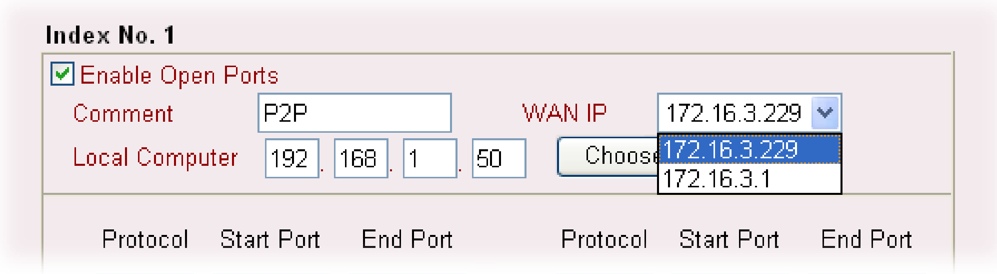
Index	Enable	Aux. WAN IP	Join NAT IP Pool
1.	v	172.16.3.229	v
2.	☑	172 . 16 . 3 . 1	☑
3.	☑	172 . 16 . 2 . 100	☑
4.	□	. . .	□
5.	□	. . .	□
6.	□	. . .	□
7.	□	. . .	□
8.	□	. . .	□

After you configure the **WAN IP Alias** feature, these addresses can be selected on **DMZ Hosts** or **Open Ports** pages.



DMZ Host Setup

Index	Enable	Aux. WAN IP	Private IP
1.	☑	172.16.3.229	192 . 168 . 1 . 50
2.	☑	172.16.3.1	192 . 168 . 1 . 25



Index No. 1

☑ Enable Open Ports

Comment: P2P

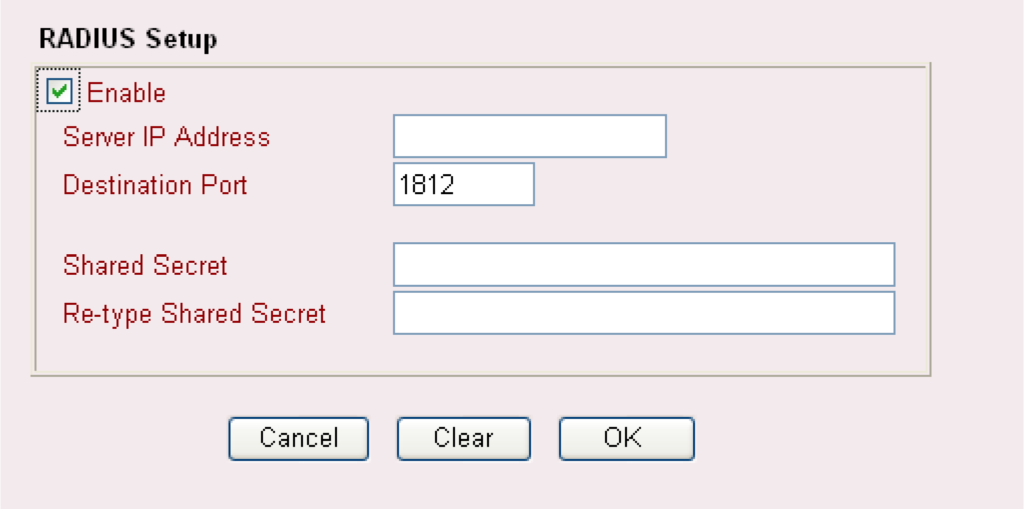
WAN IP: 172.16.3.229

Local Computer: 192 . 168 . 1 . 50

3.5 RADIUS Setup

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.



RADIUS Setup

☑ Enable

Server IP Address:

Destination Port: 1812

Shared Secret:

Re-type Shared Secret:

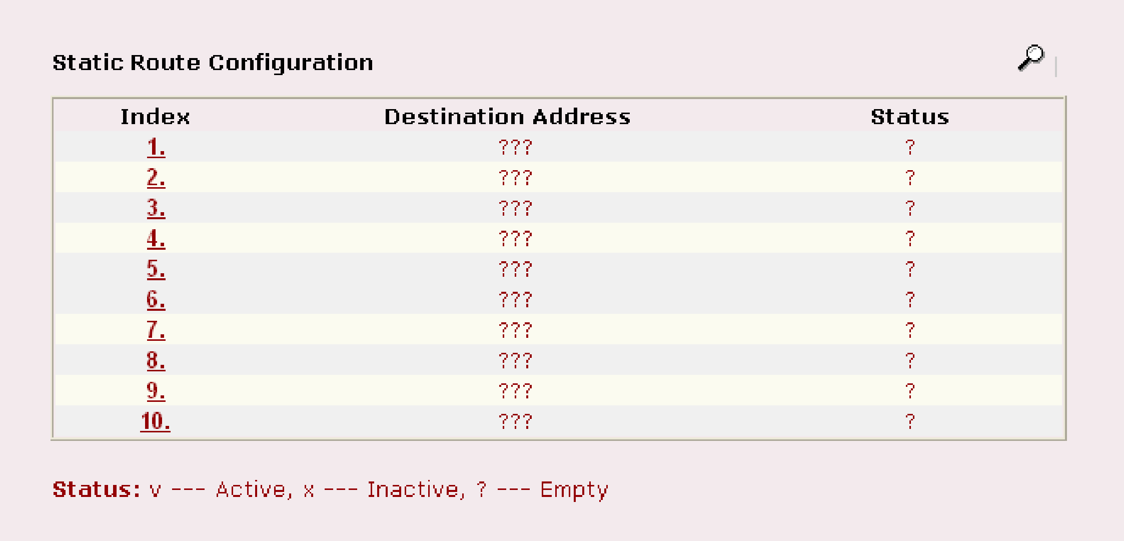
Enable	Check to enable RADIUS client feature
Server IP Address	Enter the IP address of RADIUS server
Destination Port	The UDP port number that the RADIUS server is using. The default value is 1812 , based on RFC 2138.

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.

Re-type Shared Secret Re-type the Shared Secret for confirmation.

3.6 Static Route Setup

Choose **Static Route Setup** on the **Advanced Setup** group.



Static Route Configuration

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

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

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

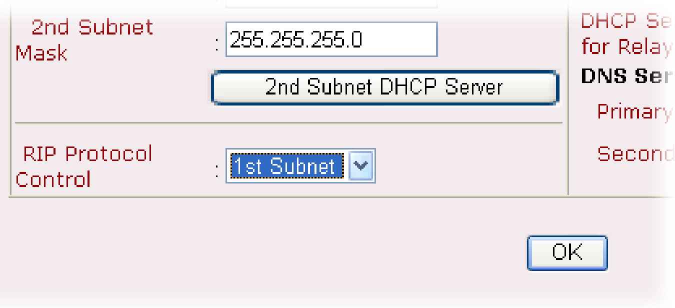
Destination Address Displays the destination address of the static route.

Status Displays the status of the static route.

Add Static Routers to Private and Public Networks

Assuming the Internet access has been configured and the router works properly, you use the 1st subnet address 192.168.1.0/24 to surf the Internet and also an internal private subnet 192.168.10.0/24 via an internal router (192.168.1.2/24), an internal public subnet 211.100.88.0/28 via an internal router (192.168.1.3/24). Also, the router 192.168.1.1/24 is a default gateway for the router 192.168.1.2/24.

1. On the **Basic Setup** group, click **LAN TCP/IP and DHCP Setup.** Select 1st Subnet as the **RIP Protocol Control.** Then click the **OK** button.

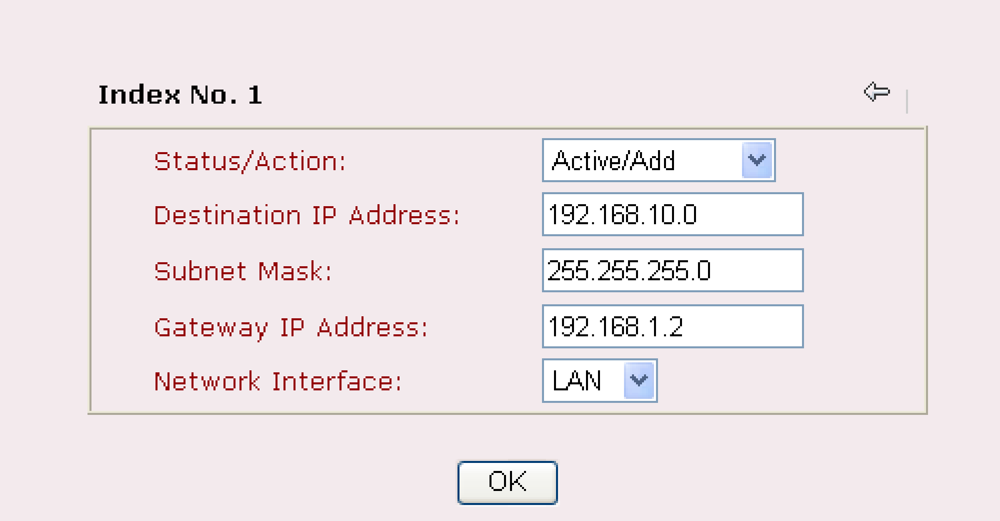


2nd Subnet Mask : 255.255.255.0

RIP Protocol Control : 1st Subnet

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.

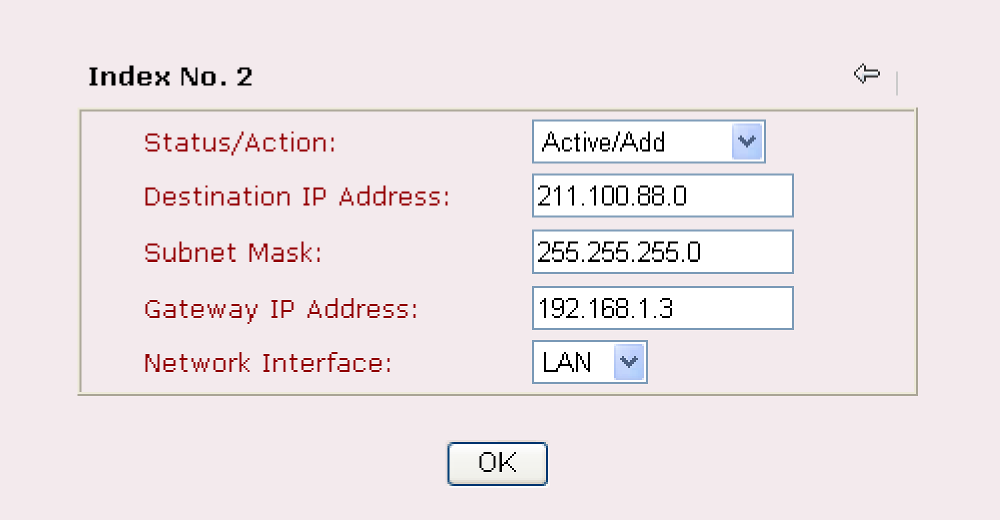
2. Click **Index Number 1** from the **Static Route Configuration** page. Please add a static route as shown below, which regulates all packets destined to 192.168.10.0 will be forwarded to 192.168.1.2. Click **OK**.



Index No. 1

Status/Action:	Active/Add
Destination IP Address:	192.168.10.0
Subnet Mask:	255.255.255.0
Gateway IP Address:	192.168.1.2
Network Interface:	LAN

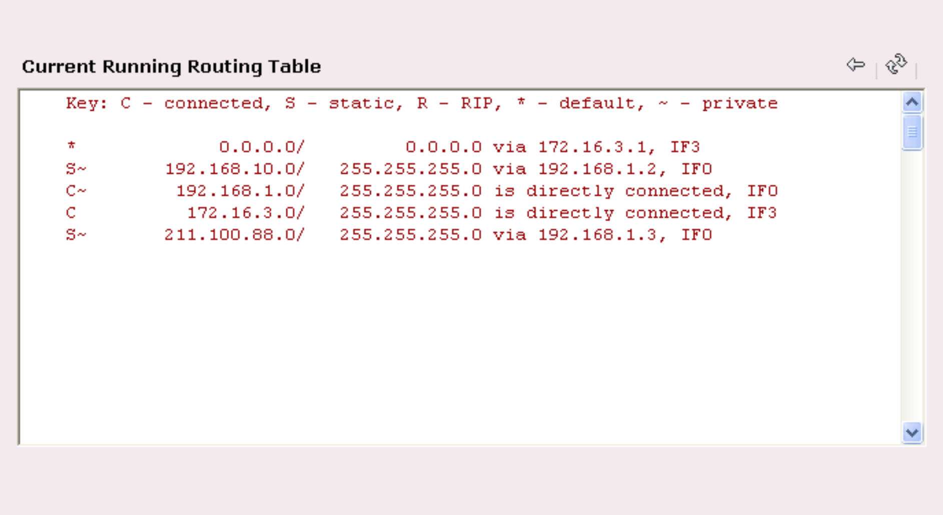
3. Return to **Static Route Setup** page. Click on another **Index Number** to add another static route as show below, which regulates all packets destined to 211.100.88.0 will be forwarded to 192.168.1.2.



Index No. 2

Status/Action:	Active/Add
Destination IP Address:	211.100.88.0
Subnet Mask:	255.255.255.0
Gateway IP Address:	192.168.1.3
Network Interface:	LAN

4. Click **Diagnostics Tools** on the **System Management** group, then choose **View Routing Table** to verify current routing table.

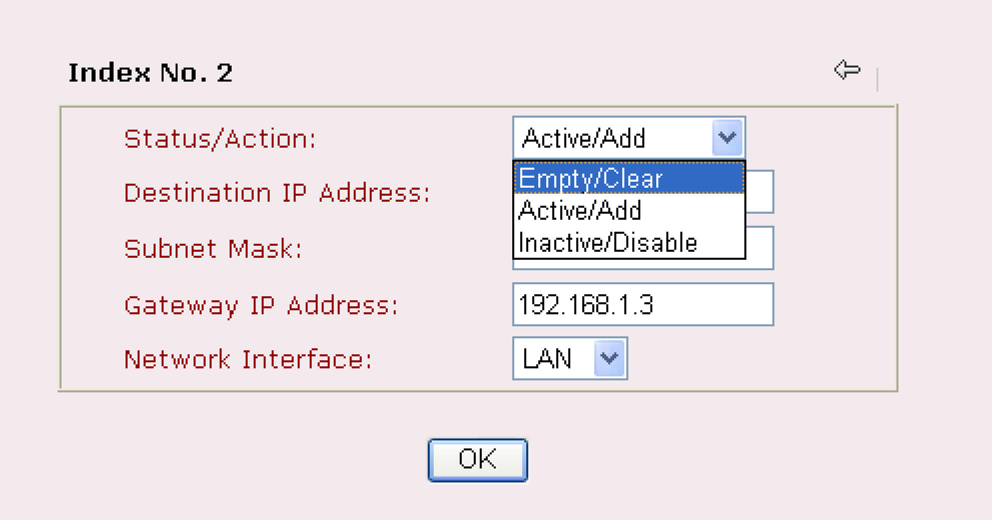


Current Running Routing Table

```
Key: C - connected, S - static, R - RIP, * - default, ~ - private

*          0.0.0.0/        0.0.0.0 via 172.16.3.1, IF3
S~       192.168.10.0/   255.255.255.0 via 192.168.1.2, IF0
C~        192.168.1.0/   255.255.255.0 is directly connected, IF0
C          172.16.3.0/   255.255.255.0 is directly connected, IF3
S~       211.100.88.0/   255.255.255.0 via 192.168.1.3, IF0
```

Delete Static Route

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



Index No. 2

Status/Action: Active/Add

Destination IP Address:

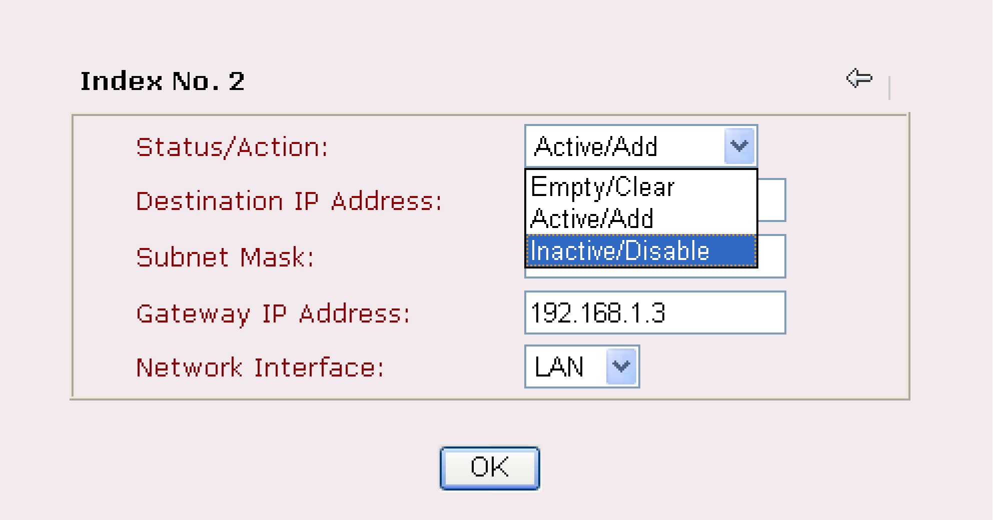
Subnet Mask:

Gateway IP Address: 192.168.1.3

Network Interface: LAN

Deactivate Static Route

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



Index No. 2

Status/Action: Active/Add

Destination IP Address:

Subnet Mask:

Gateway IP Address: 192.168.1.3

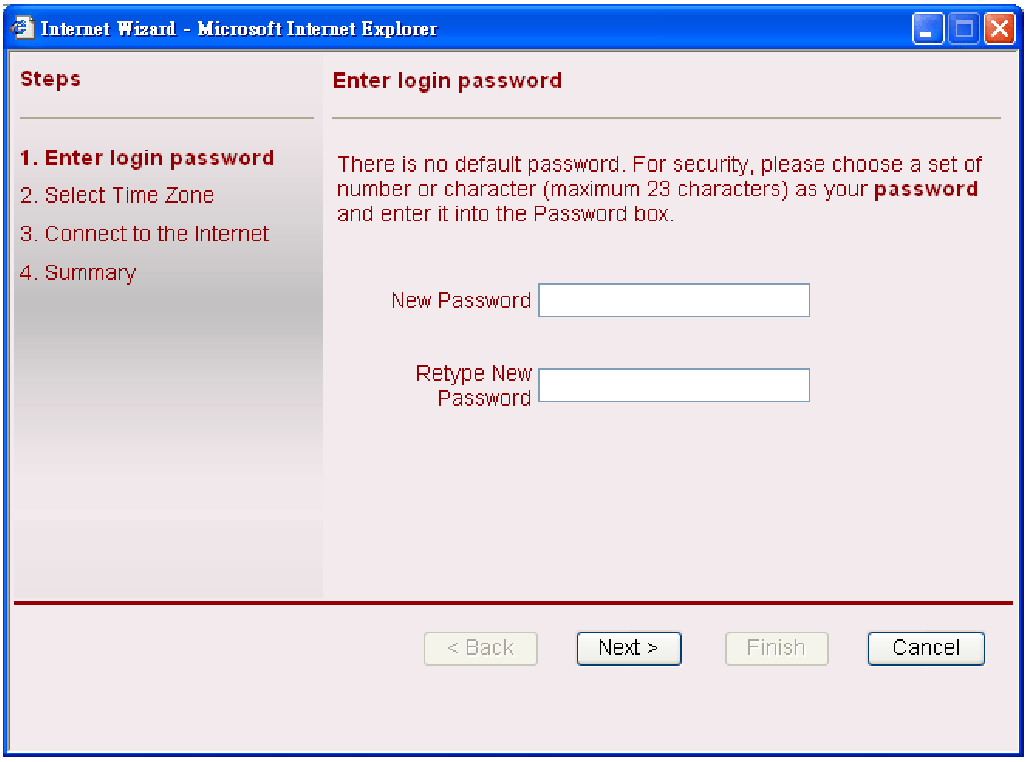
Network Interface: LAN

3.7 IP Filter/Firewall Setup

3.7.1 Basics for Firewall

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

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



Enter login password

There is no default password. For security, please choose a set of number or character (maximum 23 characters) as your **password** and enter it into the Password box.

New Password

Retype New Password

Firewall Facilities

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

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

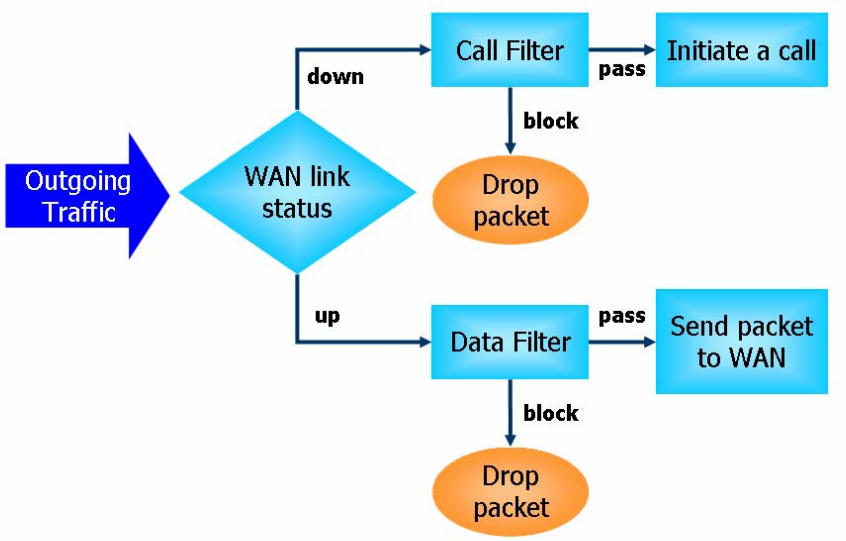
IP Filters

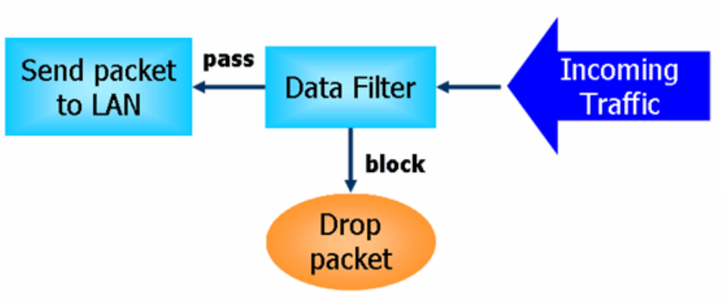
Depending on whether there is an existing Internet connection, or in other words "the WAN link status is up or down", the IP filter architecture categorizes traffic into two: **Call Filter** and **Data Filter**.

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

- **Data Filter -** When there is an existing Internet connection, **Data Filter** is applied to incoming and outgoing traffic. It will check packets according to the filter rules. If legal, the packet will pass the router.

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





Stateful Packet Inspection (SPI)

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

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

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

Denial of Service (DoS) Defense

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

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

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

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

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

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.

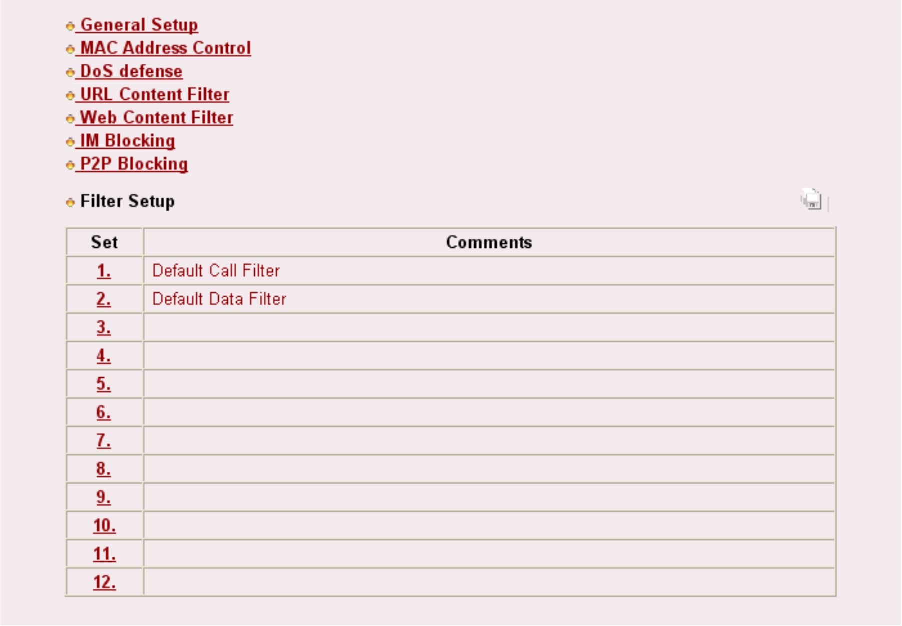
On the other hand, Vigor router can prevent user from accidentally downloading malicious codes from web pages. It’s very common that malicious codes conceal in the executable objects, such as ActiveX, Java Applet, compressed files, and other executable files. Once downloading these types of files from 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 (for V models only)

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

Once you have activated your Web Filtering service in Vigor router and chosen the categories of website you wish to restrict, each URL address requested (e.g.www.bbc.co.uk) will be checked against our server database, powered by SurfControl. The database covering over 70 languages and 200 countries, over 1 billion Web pages divided into 40 easy-to-understand categories. This database is updated as frequent as daily by a global team of Internet researchers. The server will look up the URL and return a category to your router. Your Vigor router will then decide whether to allow access to this site according to the categories you have selected. Please note that this action will not introduce any delay in your Web surfing because each of multiple load balanced database servers can handle millions of requests for categorization.

Choose **IP Filter/Firewall Setup** on the **Advanced Setup** group. Below shows the menu items for Firewall.

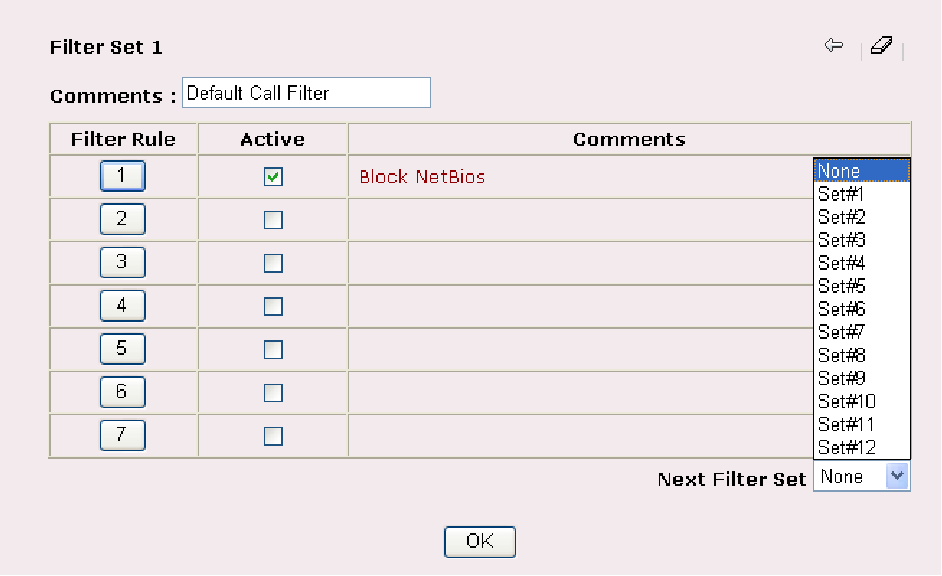


- General Setup
- MAC Address Control
- DoS defense
- URL Content Filter
- Web Content Filter
- IM Blocking
- P2P Blocking

Filter Setup

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



Filter Set 1

Comments : Default Call Filter

Filter Rule	Active	Comments
1	☑	Block NetBios
2	□	
3	□	
4	□	
5	□	
6	□	
7	□	

Next Filter Set: None

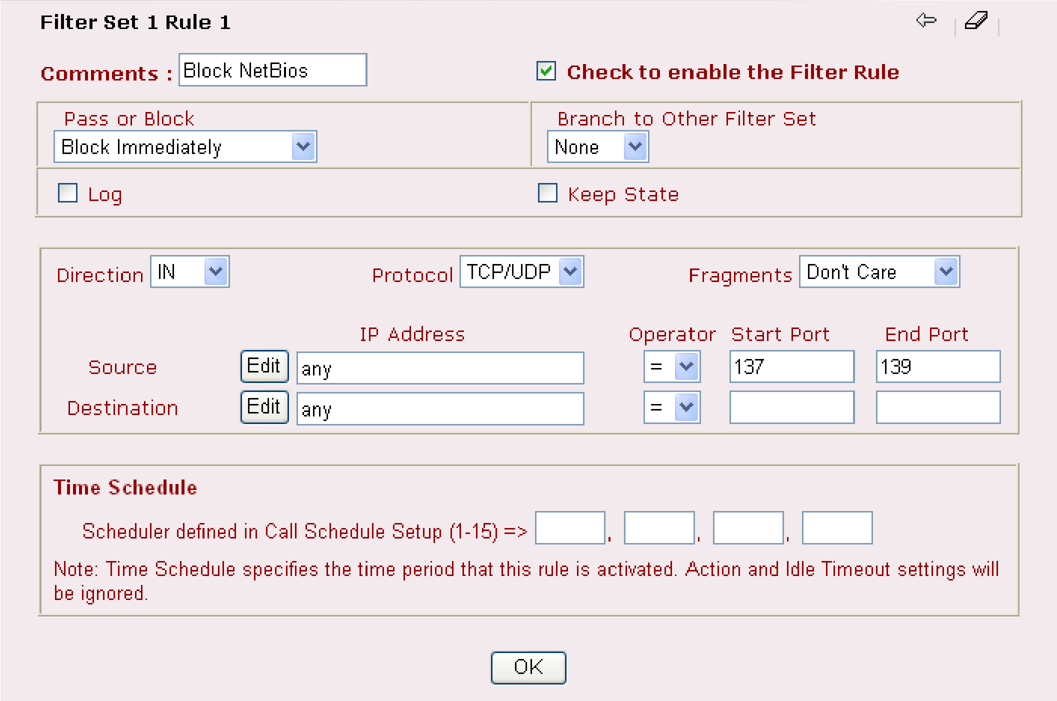
Filter Rule Click a button numbered (1 ~ 7) to edit the filter rule. Click the button will open Edit Filter Rule web page. For the detailed information, refer to the following page.

Active Enable or disable the filter rule.

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

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.



Filter Set 1 Rule 1

Comments : Block NetBios

☑ Check to enable the Filter Rule

Pass or Block: Block Immediately

Branch to Other Filter Set: None

□ Log

□ Keep State

Direction: IN

Protocol: TCP/UDP

Fragments: Don't Care

		IP Address	Operator	Start Port	End Port
Source	Edit	any	=	137	139
Destination	Edit	any	=		

Time Schedule

Scheduler defined in Call Schedule Setup (1-15) => , , ,

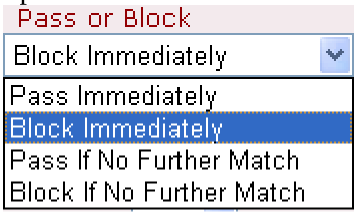
Note: Time Schedule specifies the time period that this rule is activated. Action and Idle Timeout settings will be ignored.

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

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

Pass or Block

Specifies the action to be taken when packets match the rule.



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.

Only the item of **Block If No Further Match** or **Pass If No Further Match** is selected as the **Pass or Block** action, the system will continue for inspection according to the specified filter set.

Log

Check this box to enable the log function. Use the Telnet command ***log-f*** to view the logs.

Keep State

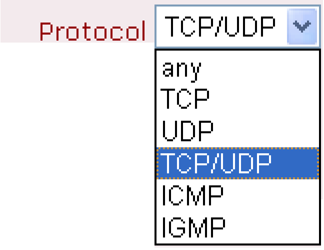
It is used for Data Filter only. Keep State is in the same nature of modern term Stateful Packet Inspection. If enabled, this rule will be added to State table when it is matched by a packet. When other packets in the same session as the matched packet is applied to Data Filer, they will be checked against the rules in State table first. If matched, they can pass immediately without having to check any rule in Data Filter. Only ICMP, TCP and UDP protocols can be added to State table.

Direction

Set the direction of packet flow. It is for **Data Filter** only. For the **Call Filter**, this setting is neglected since **Call Filter** is only applied to outgoing traffic.
IN - Specify the rule of filtering incoming packets.
OUT - Specify the rule of filtering outgoing packets.

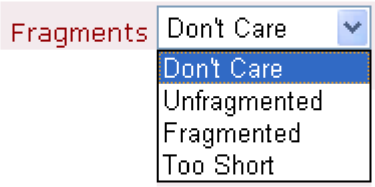
Protocol

Specify the protocol(s) which this filter rule will apply to.



Fragments

Specify the action for fragmented packets. And it is used for **Data Filter** only.

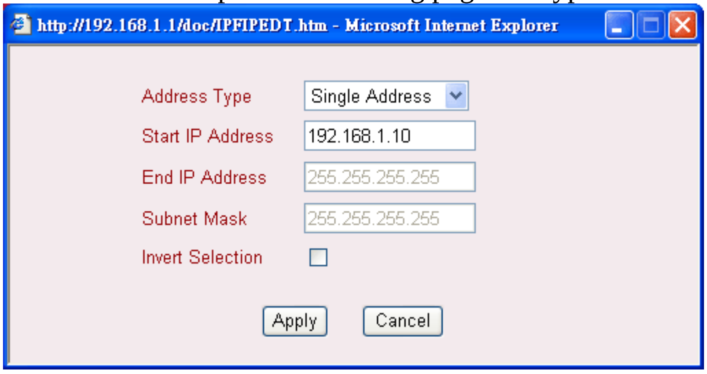


Fragments: Don't Care

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.

IP Address

Specify a source and destination IP address for this filter rule to apply to. Click **Edit** to open the following page and type in the IP address.



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

Address Type: Single Address
Start IP Address: 192.168.1.10
End IP Address: 255.255.255.255
Subnet Mask: 255.255.255.255
Invert Selection: □

Operator, Start Port and End Port

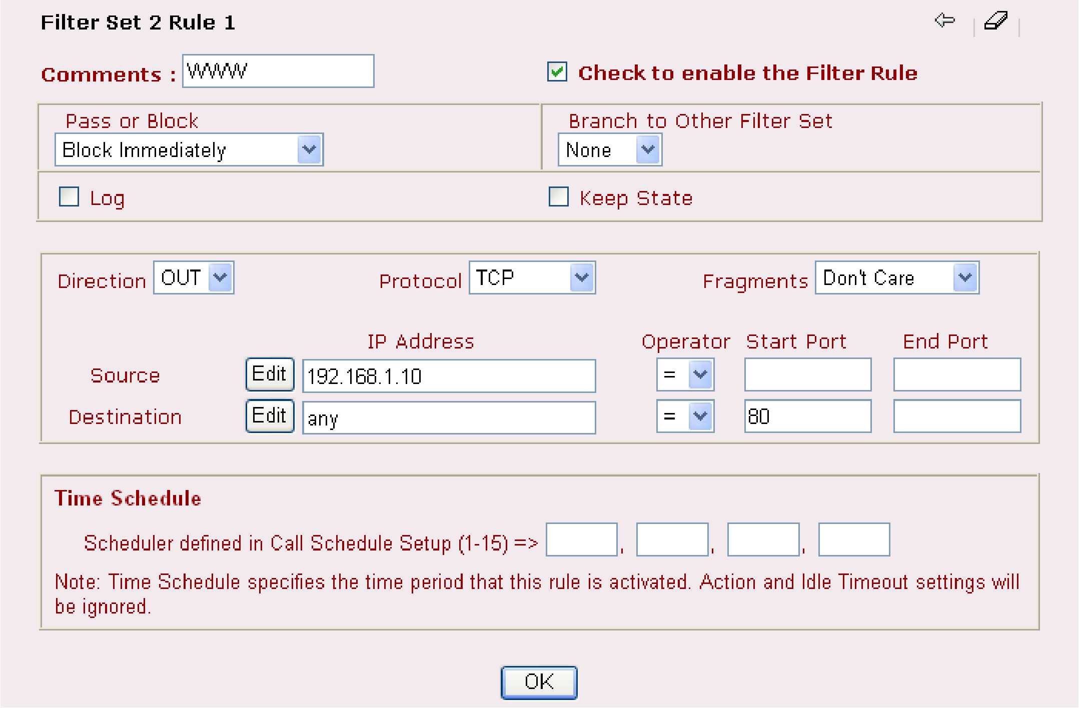
The operator column specifies the port number settings. If the **Start Port** is empty, the **Start Port** and the **End Port** column will be ignored. The filter rule will filter out any port number.
(=) If the End Port is empty, the filter rule will set the port number to be the value of the Start Port. Otherwise, the port number ranges between the Start Port and the End Port (including the Start Port and the End Port).
(!=)If the End Port is empty, the port number is not equal to the value of the Start Port. Otherwise, this port number is not between the Start Port and the End Port (including the Start Port and End Port).
(>) Specify the port number is larger than the Start Port (includes the Start Port).
(<) Specify the port number is less than the Start Port (includes the Start Port).

Time Schedule

To invoke the rules during specific periods, enter the number of the scheduler predefined in **Call Schedule Setup** on the **Advanced Setup group**.

Example of Restricting Unauthorized Internet Services

To set a simple example to restrict someone from accessing WWW services, we assume the IP address of the access-restricted user is 192.168.1.10. The filter rule is created in the Data Filter set and is shown as below.



Filter Set 2 Rule 1

Comments : WWW

☑ Check to enable the Filter Rule

Pass or Block: Block Immediately

Branch to Other Filter Set: None

□ Log

□ Keep State

Direction: OUT

Protocol: TCP

Fragments: Don't Care

	IP Address	Operator	Start Port	End Port
Source	192.168.1.10	=		
Destination	any	=	80	

Time Schedule

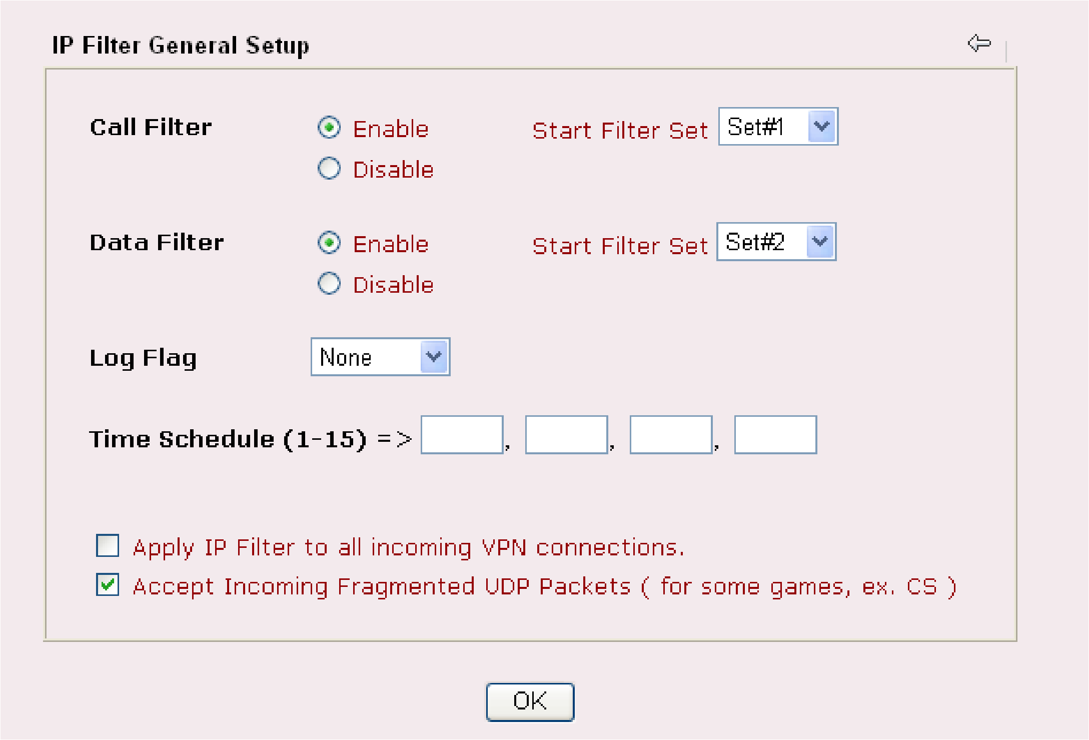
Scheduler defined in Call Schedule Setup (1-15) => , , ,

Note: Time Schedule specifies the time period that this rule is activated. Action and Idle Timeout settings will be ignored.

3.7.2 General Setup

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

Choose **IP Filter/Firewall Setup** on the **Advanced Setup** group and click the **IP Filter General Setup** link.



IP Filter General Setup

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

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

Log Flag None

Time Schedule (1-15) => , , ,

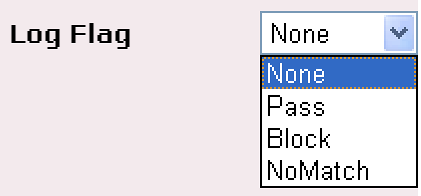
□ Apply IP Filter to all incoming VPN connections.

☑ Accept Incoming Fragmented UDP Packets (for some games, ex. CS)

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

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

Log Flag For troubleshooting needs you can specify the filter log here.



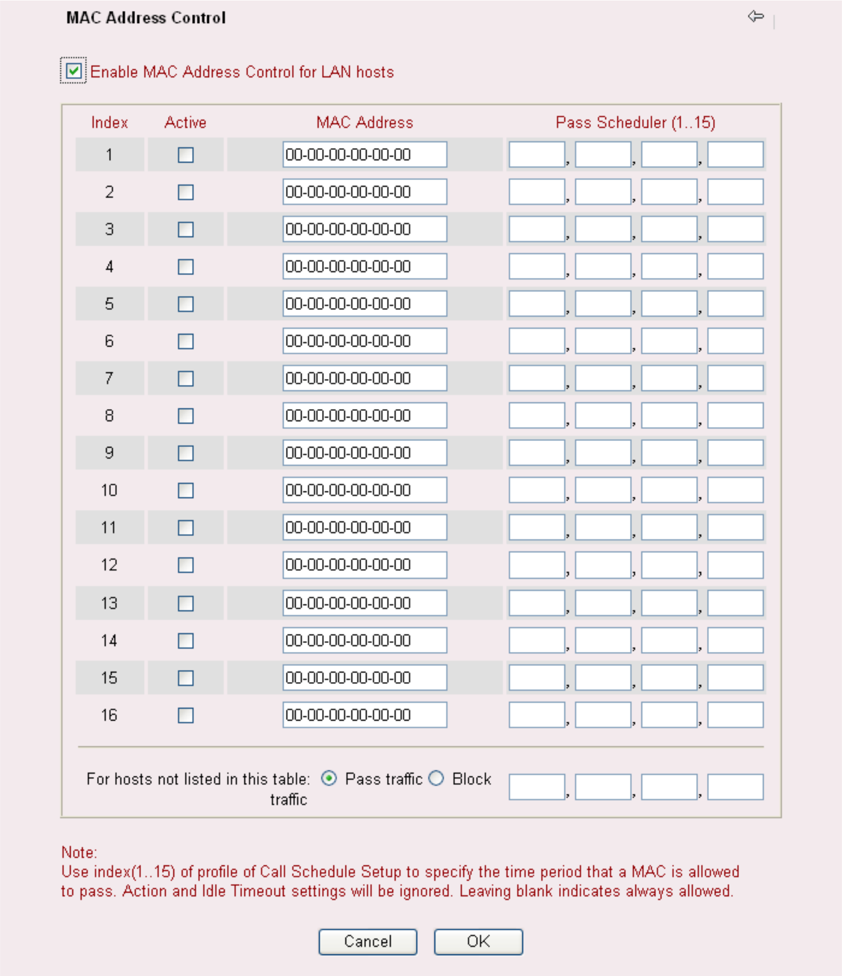
None - The log function is not activated.
Block - All blocked packets will be logged.
Pass - All passed packets will be logged.
No Match - The log function will record all packets that are not matched.
Note that the filter log will be displayed on the Telnet terminal when you type the ***log -f*** command.

Time Schedule Specify what time should perform the IP filtering facility.

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

3.7.3 MAC Address Control

Choose **IP Filter/Firewall Setup** on the **Advanced Setup** group and click the **MAC Address Control** link.



MAC Address Control

☑ Enable MAC Address Control for LAN hosts

Index	Active	MAC Address	Pass Scheduler (1..15)
1	□	00-00-00-00-00-00	, , ,
2	□	00-00-00-00-00-00	, , ,
3	□	00-00-00-00-00-00	, , ,
4	□	00-00-00-00-00-00	, , ,
5	□	00-00-00-00-00-00	, , ,
6	□	00-00-00-00-00-00	, , ,
7	□	00-00-00-00-00-00	, , ,
8	□	00-00-00-00-00-00	, , ,
9	□	00-00-00-00-00-00	, , ,
10	□	00-00-00-00-00-00	, , ,
11	□	00-00-00-00-00-00	, , ,
12	□	00-00-00-00-00-00	, , ,
13	□	00-00-00-00-00-00	, , ,
14	□	00-00-00-00-00-00	, , ,
15	□	00-00-00-00-00-00	, , ,
16	□	00-00-00-00-00-00	, , ,

For hosts not listed in this table: ● Pass traffic ○ Block traffic , , ,

Note:
Use index(1..15) of profile of Call Schedule Setup to specify the time period that a MAC is allowed to pass. Action and Idle Timeout settings will be ignored. Leaving blank indicates always allowed.

Active Check this box to invoke this setting.

MAC Address Type in the MAC Address of the device that the router connects to.

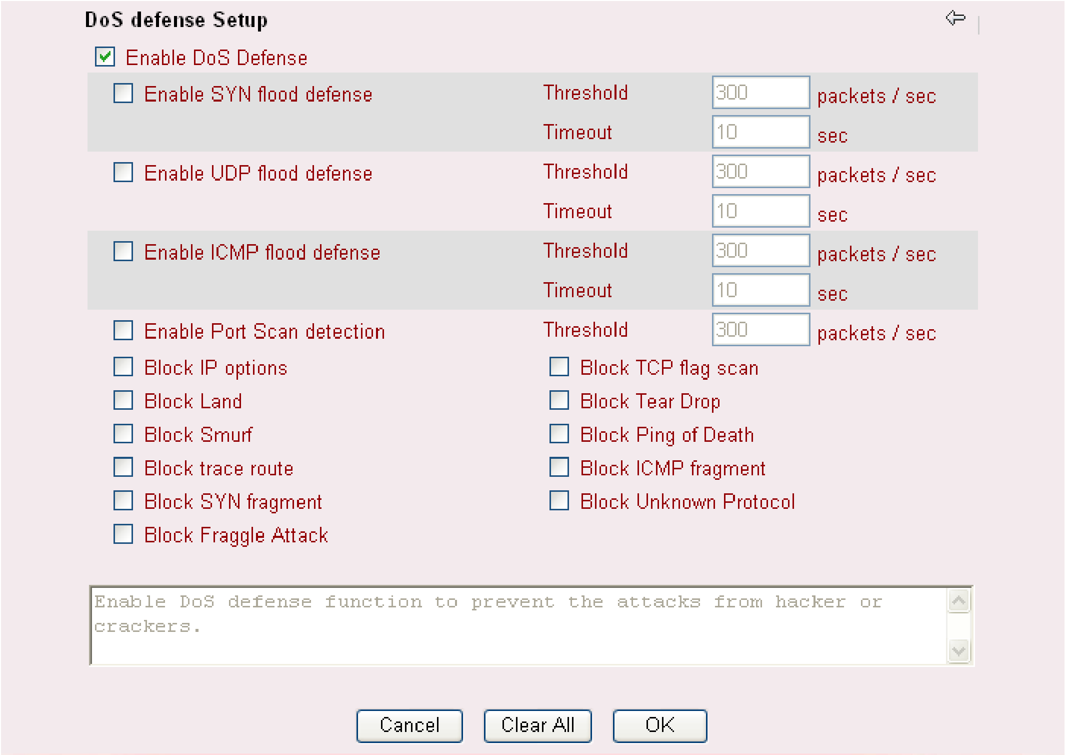
Pass Scheduler (1..15) Let the device with the specific MAC address to be passed within certain time interval only. You may choose up to 4 schedules out of the 15 schedules pre-defined in **Call Schedule Setup** in **Advanced Setup group** setup.
If the four boxes are left blank, that means the traffic for the MAC address is "always pass". If only one disabled schedule typed in the box, it means the related MAC address will be always blocked.

For hosts not listed in this table This setting allows you to set for all other hosts that not listed in the above table to be passed or be blocked in certain time. Again, please choose four schedules from Call Schedule Setup.

3.7.4 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.

Choose **IP Filter/Firewall Setup** on the **Advanced Setup** group and click the **DoS Defense** link.



DoS defense Setup

☑ Enable DoS Defense

□ Enable SYN flood defense	Threshold	300	packets / sec
	Timeout	10	sec
□ Enable UDP flood defense	Threshold	300	packets / sec
	Timeout	10	sec
□ Enable ICMP flood defense	Threshold	300	packets / sec
	Timeout	10	sec
□ Enable Port Scan detection	Threshold	300	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 Unknown Protocol
□ 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 has exceeded the defined value, the Vigor router will start to 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 has exceeded the defined value, the Vigor router will start to 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 has exceeded the defined value, the router will discard the ICMP echo requests coming from the Internet. The default setting for threshold and timeout are 50 packets per second and 10 seconds, respectively.

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

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

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

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

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

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

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

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

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

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

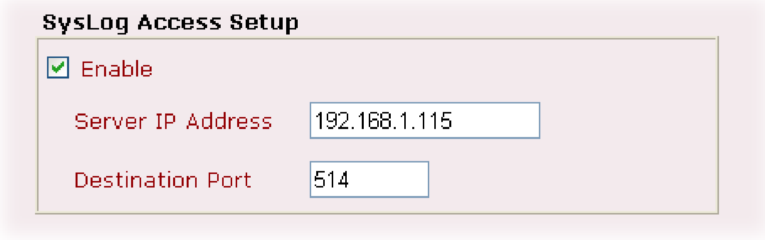
Block ICMP Fragment Check the box to activate the Block ICMP fragment function. Any ICMP packets with more fragment bit set are dropped.

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

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

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

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

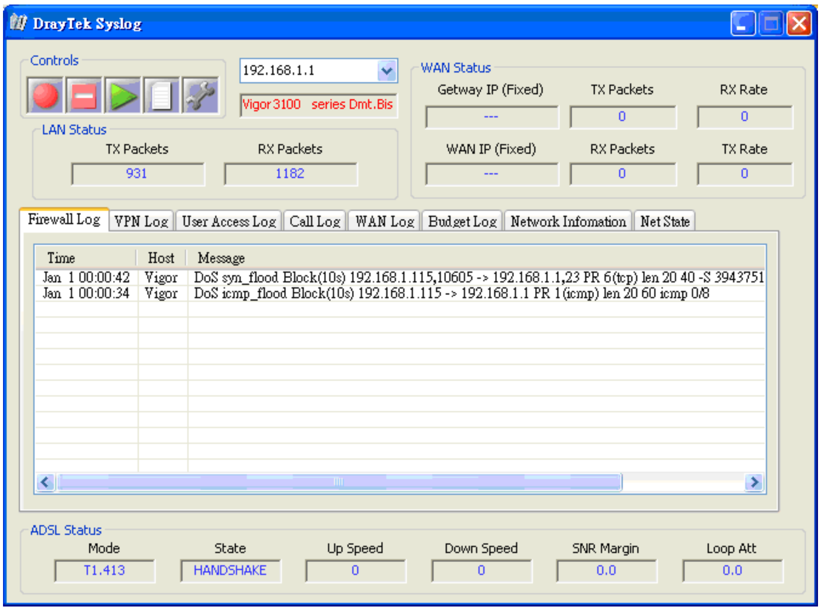


SysLog Access Setup

☑ Enable

Server IP Address: 192.168.1.115

Destination Port: 514



DrayTek Syslog

Controls: 192.168.1.1 — Vigor3100 series Dmt.Bis

LAN Status	TX Packets	RX Packets
	931	1182

WAN Status		
Getway IP (Fixed)	TX Packets	RX Rate
---	0	0
WAN IP (Fixed)	RX Packets	TX Rate
---	0	0

```
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 3943751
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
T1.413	HANDSHAKE	0	0	0.0	0.0

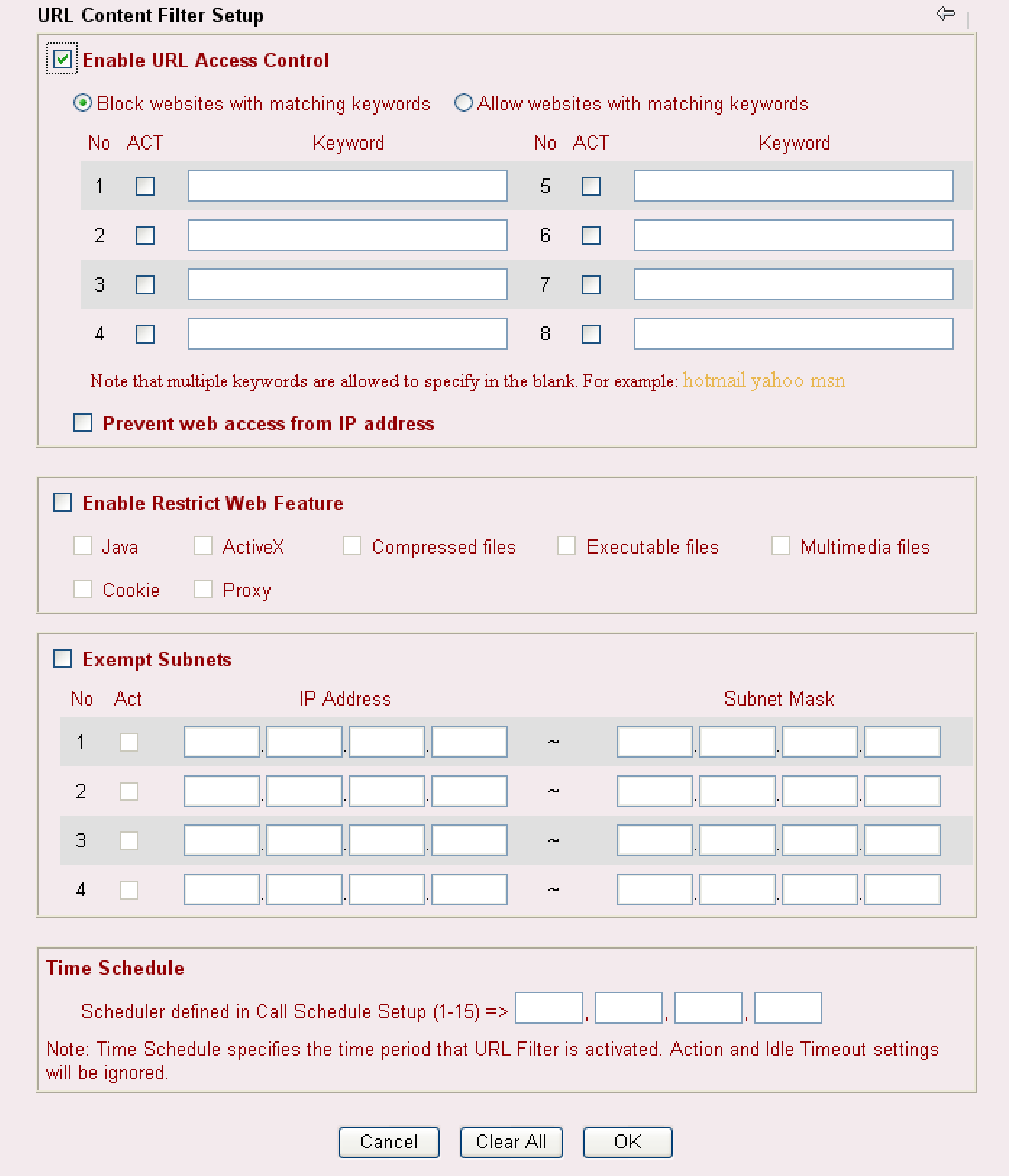
3.7.5 URL Content Filter

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

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

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

Choose **IP Filter/Firewall Setup** on the **Advanced Setup** group and click the **URL Content Filter** link.



URL Content Filter Setup

☑ Enable URL Access Control

● Block websites with matching keywords ○ Allow websites with matching keywords

No	ACT	Keyword	No	ACT	Keyword
1	□		5	□	
2	□		6	□	
3	□		7	□	
4	□		8	□	

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

□ Prevent web access from IP address

□ Enable Restrict Web Feature

□ Java □ ActiveX □ Compressed files □ Executable files □ Multimedia files

□ Cookie □ Proxy

□ Exempt Subnets

No	Act	IP Address		Subnet Mask
1	□	. . .	~	. . .
2	□	. . .	~	. . .
3	□	. . .	~	. . .
4	□	. . .	~	. . .

Time Schedule

Scheduler defined in Call Schedule Setup (1-15) => , , ,

Note: Time Schedule specifies the time period that URL Filter is activated. Action and Idle Timeout settings will be ignored.

Enable URL Access Control
Check the box to activate URL Access Control.

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

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

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

Prevent web access from IP address

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

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

Enable Restrict Web Feature

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

***ActiveX* -** Check the box to activate the Block ActiveX object function. Any ActiveX object from the Internet will be refused.
***Compressed file* -** Check the box to activate the Block Compressed file function to prevent someone from downloading any compressed file. The following list shows the types of compressed files that can be blocked by the Vigor router. .
zip, rar, .arj, .ace, .cab, .sit
***Executable file* -** Check the box to reject any downloading behavior of the executable file from the Internet.
.exe, .com, .scr, .pif, .bas, .bat, .inf, .reg
***Cookie* -** Check the box to filter out the cookie transmission from inside to outside world to protect the local user's privacy.
***Proxy* -** Check the box to reject any proxy transmission. To control efficiently the limited-bandwidth usage, it will be of great value to provide the blocking mechanism that filters out the multimedia files downloading from web pages. Accordingly, files with the following extensions will be blocked by the Vigor router.
.mov .mp3 .rm .ra .au .wmv
.wav .asf .mpg .mpeg .avi .ram

Enable Excepting Subnets

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

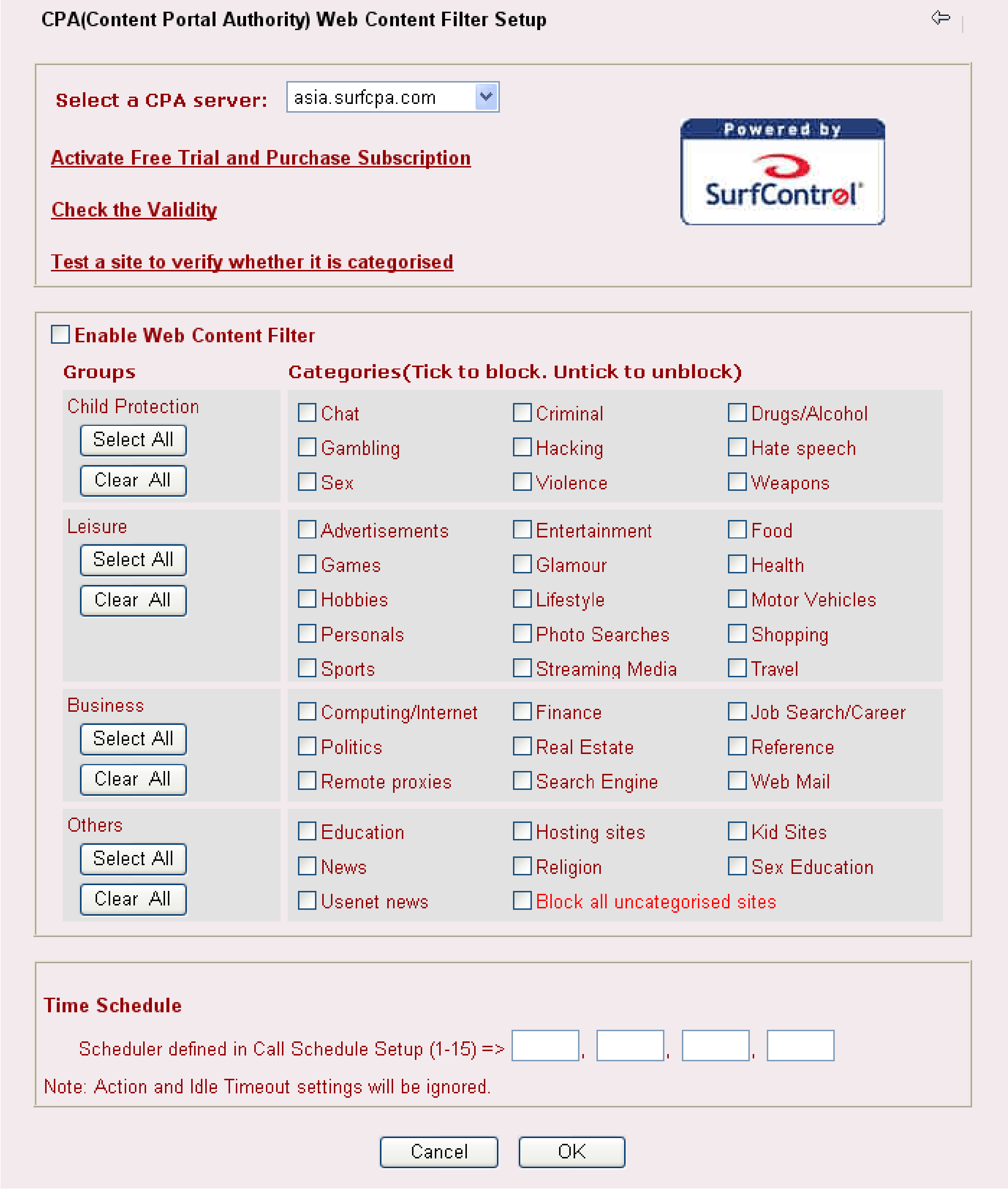
Time Schedule

Specify what time should perform the URL content filtering facility.

3.7.6 Web Content Filter (for V models only)

Choose **IP Filter/Firewall Setup** on the **Advanced Setup** group and click the **Web Content Filter** link.

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



CPA(Content Portal Authority) Web Content Filter Setup

Select a CPA server: asia.surfcpa.com

Activate Free Trial and Purchase Subscription

Check the Validity

Test a site to verify whether it is categorised

□ Enable Web Content Filter

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

Time Schedule

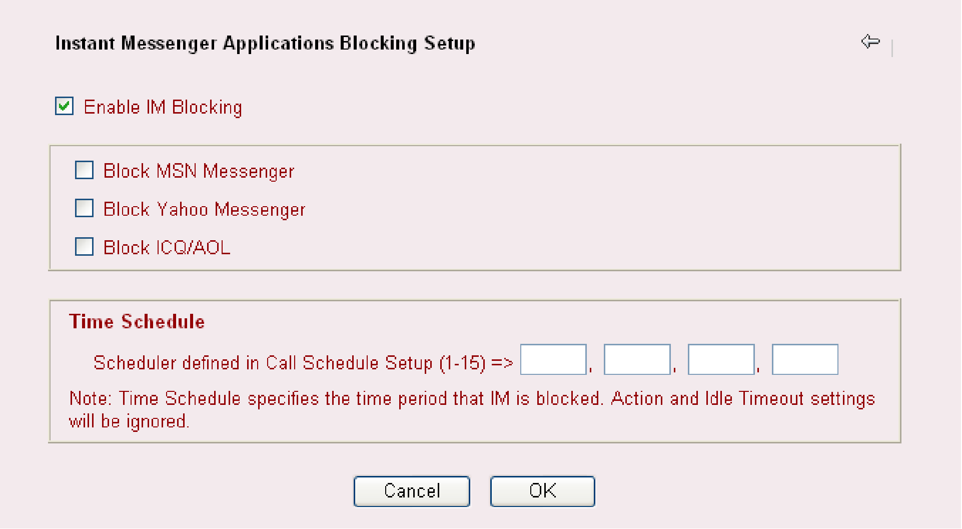
Scheduler defined in Call Schedule Setup (1-15) => [ ], [ ], [ ], [ ]

Note: Action and Idle Timeout settings will be ignored.

3.7.7 IM Blocking

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

Choose **IP Filter/Firewall Setup** on the **Advanced Setup** group and click the **IM Blocking** link.



Instant Messenger Applications Blocking Setup

☑ Enable IM Blocking

☐ Block MSN Messenger

☐ Block Yahoo Messenger

☐ Block ICQ/AOL

Time Schedule

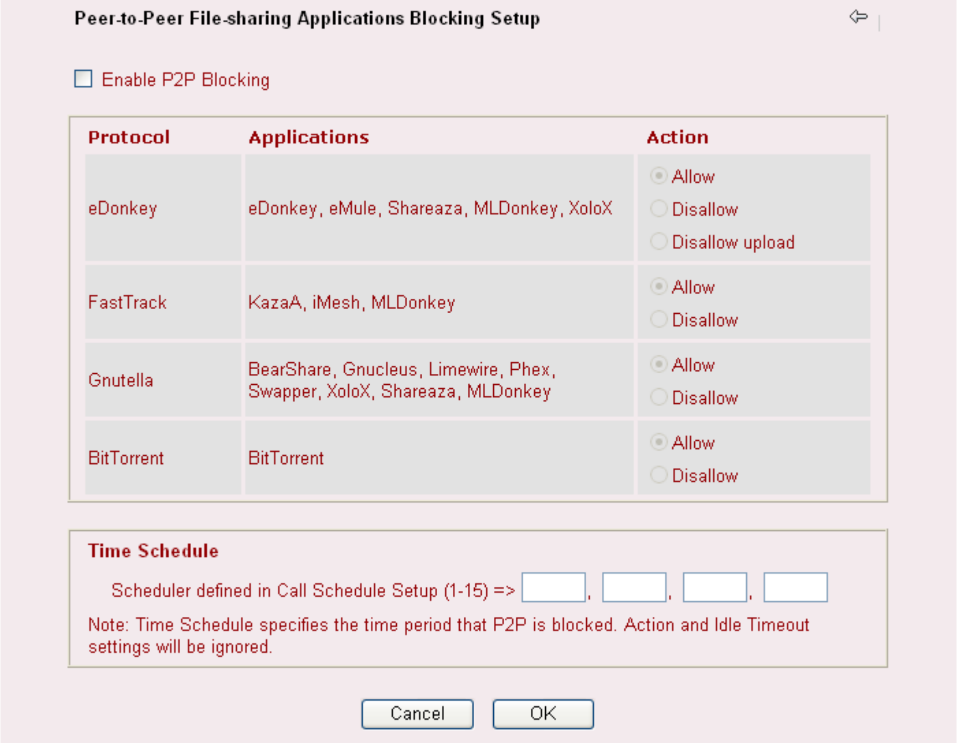
Scheduler defined in Call Schedule Setup (1-15) => [ ], [ ], [ ], [ ]

Note: Time Schedule specifies the time period that IM is blocked. Action and Idle Timeout settings will be ignored.

3.7.8 P2P Blocking

P2P is the short name of peer to peer. You will see a list of common P2P applications. Check **Enable P2P Blocking** and select the one(s) to block. To block selected P2P applications during specific periods, enter the number of the scheduler predefined in **Call Schedule Setup** in **Advanced Setup** group.

Choose **IP Filter/Firewall Setup** on the **Advanced Setup** group and click the **P2P Blocking** link.



Peer-to-Peer File-sharing Applications Blocking Setup

□ Enable P2P Blocking

Protocol	Applications	Action
eDonkey	eDonkey, eMule, Shareaza, MLDonkey, XoloX	● Allow ○ Disallow ○ Disallow upload
FastTrack	KazaA, iMesh, MLDonkey	● Allow ○ Disallow
Gnutella	BearShare, Gnucleus, Limewire, Phex, Swapper, XoloX, Shareaza, MLDonkey	● Allow ○ Disallow
BitTorrent	BitTorrent	● Allow ○ Disallow

Time Schedule

Scheduler defined in Call Schedule Setup (1-15) => ___ , ___ , ___ , ___

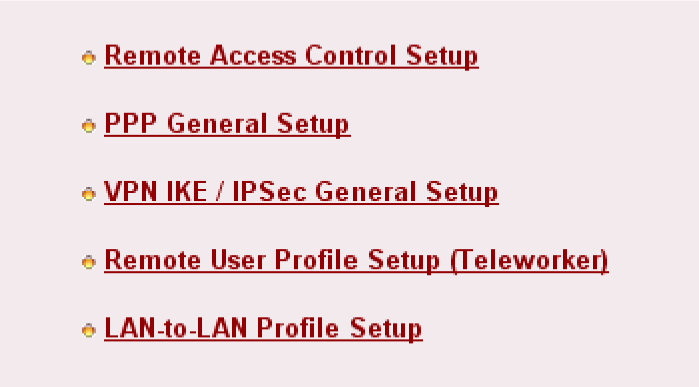
Note: Time Schedule specifies the time period that P2P is blocked. Action and Idle Timeout settings will be ignored.

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

3.8 VPN and Remote Access Setup

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.

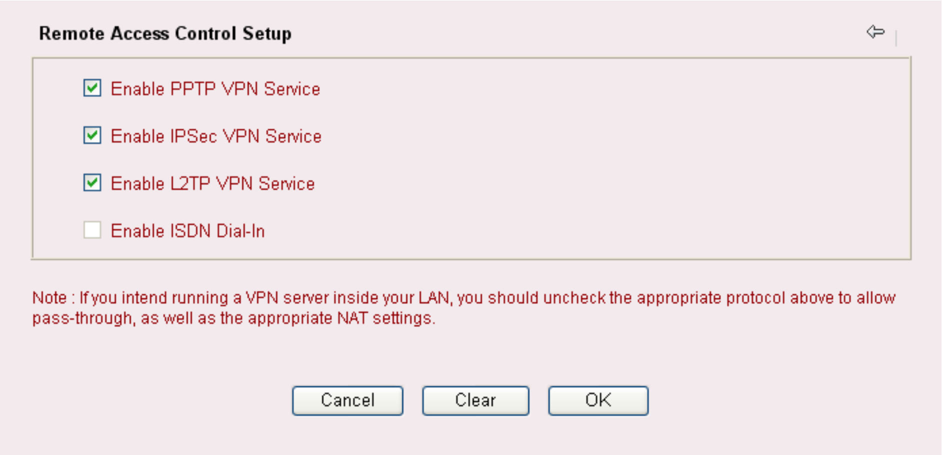
Choose **VPN and Remote Access Setup** on the **Advanced Setup** group, you can see the following page.



- Remote Access Control Setup
- PPP General Setup
- VPN IKE / IPSec General Setup
- Remote User Profile Setup (Teleworker)
- LAN-to-LAN Profile Setup

3.8.1 Remote Access Control Setup

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.



Remote Access Control Setup

☑ Enable PPTP VPN Service

☑ Enable IPSec VPN Service

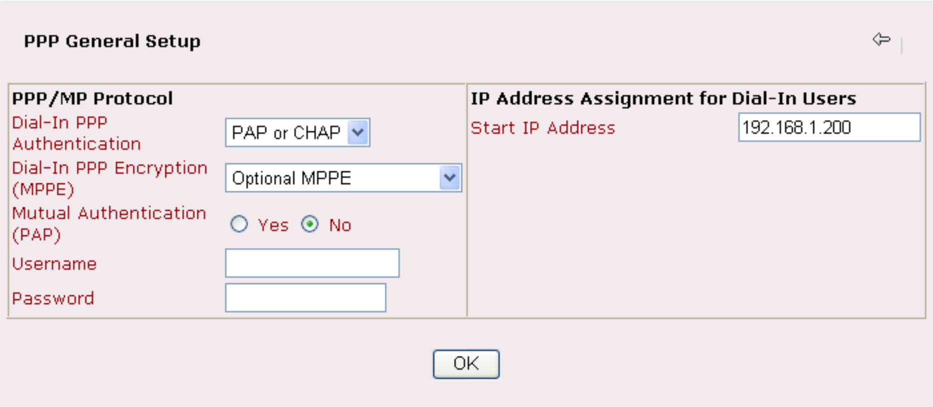
☑ Enable L2TP VPN Service

□ Enable ISDN Dial-In

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

3.8.2 PPP General Setup

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



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

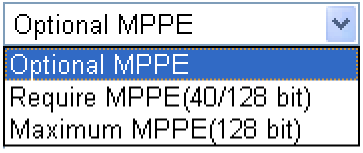
Start IP Address	192.168.1.200

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)

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 1280-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 bits) to encrypt the data.

Mutual Authentication (PAP)

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

Start IP Address

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

3.8.3 VPN IKE/IPSec General Setup

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

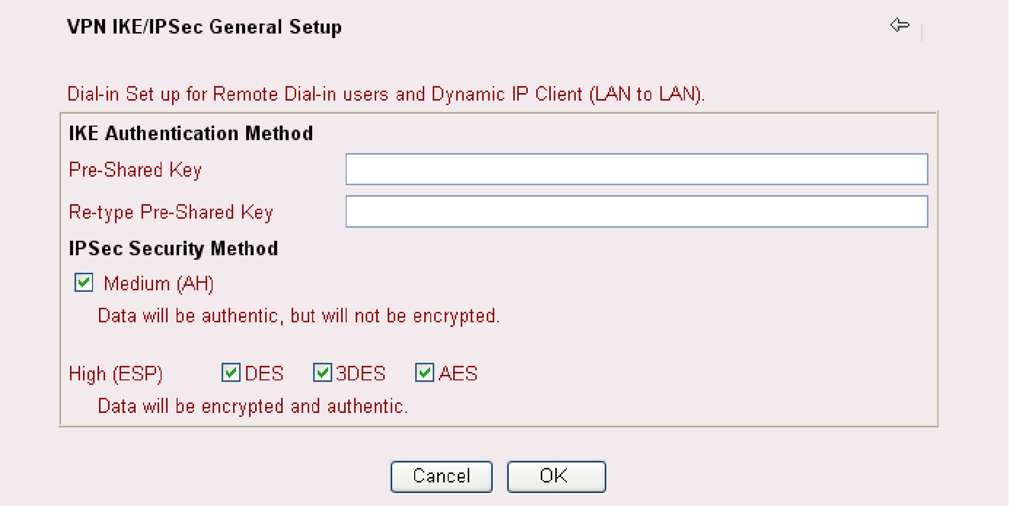
There are two phases of IPSec.

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

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

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

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



VPN IKE/IPSec General Setup

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

IKE Authentication Method

Pre-Shared Key

Re-type 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.

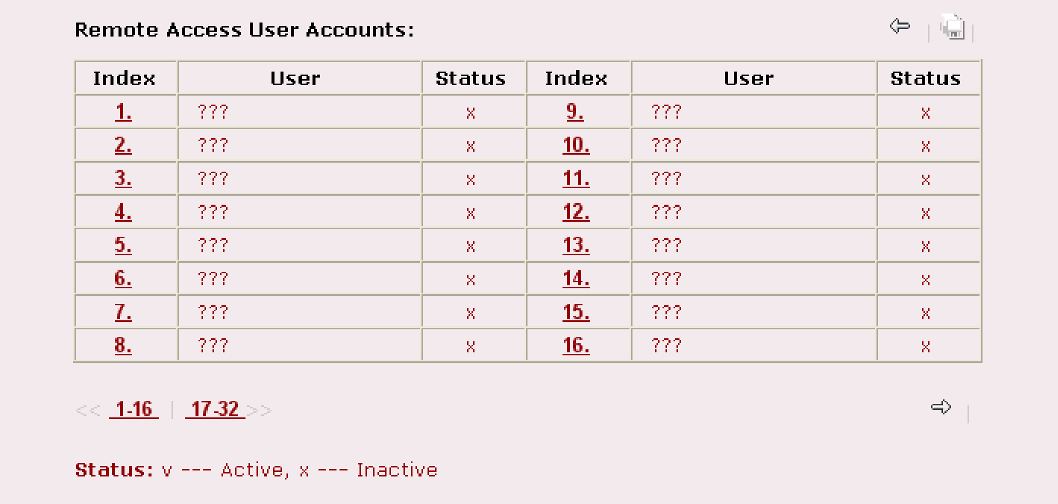
IKE Authentication Method	This usually applies to those are remote dial-in user or node (LAN-to-LAN) which uses dynamic IP address and IPSec-related VPN connections such as L2TP over IPSec and IPSec tunnel. **Pre-Shared Key** -Currently only support Pre-Shared Key authentication. Specify a key for IKE authentication. **Re-type Pre-Shared Key** -Confirm the pre-shared key.
IPSec Security Method	**Medium -** Authentication Header (AH) means data will be authenticated, but not be encrypted. By default, this option is active. **High -** Encapsulating Security Payload (ESP) means payload

(data) will be encrypted and authenticated. You may select encryption algorithm from Data Encryption Standard (DES), Triple DES (3DES), and AES.

3.8.4 Remote User Profile Setup (Teleworker)

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

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



Remote Access User Accounts: ⇦ |

Index	User	Status	Index	User	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	16.	???	x

<< 1-16 | 17-32 >> ⇨ |

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

Click to clear all indexes.

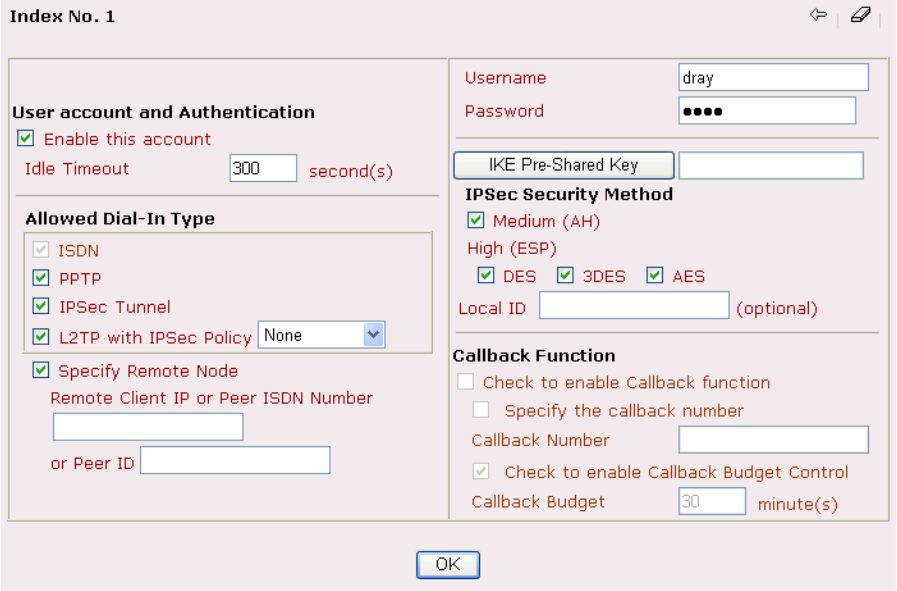
Index Click the number below Index to access into the setting page of Remote Dial-in User.

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

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



Index No. 1

User account and Authentication

☑ Enable this account

Idle Timeout 300 second(s)

Allowed Dial-In Type

☑ ISDN

☑ PPTP

☑ IPSec Tunnel

☑ L2TP with IPSec Policy None

☑ Specify Remote Node

Remote Client IP or Peer ISDN Number

or Peer ID

Username dray

Password ●●●●

IKE Pre-Shared Key

IPSec Security Method

☑ Medium (AH)

High (ESP)

☑ DES ☑ 3DES ☑ AES

Local ID (optional)

Callback Function

□ Check to enable Callback function

□ Specify the callback number

Callback Number

☑ Check to enable Callback Budget Control

Callback Budget 30 minute(s)

OK

Enable this account Check the box to enable this function.

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

ISDN Allow the remote ISDN dial-in connection. You can further set up Callback function below. You should set the User Name and Password of remote dial-in user below. This feature is for ***i*** model only.

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

IPSec Tunnel Allow the remote dial-in user to trigger 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 Remote Node **Check the checkbox-**You can specify the IP address of the remote dial-in user or peer ID (used in IKE aggressive mode).

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

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

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

IKE 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.

IPSec Security Method

This group of fields is a must for IPSec Tunnels and L2TP with IPSec Policy when you specify the remote node. Check the Medium, DES, 3DES or AES box as the security method.
Medium -Authentication Header (AH) means data will be authenticated, but not be encrypted. By default, this option is invoked. You can uncheck it to disable it.
High-Encapsulating Security Payload (ESP) means payload (data) will be encrypted and authenticated. You may select encryption algorithm from Data Encryption Standard (DES), Triple DES (3DES), and AES.
Local ID - Specify a local ID to be used for Dial-in setting in the LAN-to-LAN Profile setup. This item is optional and can be used only in IKE aggressive mode.

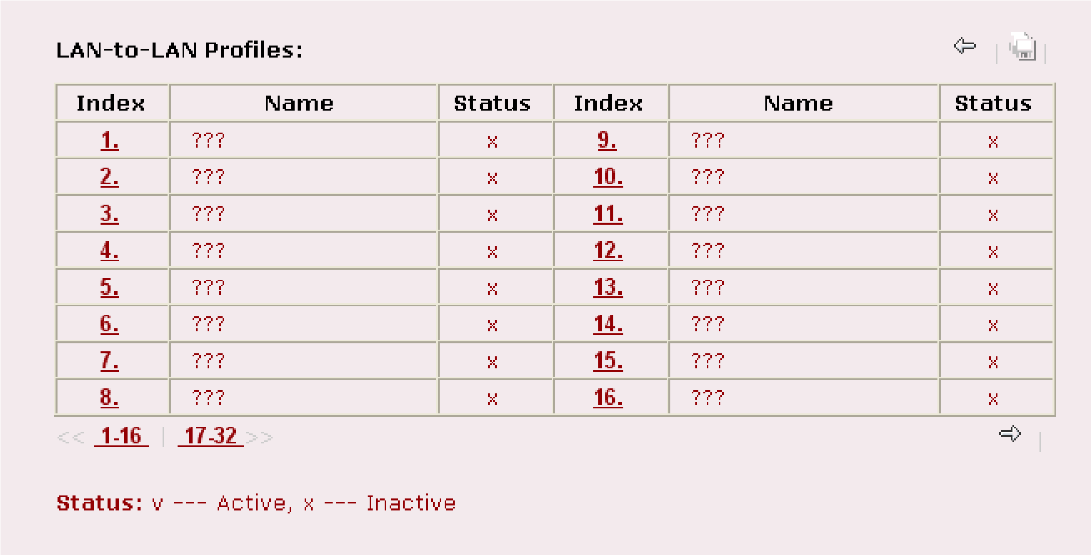
Callback Function

The callback function provides a callback service only for the ISDN dial-in user (for *i* model only). The router owner will be charged the connection fee by the telecom.
Check to enable Callback function-Enables the callback function.
Specify the callback number-The option is for extra security. Once enabled, the router will ONLY call back to the specified Callback Number.
Check to enable callback budget control-By default, the callback function has a time restriction. Once the callback budget has been exhausted, the callback mechanism will be disabled automatically.
Callback Budget (Unit: minutes)- Specify the time budget for the dial-in user. The budget will be decreased automatically per callback connection.

3.8.5 LAN to LAN Profile Setup

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

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



LAN-to-LAN Profiles:

Index	Name	Status	Index	Name	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	16.	???	x

<< 1-16 | 17-32 >>

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

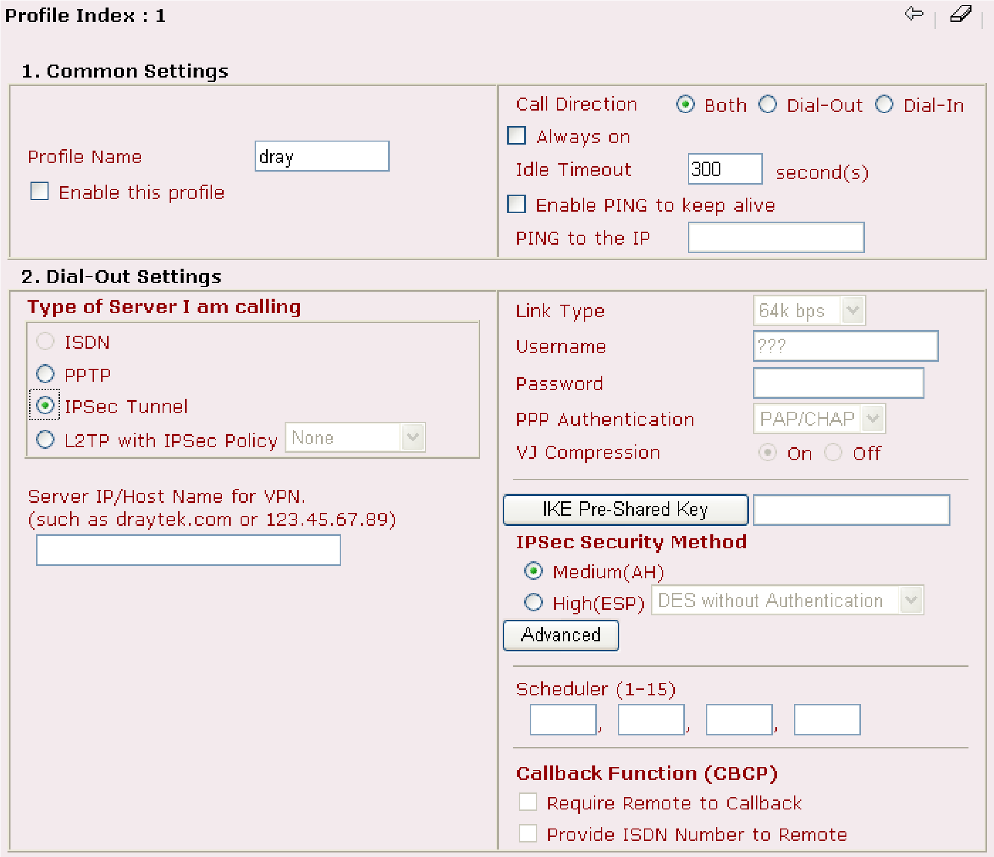
Click to clear all indexes.

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

Status Indicate the status of individual profiles. The symbol V and X represent the profile to be active and inactive, respectively.

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

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



Profile Index : 1

1. Common Settings

Profile Name: dray

□ Enable this profile

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

○ ISDN

○ PPTP

● IPSec Tunnel

○ L2TP with IPSec Policy None

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

Link Type 64k bps

Username ???

Password

PPP Authentication PAP/CHAP

VJ Compression ● On ○ Off

IKE Pre-Shared Key

IPSec Security Method

● Medium(AH)

○ High(ESP) DES without Authentication

Advanced

Scheduler (1-15)

Callback Function (CBCP)

□ Require Remote to Callback

□ Provide ISDN Number to Remote

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

Enable this profile Check here to activate this profile.

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

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

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

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

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

ISDN Build ISDN dial-out connection to the server. You should set up Link Type and identity like User Name and Password for the authentication of remote server. You can further set up Callback (CBCP) function below. This feature is useful for *i* model only.

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

IPSec Tunnel Build a IPSec VPN connection to the server through Internet.

L2TP with … Build a L2TP VPN connection through the Internet. You can select to use L2TP alone or with IPSec. Select from below:
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 w/ or w/out IPSec policy above.

Password This field is applicable when you select PPTP or L2TP w/ or w/out IPSec policy above.

PPP Authentication This field is applicable when you select PPTP or L2TP w/ or w/out IPSec policy above. PAP/CHAP is the most common selection due to wild compatibility.

VJ compression This field is applicable when you select PPTP or L2TP w/ or w/out IPSec policy above. VJ Compression is used for TCP/IP protocol header compression. Normally set to **Yes** to improve bandwidth utilization.

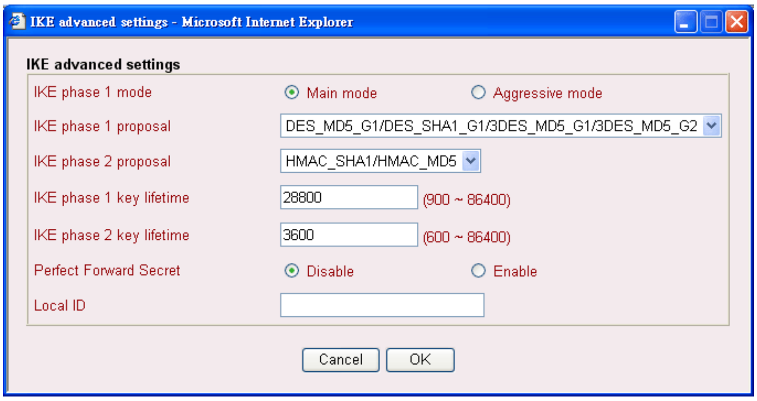
IKE Pre-Shared Key Click this button to input 1-63 characters as pre-shared key.

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

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

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

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



IKE 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.

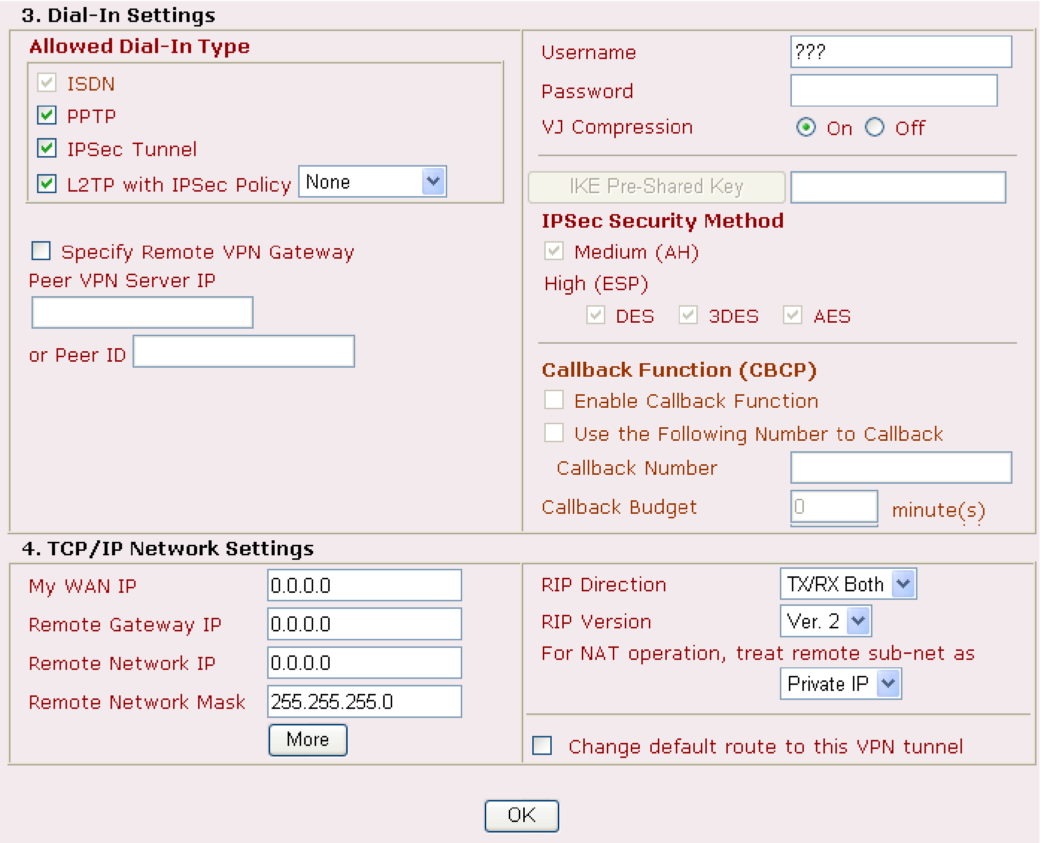
Local ID-In **Aggressive** mode, Local ID is on behalf of the IP address while identity authenticating with remote VPN server. The length of the ID is limited to 47 characters.

Callback Function (for I models only)

The callback function provides a callback service as a part of PPP suite only for the ISDN dial-in user. The router owner will be charged the connection fee by the telecom.

Require Remote to Callback-Enable this to let the router to require the remote peer to callback for the connection afterwards.

Provide ISDN Number to Remote-In the case that the remote peer requires the Vigor router to callback, the local ISDN number will be provided to the remote peer. Check here to allow the Vigor router to send the ISDN number to the remote router. This feature is useful for *i* model only.



3. Dial-In Settings

Allowed Dial-In Type

☑ ISDN

☑ 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 Pre-Shared Key:

IPSec Security Method

☑ Medium (AH)

High (ESP)

☑ DES ☑ 3DES ☑ AES

Callback Function (CBCP)

□ Enable Callback Function

□ Use the Following Number to Callback

Callback Number:

Callback Budget: 0 minute(s)

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

More

RIP Direction: TX/RX Both

RIP Version: Ver. 2

For NAT operation, treat remote sub-net as: Private IP

□ Change default route to this VPN tunnel

OK

Allowed Dial-In Type

Determine the dial-in connection with different types.

ISDN

Allow the remote ISDN dial-in connection. You can further set up Callback function below. You should set the User Name and Password of remote dial-in user below. This feature is useful for *i* model only.

PPTP

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

IPSec Tunnel

Allow the remote dial-in user to trigger 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 Remote VPN Gateway

You can specify the IP address of the remote dial-in user or peer ID (should be the same with the ID setting in dial-in type) by checking the box. Enter Peer ISDN number if you select ISDN above (This feature is useful for *i* model only.). Also, you should further specify the corresponding security methods on the right side.

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

User Name

This field is applicable when you select PPTP or L2TP w/ or w/out IPSec policy above.

Password

This field is applicable when you select PPTP or L2TP w/ or w/out IPSec policy above.

VJ Compression

VJ Compression is used for TCP/IP protocol header compression. This field is applicable when you select PPTP or L2TP w/ or w/out IPSec policy above.

IKE Pre-Shared Key

It is applicable for IPSec Tunnels and L2TP with IPSec Policy when you Specify ISDN CLID (for *i* model only) or Remote VPN Gateway Peer ISDN Number (for *i* model only) or Peer VPN Server IP. Click the **IKE Pre-Shared Key** button and input 1-63 characters as pre-shared key.

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.

Callback Function

The callback function provides a callback service only for the ISDN dial-in user (this feature is useful for *i* model only). The router owner will be charged the connection fee by the telecom.
Check to enable Callback function-Enables the callback function.
Callback number-The option is for extra security. Once enabled, the router will ONLY call back to the specified Callback Number.
Callback budget- By default, the callback function has limitation of callback period. Once the callback budget is exhausted, the function will be disabled automatically.
Callback Budget (Unit: minutes)- Specify the time budget for the dial-in user. The budget will be decreased automatically per callback connection. The default value 0 means no limitation of callback period.

My WAN IP

This field is only applicable when you select PPTP or L2TP w/ or w/out IPSec policy above. The default value is 0.0.0.0, which means the Vigor router will get a PPP IP address from the remote router during the IPCP negotiation phase. If the PPP IP address is fixed by remote side, specify the fixed IP address here.

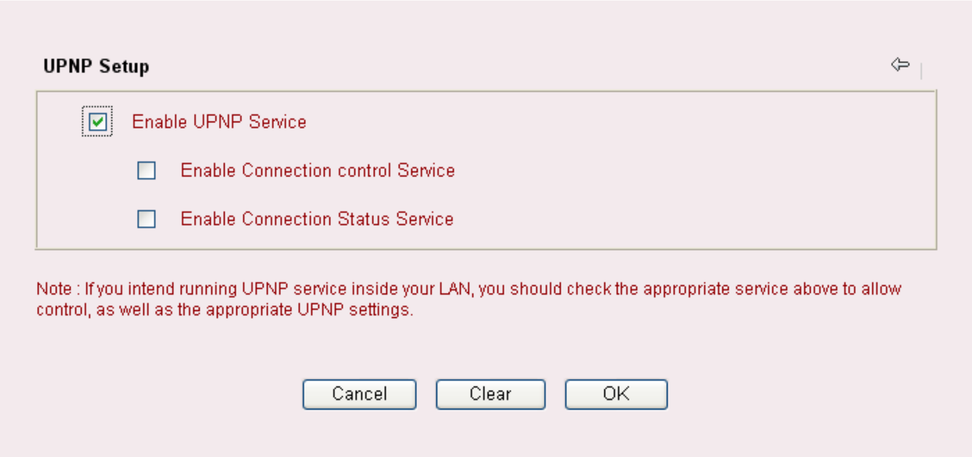
Remote Gateway IP

This field is only applicable when you select PPTP or L2TP w/ or w/out IPSec policy above. The default value is 0.0.0.0, which means the Vigor router will get a remote Gateway PPP IP address from the remote router during the IPCP negotiation

	phase. If the PPP IP address is fixed by remote side, specify the fixed IP address here.
Remote Network IP/ Remote Network Mask	Add a static router to direct all traffic destined to this Remote Network IP Address/ Remote Network Mask through the VPN connection. For IPSec, this is the destination clients IDs of phase 2 quick mode.
More	Add a static router to direct all traffic destined to more Remote Network IP Addresses/ Remote Network Mask through the VPN connection. This is usually used when you find there are several subnets behind the remote VPN router.
RIP Direction	The option specifies the direction of RIP (Routing Information Protocol) packets. You can enable/disable one of direction here. Herein, we provide four options: TX/RX Both, TX Only, RX Only, and Disable.
RIP Version	Select the RIP protocol version. Specify Ver. 2 for greatest compatibility.
For NAT operation, treat remote sub-net as	While communicating with remote subnet, the router can treat it as private subnet by sending packets with the router's private IP address, or treat it as public subnet by sending packets with the router's public IP address.

3.9 UPNP Service Setup

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


UPNP Setup

☑ Enable UPNP Service

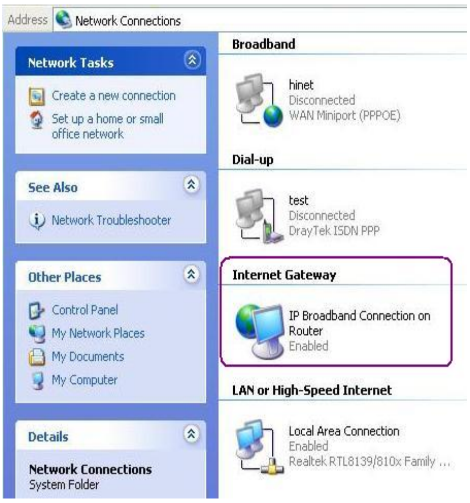
☐ Enable Connection control Service

☐ 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.



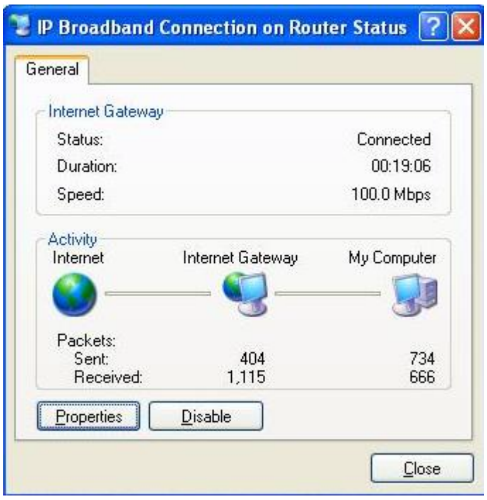
Network Connections
System Folder

Broadband
hinet
Disconnected
WAN Miniport (PPPOE)

Dial-up
test
Disconnected
DrayTek ISDN PPP

Internet Gateway
IP Broadband Connection on Router
Enabled

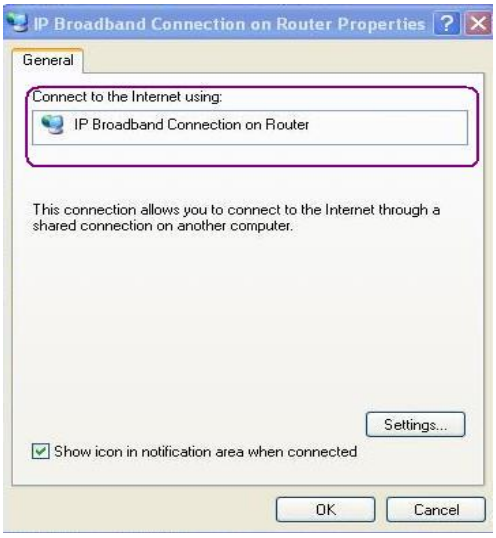
LAN or High-Speed Internet
Local Area Connection
Enabled
Realtek RTL8139/810x Family ...



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

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

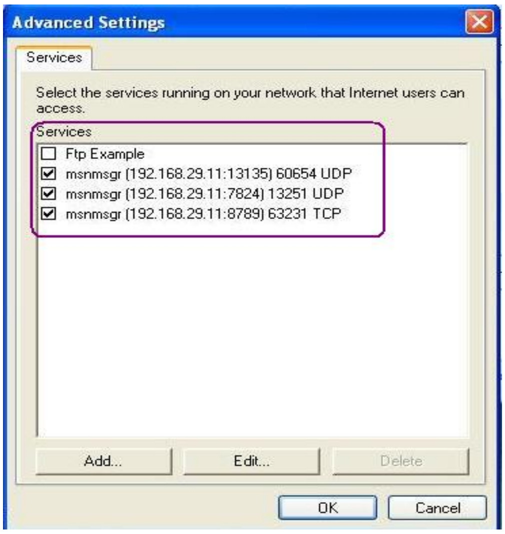
The UPnP facility on the router enables UPnP aware applications such as MSN Messenger to discover what are behind a NAT router. The application will also learn the external IP address and configure port mappings on the router. Subsequently, such a facility forwards packets from the external ports of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



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



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.

3.10 VoIP Setup

Note: This setting is available for V model series.

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

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

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

sip: user:password @ host: port

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

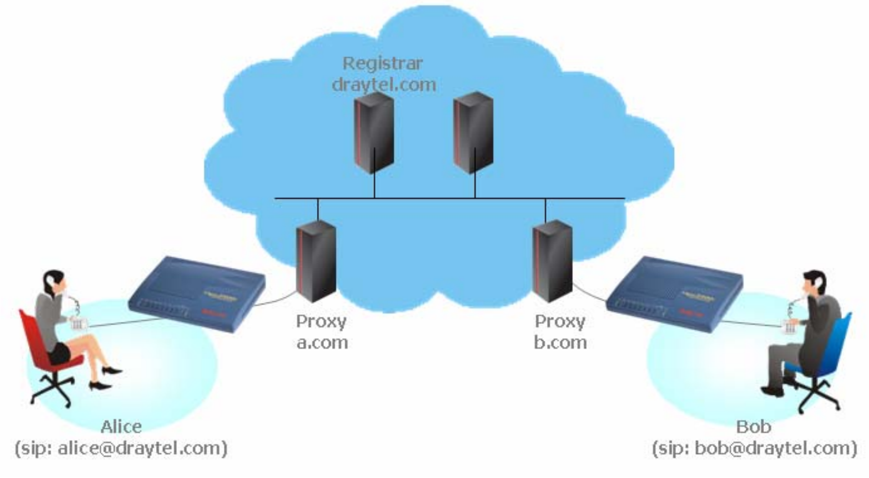
After a call is setup, the voice streams transmit via RTP (Real-Time Transport Protocol). Different codecs (methods to compress and encode the voice) can be embedded into RTP packets. Vigor V models provide various codecs, including G.711 A/μ-law, G.723, G.726 and G.729 A & B. Each codec uses a different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

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

- **Calling via SIP Servers**

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

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



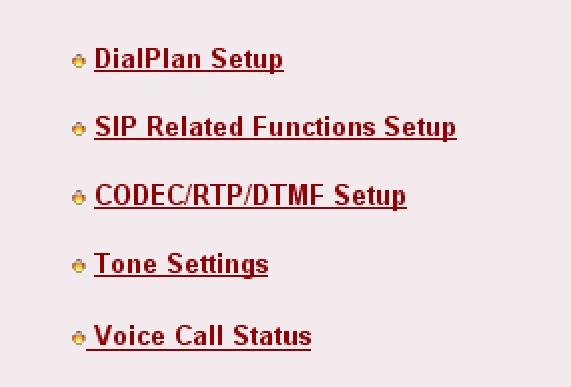
The major benefit of this mode is that you don't have to memorize your friend's IP address, which might change very frequently if it's dynamic. Instead of that, you will only have to using **dial plan** or directly dial your friend's **account name** if you are with the same SIP Registrar. Please refer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

- **Peer-to-Peer**

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

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

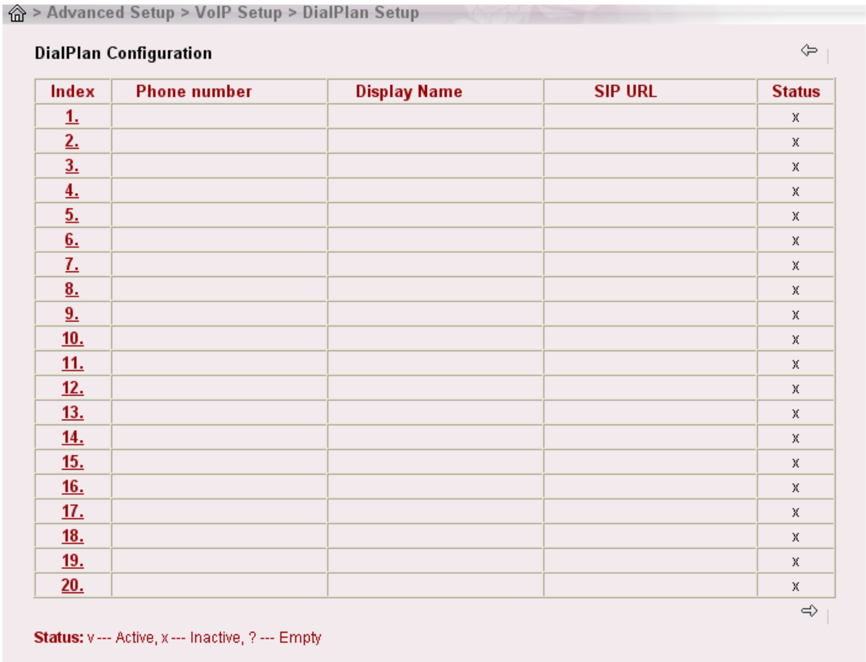
Click **VoIP Setup** on the **Advanced Setup** group. You will get the following page:



- DialPlan Setup
- SIP Related Functions Setup
- CODEC/RTP/DTMF Setup
- Tone Settings
- Voice Call Status

3.10.1 DialPlan Setup

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



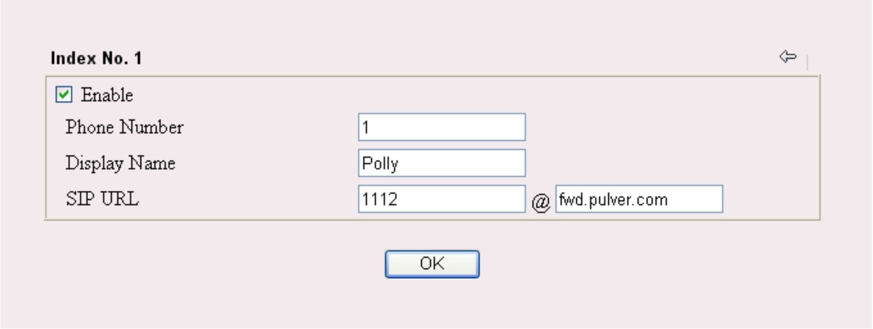
> Advanced Setup > VoIP Setup > DialPlan Setup

DialPlan Configuration

Index	Phone number	Display Name	SIP URL	Status
1.				x
2.				x
3.				x
4.				x
5.				x
6.				x
7.				x
8.				x
9.				x
10.				x
11.				x
12.				x
13.				x
14.				x
15.				x
16.				x
17.				x
18.				x
19.				x
20.				x

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

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



Index No. 1

☑ Enable

Phone Number	1
Display Name	Polly
SIP URL	1112 @ fwd.pulver.com

Enable Click this to enable this entry.

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

Display Name The Caller-ID that you want to be displayed on your friend’s screen. This let your friend can easily know who’s calling without memorizing lots of SIP URL Address.

SIP URL Enter your friend’s SIP Address.

Example 1:

If Tom gives you a SIP URL as **sip:1112@fwd.pulver.com** then you can input the number just as the previous figure, except you can change any number in the Phone Number field.

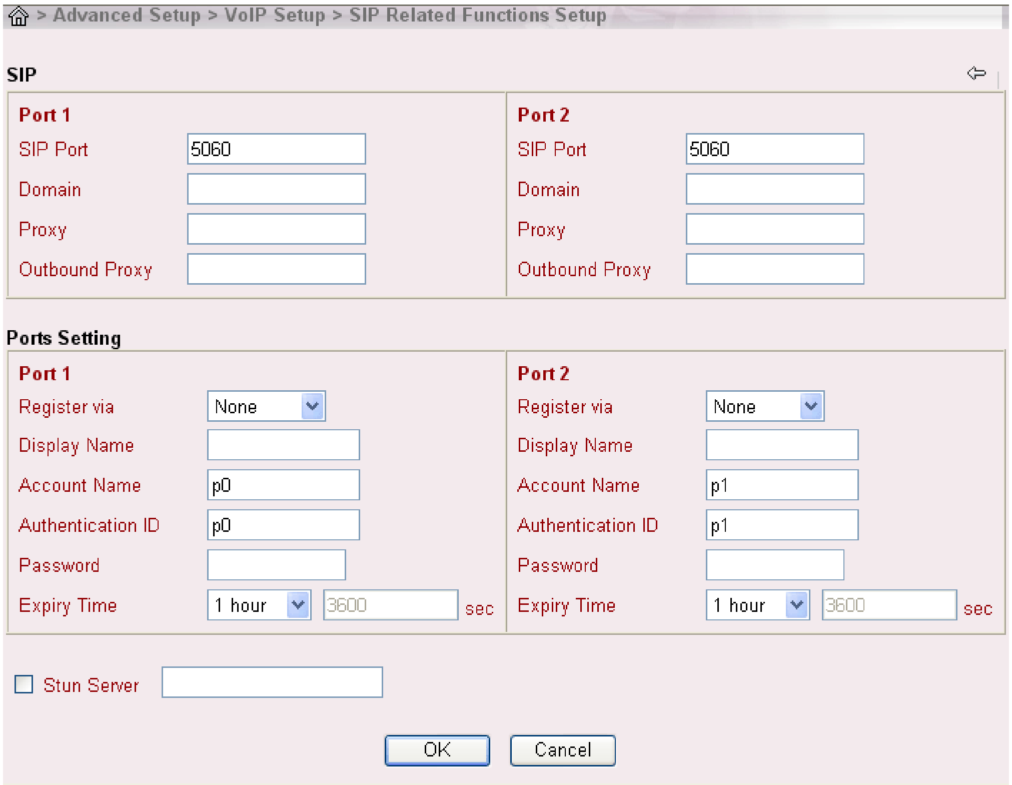
Example 2:

If Kevin gives you an IP address 203.69.175.16 only, then you can use keypad on the phone to dial directly as **#203*69*175*16#** to Kevin without setup any information on your DialPlan.

3.10.2 SIP Related Functions Setup

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

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



> Advanced Setup > VoIP Setup > SIP Related Functions Setup

SIP

Port 1		Port 2	
SIP Port	5060	SIP Port	5060
Domain		Domain	
Proxy		Proxy	
Outbound Proxy		Outbound Proxy	

Ports Setting

Port 1		Port 2	
Register via	None	Register via	None
Display Name		Display Name	
Account Name	p0	Account Name	p1
Authentication ID	p0	Authentication ID	p1
Password		Password	
Expiry Time	1 hour 3600 sec	Expiry Time	1 hour 3600 sec

□ Stun Server

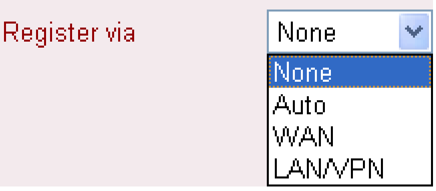
SIP Port The port number is used to send/receive SIP message for building a session. While the default value is 5060, you can change it to other number. However, this situation needs other party to change simultaneously to the same number.
By the time you can type**:port** number after the domain name to specify that port as the destination of data transmission (e.g., nat.draytel.org**:5065**)

Domain You can enter domain name or IP address of SIP Registrar server. For example, iptel.org or 195.37.77.101 is identical. You have to apply an account of SIP Registrar server before you can use it. However, it is not necessary to use sip registrar server function in order to use VoIP function.

Proxy You can enter IP address of SIP proxy server. For all SIP messages destined the **Domain** defined above, Vigor router will send to the **Proxy** and the **Proxy** will forward it.

Outbound Proxy You can enter IP address of outbound SIP proxy server. For all SIP messages, Vigor router will send to the **Outbound Proxy** and the will **Outbound Proxy** forward it.

Register via Select to specify IP address carried in the payload. If you want to make VoIP call without register personal information, please choose **None** and check the box to achieve the goal. Some SIP server allows user to use VoIP function without registering. For such server, please check the box of **make call without register**. Choosing **Auto** is recommended. The system will select a proper way for your VoIP call.



Register via None

Display Name You can enter any string as a display name in this field. This will be shown on the caller side.

Account Name You can enter the account name, usually the part of SIP URL before the character @ provided by your service provider or IP address for peer-to-peer connection.

Authentication ID You can enter the authentication ID provided by your service provider. Enter the name or number used for SIP Authorization with SIP Registrar.

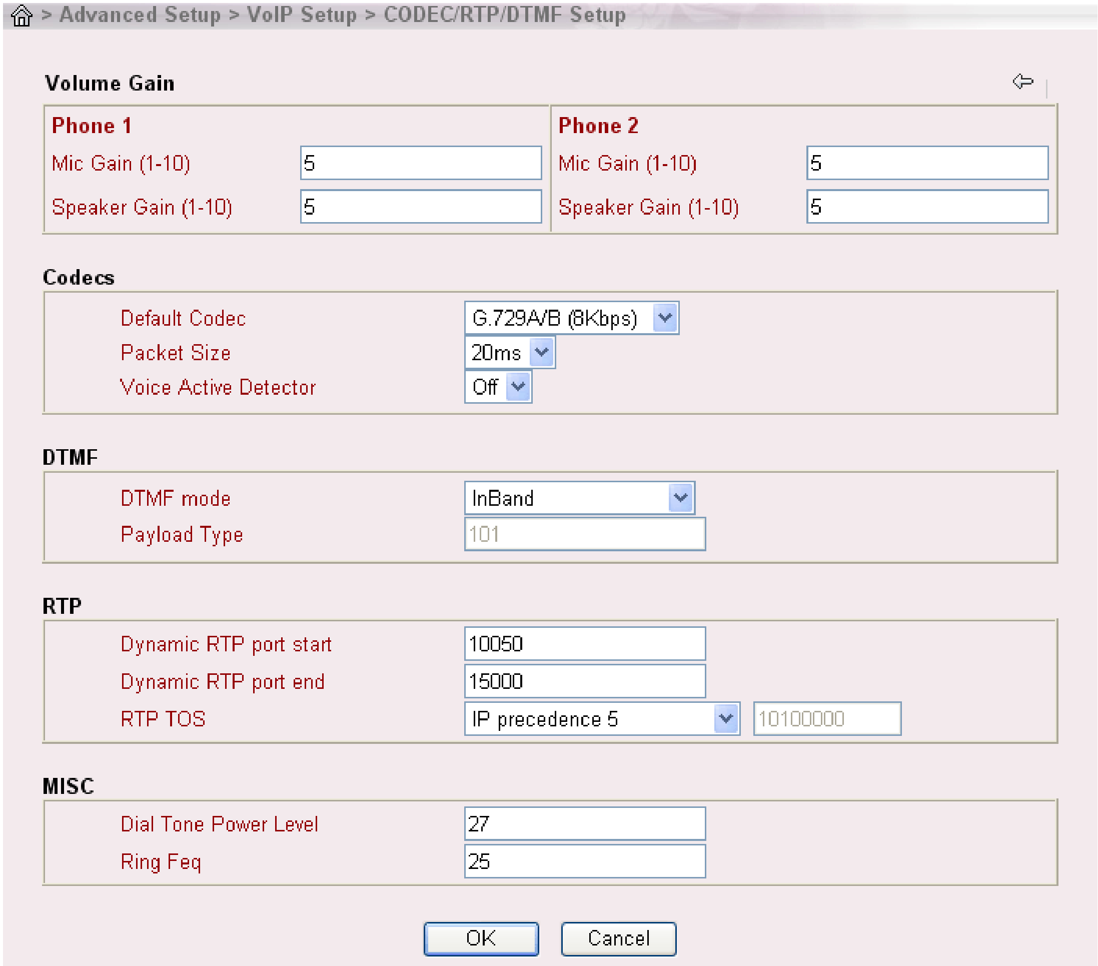
Password Enter the password when you use a SIP registrar server that needs password.

Expire Time The time duration that SIP registrar server keeps your registration record. Before the time expired, Vigor will issue another register message to registrar server again.

Stun server Check and enter the IP address of the STUN server if you are behind a NAT router.

3.10.3 CODEC/RTP/DTMF Setup

The codec used for each call can be negotiated with the peer party before each session.



> Advanced Setup > VoIP Setup > CODEC/RTP/DTMF Setup

Volume Gain

Phone 1		Phone 2	
Mic Gain (1-10)	5	Mic Gain (1-10)	5
Speaker Gain (1-10)	5	Speaker Gain (1-10)	5

Codecs

Default Codec	G.729A/B (8Kbps)
Packet Size	20ms
Voice Active Detector	Off

DTMF

DTMF mode	InBand
Payload Type	101

RTP

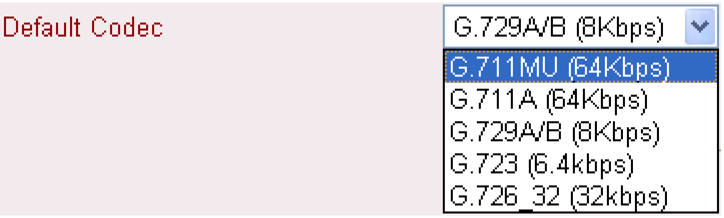
Dynamic RTP port start	10050	
Dynamic RTP port end	15000	
RTP TOS	IP precedence 5	10100000

MISC

Dial Tone Power Level	27
Ring Feq	25

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

Default Codec There are five different CODECs you can choose as your prefer CODEC that you wish to use. However, the real CODEC be used was negotiate with peer party before session was established. The default CODEC is G.729A/B; it occupied less bandwidth while still have good voice quality. It is better for you to have at least 256Kbps upstream if you would like to use G.711.



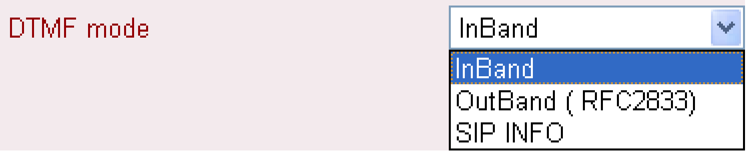
Default Codec: G.729A/B (8Kbps)

NOTE: If your upstream speed only supports 64Kbps, do not use G.711 CODEC.

Packet Size The amount of data contains in a single packets (10, 20, 30, 40, 50 and 60). The default value is 20 ms, it means the data packet will contains 20 ms voice information. The more data contains in a single packet the less overhead it creates but may increase.

Voice Active Detector Choose **On** to enable this function to detect if the user is talking or not. If it is silent, the Vigor router will take action to save the bandwidth.

DTMF Mode **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.



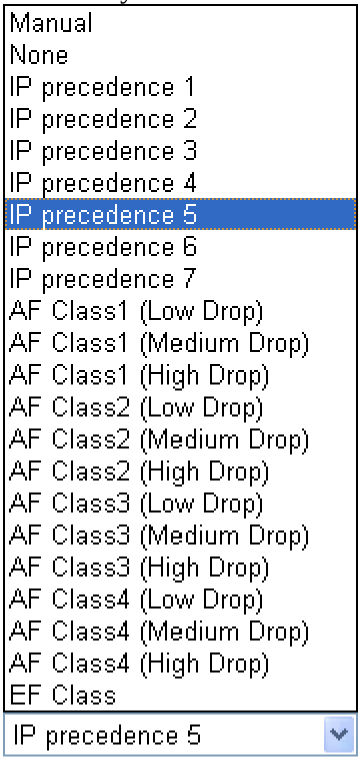
DTMF mode InBand

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

Dynamic RTP port start Specify the start port for RTP stream. The default value is 10050.

Dynamic RTP port end Specify the end port for RTP stream. The default value is 15000.

RTP TOS It decides the level of VoIP package. Use the drop down list to choose any one of them.



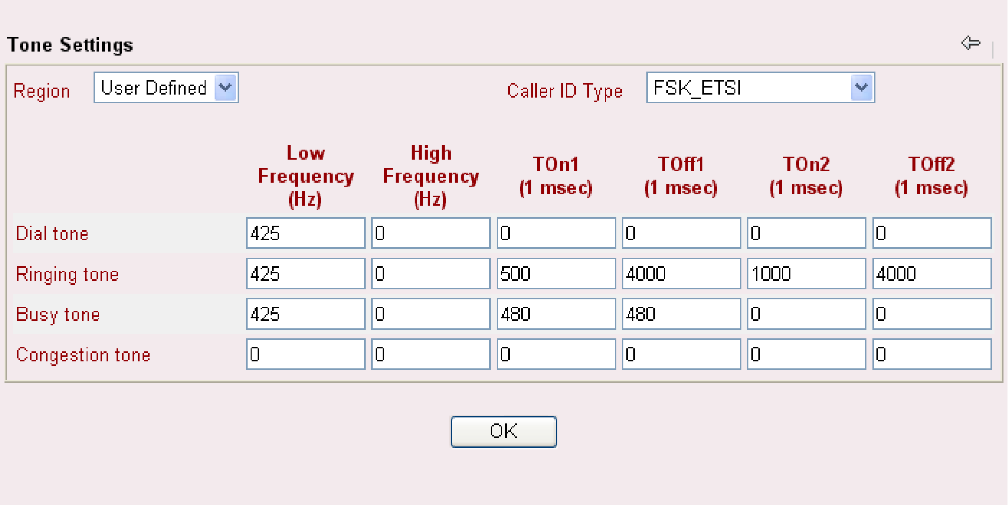
IP precedence 5

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

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

3.10.4 Tone Settings

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

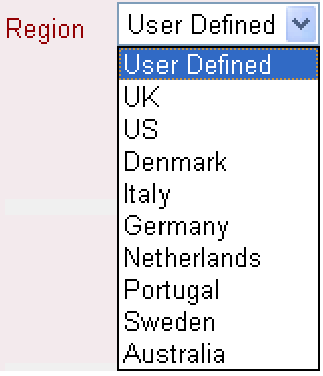


Tone Settings

Region: User Defined   Caller ID Type: FSK_ETSI

	Low Frequency (Hz)	High Frequency (Hz)	TOn1 (1 msec)	TOff1 (1 msec)	TOn2 (1 msec)	TOff2 (1 msec)
Dial tone	425	0	0	0	0	0
Ringing tone	425	0	500	4000	1000	4000
Busy tone	425	0	480	480	0	0
Congestion tone	0	0	0	0	0	0

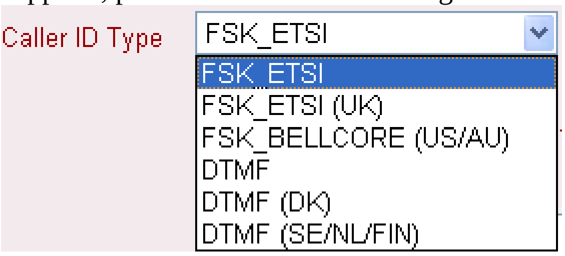
Region Select the proper region which you are located. The common settings of **Caller ID Type**, **Dial tone**, **Ringing tone**, **Busy tone** and **Congestion tone** will be shown automatically on the page.



Region: User Defined

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

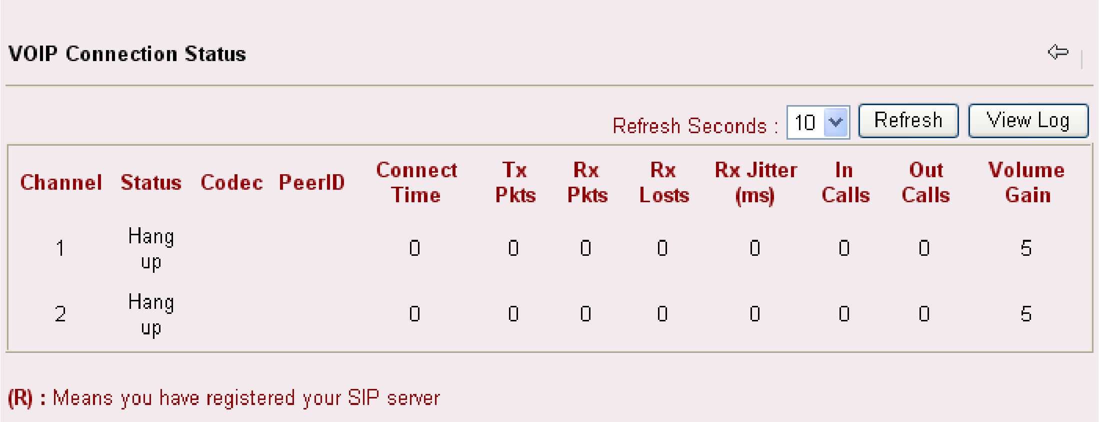
Caller ID Type There are several standards provided here for displaying the caller ID on the panel of the telephone set. Choose the one that is suitable for the phone set according to the area of the router installed. If you don't know what standard that the phone set supports, please use the default setting.



Caller ID Type: FSK_ETSI

3.10.5 Voice Call Status

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



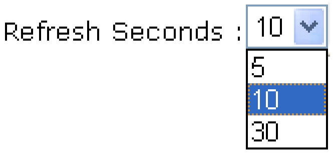
VOIP Connection Status

Refresh Seconds : 10

Channel	Status	Codec	PeerID	Connect Time	Tx Pkts	Rx Pkts	Rx Losts	Rx Jitter (ms)	In Calls	Out Calls	Volume Gain
1	Hang up			0	0	0	0	0	0	0	5
2	Hang up			0	0	0	0	0	0	0	5

(R) : Means you have registered your SIP server

Refresh Seconds Specify the interval of refresh time to obtain the latest VoIP calling information. The information will update immediately when the Refresh button is clicked.



Refresh Seconds : 10

Refresh Update current VoIP communication status.

Channel It shows current connection status for the port of VoIP1 and VoIP2.

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

Codec Indicates the voice codec employed by present channel.

PeerID The present in-call or out-call peer ID (the format may be IP or Domain).

Connect Time The format is represented as seconds.

Tx Pkts Total number of transmitted voice packets during this connection session.

Rx Pkts Total number of received voice packets during this connection session.

Rx Losts Total number of lost packets during this connection session.

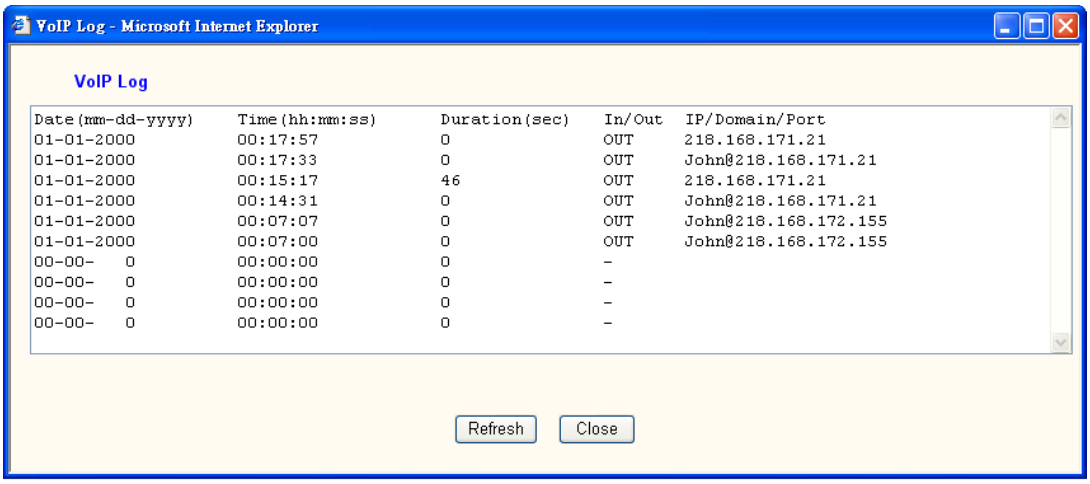
Rx Jitter The jitter of received voice packets.

In Calls The accumulating in-call times.

Out Calls The accumulating out-call times.

Volume Gain The volume of present call.

Log Display logs of VoIP calls.

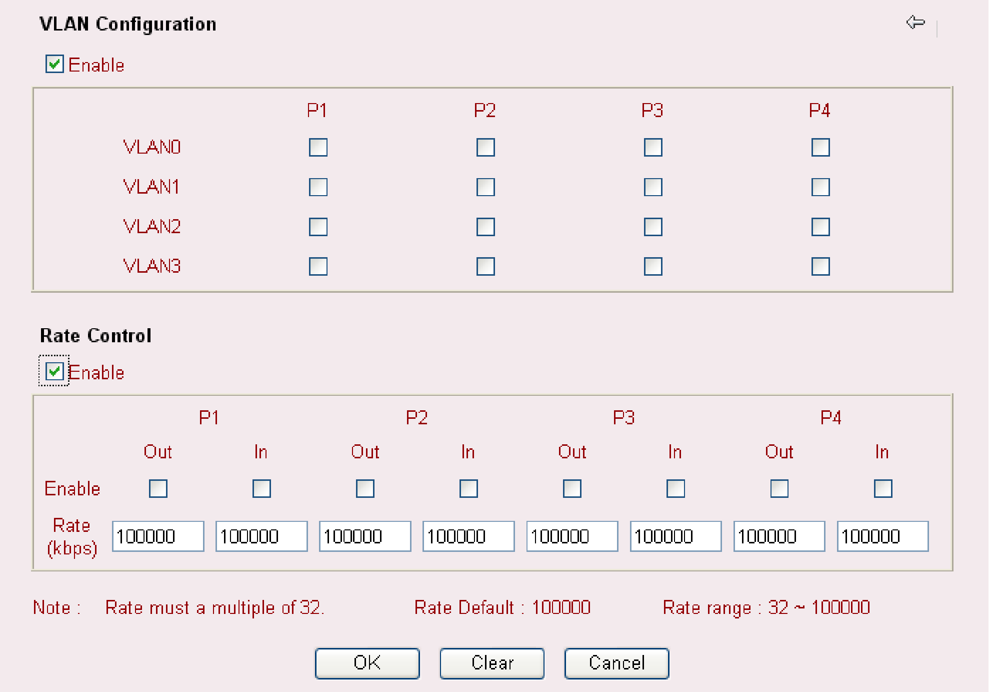


VoIP Log

```
Date(mm-dd-yyyy)    Time(hh:mm:ss)     Duration(sec)    In/Out   IP/Domain/Port
01-01-2000          00:17:57           0                OUT      218.168.171.21
01-01-2000          00:17:33           0                OUT      John@218.168.171.21
01-01-2000          00:15:17           46               OUT      218.168.171.21
01-01-2000          00:14:31           0                OUT      John@218.168.171.21
01-01-2000          00:07:07           0                OUT      John@218.168.172.155
01-01-2000          00:07:00           0                OUT      John@218.168.172.155
00-00-    0         00:00:00           0                -
00-00-    0         00:00:00           0                -
00-00-    0         00:00:00           0                -
00-00-    0         00:00:00           0                -
```

3.11 VLAN/Rate Control

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. Click **VLAN/Rate Control** on the **Advanced Setup** group. The following page will appear. Click **Enable** to invoke VLAN function. **Rate Control** manages the transmission rate of data in and out through the router.



VLAN Configuration

☑ Enable

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

Rate Control

☑ Enable

	P1		P2		P3		P4	
	Out	In	Out	In	Out	In	Out	In
Enable	□	□	□	□	□	□	□	□
Rate (kbps)	100000	100000	100000	100000	100000	100000	100000	100000

Note : Rate must a multiple of 32. Rate Default : 100000 Rate range : 32 ~ 100000

Enable Check this box to enable this function (for VLAN Configuration).

P1 – P4 Check the box to make the computer connecting to the port being grouped in specified VLAN. Be aware that each port can be grouped in different VLAN at the same time only if you check the box. For example, if you check the boxes of VLAN0-P1 and VLAN1-P1, you can make P1 to be grouped under VLAN0 and VLAN1 simultaneously.

VLAN0-3 This router allows you to set 4 groups of virtual LAN.

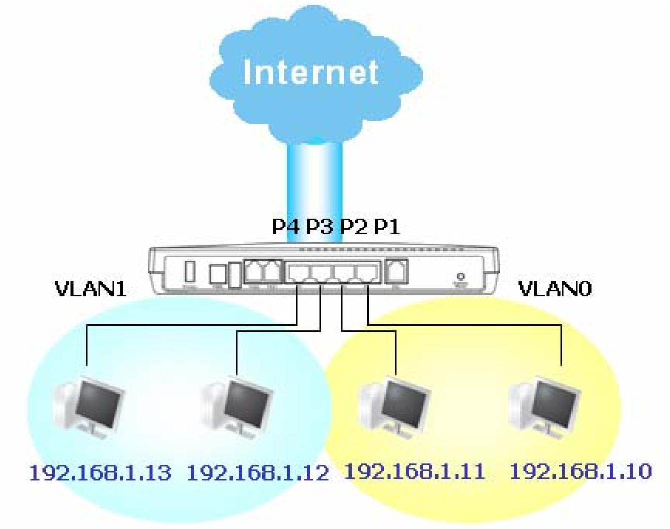
Enable(for Rate Control) Check this box to enable this function (for Rate Control). The rate control will limit the transmission rate for data in and out. Check the corresponding boxes to enable the rate control function for different ports.

Out It decides the rate of data transmission for output. When you check the box of **Enable**, please also decide the rate by using the drop down list of **Rate**.

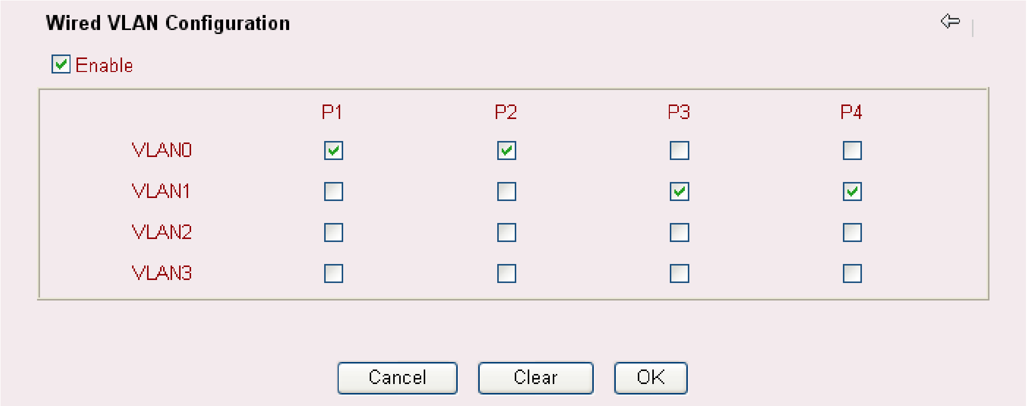
In It decides the rate of data transmission for input. When you check the box of **Enable**, please also decide the rate by using the drop down list of **Rate**.

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.



Wired VLAN Configuration

☑ Enable

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

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

3.12 QoS Control Setup

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

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

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

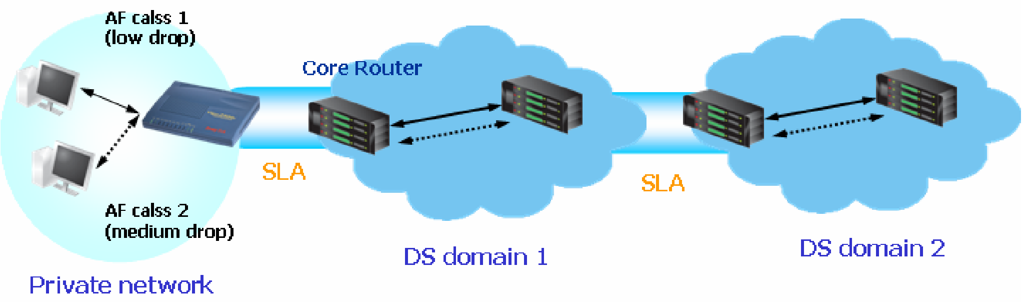
There are two components within Primary configuration of QoS deployment:

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

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

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

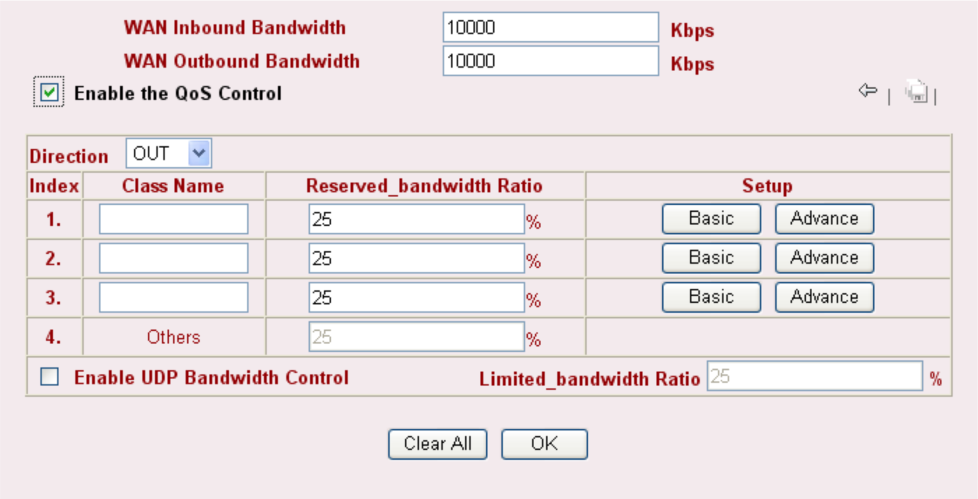
Vigor routers as edge routers of DS domain shall check the marked DSCP value in the IP header of bypassing traffic, thus to allocate certain amount of resource execute appropriate policing, classification or scheduling. The core routers in the backbone will do the same checking before executing treatments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



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

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

Click on **QoS Control** on the **Advanced Setup** group. The following screen will appear.



WAN Inbound Bandwidth 10000 Kbps

WAN Outbound Bandwidth 10000 Kbps

☑ Enable the QoS Control

Direction OUT

Index	Class Name	Reserved_bandwidth Ratio	Setup
1.		25 %	Basic Advance
2.		25 %	Basic Advance
3.		25 %	Basic Advance
4.	Others	25 %	

□ Enable UDP Bandwidth Control Limited_bandwidth Ratio 25 %

Clear All OK

WAN Inbound Bandwidth Type the inbound bandwidth for WAN interface.

WAN Outbound Bandwidth Type the outbound bandwidth for WAN interface.

Enable the QoS Control For V models, the factory default for this is checked to enable.

Direction Define which traffic the QoS Control settings apply to.
IN- apply to incoming traffic only.
OUT-apply to outgoing traffic only.
BOTH- apply to both incoming and outgoing traffic.

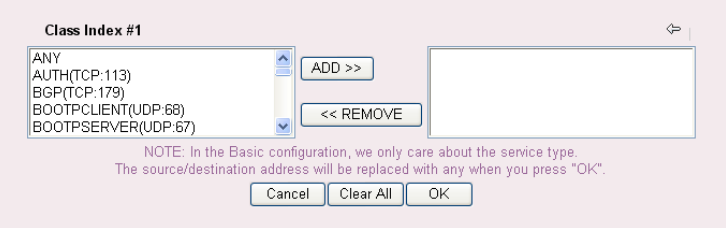
Index The group index number of QoS Control settings. There are total 4 groups.

Class Name Define the name for the group index.

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

Setup There are two-level of settings:

Basic - setup Reserved Bandwidth Ratio according to the traffic service type. We provide a list of common service types. Click this button to open basic configuration for each index number.



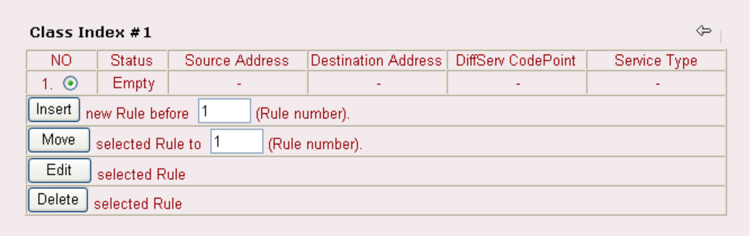
Class Index #1

- ANY
- AUTH(TCP:113)
- BGP(TCP:179)
- BOOTPCLIENT(UDP:68)
- BOOTPSERVER(UDP:67)

NOTE: In the Basic configuration, we only care about the service type.
The source/destination address will be replaced with any when you press "OK".

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

Advance - custom setting of Reserved Bandwidth Ratio based on the source address, destination address, DiffServ CodePoint, and service type. Click this button to open advanced configuration for each index number**.** You can insert, move, edit or delete select rule in this page.



Class Index #1

NO	Status	Source Address	Destination Address	DiffServ CodePoint	Service Type
1. ●	Empty	-	-	-	-

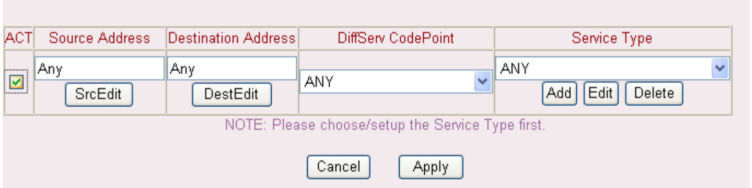
Insert new Rule before 1 (Rule number).

Move selected Rule to 1 (Rule number).

Edit selected Rule

Delete selected Rule

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

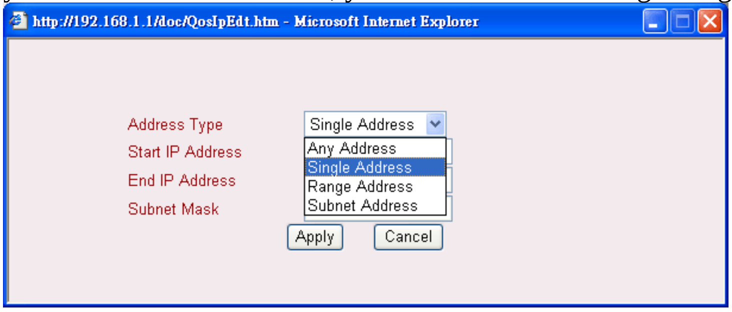


ACT	Source Address	Destination Address	DiffServ CodePoint	Service Type
☑	Any SrcEdit	Any DestEdit	ANY	ANY Add Edit Delete

NOTE: Please choose/setup the Service Type first.

SrcEdit - allows you to edit source address information.

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

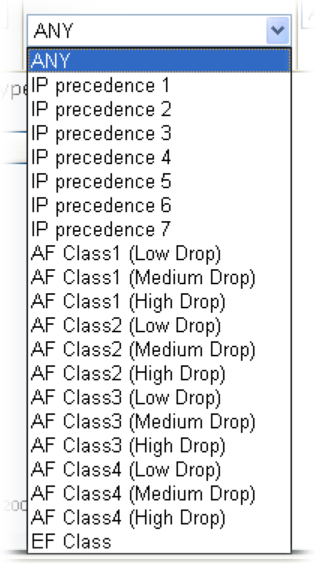


http://192.168.1.1/doc/QosIpEdt.htm - Microsoft Internet Explorer

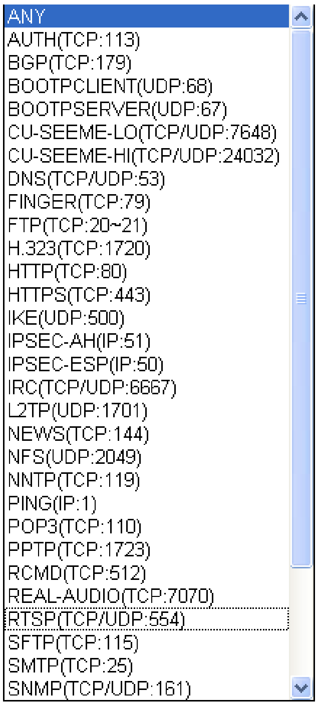
Address Type: Single Address

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

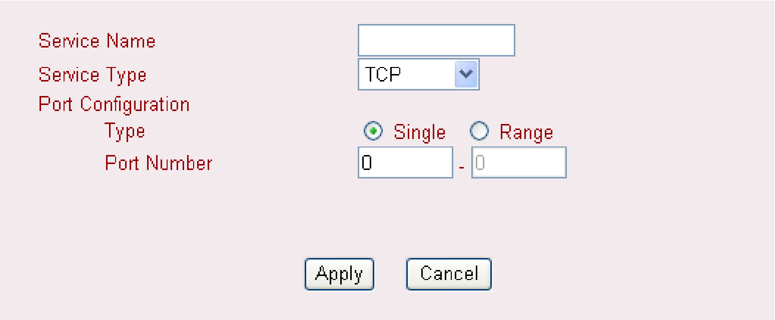
DiffServ CodePoint – all the packets of data will be divided with different levels and will be processed according to the level type by the system. Please assign one of the levels of the data for processing with QoS control.



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



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



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

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

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

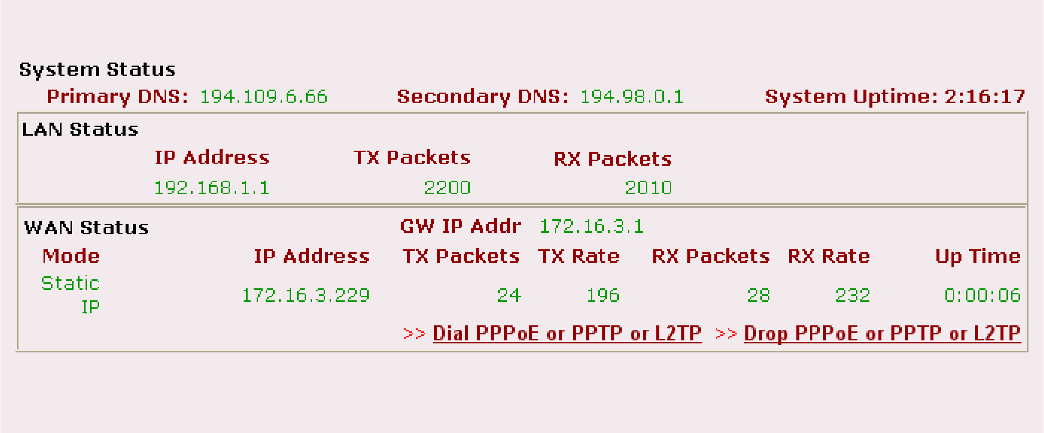
Limited_bandwidth Ratio The ratio typed here is used to limit the total bandwidth of UDP application.

This page is left blank.

4 System Management

4.1 Online Status

The **Online 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

Primary DNS: 194.109.6.66   Secondary DNS: 194.98.0.1   System Uptime: 2:16:17

LAN Status

IP Address	TX Packets	RX Packets
192.168.1.1	2200	2010

WAN Status   GW IP Addr 172.16.3.1

Mode	IP Address	TX Packets	TX Rate	RX Packets	RX Rate	Up Time
Static IP	172.16.3.229	24	196	28	232	0:00:06

>> Dial PPPoE or PPTP or L2TP   >> Drop PPPoE or PPTP or L2TP

Primary DNS Displays the assigned IP address of the primary DNS.

Secondary DNS Displays the assigned IP address of the secondary DNS.

IP Address (in LAN) Displays the IP address of the LAN interface.

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

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

GW IP Addr Displays the assigned IP address of the default gateway.

IP Address (in WAN) Displays the IP address of the WAN interface.

TX Packets(in WAN) Displays the total transmitted packets at the WAN interface.

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

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

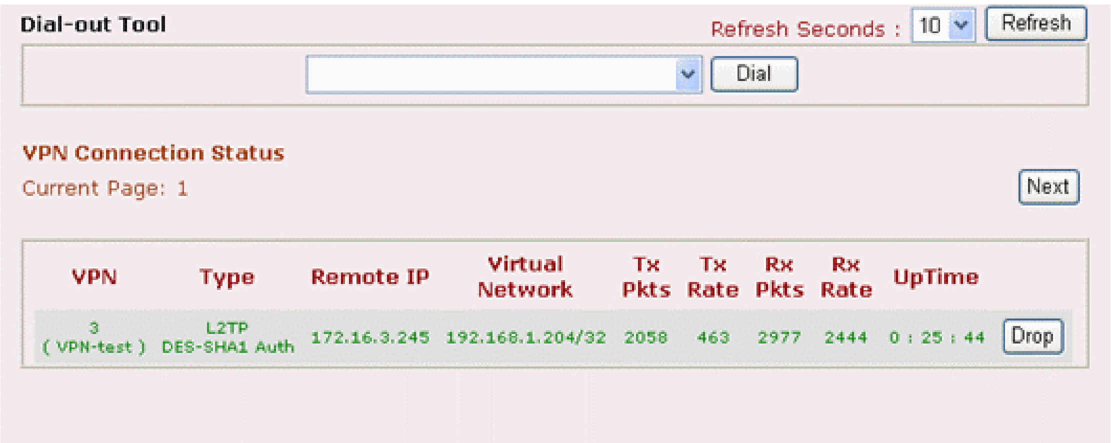
RX Rate Displays the speed of received packets at the WAN interface.

Up Time Displays the total system uptime of the interface.

State Displays the DSL line status.

4.2 VPN Connection Management

Once the VPN configuration is completed, any traffic from local LAN to remote LAN will trigger the VPN connection. Or you can use VPN Connection Management in System Management to direct **Dial** or connect a VPN from dial-out router. Once the link is OK, the VPN connection status/information will be shown in **VPN Connection Management** page. A **Drop** button will let you to disconnect the link.



VPN Connection Status

Current Page: 1

VPN	Type	Remote IP	Virtual Network	Tx Pkts	Tx Rate	Rx Pkts	Rx Rate	UpTime	
3 (VPN-test)	L2TP DES-SHA1 Auth	172.16.3.245	192.168.1.204/32	2058	463	2977	2444	0 : 25 : 44	Drop

VPN Displays the VPN connection name.

Type Displays the VPN connection type.

Remote IP Displays the remote IP of VPN connection.

Virtual Network Displays the IP address and subnet mask of virtual network.

Tx Pkts Displays the total transmitted packets.

Tx Rate Displays the speed of transmitted packets.

Rx Pkets Displays the total number of received packets.

Rx Rate Displays the speed of received packets

Uptime Displays the total system uptime of the VPN connection.

Drop Disconnects the VPN connection.

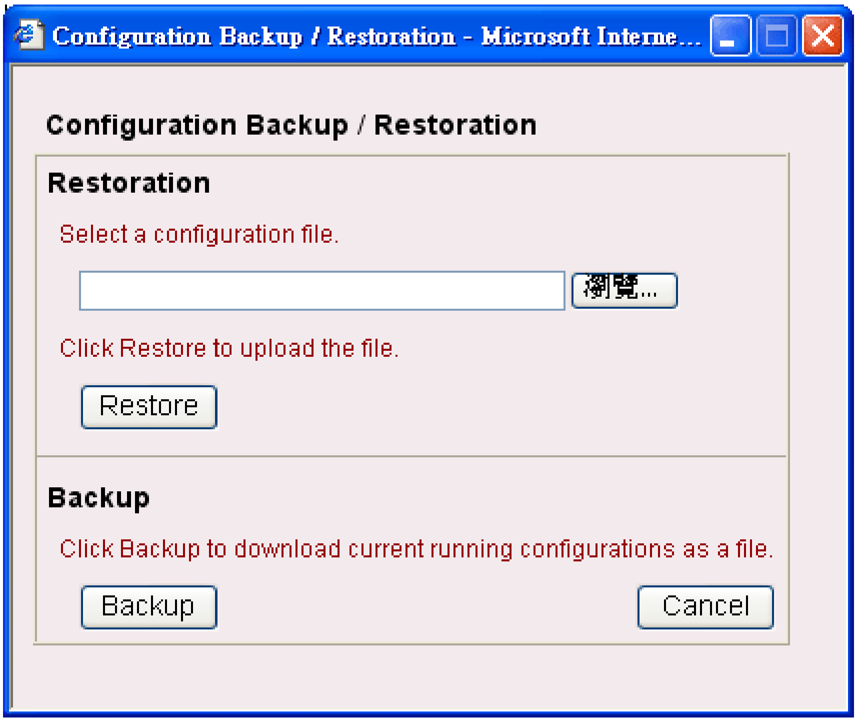
4.3 Configuration Backup/Restoration

Sometimes you want to keep running configurations of your current router as a file or restore the configurations with the file. The router provides a web-based way to let you backup or restore the configuration very simple.

Backup the Configuration

Follow the steps below to backup your configuration.

1. Click **Configuration Backup/Restoration** on the **System Management** group. The following window will be popped-up.



Configuration Backup / Restoration - Microsoft Interne...

Configuration Backup / Restoration

Restoration

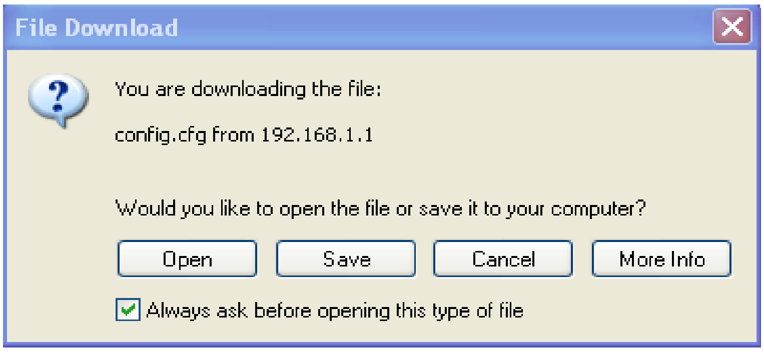
Select a configuration file.

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.



File Download

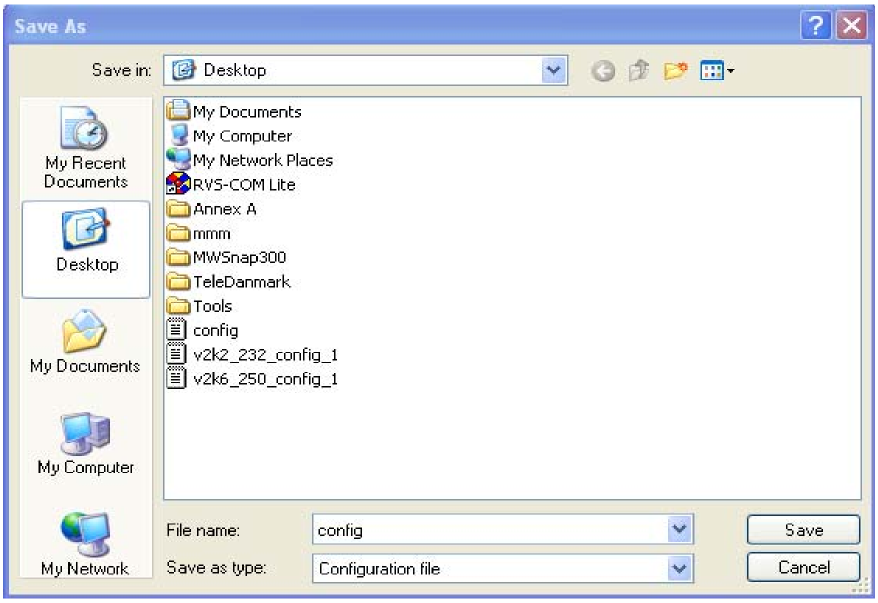
You are downloading the file:

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. Click **Save** button to open another dialog for saving configuration as a file. In **Save As** dialog, the default filename is **config.cfg**. You could give it another name by yourself.



File name: config

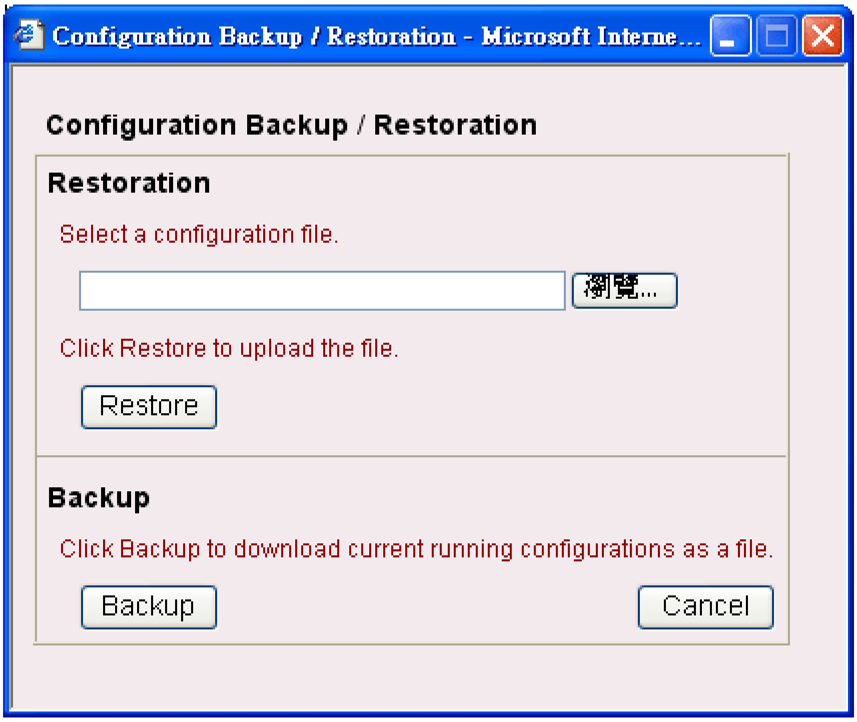
Save as type: Configuration file

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.

Restore Configuration

1. Click **Configuration Backup/Restoration** on the **System Management** group. The following window will be popped-up.



Configuration Backup / Restoration - Microsoft Interne...

Configuration Backup / Restoration

Restoration

Select a configuration file.

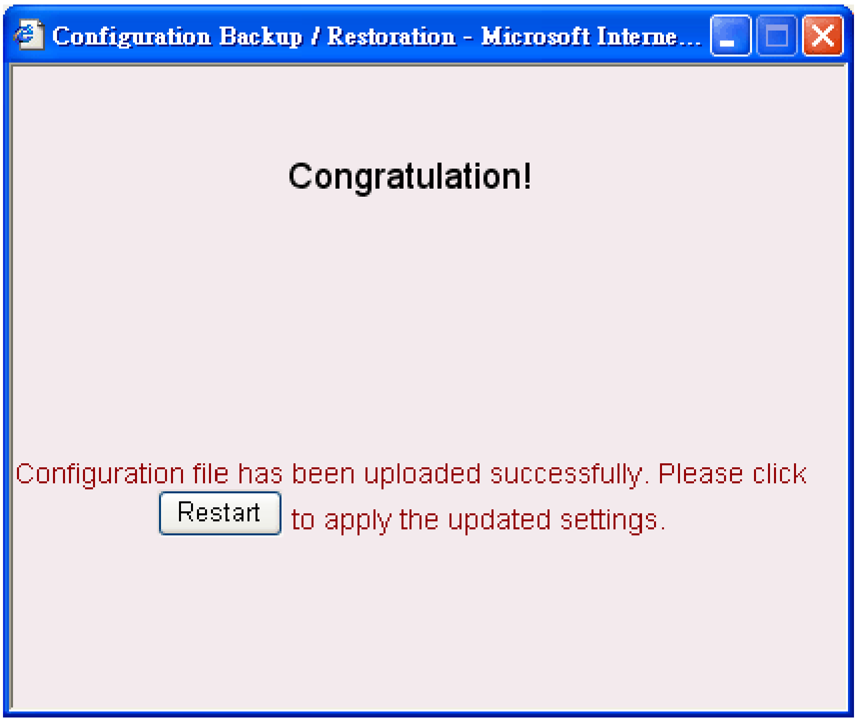
Click Restore to upload the file.

Backup

Click Backup to download current running configurations as a file.

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

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



Configuration Backup / Restoration - Microsoft Interne...

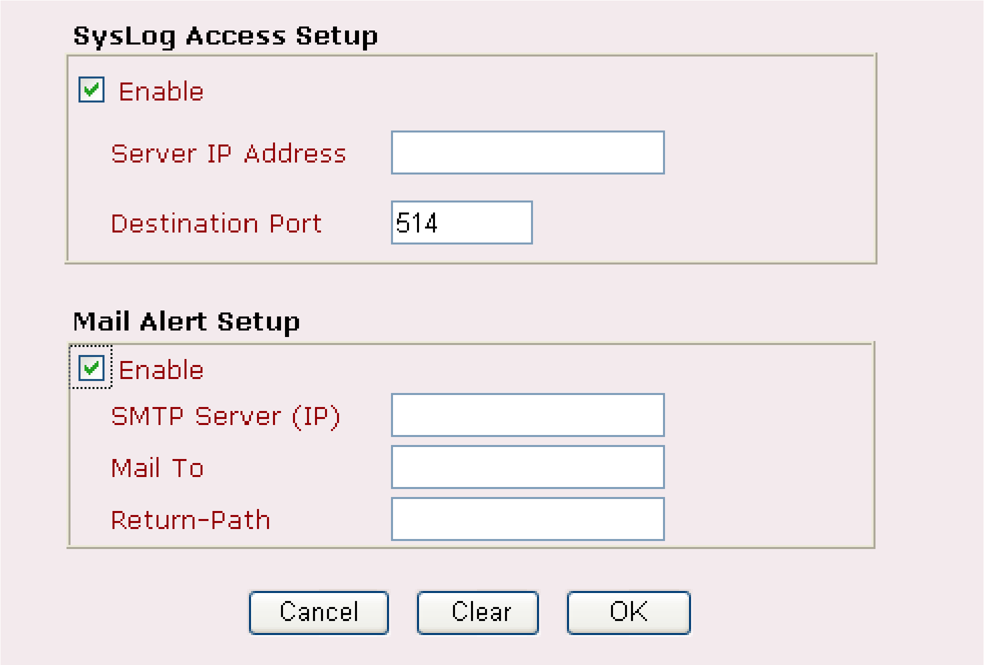
Congratulation!

Configuration file has been uploaded successfully. Please click Restart to apply the updated settings.

4.4 SysLog/Mail Alert Setup

SysLog is a popular utility in Unix world. To monitor router activity, you can run a SysLog Daemon to capture all activities from the router. This Daemon program can run on a local PC or a remote one elsewhere on the Internet. In addition, the Vigor routers provide the Mail Alert facility so that the SysLog messages can be packed as an e-mail for someone who wants to receive these messages. In the following, we explain how to setup the SysLog and mail alert functions.

Click **SysLog/Mail Alert Setup** on the **System Management** group.



SysLog Access Setup

☑ Enable

Server IP Address

Destination Port 514

Mail Alert Setup

☑ Enable

SMTP Server (IP)

Mail To

Return-Path

Enable(Syslog Access) Check the **Enable** box to activate the SysLog service.

Server IP Address Specify an IP address to which all SysLog messages will be sent.

Destination Port Specify a UDP port number to which the SysLog server is listening. The default value is 514.

Enable(Mail Alert) Check the **Enable** box to activate the mail alert service.

SMTP Server (IP) Specify an IP address of the SMTP server which can send mails from your Vigor router to the recipients' mailboxes directly.

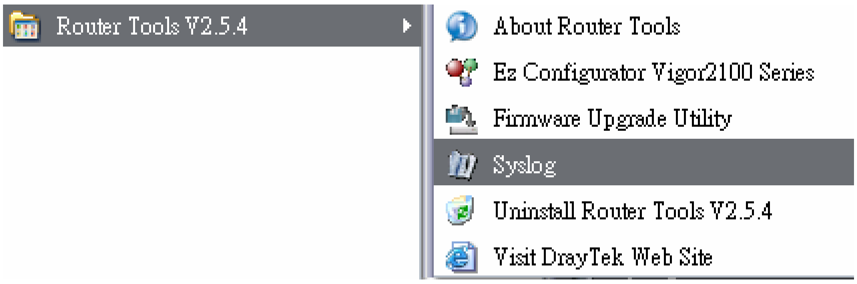
Mail To Specify an e-mail address of the recipient's mailbox to which all SysLog messages will be sent. The recipient could be an administrator who intends to view or analyze the SysLog messages.

Return-Path Specify an e-mail address of another mailbox to accept all returned messages if some fatal problems occur at the recipient mailbox.

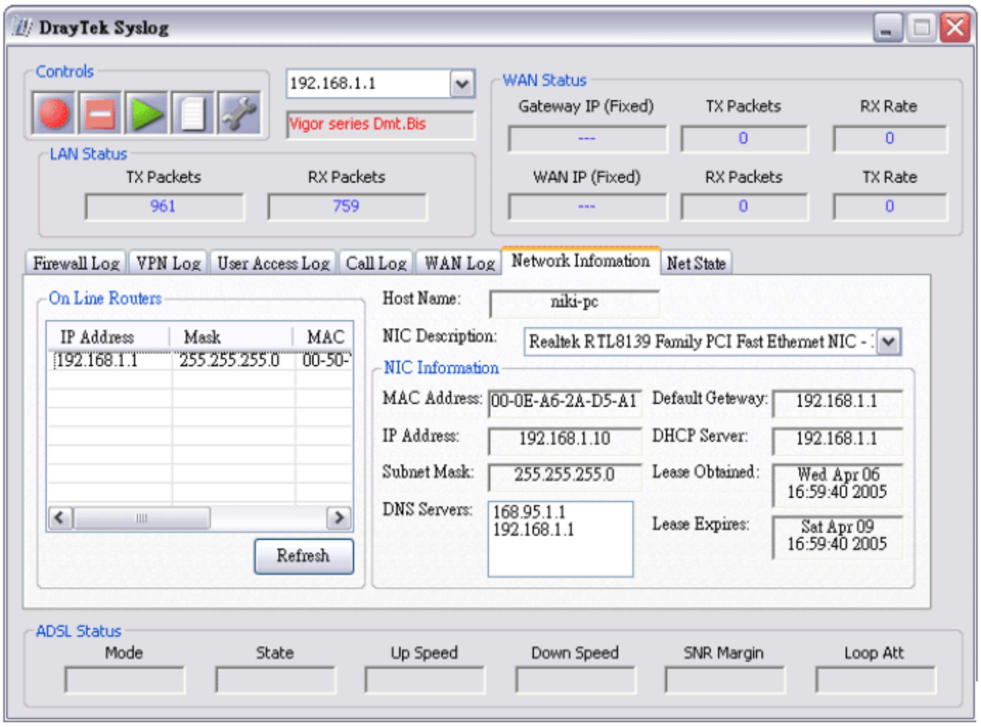
For viewing the Syslog, please do the following:

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

Controls: 192.168.1.1 — Vigor series Dmt.Bis

LAN Status: TX Packets 961, RX Packets 759

WAN Status: Gateway IP (Fixed) ---, TX Packets 0, RX Rate 0; WAN IP (Fixed) ---, RX Packets 0, TX Rate 0

Firewall Log | VPN Log | User Access Log | Call Log | WAN Log | Network Infomation | Net State

On Line Routers

IP Address	Mask	MAC
192.168.1.1	255.255.255.0	00-50-

Refresh

Host Name: niki-pc

NIC Description: Realtek RTL8139 Family PCI Fast Ethernet NIC -

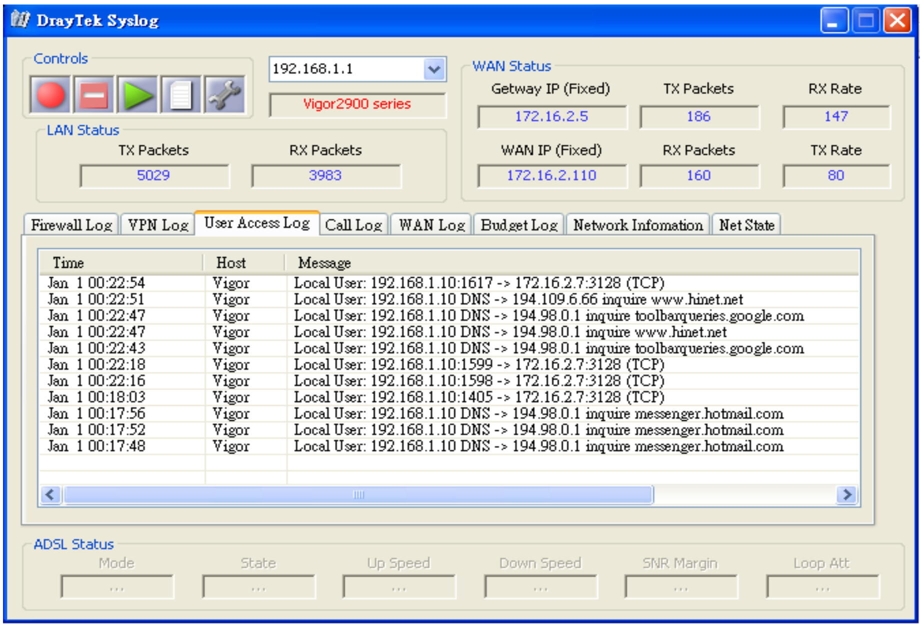
NIC Information

MAC Address: 00-0E-A6-2A-D5-A1
Default Geteway: 192.168.1.1
IP Address: 192.168.1.10
DHCP Server: 192.168.1.1
Subnet Mask: 255.255.255.0
Lease Obtained: Wed Apr 06 16:59:40 2005
DNS Servers: 168.95.1.1 192.168.1.1
Lease Expires: Sat Apr 09 16:59:40 2005

ADSL Status: Mode, State, Up Speed, Down Speed, SNR Margin, Loop Att

The Vigor router will send many types of SysLog messages. Some examples of the SysLog messages with their individual formats are shown below.

An example of User Access log message:



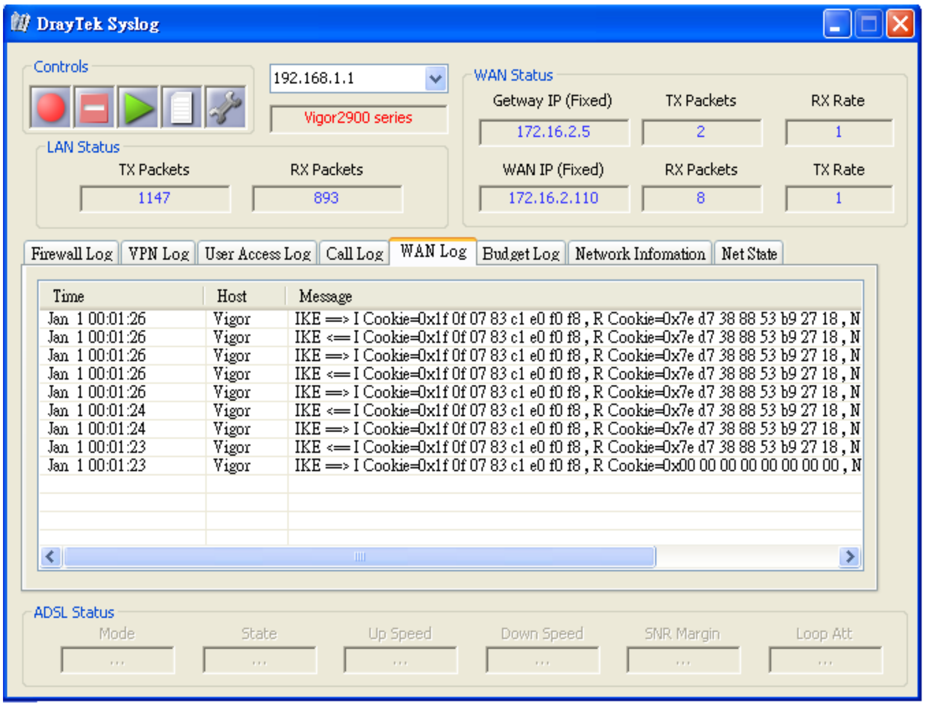
192.168.1.1

WAN Status: Getway IP (Fixed) 172.16.2.5, TX Packets 186, RX Rate 147, WAN IP (Fixed) 172.16.2.110, RX Packets 160, TX Rate 80

LAN Status: TX Packets 5029, RX Packets 3983

```
Time              Host     Message
Jan  1 00:22:54   Vigor    Local User: 192.168.1.10:1617 -> 172.16.2.7:3128 (TCP)
Jan  1 00:22:51   Vigor    Local User: 192.168.1.10 DNS -> 194.109.6.66 inquire www.hinet.net
Jan  1 00:22:47   Vigor    Local User: 192.168.1.10 DNS -> 194.98.0.1 inquire toolbarqueries.google.com
Jan  1 00:22:47   Vigor    Local User: 192.168.1.10 DNS -> 194.98.0.1 inquire www.hinet.net
Jan  1 00:22:43   Vigor    Local User: 192.168.1.10 DNS -> 194.98.0.1 inquire toolbarqueries.google.com
Jan  1 00:22:18   Vigor    Local User: 192.168.1.10:1599 -> 172.16.2.7:3128 (TCP)
Jan  1 00:22:16   Vigor    Local User: 192.168.1.10:1598 -> 172.16.2.7:3128 (TCP)
Jan  1 00:18:03   Vigor    Local User: 192.168.1.10:1405 -> 172.16.2.7:3128 (TCP)
Jan  1 00:17:56   Vigor    Local User: 192.168.1.10 DNS -> 194.98.0.1 inquire messenger.hotmail.com
Jan  1 00:17:52   Vigor    Local User: 192.168.1.10 DNS -> 194.98.0.1 inquire messenger.hotmail.com
Jan  1 00:17:48   Vigor    Local User: 192.168.1.10 DNS -> 194.98.0.1 inquire messenger.hotmail.com
```

An example of WAN log message to record the status of VPN/IPSec tunnel:



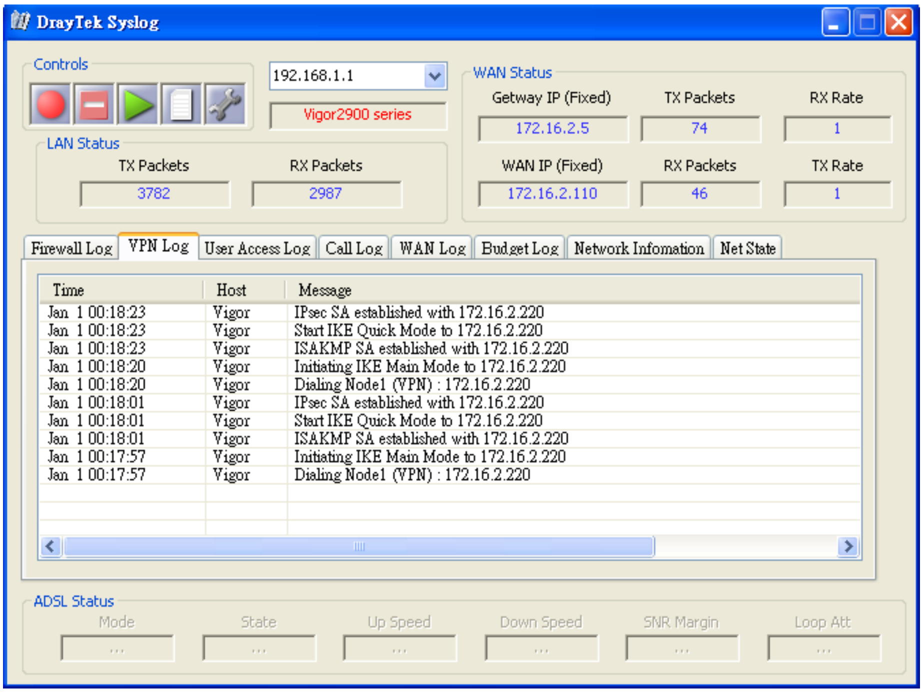
192.168.1.1

WAN Status: Getway IP (Fixed) 172.16.2.5, TX Packets 2, RX Rate 1, WAN IP (Fixed) 172.16.2.110, RX Packets 8, TX Rate 1

LAN Status: TX Packets 1147, RX Packets 893

```
Time              Host     Message
Jan  1 00:01:26   Vigor    IKE ==> I Cookie=0x1f 0f 07 83 c1 e0 f0 f8 , R Cookie=0x7e d7 38 88 53 b9 27 18 , N
Jan  1 00:01:26   Vigor    IKE <== I Cookie=0x1f 0f 07 83 c1 e0 f0 f8 , R Cookie=0x7e d7 38 88 53 b9 27 18 , N
Jan  1 00:01:26   Vigor    IKE ==> I Cookie=0x1f 0f 07 83 c1 e0 f0 f8 , R Cookie=0x7e d7 38 88 53 b9 27 18 , N
Jan  1 00:01:26   Vigor    IKE <== I Cookie=0x1f 0f 07 83 c1 e0 f0 f8 , R Cookie=0x7e d7 38 88 53 b9 27 18 , N
Jan  1 00:01:26   Vigor    IKE ==> I Cookie=0x1f 0f 07 83 c1 e0 f0 f8 , R Cookie=0x7e d7 38 88 53 b9 27 18 , N
Jan  1 00:01:24   Vigor    IKE <== I Cookie=0x1f 0f 07 83 c1 e0 f0 f8 , R Cookie=0x7e d7 38 88 53 b9 27 18 , N
Jan  1 00:01:24   Vigor    IKE ==> I Cookie=0x1f 0f 07 83 c1 e0 f0 f8 , R Cookie=0x7e d7 38 88 53 b9 27 18 , N
Jan  1 00:01:23   Vigor    IKE <== I Cookie=0x1f 0f 07 83 c1 e0 f0 f8 , R Cookie=0x7e d7 38 88 53 b9 27 18 , N
Jan  1 00:01:23   Vigor    IKE ==> I Cookie=0x1f 0f 07 83 c1 e0 f0 f8 , R Cookie=0x00 00 00 00 00 00 00 00 , N
```

An example of VPN (IPSec) log message to record the status of the VPN/IPSec tunnel:



192.168.1.1

Vigor2900 series

Getway IP (Fixed)	TX Packets	RX Rate
172.16.2.5	74	1
WAN IP (Fixed)	**RX Packets**	**TX Rate**
172.16.2.110	46	1

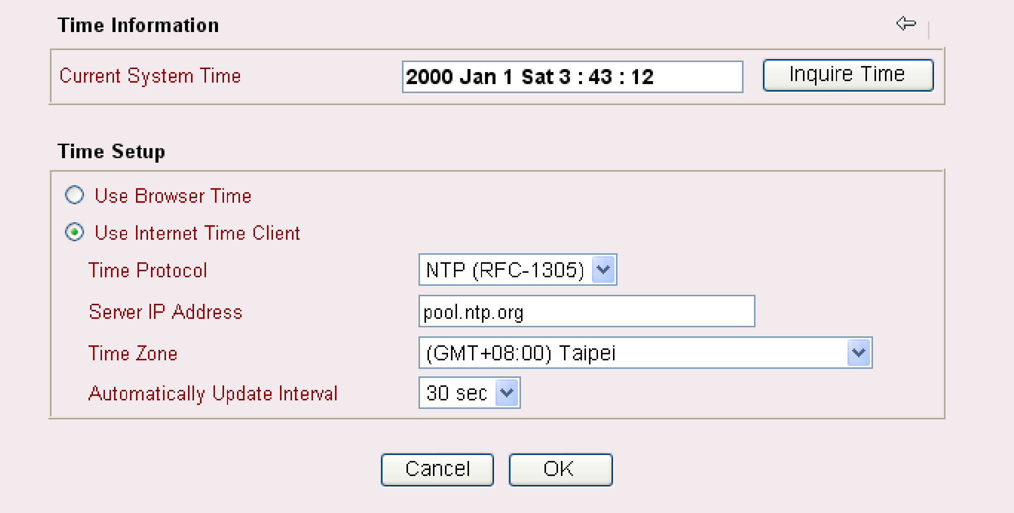
TX Packets	RX Packets
3782	2987

```
Time             Host    Message
Jan  1 00:18:23  Vigor   IPsec SA established with 172.16.2.220
Jan  1 00:18:23  Vigor   Start IKE Quick Mode to 172.16.2.220
Jan  1 00:18:23  Vigor   ISAKMP SA established with 172.16.2.220
Jan  1 00:18:20  Vigor   Initiating IKE Main Mode to 172.16.2.220
Jan  1 00:18:20  Vigor   Dialing Node1 (VPN) : 172.16.2.220
Jan  1 00:18:01  Vigor   IPsec SA established with 172.16.2.220
Jan  1 00:18:01  Vigor   Start IKE Quick Mode to 172.16.2.220
Jan  1 00:18:01  Vigor   ISAKMP SA established with 172.16.2.220
Jan  1 00:17:57  Vigor   Initiating IKE Main Mode to 172.16.2.220
Jan  1 00:17:57  Vigor   Dialing Node1 (VPN) : 172.16.2.220
```

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

4.5 Time Setup

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



Time Information

Current System Time	2000 Jan 1 Sat 3 : 43 : 12	Inquire Time

Time Setup

○ Use Browser Time

● Use Internet Time Client

Time Protocol	NTP (RFC-1305)
Server IP Address	pool.ntp.org
Time Zone	(GMT+08:00) Taipei
Automatically Update Interval	30 sec

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 sever.

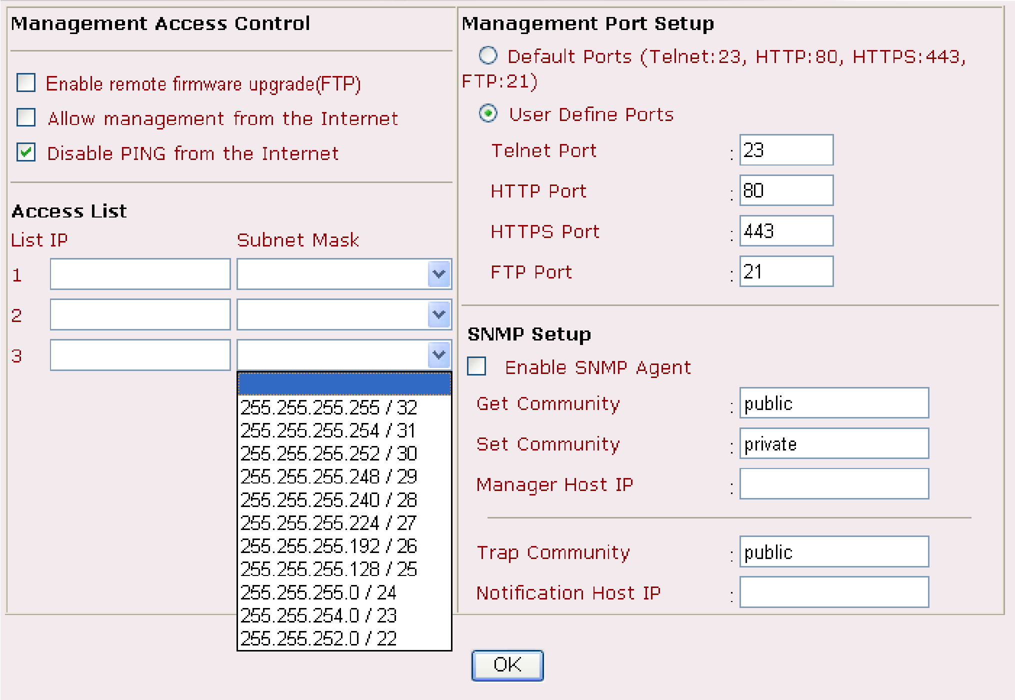
Time Zone Select the time zone where the router is located.

Automatically Update Interval Select a time interval for updating from the NTP server.

Click **OK** to save these settings.

4.6 Management Setup

The port number 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.



Management Access Control

☐ Enable remote firmware upgrade(FTP)
☐ Allow management from the Internet
☑ Disable PING from the Internet

Access List

List IP		Subnet Mask
1		
2		
3		

255.255.255.255 / 32
255.255.255.254 / 31
255.255.255.252 / 30
255.255.255.248 / 29
255.255.255.240 / 28
255.255.255.224 / 27
255.255.255.192 / 26
255.255.255.128 / 25
255.255.255.0 / 24
255.255.254.0 / 23
255.255.252.0 / 22

Management Port Setup

○ Default Ports (Telnet:23, HTTP:80, HTTPS:443, FTP:21)
● User Define Ports

Telnet Port : 23
HTTP Port : 80
HTTPS Port : 443
FTP Port : 21

SNMP Setup

☐ Enable SNMP Agent

Get Community : public
Set Community : private
Manager Host IP :

Trap Community : public
Notification Host IP :

Enable remote firmware upgrade
Chick the checkbox to allow remote firmware upgrade through FTP (File Transfer Protocol).

Allow management from the Internet
Enable the checkbox to allow system administrators to login from the Internet. By default, it is not allowed.

Disable PING from the Internet
Check the checkbox to reject all PING packets from the Internet. For security issue, this function is enabled by default.

Access List
You could specify that the system administrator can only login from a specific host or network defined in the list. A maximum of three IPs/subnet masks is allowed.
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 and HTTP servers.

Enable SNMP Agent
Check it to enable this function.

Get Community
Set the name for getting community by typing a proper character. The default setting is **public.**

Set Community
Set community by typing a proper name. The default setting is **private.**

Manager Host IP
Set one host as the manager to execute SNMP function. Please type in IP address to specify certain host.

Trap Community Set trap community by typing a proper name. The default setting is **public.**

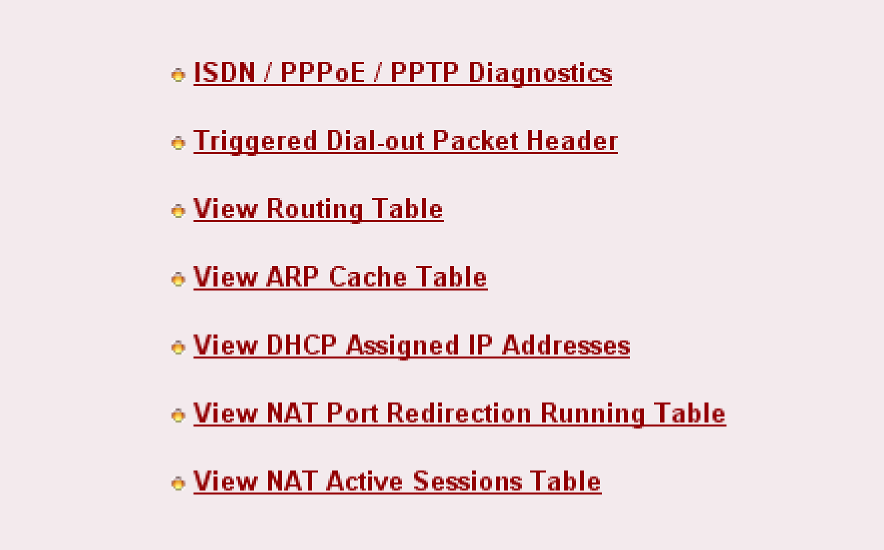
Notification Host IP Set the IP address of the host that will receive the trap community.

Trap Timeout The default setting is 10 seconds.

4.7 Diagnostic Tools

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

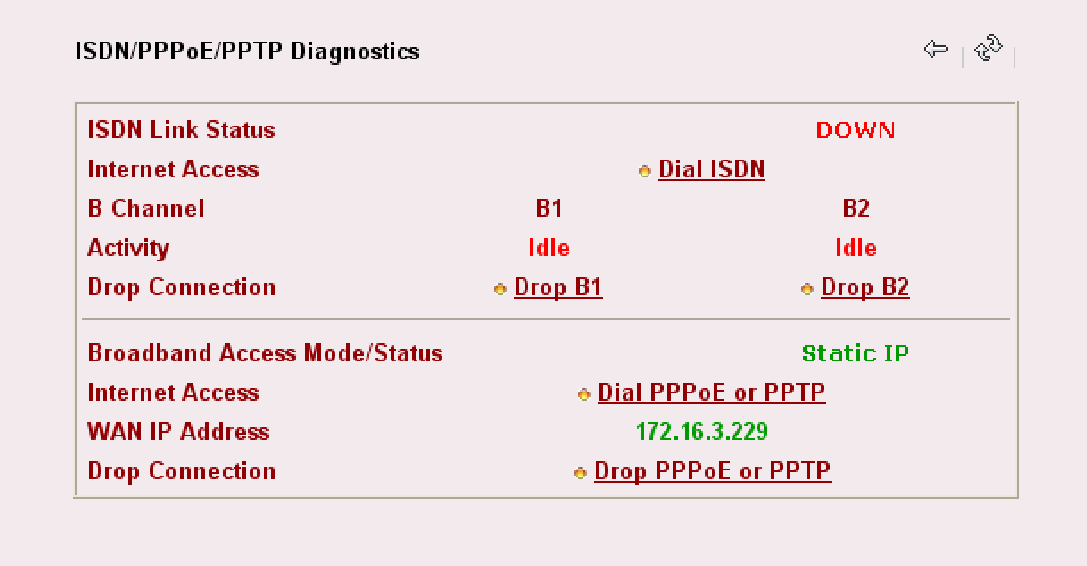
Below shows the menu items for Diagnostics.



- ISDN / PPPoE / PPTP Diagnostics
- Triggered Dial-out Packet Header
- View Routing Table
- View ARP Cache Table
- View DHCP Assigned IP Addresses
- View NAT Port Redirection Running Table
- View NAT Active Sessions Table

4.7.1 ISDN/PPPoE/PPTP Diagnostics

Click **Diagnostics** and click **WAN Connection** to open the web page. For different model of the router, this page might change slightly.



ISDN/PPPoE/PPTP Diagnostics

ISDN Link Status		DOWN
Internet Access	Dial ISDN	
B Channel	B1	B2
Activity	Idle	Idle
Drop Connection	Drop B1	Drop B2
Broadband Access Mode/Status		Static IP
Internet Access	Dial PPPoE or PPTP	
WAN IP Address	172.16.3.229	
Drop Connection	Drop PPPoE or PPTP	

⟳ To obtain the latest information, click here to reload the page.

ISDN Link Status If the link is active, this field will show **UP**. Otherwise, it shows **DOWN**.

Dial ISDN Clicking here causes the router to dial to the preset ISP. Click **Internet Access Setup > Dial to a Single ISP** to configure dial-up settings.

Activity Display the connection name for each B channel. If the B channel is idle, it will show **Idle**.

Drop B1 Click it to disconnect the B1 channel.

Drop B2 Click it to disconnect the B2 channel.

Broadband Access Mode/Status Display the broadband access mode and status. If the broadband connection is active, it will show Internet access mode is enabled. If the connection is idle, it will show "---".

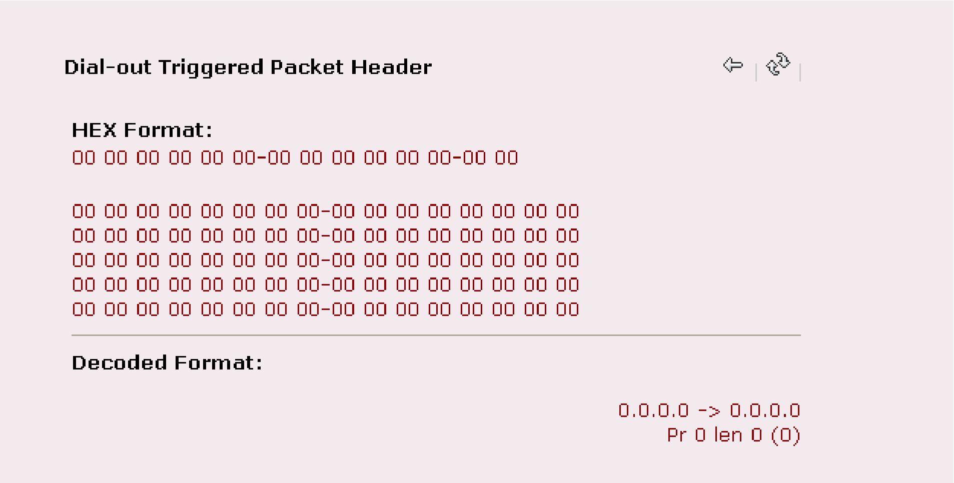
WAN IP Address The WAN IP address for the active connection.

Dial PPPoE or PPPoA Click it to force the router to establish a PPPoE or PPPoA connection.

Drop PPPoE or PPTP Click it to force the router to disconnect the current active PPPoE or PPTP connection.

4.7.2 Triggered Dial-out Packet Header

Triggered Dial-out Packet Header shows the last IP packet header that triggered the router to dial out. Click **Triggered Dial-out Packet Header** to view the triggered dial-out packet header.



Dial-out Triggered Packet Header

HEX Format:

```
00 00 00 00 00 00-00 00 00 00 00 00-00 00

00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00
```

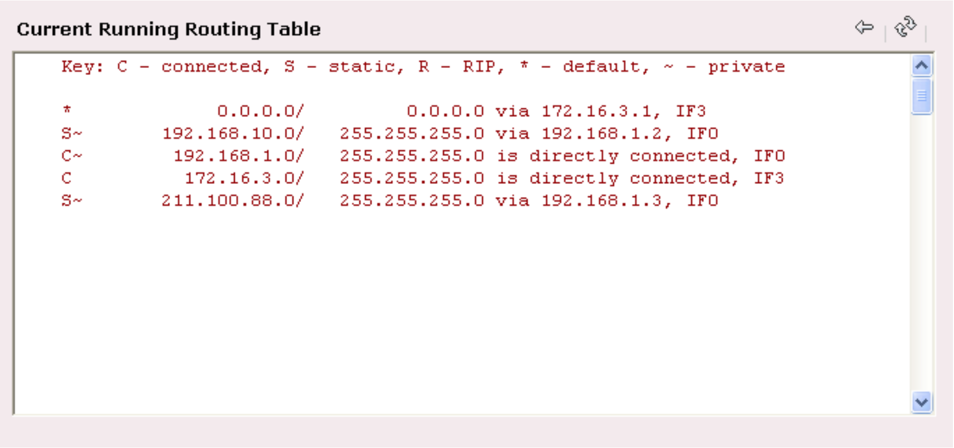
Decoded Format:

```
0.0.0.0 -> 0.0.0.0
 Pr 0 len 0 (0)
```

Click it to reload the page.

4.7.3 Viewing Routing Table

Click **View Routing Table** to view the routing table of your Vigor router. The table provides current IP routing information held in the router.



Current Running Routing Table

```
Key: C - connected, S - static, R - RIP, * - default, ~ - private

*           0.0.0.0/         0.0.0.0 via 172.16.3.1, IF3
S~       192.168.10.0/   255.255.255.0 via 192.168.1.2, IF0
C~        192.168.1.0/   255.255.255.0 is directly connected, IF0
C          172.16.3.0/   255.255.255.0 is directly connected, IF3
S~       211.100.88.0/   255.255.255.0 via 192.168.1.3, IF0
```

Click it to reload the page.

In the left of each routing rule, you will see a key. These keys are defined as follows.

C --- Directly connected.

S --- Static route.

R --- RIP.

***** --- Default route.

~ --- Routes for private routing domain.

In the right of each routing rule, you will see an interface identifier which is defined as follows.

IF0 --- Local LAN interface.

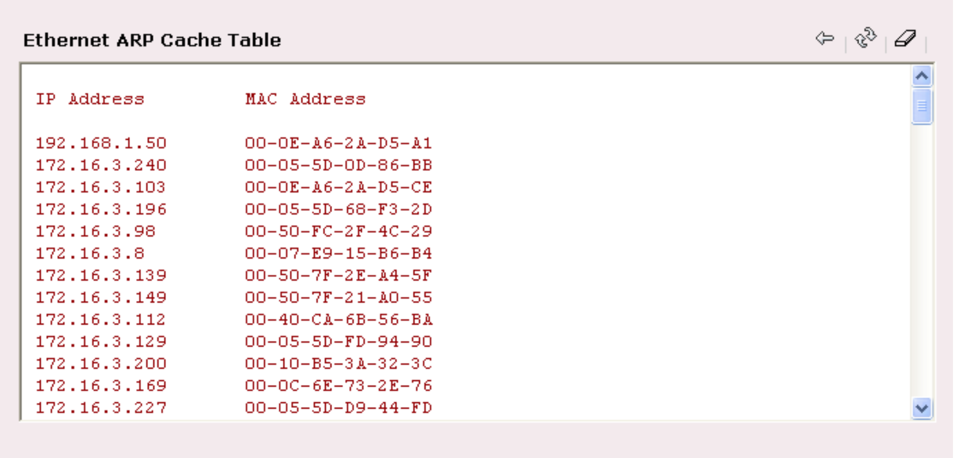
IF1 --- ISDN B1 channel.

IF2 --- ISDN B2 channel.

IF3 --- WAN interface.

4.7.4 View ARP Cache Table

Click **View 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.



Ethernet ARP Cache Table

```
IP Address          MAC Address

192.168.1.50        00-0E-A6-2A-D5-A1
172.16.3.240        00-05-5D-0D-86-BB
172.16.3.103        00-0E-A6-2A-D5-CE
172.16.3.196        00-05-5D-68-F3-2D
172.16.3.98         00-50-FC-2F-4C-29
172.16.3.8          00-07-E9-15-B6-B4
172.16.3.139        00-50-7F-2E-A4-5F
172.16.3.149        00-50-7F-21-A0-55
172.16.3.112        00-40-CA-6B-56-BA
172.16.3.129        00-05-5D-FD-94-90
172.16.3.200        00-10-B5-3A-32-3C
172.16.3.169        00-0C-6E-73-2E-76
172.16.3.227        00-05-5D-D9-44-FD
```

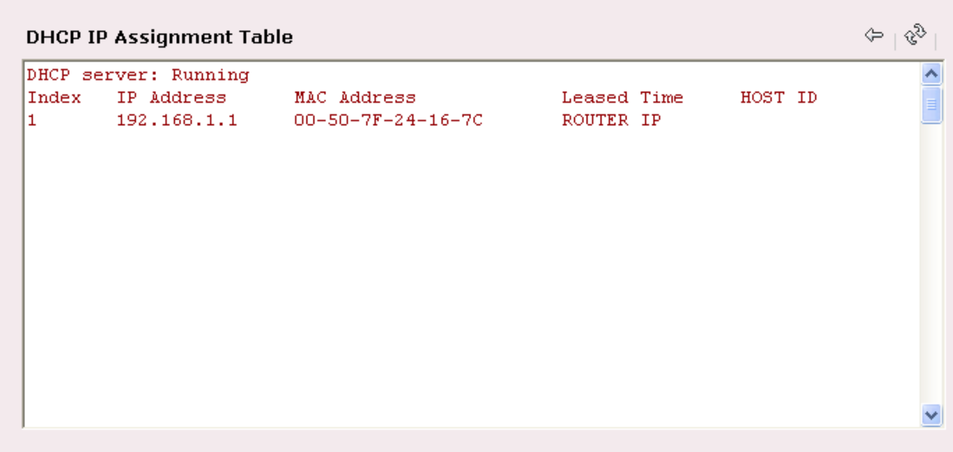
Click it to reload the page.

Click it to clear the whole table.

4.7.5 Viewing DHCP Assigned IP Addresses

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.



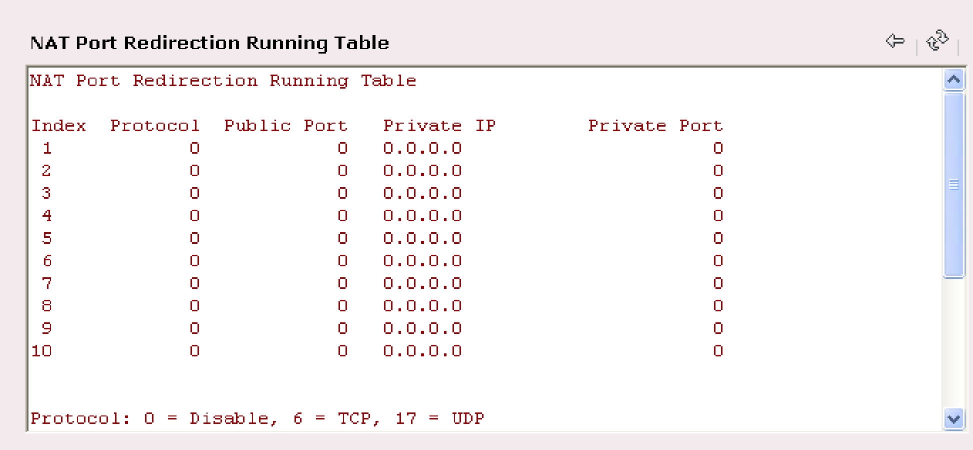
DHCP IP Assignment Table

```
DHCP server: Running
Index    IP Address      MAC Address            Leased Time     HOST ID
1        192.168.1.1     00-50-7F-24-16-7C      ROUTER IP
```

Click it to reload the page.

4.7.6 View NAT Port Redirection Running Table

If you have configured **Port Redirection** (under **NAT Setup**), click it to verify that your settings are correct for redirecting specific port numbers to specified internal users.

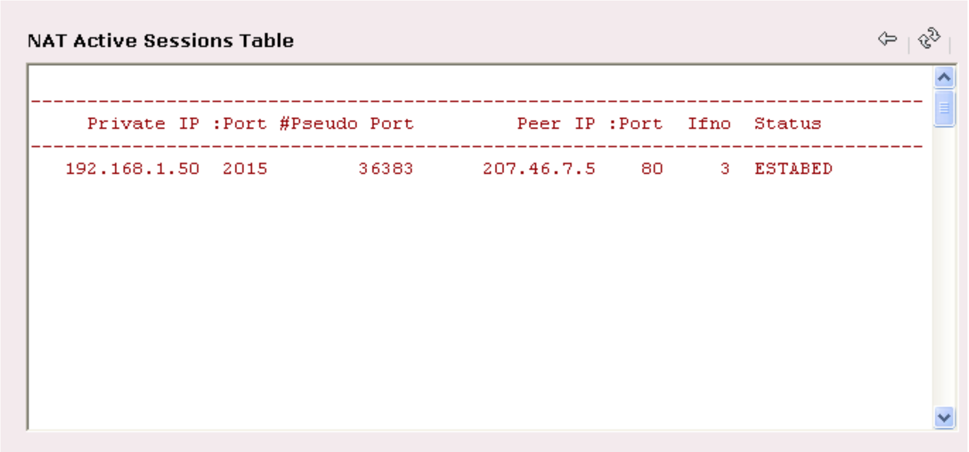


NAT Port Redirection Running Table

```
NAT Port Redirection Running Table

Index  Protocol  Public Port  Private IP        Private Port
 1            0            0  0.0.0.0                      0
 2            0            0  0.0.0.0                      0
 3            0            0  0.0.0.0                      0
 4            0            0  0.0.0.0                      0
 5            0            0  0.0.0.0                      0
 6            0            0  0.0.0.0                      0
 7            0            0  0.0.0.0                      0
 8            0            0  0.0.0.0                      0
 9            0            0  0.0.0.0                      0
10            0            0  0.0.0.0                      0


Protocol: 0 = Disable, 6 = TCP, 17 = UDP
```

4.7.7 View NAT Active Sessions Table

As the router accesses the Internet through the built-in NAT engine, click **View NAT Active Sessions Table** to see which active outgoing sessions are online.



NAT Active Sessions Table

```
---------------------------------------------------------------------------------
     Private IP :Port #Pseudo Port          Peer IP :Port  Ifno  Status
---------------------------------------------------------------------------------
   192.168.1.50  2015        36383       207.46.7.5     80      3  ESTABED
```

Click it to reload the page.

Each line across the screen indicates an active session. The following information is displayed:

Private IP:Port The internal user's (PC's) IP address and port number.

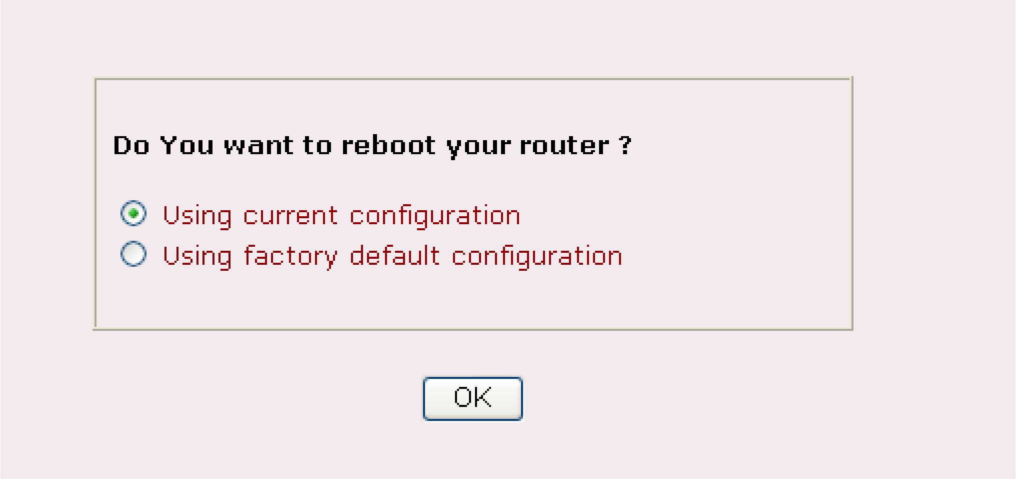
#Pseudo Port The public port number.

Peer IP:Port The peer user's (PC's) IP address and port number.

Ifno Stands for interface number. The definition is listed below:
0 --- LAN interface.
1 --- B1 interface.
2 --- B2 interface.
3 --- WAN interface.

4.8 Reboot System

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



Do You want to reboot your router ?

● Using current configuration
○ Using factory default configuration

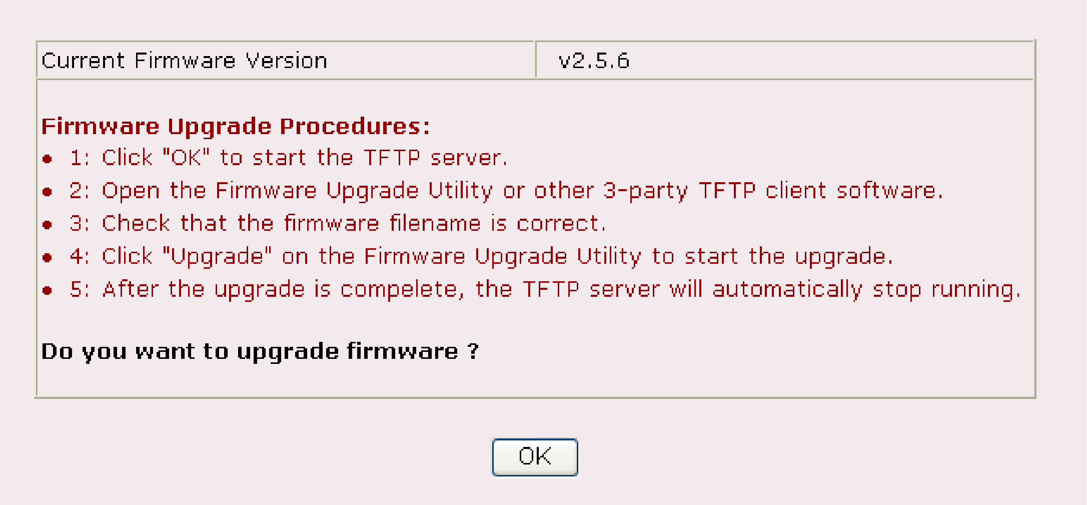
If you want to reboot the router using the current configuration, check **Using current configuration** and click **OK**. To reset the router settings to default values, check **Using factory default configuration** and click **OK**. The router will take 5 seconds to reboot the system.

4.9 Firmware Upgrade (TFTP Server)

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 **Firmware Upgrade** from **System Management** to launch the Firmware Upgrade Utility.



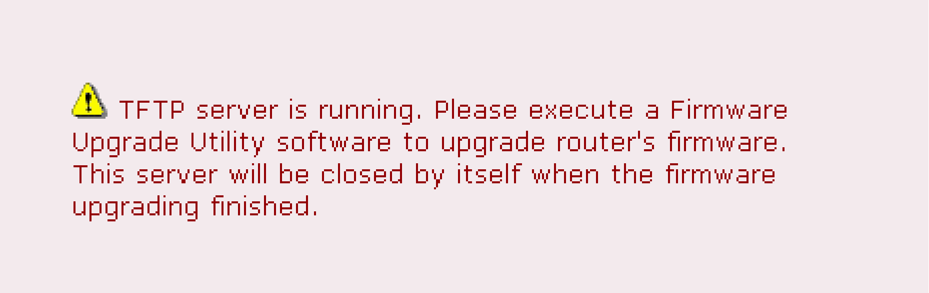
Current Firmware Version v2.5.6

Firmware Upgrade Procedures:

- 1: Click "OK" to start the TFTP server.
- 2: Open the Firmware Upgrade Utility or other 3-party TFTP client software.
- 3: Check that the firmware filename is correct.
- 4: Click "Upgrade" on the Firmware Upgrade Utility to start the upgrade.
- 5: After the upgrade is compelete, the TFTP server will automatically stop running.

Do you want to upgrade firmware ?

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



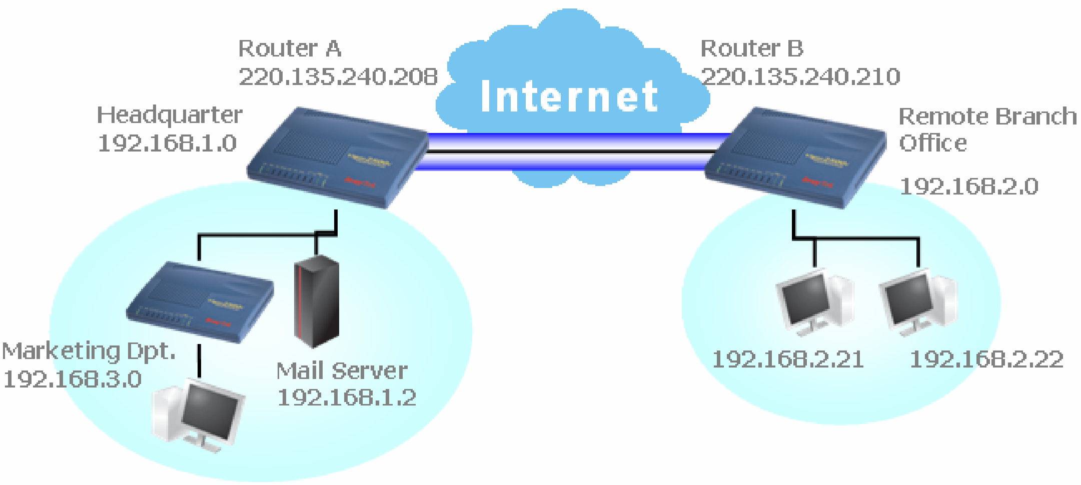
TFTP server is running. Please execute a Firmware Upgrade Utility software to upgrade router's firmware. This server will be closed by itself when the firmware upgrading finished.

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

5 Application and Examples

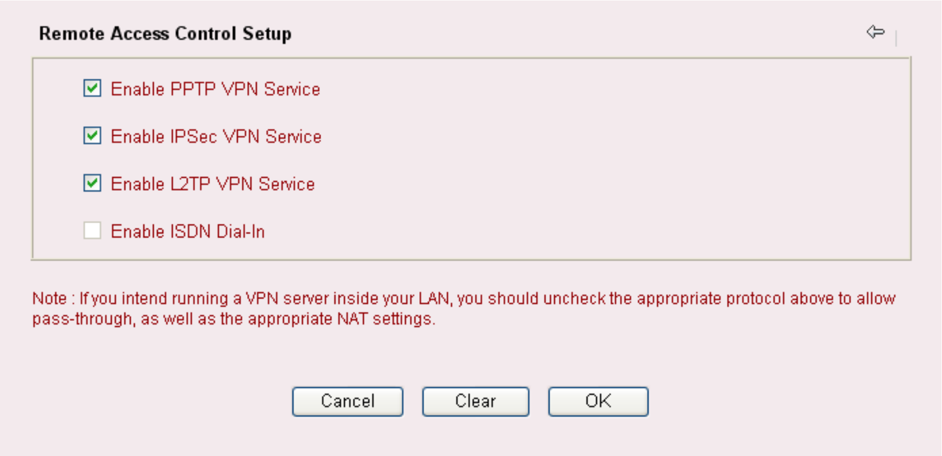
5.1 Create a LAN-to-LAN Connection Between Remote Office and Headquarter

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. Choose **VPN and Remote Access Setup** on the **Advanced Setup** group.
2. Select **Remote Access Control Setup**. The following page will appear. Enable the necessary VPN service and click **OK**.



Remote Access Control Setup

☑ Enable PPTP VPN Service

☑ Enable IPSec VPN Service

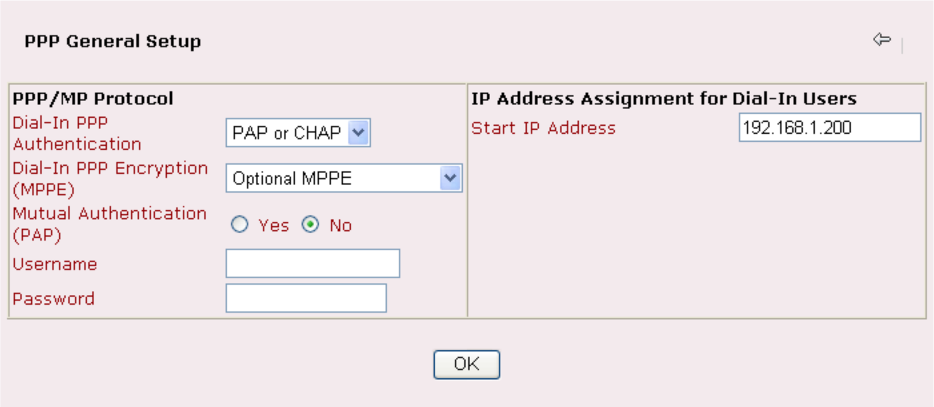
☑ Enable L2TP VPN Service

□ Enable ISDN Dial-In

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

3. Then, return to **VPN and Remote Access Setup** page and choose **PPP General Setup**.

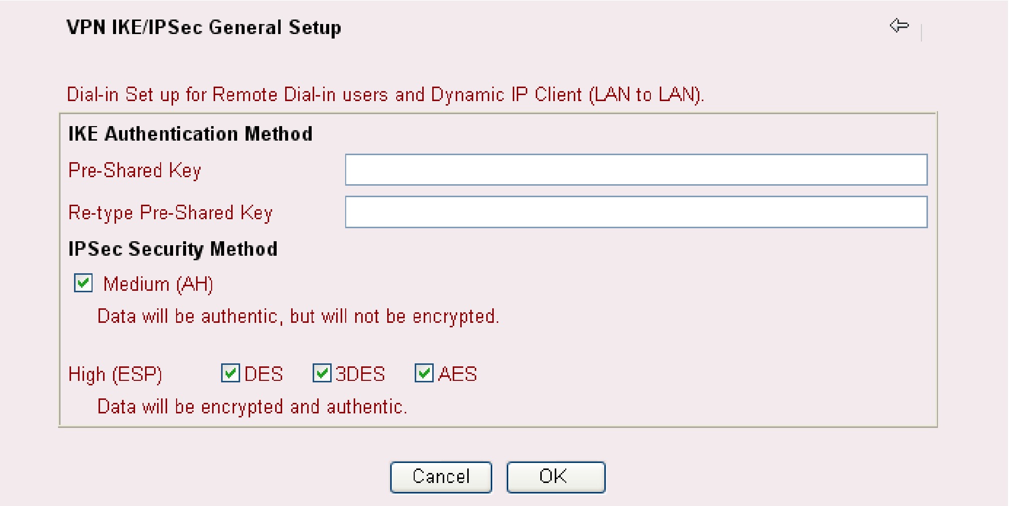
4. For using **PPP** based services, such as PPTP, L2TP, you have to set general settings in **PPP General Setup**.



PPP General Setup

PPP/MP Protocol		**IP Address Assignment for Dial-In Users**	
Dial-In PPP Authentication	PAP or CHAP	Start IP Address	192.168.1.200
Dial-In PPP Encryption (MPPE)	Optional MPPE		
Mutual Authentication (PAP)	○ Yes ● No		
Username			
Password			

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

Re-type Pre-Shared Key

IPSec Security Method

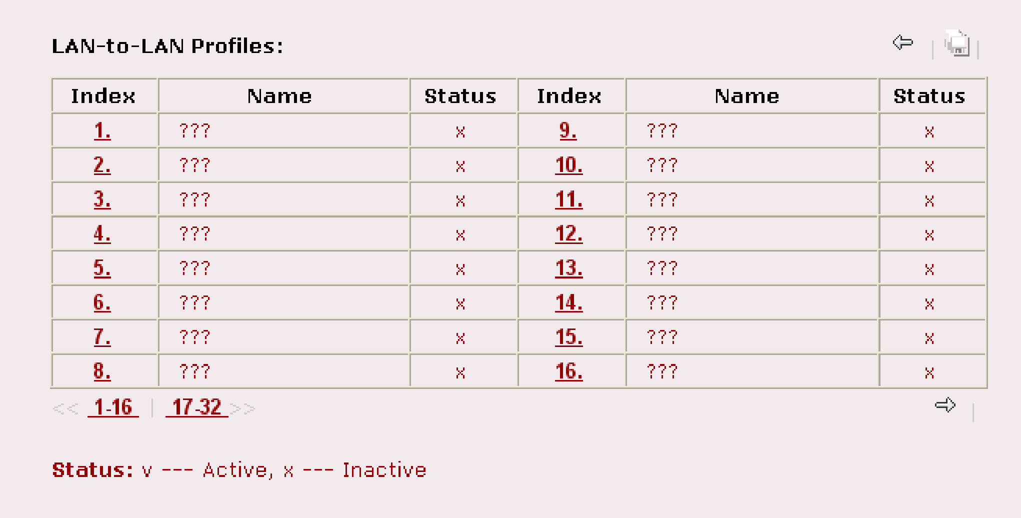
☑ Medium (AH)

Data will be authentic, but will not be encrypted.

High (ESP) ☑ DES ☑ 3DES ☑ AES

Data will be encrypted and authentic.

5. Return to **VPN and Remote Access Setup** page and choose **LAN-to-LAN Profile Setup.** Click on one index number to edit a profile.



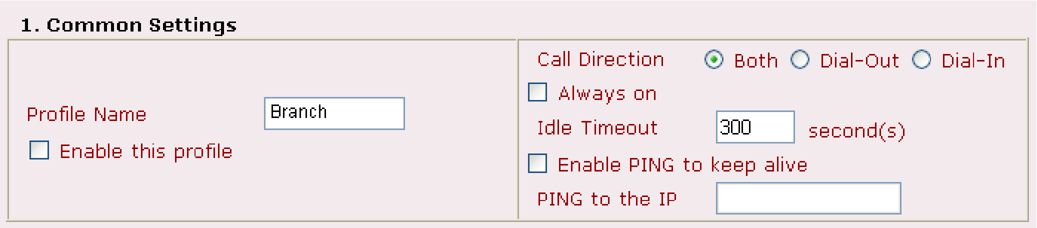
LAN-to-LAN Profiles:

Index	Name	Status	Index	Name	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	16.	???	x

<< 1-16 | 17-32 >>

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

6. Set **Common Settings** as shown below. You should **enable** this profile.



1. Common Settings

Profile Name: Branch

□ Enable this profile

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

□ Always on

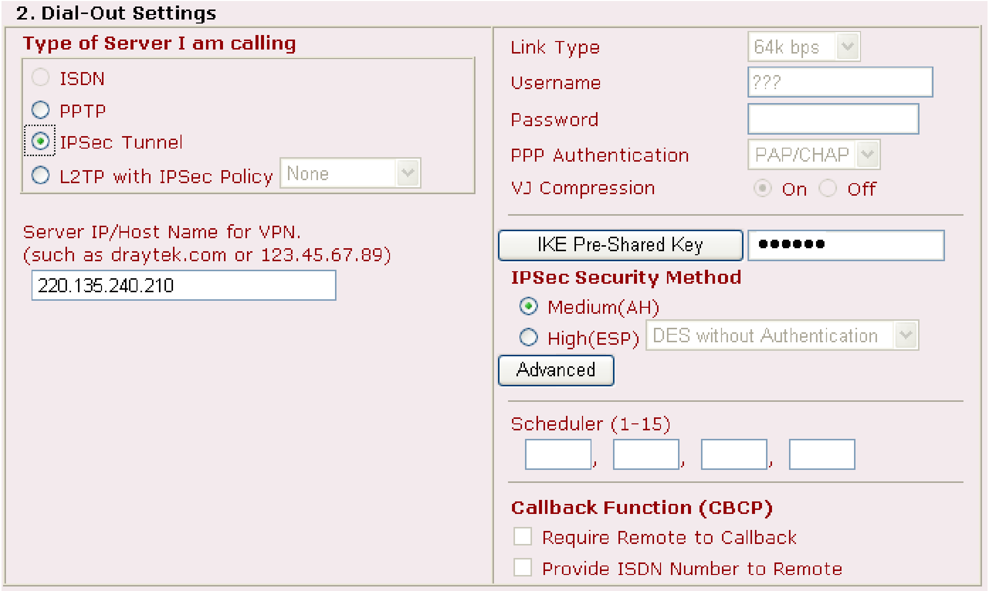
Idle Timeout: 300 second(s)

□ Enable PING to keep alive

PING to the IP:

7. 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

○ ISDN

○ PPTP

● IPSec Tunnel

○ L2TP with IPSec Policy: None

Server IP/Host Name for VPN.
(such as 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 Pre-Shared Key: ●●●●●●

IPSec Security Method

● Medium(AH)

○ High(ESP): DES without Authentication

Advanced

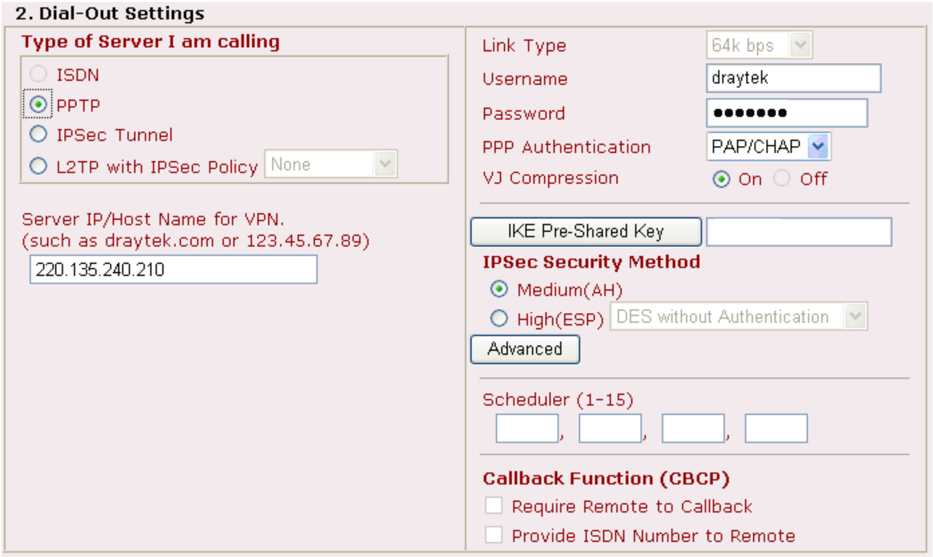
Scheduler (1-15): , , ,

Callback Function (CBCP)

□ Require Remote to Callback

□ Provide ISDN Number to Remote

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

○ ISDN

● PPTP

○ IPSec Tunnel

○ L2TP with IPSec Policy: None

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

220.135.240.210

Link Type: 64k bps

Username: draytek

Password: ●●●●●●●

PPP Authentication: PAP/CHAP

VJ Compression: ● On ○ Off

IKE Pre-Shared Key:

IPSec Security Method

● Medium(AH)

○ High(ESP): DES without Authentication

Advanced

Scheduler (1-15): , , ,

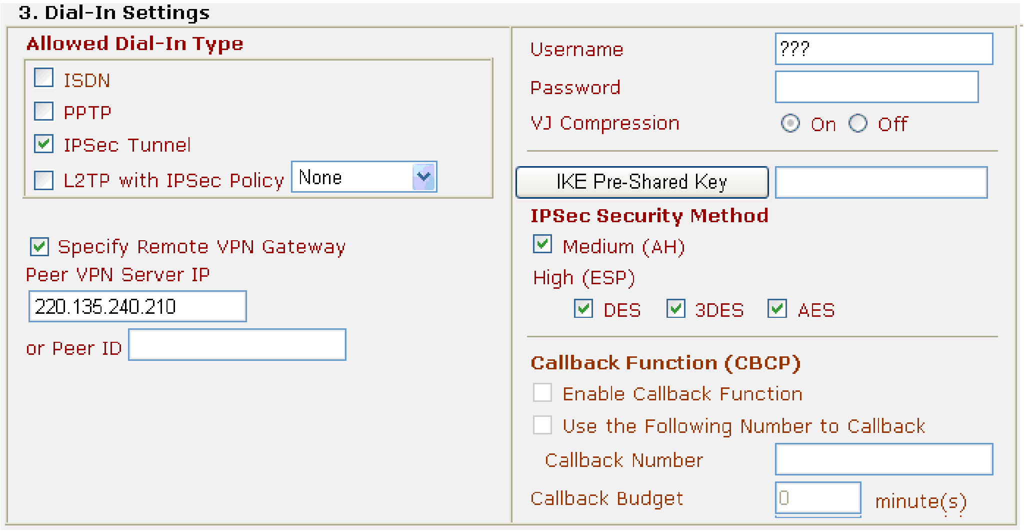
Callback Function (CBCP)

□ Require Remote to Callback

□ Provide ISDN Number to Remote

8. Set **Dial-In settings** 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
- □ ISDN
- □ PPTP
- ☑ IPSec Tunnel
- □ L2TP with IPSec Policy: None

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

Username: ???
Password:
VJ Compression: ● On ○ Off

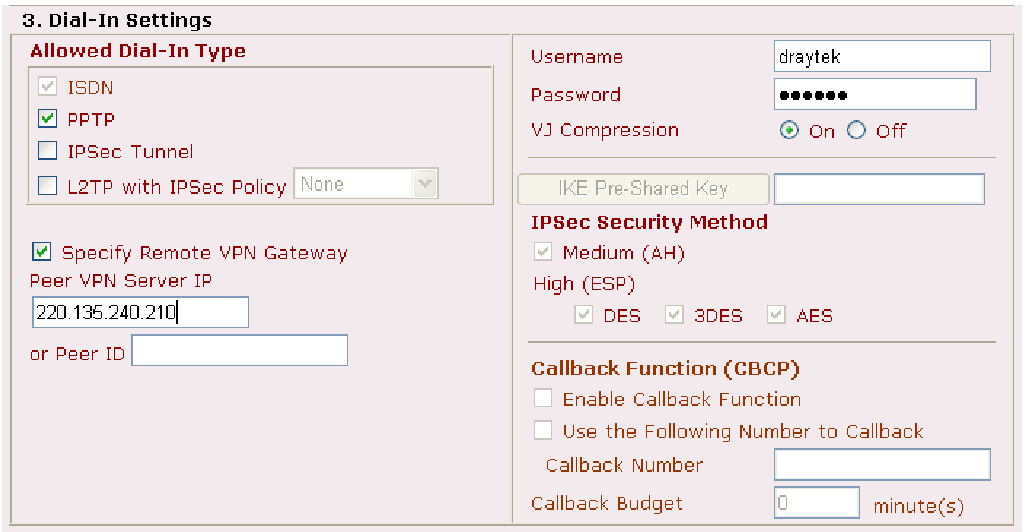
IKE Pre-Shared Key:

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

Callback Function (CBCP)
- □ Enable Callback Function
- □ Use the Following Number to Callback

Callback Number:
Callback Budget: 0 minute(s)

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



3. Dial-In Settings

Allowed Dial-In Type
- ☑ ISDN
- ☑ PPTP
- □ IPSec Tunnel
- □ L2TP with IPSec Policy: None

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

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

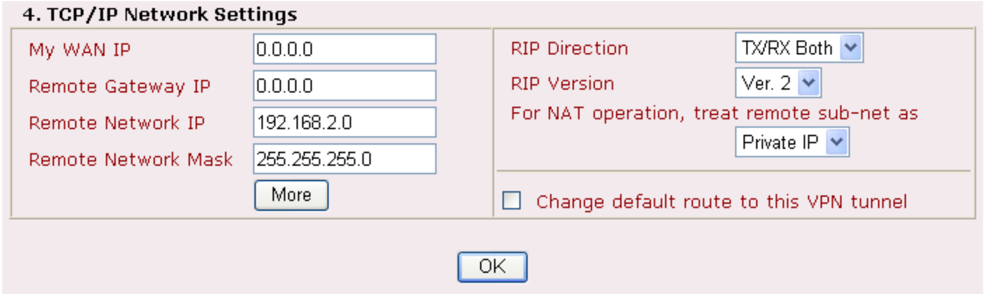
IKE Pre-Shared Key:

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

Callback Function (CBCP)
- □ Enable Callback Function
- □ Use the Following Number to Callback

Callback Number:
Callback Budget: 0 minute(s)

9. 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

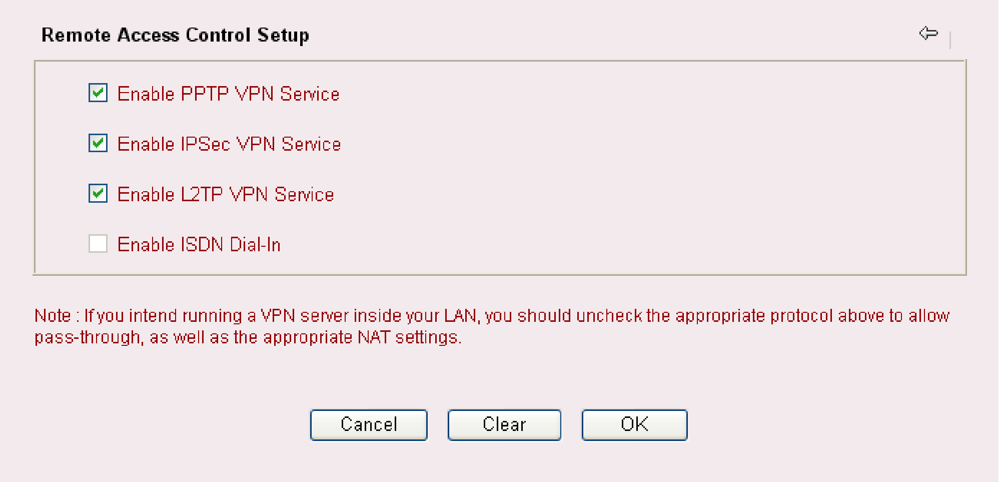
RIP Direction: TX/RX Both
RIP Version: Ver. 2
For NAT operation, treat remote sub-net as: Private IP

□ Change default route to this VPN tunnel

OK

Settings in Router B in the remote office:

1. Choose **VPN and Remote Access Setup** on the **Advanced Setup** group.
2. Select **Remote Access Control Setup**. The following page will appear. Enable the necessary VPN service and click **OK**.



Remote Access Control Setup

☑ Enable PPTP VPN Service

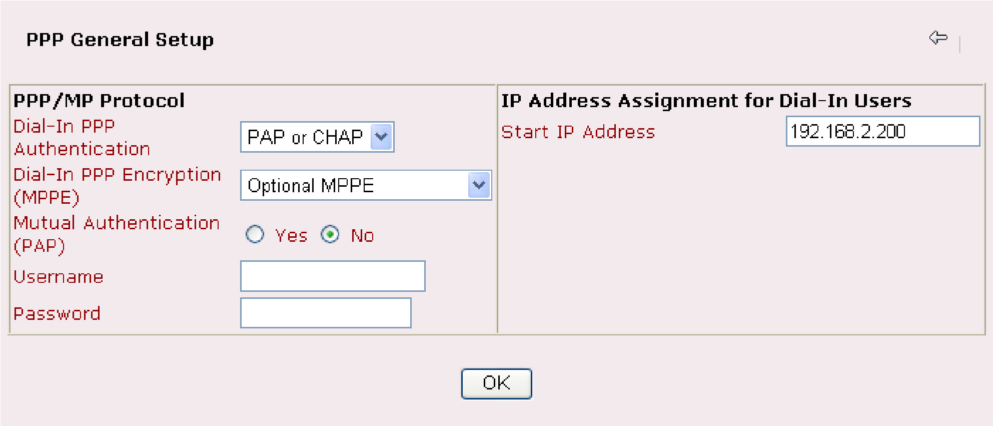
☑ Enable IPSec VPN Service

☑ Enable L2TP VPN Service

□ Enable ISDN Dial-In

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

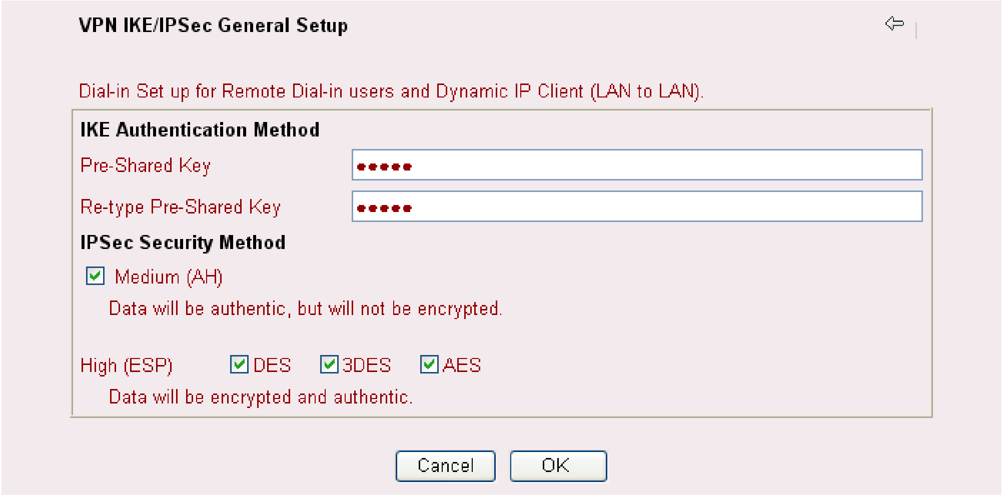
3. Then, return to **VPN and Remote Access Setup** page and choose **PPP General Setup**.
4. For using **PPP based** services, such as PPTP, L2TP, you have to set general settings in **PPP General Setup**.



PPP General Setup

PPP/MP Protocol		IP Address Assignment for Dial-In Users	
Dial-In PPP Authentication	PAP or CHAP	Start IP Address	192.168.2.200
Dial-In PPP Encryption (MPPE)	Optional MPPE		
Mutual Authentication (PAP)	○ Yes ● No		
Username			
Password			

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



VPN 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: ●●●●●

Re-type Pre-Shared Key: ●●●●●

IPSec Security Method

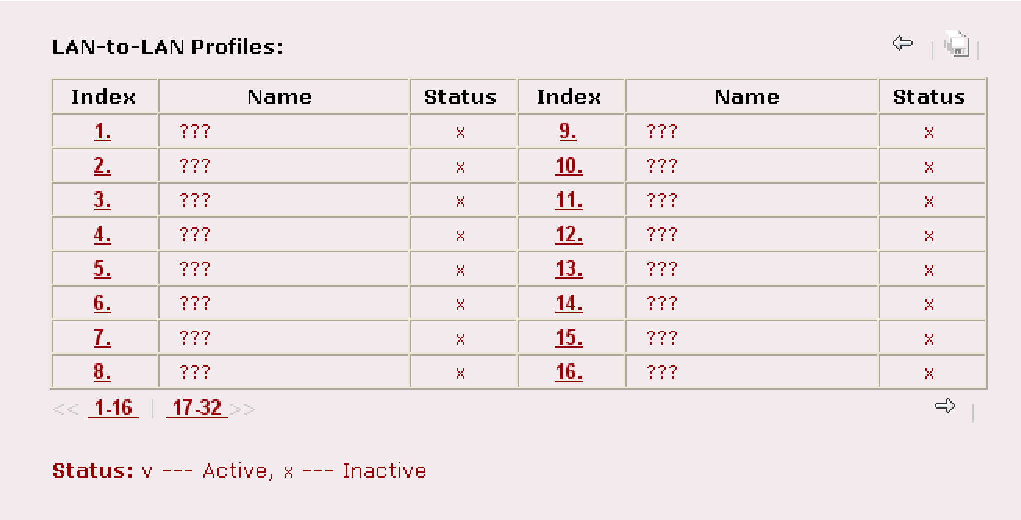
☑ Medium (AH)

Data will be authentic, but will not be encrypted.

High (ESP) ☑ DES ☑ 3DES ☑ AES

Data will be encrypted and authentic.

5. Return to **VPN and Remote Access Setup** page and choose **LAN-to-LAN Profile Setup.** Click on one index number to edit a profile.

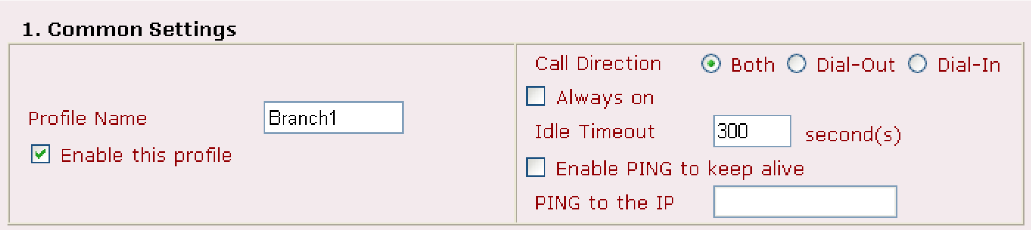


LAN-to-LAN Profiles:

Index	Name	Status	Index	Name	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	16.	???	x

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

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



1. Common Settings

Profile Name: Branch1

☑ Enable this profile

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

□ Always on

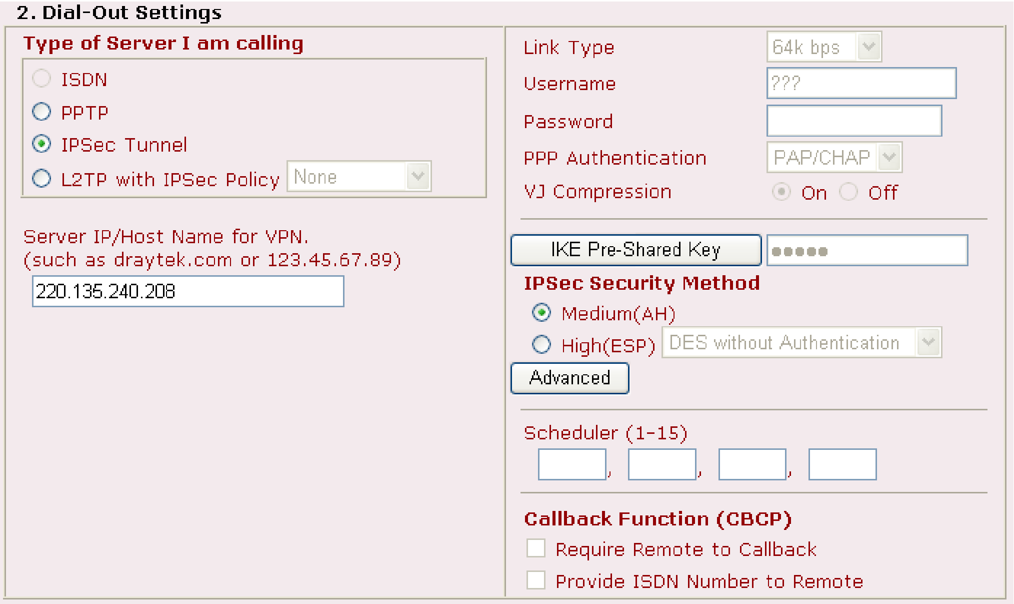
Idle Timeout: 300 second(s)

□ Enable PING to keep alive

PING to the IP:

7. 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

○ ISDN
○ PPTP
● IPSec Tunnel
○ L2TP with IPSec Policy: None

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

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

IKE Pre-Shared Key: •••••

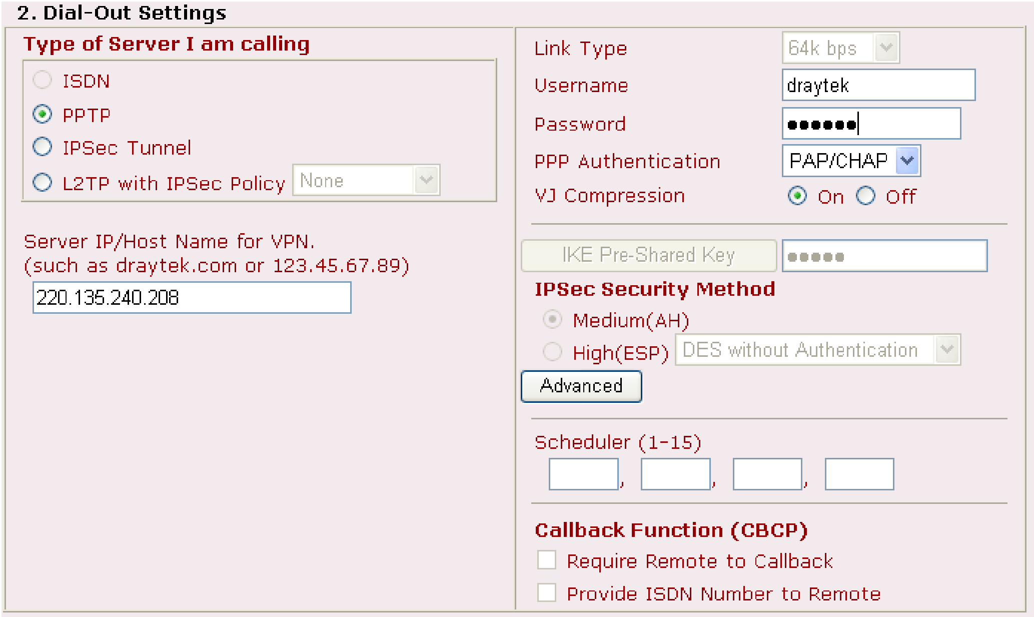
IPSec Security Method
● Medium(AH)
○ High(ESP): DES without Authentication

Advanced

Scheduler (1-15): , , ,

Callback Function (CBCP)
□ Require Remote to Callback
□ Provide ISDN Number to Remote

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

○ ISDN
● PPTP
○ IPSec Tunnel
○ L2TP with IPSec Policy: None

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

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

IKE Pre-Shared Key: •••••

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

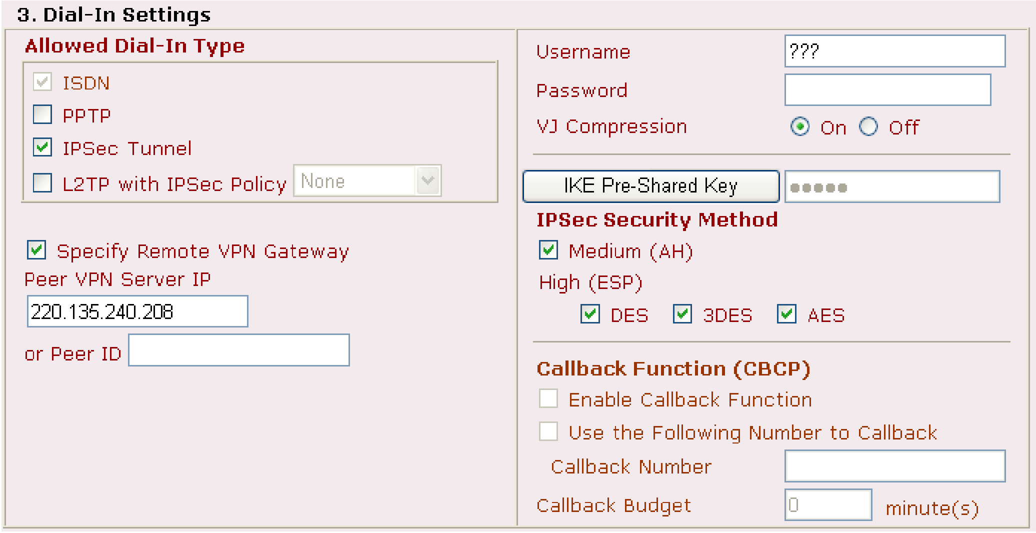
Advanced

Scheduler (1-15): , , ,

Callback Function (CBCP)
□ Require Remote to Callback
□ Provide ISDN Number to Remote

8. Set **Dial-In settings** 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

☑ ISDN

□ PPTP

☑ IPSec Tunnel

□ L2TP with IPSec Policy None

☑ Specify Remote VPN Gateway

Peer VPN Server IP 220.135.240.208

or Peer ID

Username ???

Password

VJ Compression ● On ○ Off

IKE Pre-Shared Key ●●●●●

IPSec Security Method

☑ Medium (AH)

High (ESP)

☑ DES ☑ 3DES ☑ AES

Callback Function (CBCP)

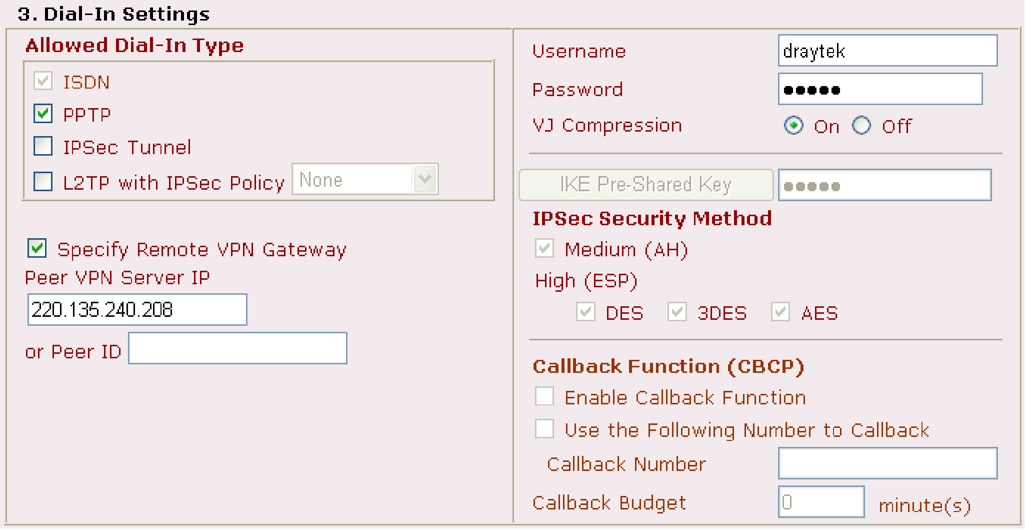
□ Enable Callback Function

□ Use the Following Number to Callback

Callback Number

Callback Budget 0 minute(s)

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



3. Dial-In Settings

Allowed Dial-In Type

☑ ISDN

☑ PPTP

□ IPSec Tunnel

□ L2TP with IPSec Policy None

☑ Specify Remote VPN Gateway

Peer VPN Server IP 220.135.240.208

or Peer ID

Username draytek

Password ●●●●●

VJ Compression ● On ○ Off

IKE Pre-Shared Key ●●●●●

IPSec Security Method

☑ Medium (AH)

High (ESP)

☑ DES ☑ 3DES ☑ AES

Callback Function (CBCP)

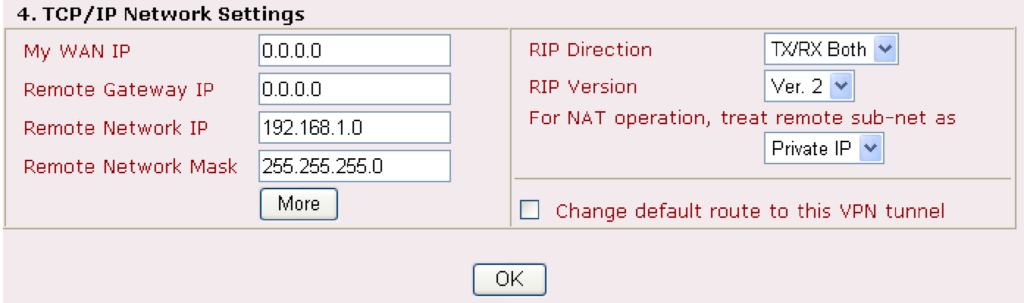
□ Enable Callback Function

□ Use the Following Number to Callback

Callback Number

Callback Budget 0 minute(s)

9. 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 TX/RX Both

RIP Version Ver. 2

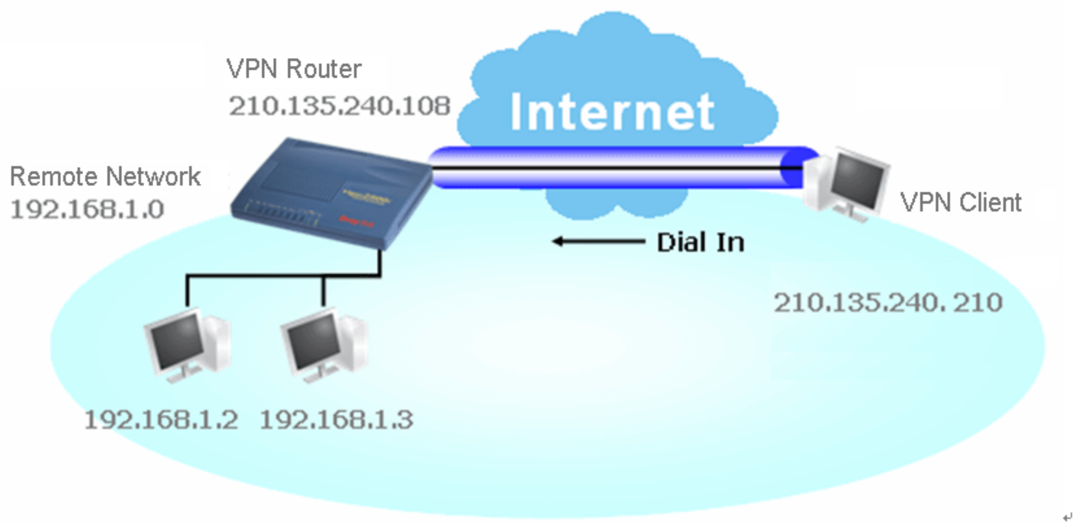
For NAT operation, treat remote sub-net as Private IP

□ Change default route to this VPN tunnel

OK

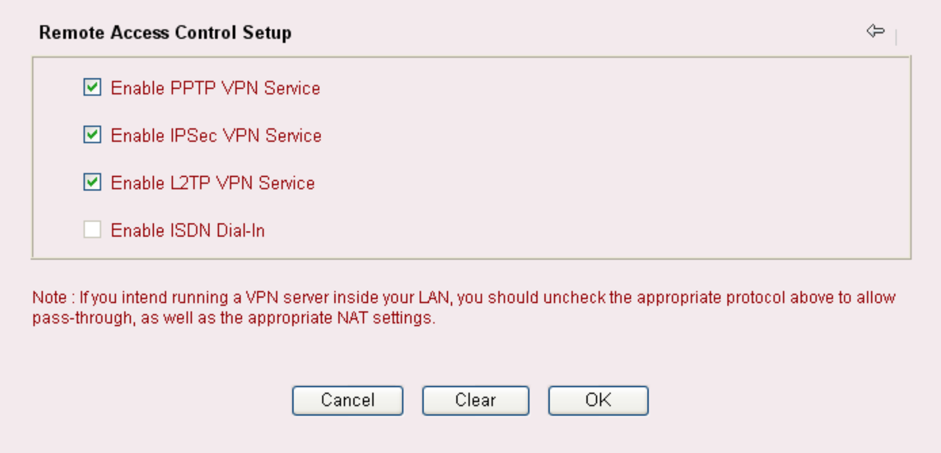
5.2 Create a Remote Dial-in User Connection Between the Teleworker and Headquarter

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. Choose **VPN and Remote Access Setup** on the **Advanced Setup** group.
2. Select **Remote Access Control Setup**. The following page will appear. Enable the necessary VPN service and click **OK**.



Remote Access Control Setup

☑ Enable PPTP VPN Service

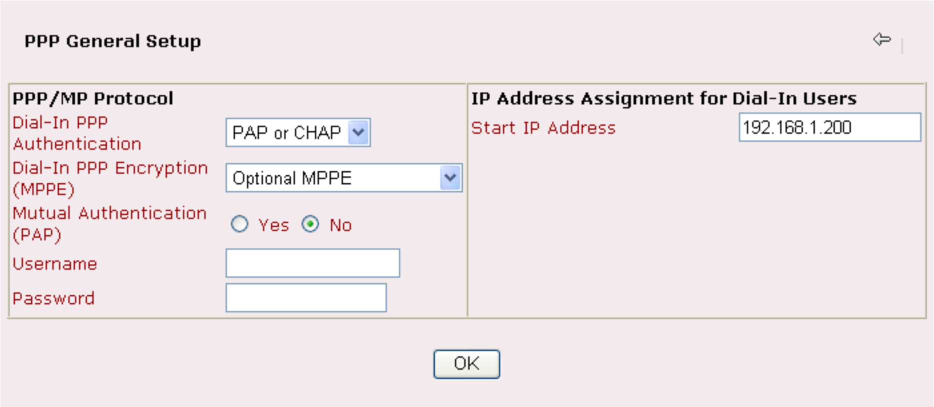
☑ Enable IPSec VPN Service

☑ Enable L2TP VPN Service

□ Enable ISDN Dial-In

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

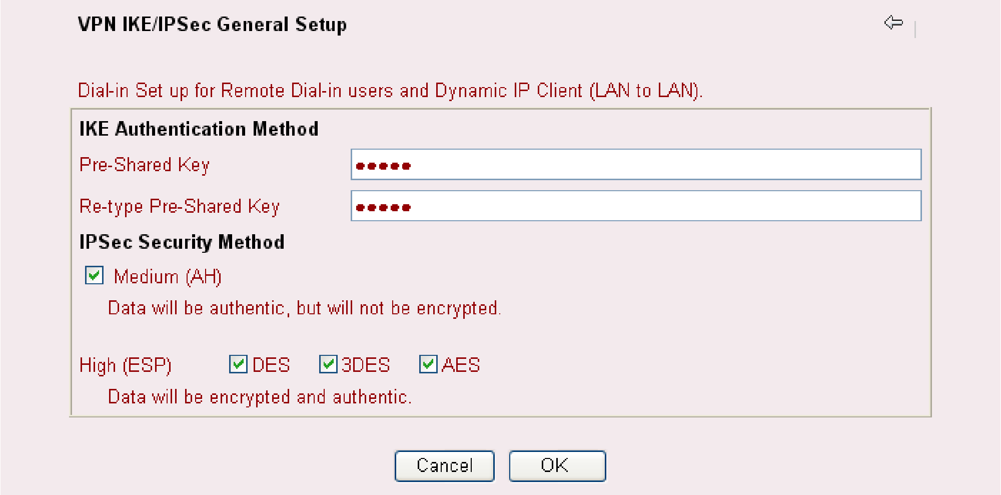
3. Then, return to **VPN and Remote Access Setup** page and choose **PPP General Setup**.
4. For using PPP based services, such as PPTP, L2TP, you have to set general settings in **PPP General Setup**.



PPP General Setup

PPP/MP Protocol		IP Address Assignment for Dial-In Users	
Dial-In PPP Authentication	PAP or CHAP	Start IP Address	192.168.1.200
Dial-In PPP Encryption (MPPE)	Optional MPPE		
Mutual Authentication (PAP)	○ Yes ● No		
Username			
Password			

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 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: •••••

Re-type Pre-Shared Key: •••••

IPSec Security Method

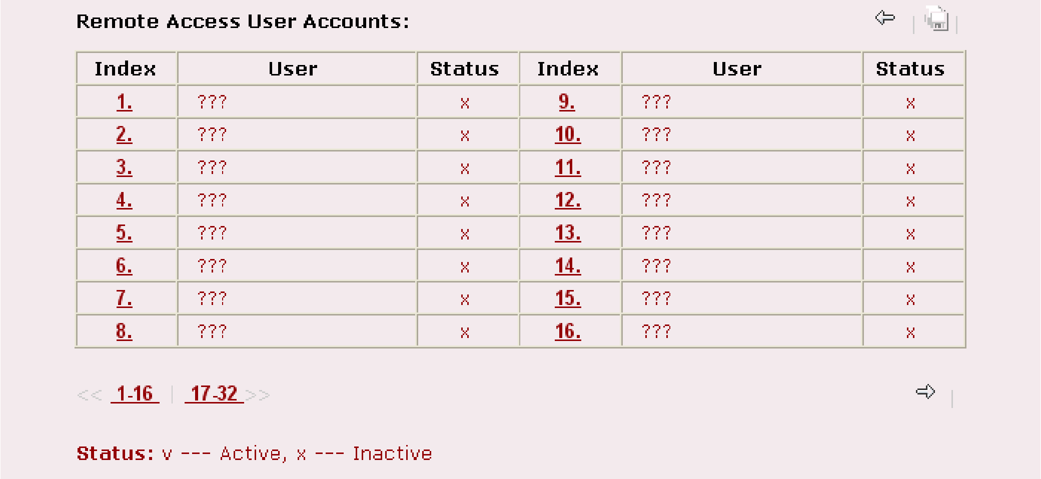
☑ Medium (AH)

Data will be authentic, but will not be encrypted.

High (ESP) ☑ DES ☑ 3DES ☑ AES

Data will be encrypted and authentic.

5. Return to **VPN and Remote Access Setup** page and choose **Remote User Profile Setup (Teleworker).** Click on one index number to edit a profile.



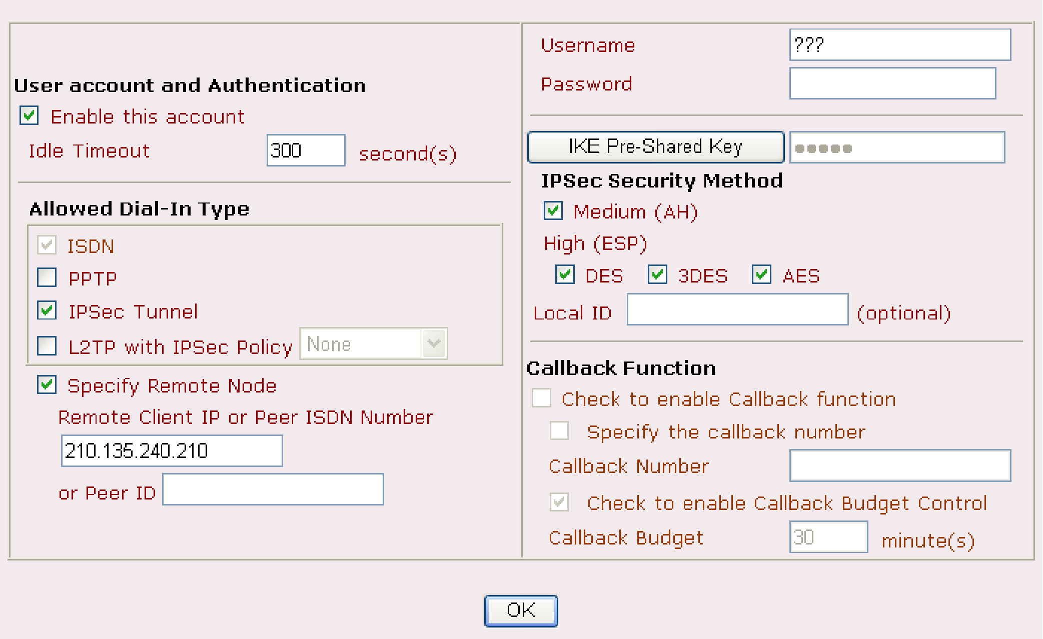
Remote Access User Accounts:

Index	User	Status	Index	User	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	16.	???	x

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

6. Set **Dial-In** settings 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.



User account and Authentication

☑ Enable this account

Idle Timeout 300 second(s)

Allowed Dial-In Type

☑ ISDN

□ PPTP

☑ IPSec Tunnel

□ L2TP with IPSec Policy None

☑ Specify Remote Node

Remote Client IP or Peer ISDN Number 210.135.240.210

or Peer ID

Username ???

Password

IKE Pre-Shared Key ●●●●●

IPSec Security Method

☑ Medium (AH)

High (ESP) ☑ DES ☑ 3DES ☑ AES

Local ID (optional)

Callback Function

□ Check to enable Callback function

□ Specify the callback number

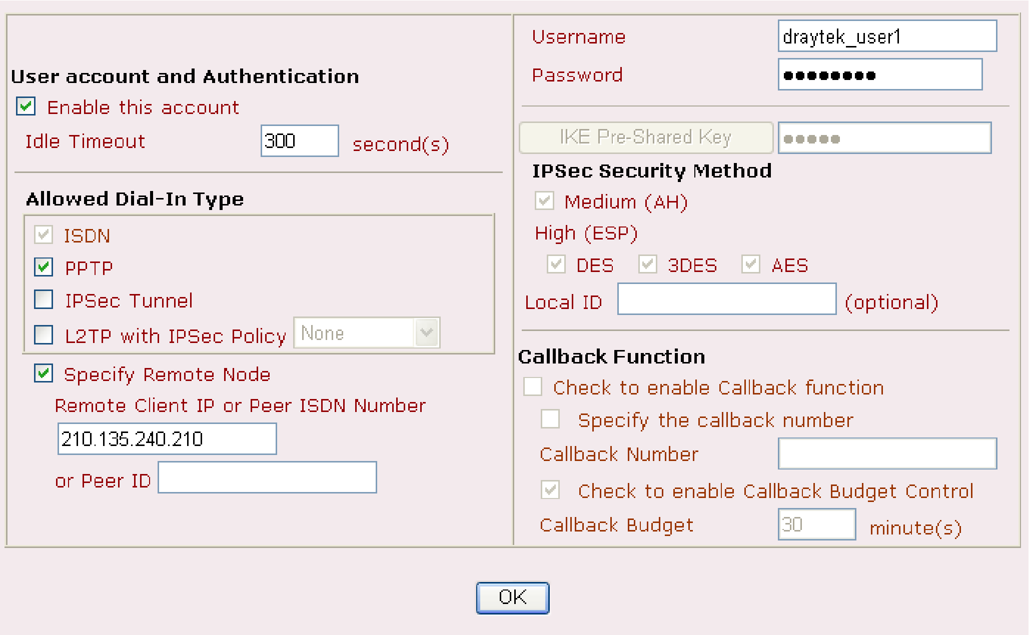
Callback Number

☑ Check to enable Callback Budget Control

Callback Budget 30 minute(s)

OK

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.



User account and Authentication

☑ Enable this account

Idle Timeout 300 second(s)

Allowed Dial-In Type

☑ ISDN

☑ PPTP

□ IPSec Tunnel

□ L2TP with IPSec Policy None

☑ Specify Remote Node

Remote Client IP or Peer ISDN Number 210.135.240.210

or Peer ID

Username draytek_user1

Password ●●●●●●●●

IKE Pre-Shared Key ●●●●●

IPSec Security Method

☑ Medium (AH)

High (ESP) ☑ DES ☑ 3DES ☑ AES

Local ID (optional)

Callback Function

□ Check to enable Callback function

□ Specify the callback number

Callback Number

☑ Check to enable Callback Budget Control

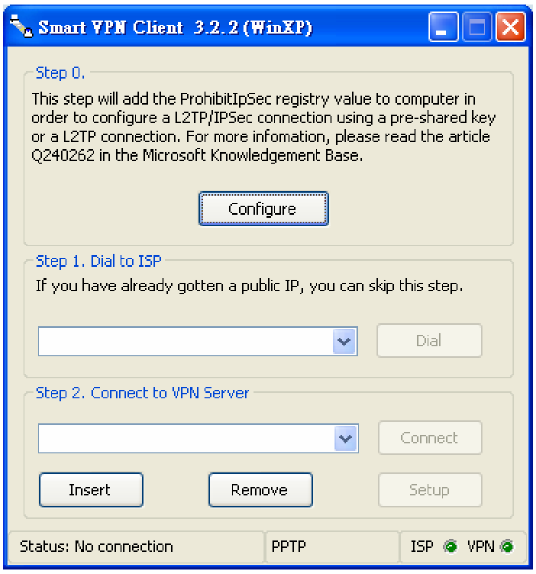
Callback Budget 30 minute(s)

OK

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.



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

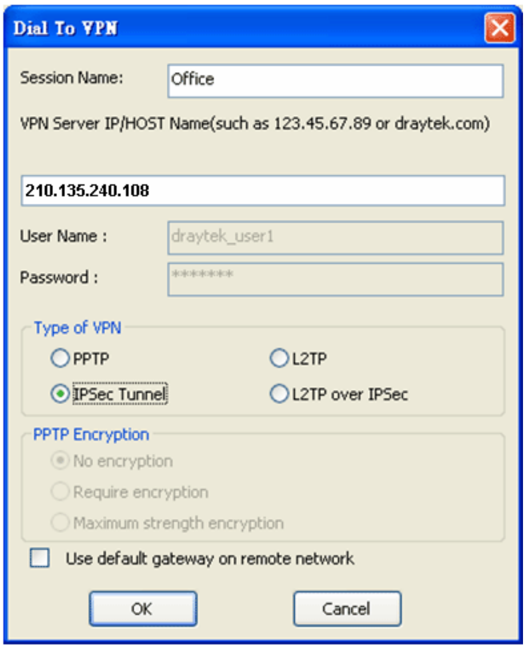
If you have already gotten a public IP, you can skip this step.

Step 2. Connect to VPN Server

Status: No connection

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)

210.135.240.108

User Name : draytek_user1

Password : *******

Type of VPN

○ PPTP ○ L2TP

● IPSec Tunnel ○ L2TP over IPSec

PPTP Encryption

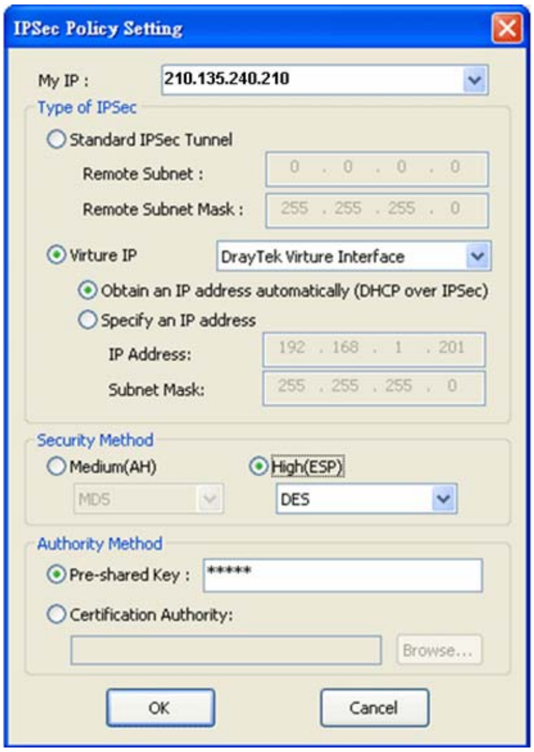
● No encryption

○ Require encryption

○ Maximum strength encryption

□ Use default gateway on remote network

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.



IPSec Policy Setting

My IP : 210.135.240.210

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 . 201

Subnet Mask: 255 . 255 . 255 . 0

Security Method

○ Medium(AH): MD5

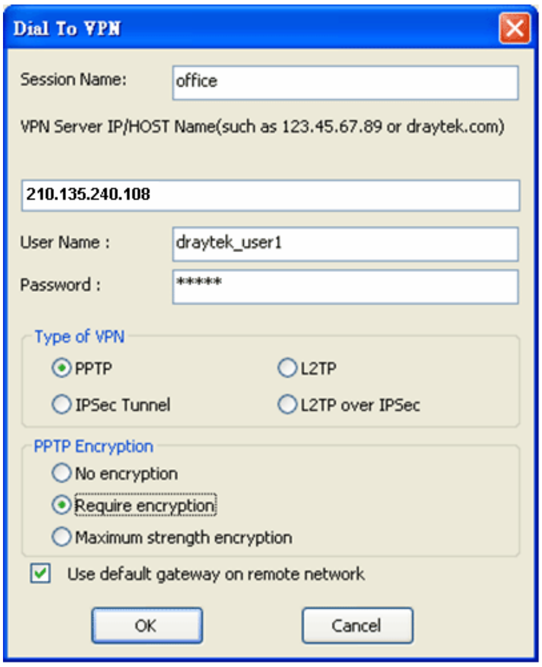
● High(ESP): DES

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)

210.135.240.108

User Name : draytek_user1

Password : *****

Type of VPN

● PPTP ○ L2TP

○ IPSec Tunnel ○ L2TP over IPSec

PPTP Encryption

○ No encryption

● Require encryption

○ Maximum strength encryption

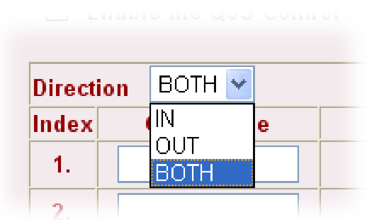
☑ Use default gateway on remote network

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

5.3 QoS Setting Example

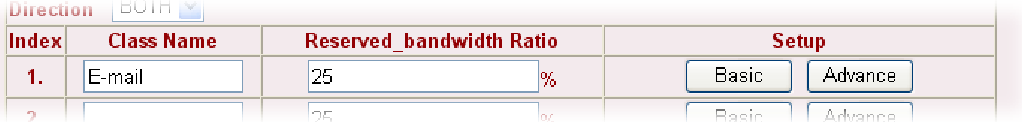
Assume a teleworker sometimes works at home and takes care of children. When working time, he would use Vigor router at home to connect to the server in the headquater office downtown via either HTTPS or VPN to check email and access internal database. Meanwhile, children may chat on VoIP or Skype in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

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



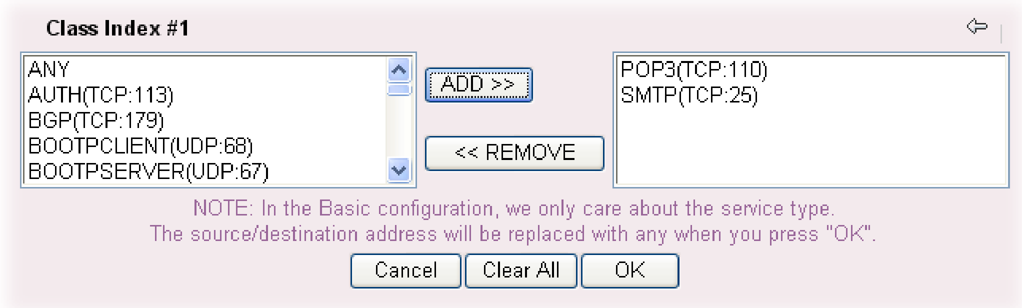
Direction: BOTH

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



Index	Class Name	Reserved_bandwidth Ratio	Setup
1.	E-mail	25 %	Basic Advance

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



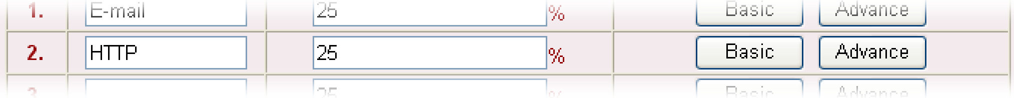
Class Index #1

ANY
AUTH(TCP:113)
BGP(TCP:179)
BOOTPCLIENT(UDP:68)
BOOTPSERVER(UDP:67)

POP3(TCP:110)
SMTP(TCP:25)

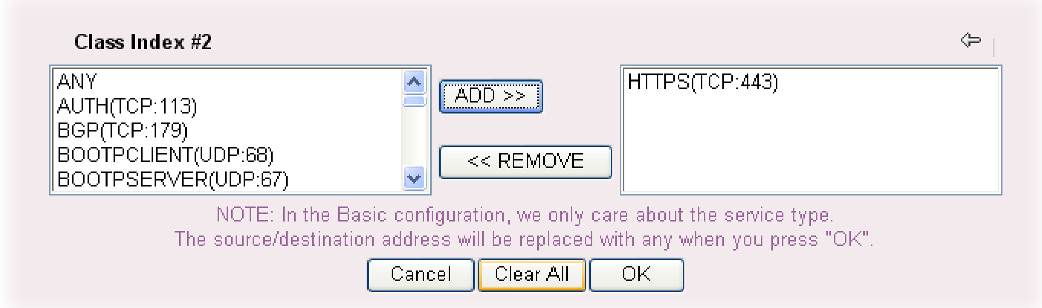
NOTE: In the Basic configuration, we only care about the service type.
The source/destination address will be replaced with any when you press "OK".

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



1.	E-mail	25 %	Basic Advance
2.	HTTP	25 %	Basic Advance

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



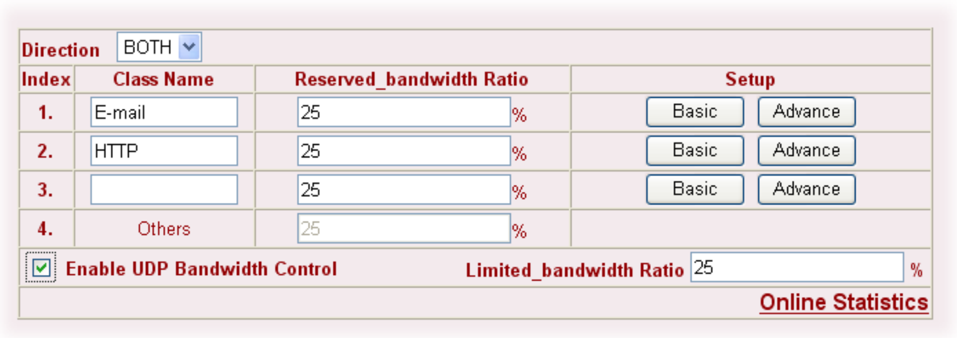
Class Index #2

ANY
AUTH(TCP:113)
BGP(TCP:179)
BOOTPCLIENT(UDP:68)
BOOTPSERVER(UDP:67)

HTTPS(TCP:443)

NOTE: In the Basic configuration, we only care about the service type.
The source/destination address will be replaced with any when you press "OK".

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



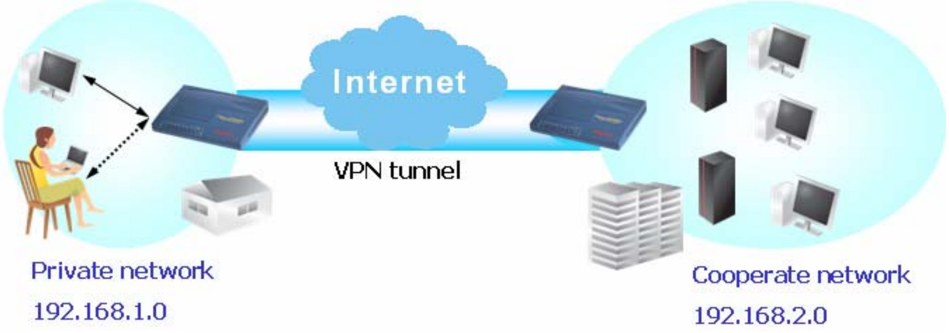
Direction BOTH

Index	Class Name	Reserved_bandwidth Ratio	Setup
1.	E-mail	25 %	Basic Advance
2.	HTTP	25 %	Basic Advance
3.		25 %	Basic Advance
4.	Others	25 %	

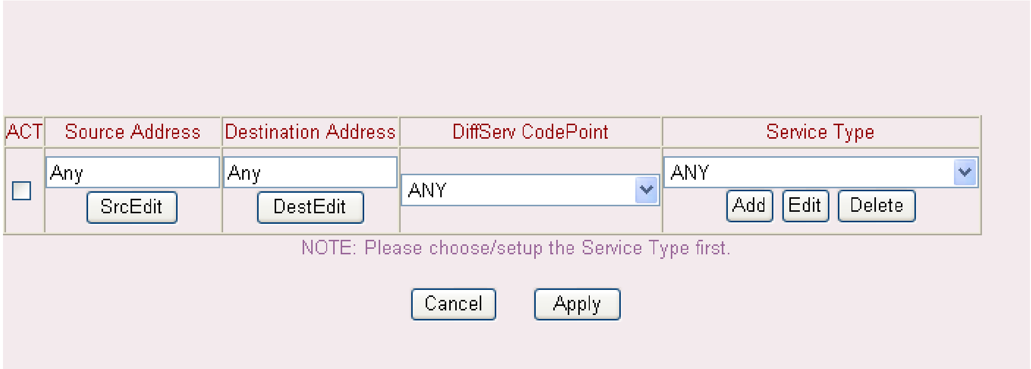
☑ Enable UDP Bandwidth Control Limited_bandwidth Ratio 25 %

Online Statistics

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



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



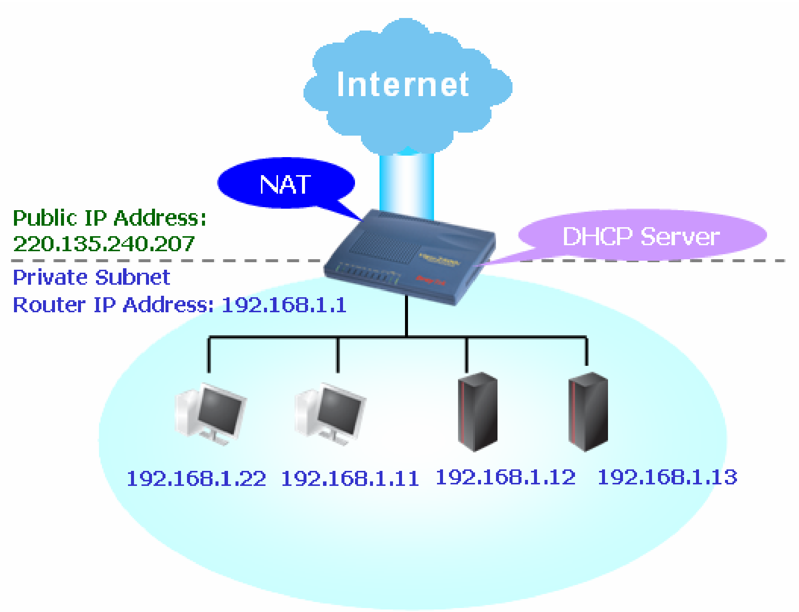
ACT	Source Address	Destination Address	DiffServ CodePoint	Service Type
□	Any SrcEdit	Any DestEdit	ANY	ANY Add Edit Delete

NOTE: Please choose/setup the Service Type first.

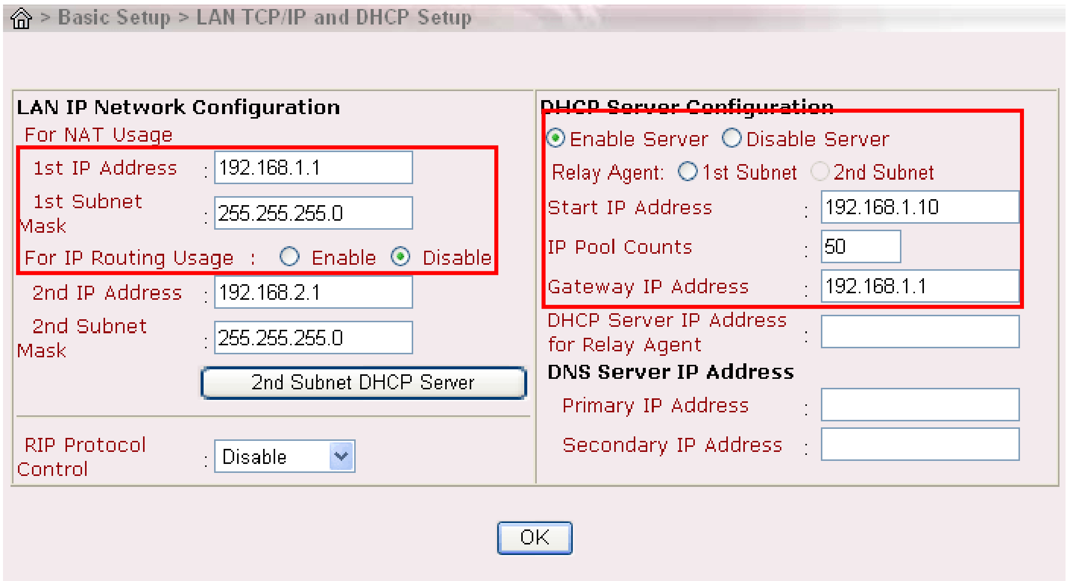
Cancel Apply

5.4 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.



> Basic Setup > LAN TCP/IP and DHCP Setup

LAN IP Network Configuration

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

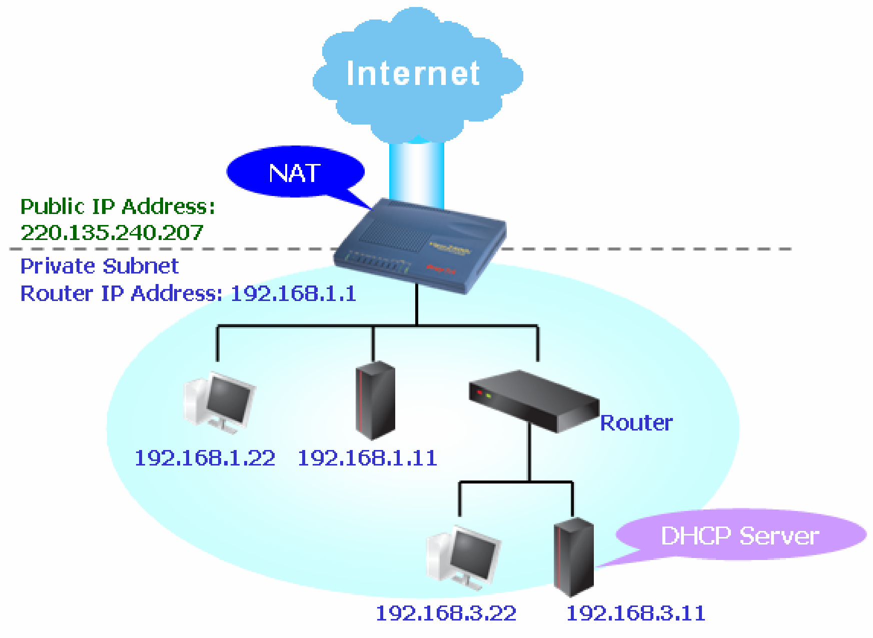
DHCP Server IP Address for Relay Agent :

DNS Server IP Address

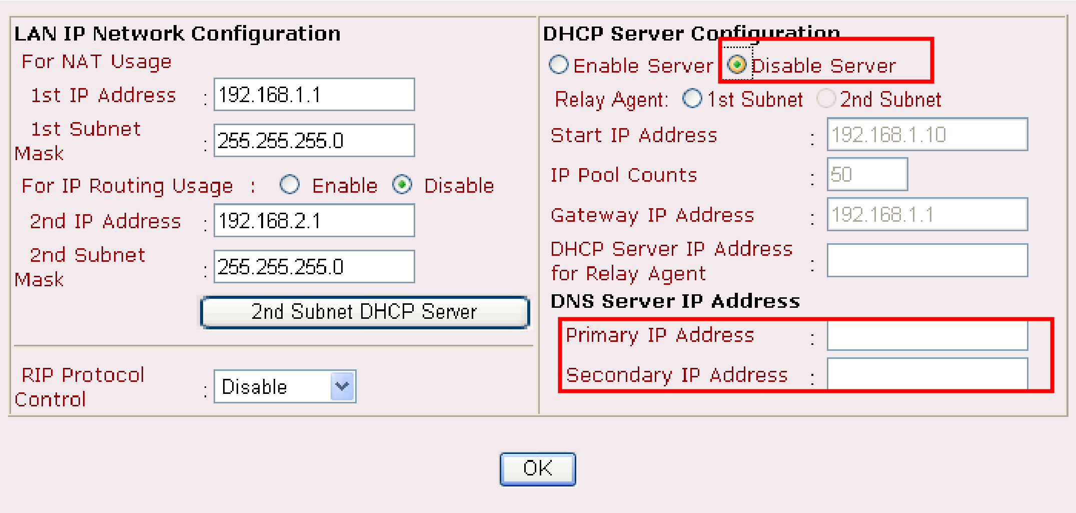
Primary IP Address :

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 IP Network Configuration

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

2nd Subnet DHCP Server

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

Primary IP Address :

Secondary IP Address :

OK

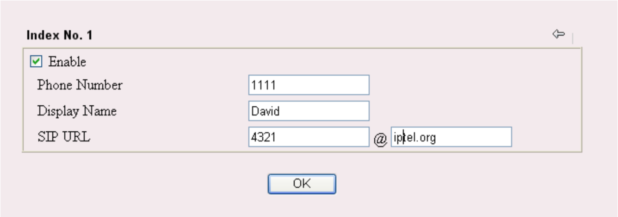
5.5 Calling Scenario for VoIP function

5.5.1 Calling via SIP Sever

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

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

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



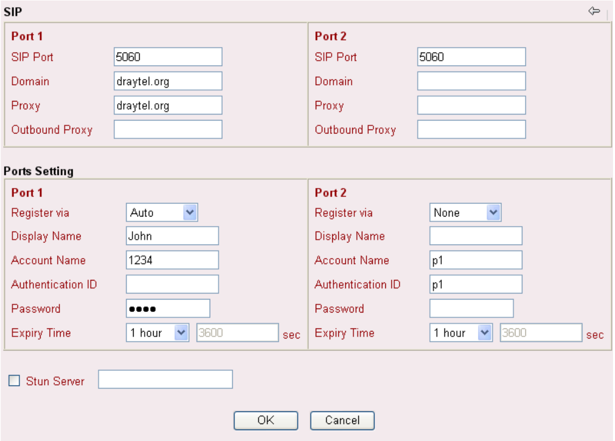
Index No. 1

☑ Enable

Phone Number	1111
Display Name	David
SIP URL	4321 @ iptel.org

SIP Accounts Settings ---

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



SIP

Port 1		Port 2	
SIP Port	5060	SIP Port	5060
Domain	draytel.org	Domain	
Proxy	draytel.org	Proxy	
Outbound Proxy		Outbound Proxy	

Ports Setting

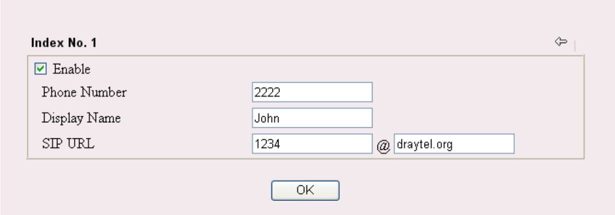
Port 1		Port 2	
Register via	Auto	Register via	None
Display Name	John	Display Name	
Account Name	1234	Account Name	p1
Authentication ID		Authentication ID	p1
Password	••••	Password	
Expiry Time	1 hour 3600 sec	Expiry Time	1 hour 3600 sec

□ Stun Server

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

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

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

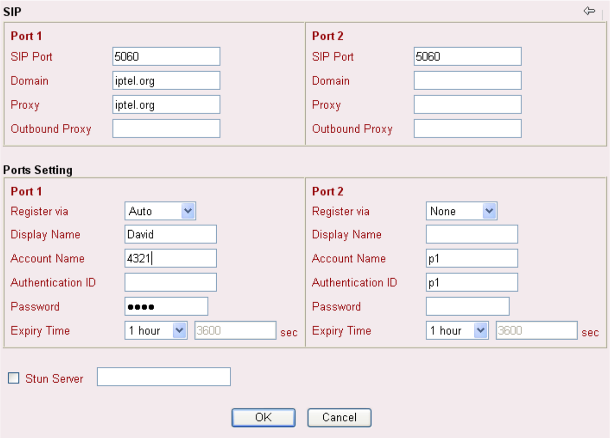


Index No. 1

☑ Enable

Phone Number	2222
Display Name	John
SIP URL	1234 @ draytel.org

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



SIP

Port 1		Port 2	
SIP Port	5060	SIP Port	5060
Domain	iptel.org	Domain	
Proxy	iptel.org	Proxy	
Outbound Proxy		Outbound Proxy	

Ports Setting

Port 1		Port 2	
Register via	Auto	Register via	None
Display Name	David	Display Name	
Account Name	4321	Account Name	p1
Authentication ID		Authentication ID	p1
Password	••••	Password	
Expiry Time	1 hour 3600 sec	Expiry Time	1 hour 3600 sec

□ Stun Server

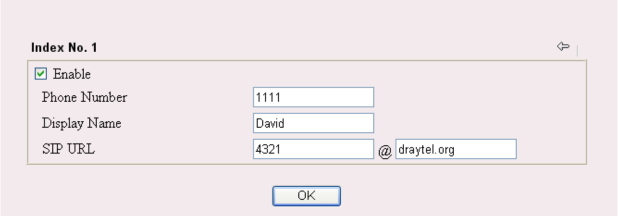
CODEC/RTP/DTMF ---
(Use default value)

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

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

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

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



Index No. 1

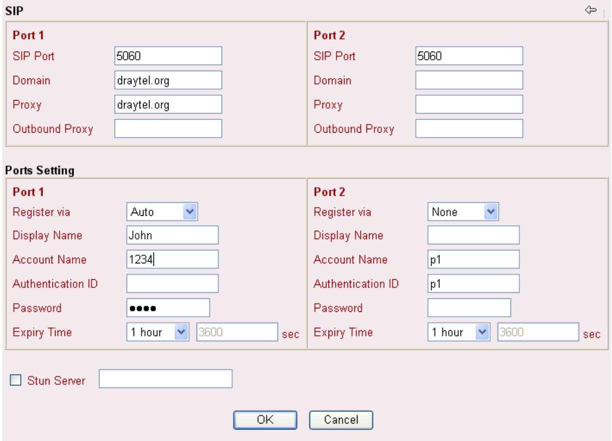
☑ Enable

Phone Number	1111
Display Name	David
SIP URL	4321 @ draytel.org

OK

SIP Accounts Settings ---

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



SIP

Port 1		Port 2	
SIP Port	5060	SIP Port	5060
Domain	draytel.org	Domain	
Proxy	draytel.org	Proxy	
Outbound Proxy		Outbound Proxy	

Ports Setting

Port 1		Port 2	
Register via	Auto	Register via	None
Display Name	John	Display Name	
Account Name	1234	Account Name	p1
Authentication ID		Authentication ID	p1
Password	●●●●	Password	
Expiry Time	1 hour 3600 sec	Expiry Time	1 hour 3600 sec

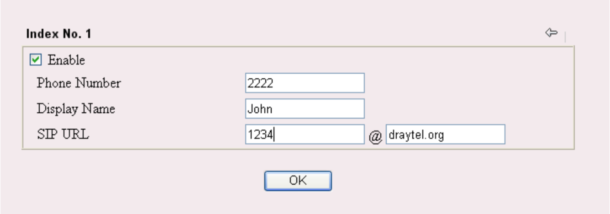
□ Stun Server

OK Cancel

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

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

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



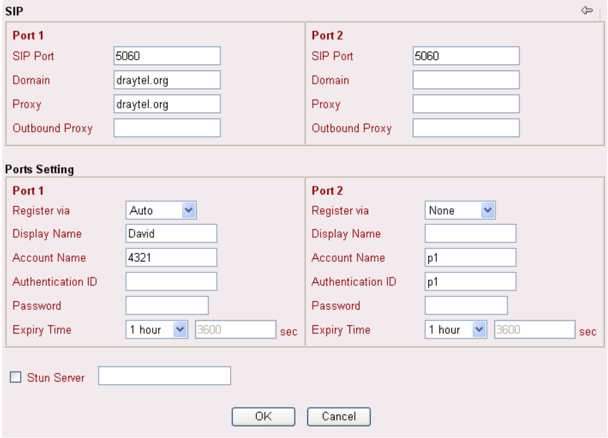
Index No. 1

☑ Enable

Phone Number	2222
Display Name	John
SIP URL	1234 @ draytel.org

OK

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



SIP

Port 1		Port 2	
SIP Port	5060	SIP Port	5060
Domain	draytel.org	Domain	
Proxy	draytel.org	Proxy	
Outbound Proxy		Outbound Proxy	

Ports Setting

Port 1		Port 2	
Register via	Auto	Register via	None
Display Name	David	Display Name	
Account Name	4321	Account Name	p1
Authentication ID		Authentication ID	p1
Password		Password	
Expiry Time	1 hour 3600 sec	Expiry Time	1 hour 3600 sec

□ Stun Server

OK Cancel

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

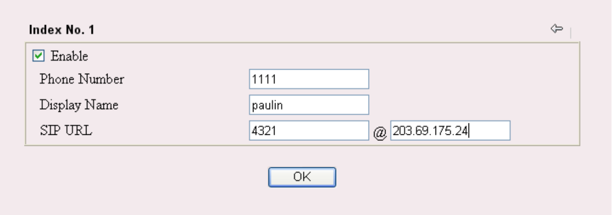
David calls John
He picks up the phone and dials 2222# (DialPlan Phone Number for John) Or,
He picks up the phone and dials 1234# (John’s Account Name)

5.5.2 Peer-to-Peer Calling

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

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

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

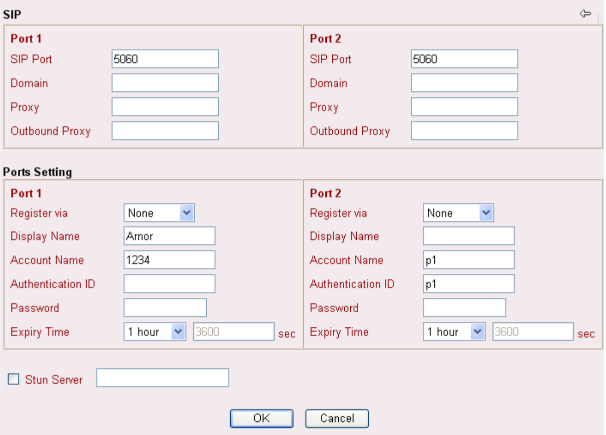


Index No. 1

☑ Enable

Phone Number	1111
Display Name	paulin
SIP URL	4321 @ 203.69.175.24

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



SIP

	Port 1		Port 2
SIP Port	5060	SIP Port	5060
Domain		Domain	
Proxy		Proxy	
Outbound Proxy		Outbound Proxy	

Ports Setting

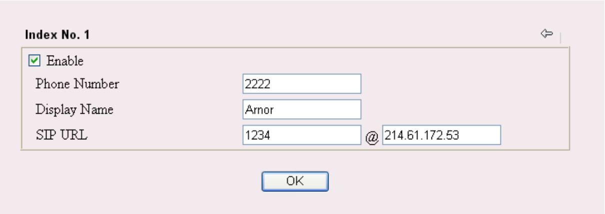
	Port 1		Port 2
Register via	None	Register via	None
Display Name	Arnor	Display Name	
Account Name	1234	Account Name	p1
Authentication ID		Authentication ID	p1
Password		Password	
Expiry Time	1 hour 3600 sec	Expiry Time	1 hour 3600 sec

□ Stun Server

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

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

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

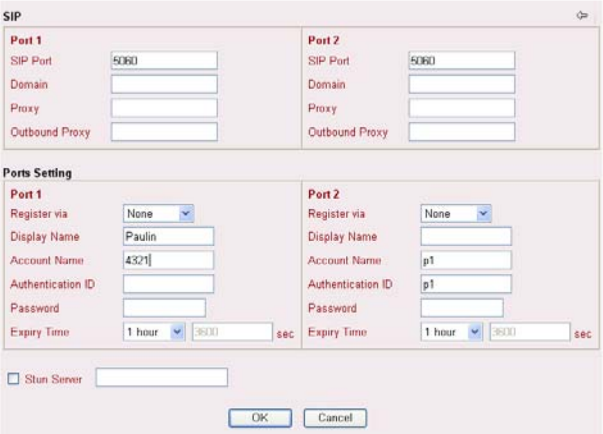


Index No. 1

☑ Enable

Phone Number	2222
Display Name	Arnor
SIP URL	1234 @ 214.61.172.53

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



SIP

	Port 1		Port 2
SIP Port	5060	SIP Port	5060
Domain		Domain	
Proxy		Proxy	
Outbound Proxy		Outbound Proxy	

Ports Setting

	Port 1		Port 2
Register via	None	Register via	None
Display Name	Paulin	Display Name	
Account Name	4321	Account Name	p1
Authentication ID		Authentication ID	p1
Password		Password	
Expiry Time	1 hour 3600 sec	Expiry Time	1 hour 3600 sec

□ Stun Server

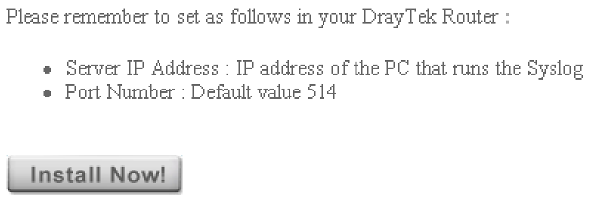
CODEC/RTP/DTMF---
(Use default value)

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

5.6 Upgrade Firmware for Your Router

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

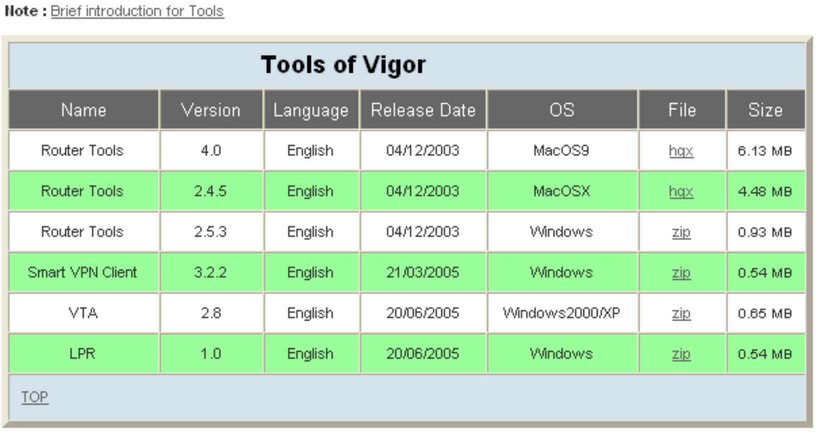
1. Insert CD of the router to your CD ROM.
2. From the webpage, please find out **Utility** menu and click it.
3. On the webpage of Utility, click **Install Now!** (under Syslog description) to install the corresponding program.



Please remember to set as follows in your DrayTek Router :

- Server IP Address : IP address of the PC that runs the Syslog
- Port Number : Default value 514

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



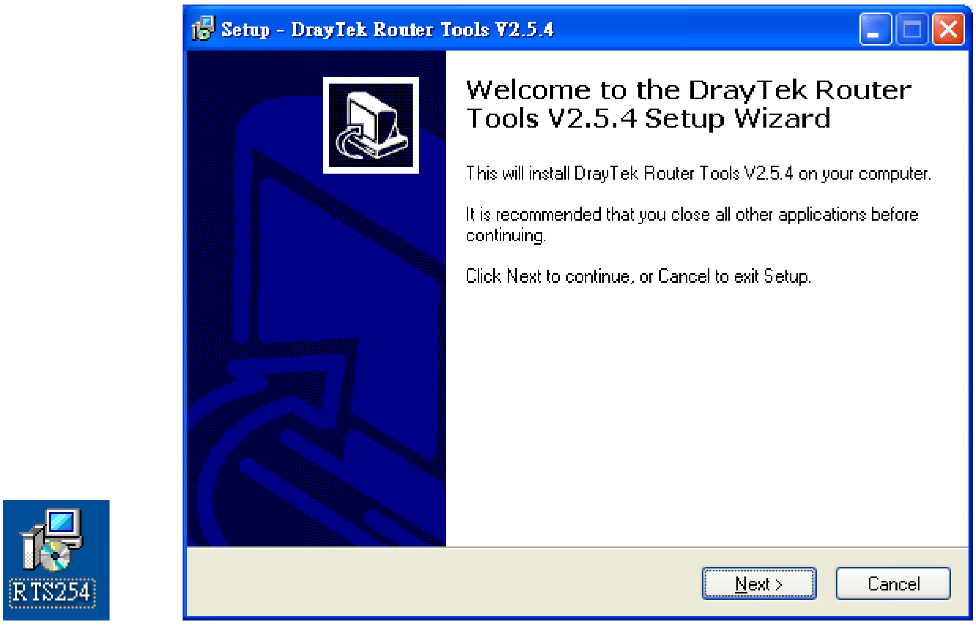
Note : Brief introduction for Tools

Tools of Vigor

Name	Version	Language	Release Date	OS	File	Size
Router Tools	4.0	English	04/12/2003	MacOS9	hqx	6.13 MB
Router Tools	2.4.5	English	04/12/2003	MacOSX	hqx	4.48 MB
Router Tools	2.5.3	English	04/12/2003	Windows	zip	0.93 MB
Smart VPN Client	3.2.2	English	21/03/2005	Windows	zip	0.54 MB
VTA	2.8	English	20/06/2005	Windows2000/XP	zip	0.65 MB
LPR	1.0	English	20/06/2005	Windows	zip	0.54 MB

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

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



Welcome to the DrayTek Router Tools V2.5.4 Setup Wizard

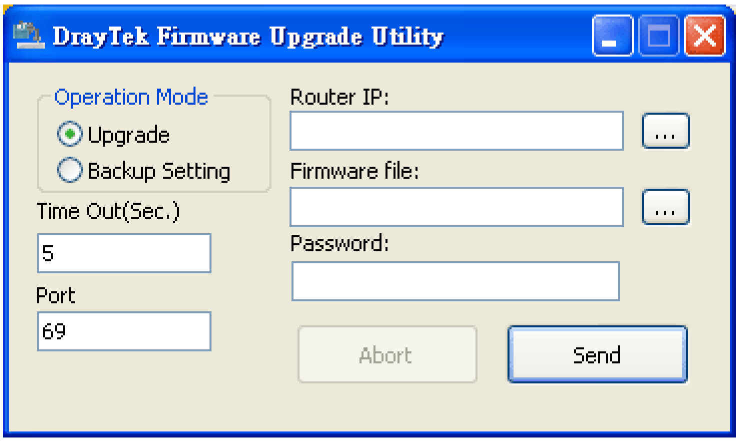
This will install DrayTek Router Tools V2.5.4 on your computer.

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

Click Next to continue, or Cancel to exit Setup.

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

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



Operation Mode
- ● Upgrade
- ○ Backup Setting

Time Out(Sec.): 5

Port: 69

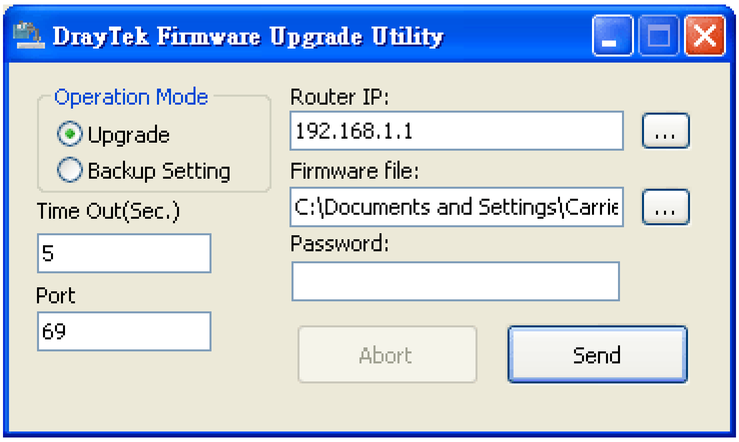
Router IP:

Firmware file:

Password:

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

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



Operation Mode
● Upgrade
○ Backup Setting

Time Out(Sec.): 5

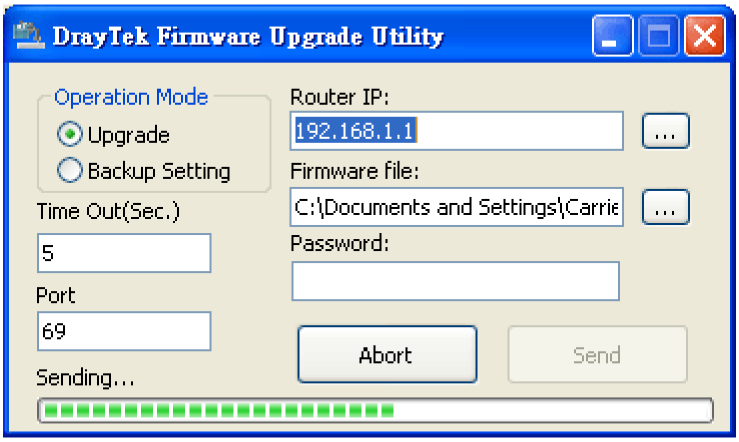
Port: 69

Router IP: 192.168.1.1

Firmware file: C:\Documents and Settings\Carrie

Password:

14. Click **Send**.



Operation Mode
● Upgrade
○ Backup Setting

Time Out(Sec.): 5

Port: 69

Router IP: 192.168.1.1

Firmware file: C:\Documents and Settings\Carrie

Password:

Sending...

15. Now the firmware update is finished.

This page is left blank.

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.

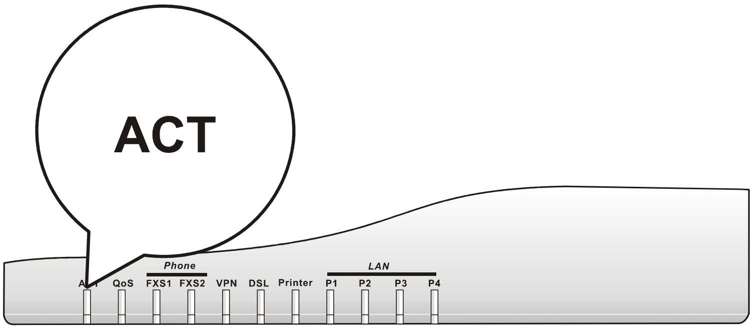
If all above stages are done and the router still cannot run normally, it is the time for you to contact your dealer for advanced help.

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 "**2.1 Hardware Installation**" for details.

2. Turn on the router. Make sure the **ACT LED** blink once per second and the correspondent **LAN LED** is bright.



3. If not, it means that there is something wrong with the hardware status. Simply back to **"2.1 Hardware Installation"** to execute the hardware installation again. And then, try again.

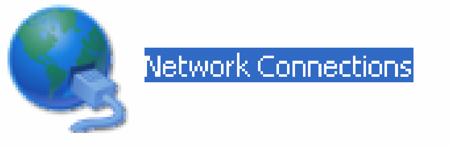
6.2 Checking If the Network Connection Settings on Your Computer Is OK or Not

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.

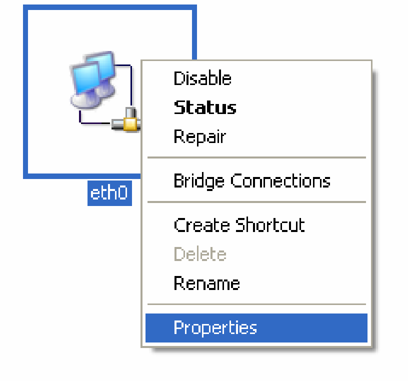
For Windows

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**.

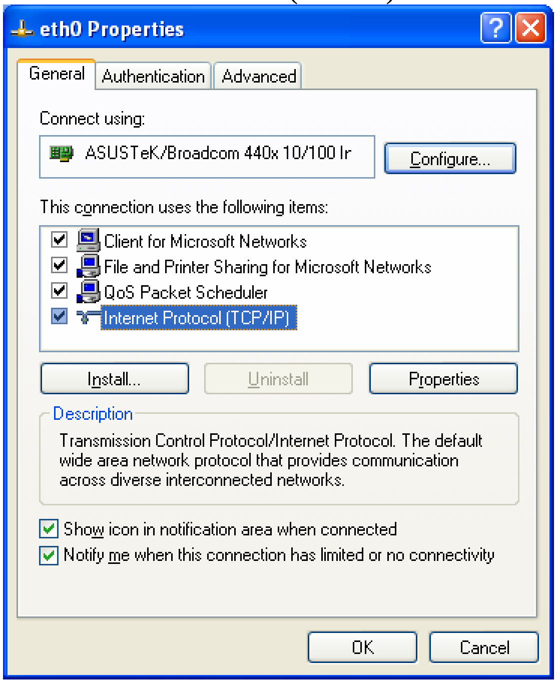
1. Go to Control Panel and then double-click on Network Connections.



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



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



Connect using:

ASUSTeK/Broadcom 440x 10/100 Ir

This connection uses the following items:

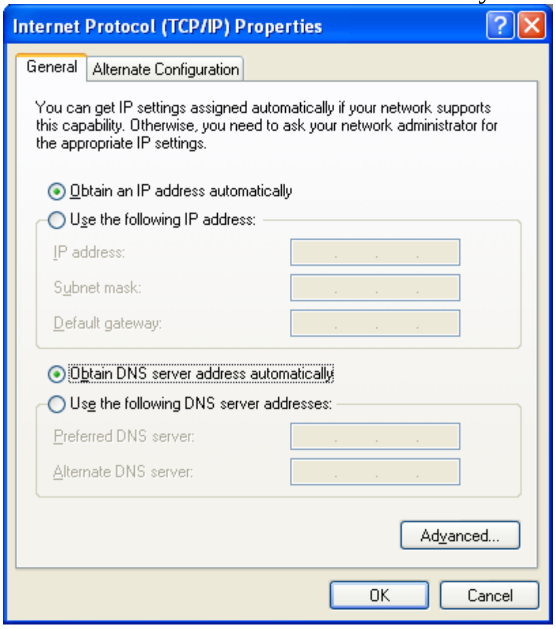
☑ Client for Microsoft Networks
☑ File and Printer Sharing for Microsoft Networks
☑ QoS Packet Scheduler
☑ Internet Protocol (TCP/IP)

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

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



Internet Protocol (TCP/IP) Properties

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

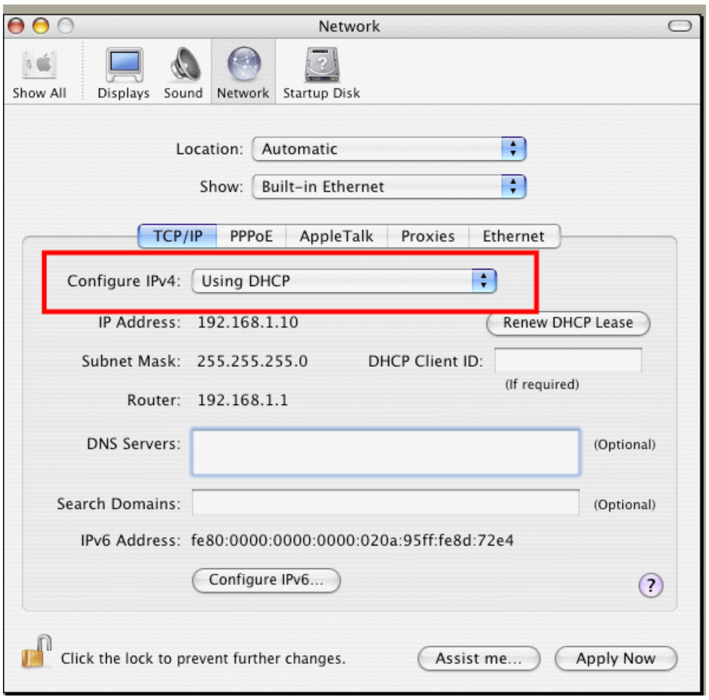
○ Use the following DNS server addresses:

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.



Network

Location: Automatic

Show: Built-in Ethernet

Configure IPv4: Using DHCP

IP Address: 192.168.1.10

Subnet Mask: 255.255.255.0

Router: 192.168.1.1

DHCP Client ID: (If required)

DNS Servers: (Optional)

Search Domains: (Optional)

IPv6 Address: fe80:0000:0000:0000:020a:95ff:fe8d:72e4

Click the lock to prevent further changes.

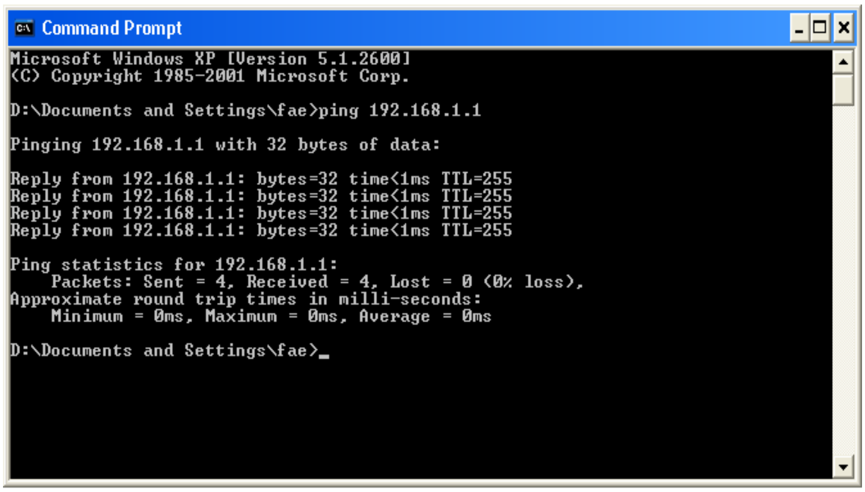
6.3 Pinging the Router from Your Computer

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 4.2)

Please follow the steps below to ping the router correctly.

For Windows

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

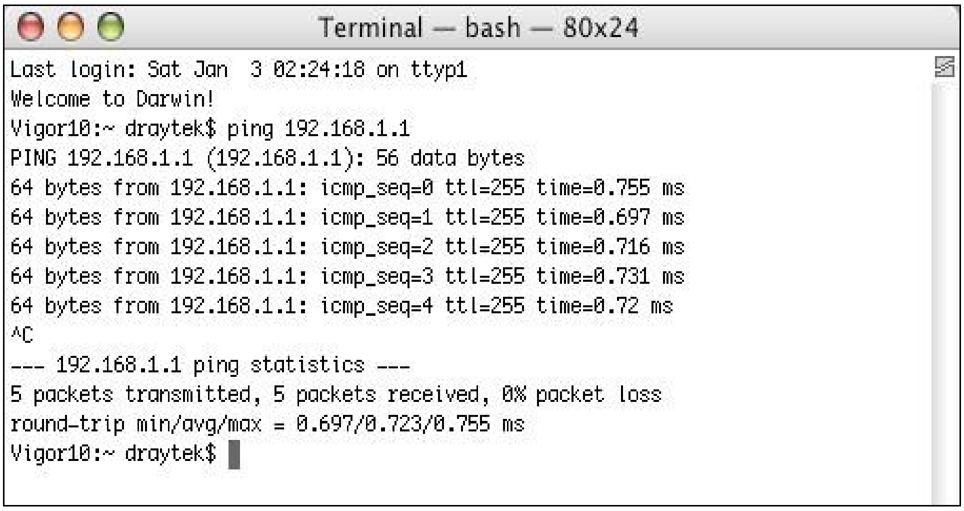


```
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

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]. It the link is OK, the line of “Reply from 192.168.1.1:bytes=32 time<1ms TTL=25” will appear.
4. If the line does not appear, please check the IP address setting of your computer.

For MacOs (Terminal)

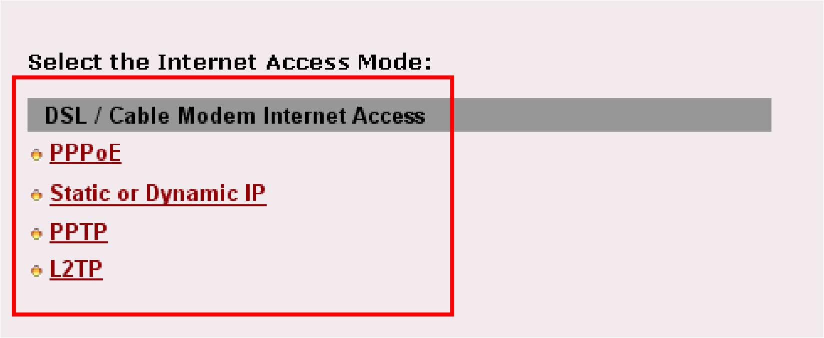
1. Double click on the current used MacOs on the desktop.
2. Open the **Application** folder and get into **Utilities**.
3. Double click **Terminal**. The Terminal window will appear.
4. Type **ping 192.168.1.1** and press [Enter]. It the link is OK, the line of **“64 bytes from 192.168.1.1: icmp_seq=0 ttl=255 time=xxxx ms**” will appear.



```
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

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



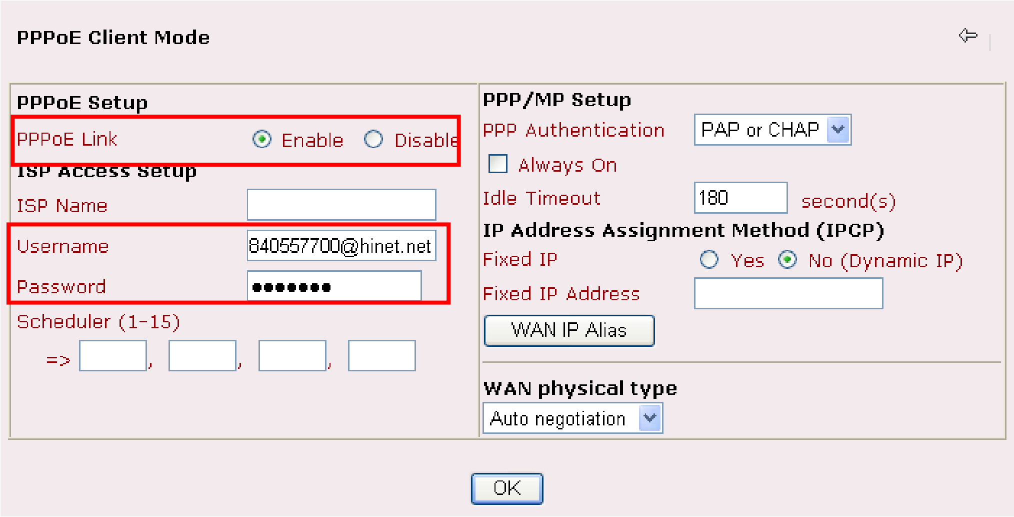
Select the Internet Access Mode:

DSL / Cable Modem Internet Access

- PPPoE
- Static or Dynamic IP
- PPTP
- L2TP

Here, we take PPPoE for an example.

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**.



PPPoE Client Mode

PPPoE Setup

PPPoE Link	● Enable ○ Disable

ISP Access Setup

ISP Name	
Username	840557700@hinet.net
Password	●●●●●●●
Scheduler (1-15)	
=>	, , ,

PPP/MP Setup

PPP Authentication	PAP or CHAP
□ Always On	
Idle Timeout	180 second(s)

IP Address Assignment Method (IPCP)

Fixed IP	○ Yes ● No (Dynamic IP)
Fixed IP Address	

WAN physical type

Auto negotiation

6.5 Backing to Factory Default Setting If Necessary

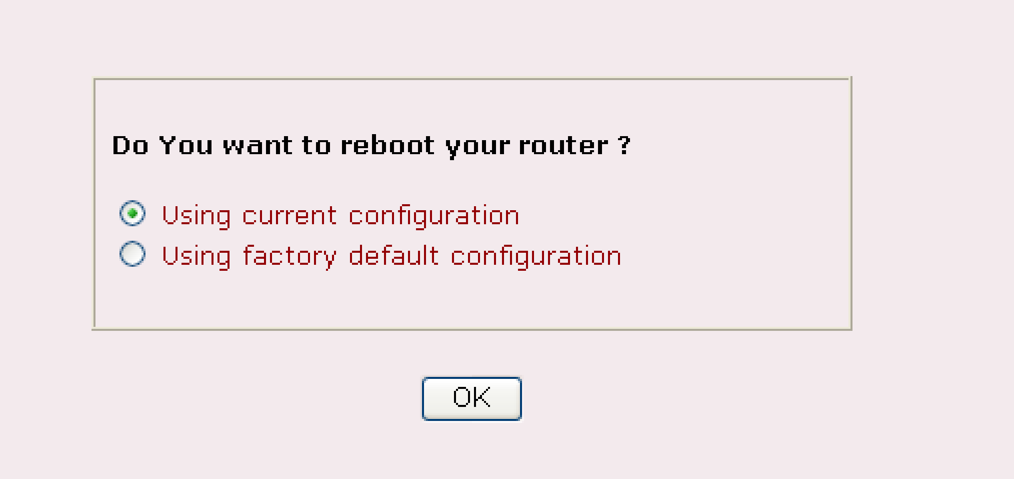
Sometimes, a wrong connection can be improved by returning to the default settings. Try to reset the router by software or hardware.

> **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 Management** 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.



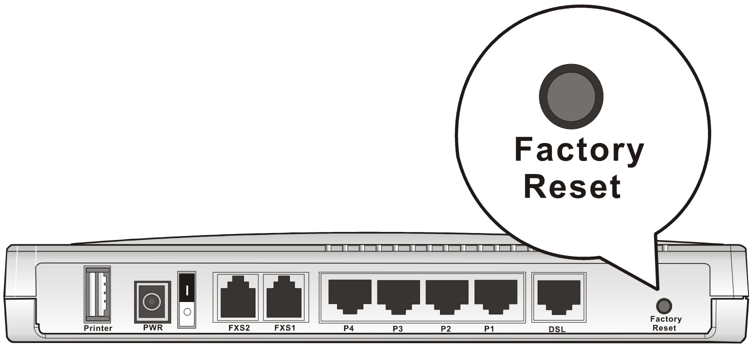
Do You want to reboot your router ?

● Using current configuration

○ Using factory default configuration

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.