



Vigor2110 Series Broadband Firewall Router User's Guide

Version: 1.0

Date: 2008/09/08

Copyright Information

Copyright Declarations

Copyright 2008 All rights reserved. This publication contains information that is protected by copyright. No part may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language without written permission from the copyright holders.

Trademarks

The following trademarks are used in this document:

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

Safety Instructions and Approval

Safety Instructions

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

Warranty

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

Be a Registered Owner

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

Firmware & Tools Updates

Due to the continuous evolution of DrayTek technology, all routers will be regularly upgraded. Please consult the DrayTek web site for more information on newest firmware, tools and documents.

<http://www.draytek.com>

European Community Declarations

Manufacturer: DrayTek Corp.

Address: No. 26, Fu Shing Road, HuKou County, HsinChu Industrial Park, Hsin-Chu, Taiwan 303

Product: Vigor2110 Series Router

DrayTek Corp. declares that Vigor2110 Series of routers are in compliance with the following essential requirements and other relevant provisions of R&TTE Directive 1999/5/EEC.

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

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

Regulatory Information

Federal Communication Commission Interference Statement

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

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

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

- (1) This device may not cause harmful interference, and
- (2) This device may accept any interference received, including interference that may cause undesired operation.

.

Please visit http://www.draytek.com/about_us/R_TTE_Certification.php.



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

Table of Contents

1

| | |
|---|----------|
| Preface | 1 |
| 1.1 Web Configuration Buttons Explanation | 1 |
| 1.2 LED Indicators and Connectors | 2 |
| 1.2.1 For Vigor2110 | 2 |
| 1.2.2 For Vigor2110n | 4 |
| 1.2.3 For Vigor2110Vn | 6 |
| 1.3 Hardware Installation | 8 |
| Stand Installation | 9 |
| 1.4 Printer Installation | 10 |

2

| | |
|---|-----------|
| Configuring Basic Settings | 15 |
| 2.1 Two-Level Management | 15 |
| 2.2 Accessing Web Page | 15 |
| 2.3 Changing Password | 16 |
| 2.4 Quick Start Wizard | 18 |
| 2.4.2 PPPoE | 19 |
| 2.4.3 PPTP | 20 |
| 2.4.4 Static IP | 21 |
| 2.4.5 DHCP | 22 |
| 2.5 Online Status | 22 |
| 2.6 Saving Configuration | 23 |

3

| | |
|--|-----------|
| User Mode Operation | 25 |
| 3.1 Internet Access | 25 |
| 3.1.1 Basics of Internet Protocol (IP) Network | 25 |
| 3.1.2 PPPoE | 26 |
| 3.1.3 Static or Dynamic IP | 28 |
| 3.1.4 PPTP/L2TP | 30 |
| 3.2 LAN | 32 |
| 3.2.1 Basics of LAN | 32 |
| 3.2.2 General Setup | 33 |
| 3.3 NAT | 36 |
| 3.3.1 Port Redirection | 36 |
| 3.3.2 DMZ Host | 38 |
| 3.3.3 Open Ports | 41 |
| 3.4 Applications | 42 |
| 3.4.1 Dynamic DNS | 42 |

| | |
|------------------------------|----|
| 3.4.2 UPnP | 44 |
| 3.5 Wireless LAN | 46 |
| 3.5.1 Basic Concepts | 46 |
| 3.5.2 General Setup | 48 |
| 3.5.3 Security | 51 |
| 3.5.4 Access Control | 52 |
| 3.5.5 Station List | 53 |
| 3.6 System Maintenance | 53 |
| 3.6.1 System Status | 54 |
| 3.6.2 User Password | 55 |
| 3.6.3 Time and Date | 55 |
| 3.6.4 Reboot System | 56 |
| 3.7 Diagnostics | 56 |
| 3.7.1 DHCP Table | 56 |
| 3.7.2 Ping Diagnosis | 57 |
| 3.7.3 Trace Route | 58 |

4

Admin Mode Operation59

| | |
|--|-----|
| 4.1 Internet Access | 59 |
| 4.1.1 Basics of Internet Protocol (IP) Network | 59 |
| 4.1.2 PPPoE | 60 |
| 4.1.3 Static or Dynamic IP | 62 |
| 4.1.4 PPTP/L2TP | 64 |
| 4.2 LAN | 66 |
| 4.2.1 Basics of LAN | 66 |
| 4.2.2 General Setup | 68 |
| 4.2.3 Static Route | 71 |
| 4.2.4 VLAN | 74 |
| 4.2.5 Bind IP to MAC | 75 |
| 4.3 NAT | 76 |
| 4.3.1 Port Redirection | 76 |
| 4.3.2 DMZ Host | 79 |
| 4.3.3 Open Ports | 81 |
| 4.4 Firewall | 83 |
| 4.4.1 Basics for Firewall | 83 |
| 4.4.2 General Setup | 85 |
| 4.4.3 Filter Setup | 87 |
| 4.4.4 DoS Defense | 92 |
| 4.5 Objects Settings | 95 |
| 4.5.1 IP Object | 95 |
| 4.5.2 IP Group | 97 |
| 4.5.3 Service Type Object | 99 |
| 4.5.4 Service Type Group | 100 |
| 4.5.5 Keyword Object | 101 |
| 4.5.6 Keyword Group | 102 |
| 4.5.7 File Extension Object | 103 |
| 4.5.8 IM Object | 105 |
| 4.5.9 P2P Object | 106 |
| 4.5.10 Misc Object | 107 |

| | |
|--|-----|
| 4.6 CSM Profile | 108 |
| 4.6.1 IM/P2P Filter Profile | 109 |
| 4.6.2 URL Content Filter Profile | 110 |
| 4.6.3 Web Content Filter Profile | 114 |
| 4.7 Bandwidth Management | 116 |
| 4.7.1 Sessions Limit | 116 |
| 4.7.2 Bandwidth Limit | 118 |
| 4.7.3 Quality of Service | 119 |
| 4.8 Applications | 126 |
| 4.8.1 Dynamic DNS | 126 |
| 4.8.2 Schedule | 128 |
| 4.8.3 RADIUS | 129 |
| 4.8.4 UPnP | 131 |
| 4.8.5 IGMP | 133 |
| 4.8.6 Wake on LAN | 133 |
| 4.9 VPN and Remote Access | 135 |
| 4.9.1 Remote Access Control | 135 |
| 4.9.2 PPP General Setup | 135 |
| 4.9.3 IPsec General Setup | 136 |
| 4.9.4 IPsec Peer Identity | 137 |
| 4.9.5 Remote Dial-in User | 140 |
| 4.9.6 LAN to LAN | 142 |
| 4.9.7 Connection Management | 149 |
| 4.10 Certificate Management | 150 |
| 4.10.1 Local Certificate | 150 |
| 4.10.2 Trusted CA Certificate | 152 |
| 4.10.3 Certificate Backup | 153 |
| 4.11 Wireless LAN | 153 |
| 4.11.1 Basic Concepts | 153 |
| 4.11.2 General Setup | 155 |
| 4.11.3 Security | 158 |
| 4.11.4 Access Control | 160 |
| 4.11.5 WPS | 161 |
| 4.11.6 WDS | 163 |
| 4.11.7 AP Discovery | 166 |
| 4.11.8 Station List | 167 |
| 4.12 System Maintenance | 169 |
| 4.12.1 System Status | 169 |
| 4.12.2 TR-069 | 170 |
| 4.12.3 Administrator Password | 171 |
| 4.12.4 Configuration Backup | 171 |
| 4.12.5 Syslog/Mail Alert | 173 |
| 4.12.6 Time and Date | 175 |
| 4.12.7 Management | 176 |
| 4.12.8 Reboot System | 177 |
| 4.12.9 Firmware Upgrade | 178 |
| 4.13 Diagnostics | 179 |
| 4.13.1 Dial-out Trigger | 179 |
| 4.13.2 Routing Table | 180 |
| 4.13.3 ARP Cache Table | 180 |
| 4.13.4 DHCP Table | 181 |
| 4.13.5 NAT Sessions Table | 181 |

| | |
|-------------------------------|-----|
| 4.13.6 Data Flow Monitor..... | 182 |
| 4.13.7 Ping Diagnosis..... | 183 |
| 4.13.8 Trace Route | 184 |

5

Application and Examples185

| | |
|---|-----|
| 5.1 Create a LAN-to-LAN Connection Between Remote Office and Headquarter | 185 |
| 5.2 Create a Remote Dial-in User Connection Between the Teleworker and Headquarter..... | 192 |
| 5.3 QoS Setting Example..... | 196 |
| 5.4 LAN – Created by Using NAT | 199 |
| 4.5 Upgrade Firmware for Your Router | 201 |
| 5.6 Request a certificate from a CA server on Windows CA Server | 204 |
| 5.7 Request a CA Certificate and Set as Trusted on Windows CA Server | 208 |

6

Trouble Shooting211

| | |
|---|-----|
| 6.1 Checking If the Hardware Status Is OK or Not..... | 211 |
| 6.2 Checking If the Network Connection Settings on Your Computer Is OK or Not | 212 |
| 6.3 Pinging the Router from Your Computer | 214 |
| 6.4 Checking If the ISP Settings are OK or Not | 215 |
| 6.5 Backing to Factory Default Setting If Necessary | 217 |
| 6.6 Contacting Your Dealer | 218 |

1

Preface

Vigor2110 series is a broadband router. It integrates IP layer QoS, NAT session/bandwidth management to help users control works well with large bandwidth.

By adopting hardware-based VPN platform and hardware encryption of AES/DES/3DS, the router increases the performance of VPN greatly, and offers several protocols (such as IPSec/PPTP/L2TP) with up to 2 VPN tunnels.


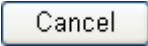
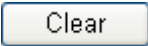
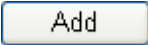

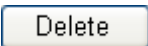
The object-based design used in SPI (Stateful Packet Inspection) firewall allows users to set firewall policy with ease. CSM (Content Security Management) provides users control and management in IM (Instant Messenger) and P2P (Peer to Peer) more efficiency than before. By the way, DoS/DDoS prevention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

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

In addition, Vigor2110 series supports USB interface for connecting USB printer to share printer or USB storage device for sharing files. Vigor2110 series provides two-level management to simplify the configuration of network connection. The user mode allows user accessing into WEB interface via simple configuration. However, if users want to have advanced configurations, they can access into WEB interface through admin mode.

1.1 Web Configuration Buttons Explanation

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

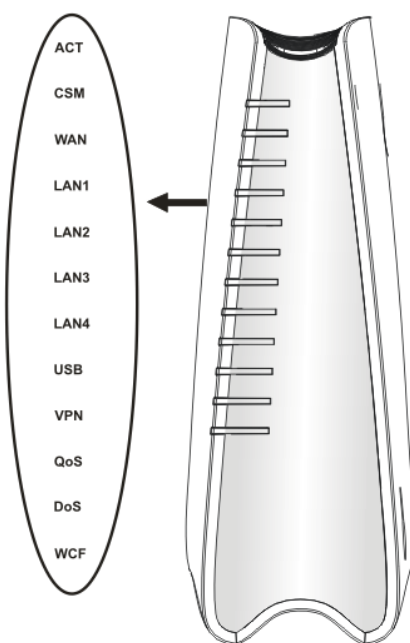
| | |
|---|--|
|  | Save and apply current settings. |
|  | Cancel current settings and recover to the previous saved settings. |
|  | Clear all the selections and parameters settings, including selection from drop-down list. All the values must be reset with factory default settings. |
|  | Add new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

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

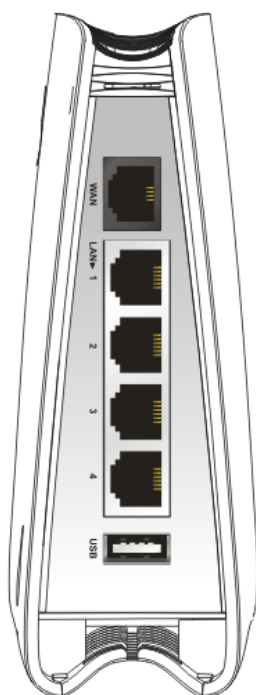
1.2 LED Indicators and Connectors

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

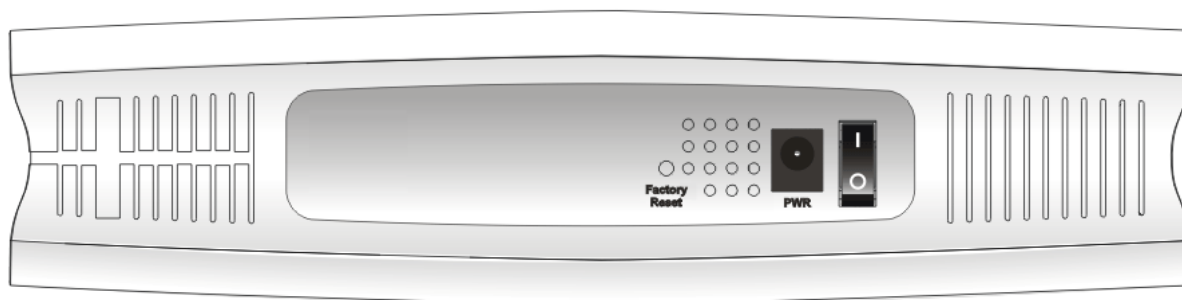
1.2.1 For Vigor2110



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

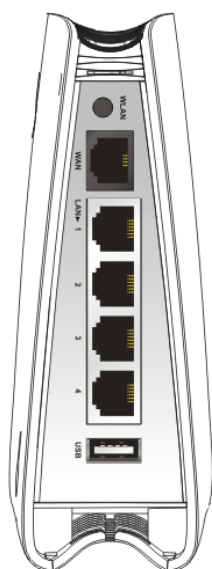
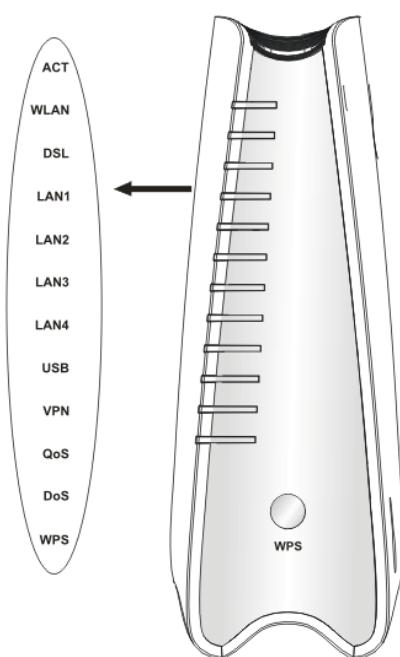


| Interface | Description |
|-----------|---|
| WAN | Connector for accessing the Internet. |
| LAN (1-4) | Connectors for local networked devices. |
| USB | Connector for USB storage device (Pen Driver/Mobile HD) or printer. |

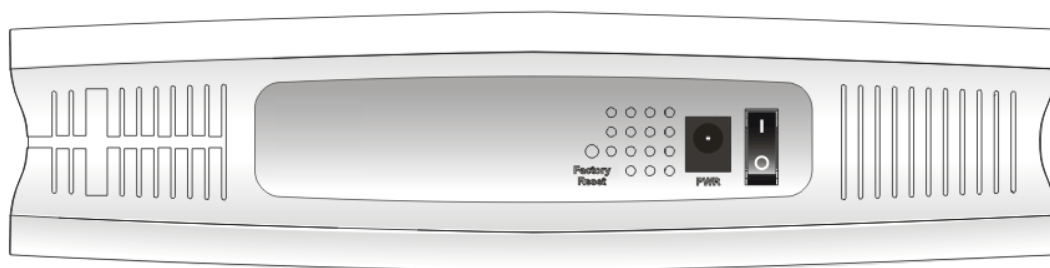


| Interface | Description |
|---------------|---|
| Factory Reset | Restore the default settings. Usage: Turn on the router (ACT LED is blinking). Press the hole and keep for more than 5 seconds. When you see the ACT LED begins to blink rapidly than usual, release the button. Then the router will restart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

1.2.2 For Vigor2110n

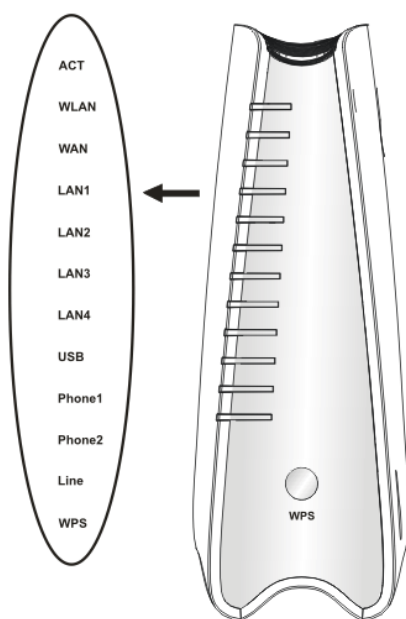


| LED | Status | Explanation |
|----------------|--|--|
| ACT (Activity) | Blinking | The router is powered on and running normally. |
| | Off | The router is powered off. |
| WLAN | On | Wireless access point is ready. |
| | Blinking | It will blink while wireless traffic goes through. |
| WAN | On | The WAN port is connected. |
| | Blinking | It will blink while transmitting data. |
| LAN 1/2/3/4 | On | The port is connected. |
| | Off | The port is disconnected. |
| | Blinking | The data is transmitting. |
| USB | On | A USB device is connected and active. |
| | Blinking | The data is transmitting. |
| VPN | On | The VPN tunnel is active. |
| QoS | On | The QoS function is active. |
| DoS | On | The DoS/DDoS function is active. |
| | Blinking | It will blink while detecting an attack. |
| WPS | On | The WPS is on. |
| | Off | The WPS is off. |
| | Blinking | Waiting for wireless client sending requests for connection about two minutes. |
| WPS Button | On | Press this button for 2 seconds to wait for client device making network connection through WPS. When the LED lights up, the WPS will be on. |
| | Off | The WPS is off. |
| | Blinking | Waiting for wireless client sending requests for connection about two minutes. |
| Interface | Description | |
| WLAN | Press the button once to enable (WLAN LED on) or disable (WLAN LED off) wireless connection. | |
| WAN | Connector for accessing the Internet. | |
| LAN (1-4) | Connectors for local networked devices. | |
| USB | Connector for USB storage (Pen Driver Mobile/HD) or printer. | |

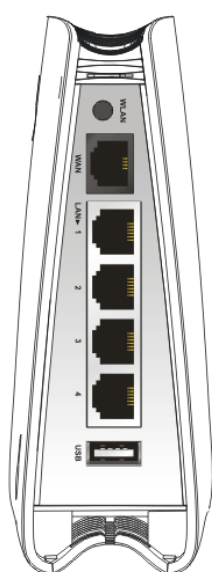


| Interface | Description |
|---------------|---|
| Factory Reset | Restore the default settings. Usage: Turn on the router (ACT LED is blinking). Press the hole and keep for more than 5 seconds. When you see the ACT LED begins to blink rapidly than usual, release the button. Then the router will restart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

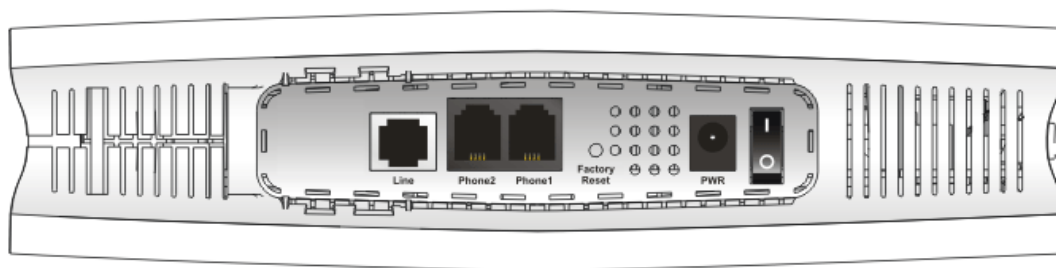
1.2.3 For Vigor2110Vn



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



| Interface | Description |
|-----------|--|
| WLAN | Press the button once to enable (WLAN LED on) or disable (WLAN LED off) wireless connection. |
| WAN | Connector for accessing the Internet. |
| LAN (1-4) | Connectors for local networked devices. |
| USB | Connector for USB storage (Pen Driver Mobile/HD) or printer. |

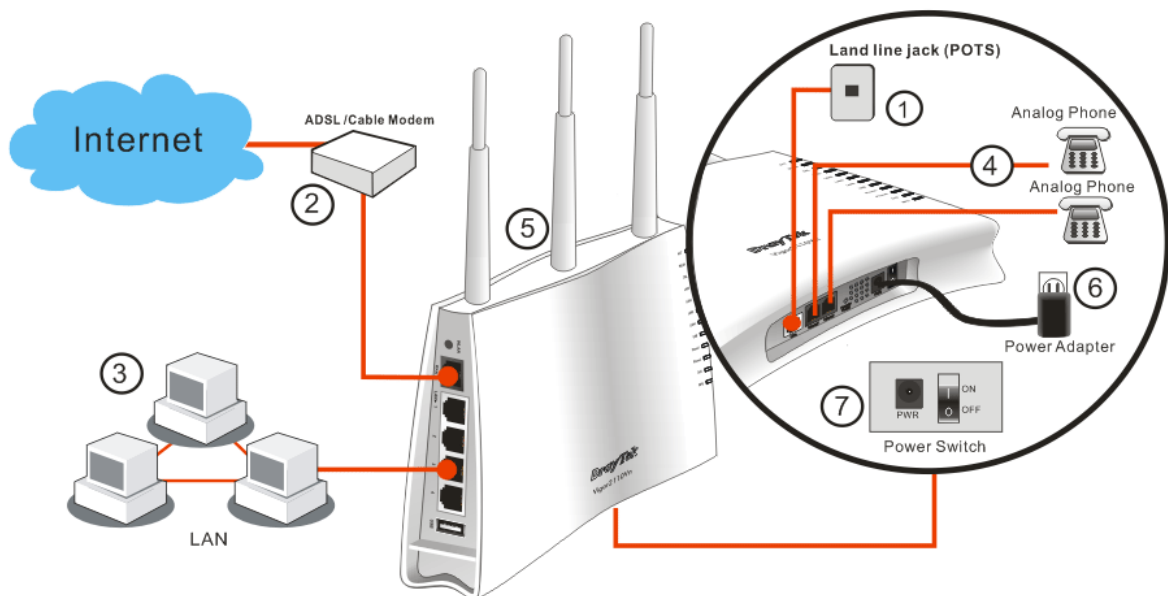


| Interface | Description |
|---------------|---|
| Line | Connector for PSTN life line. |
| Phone2/Phone1 | Connector of analog phone for VoIP communication. |
| Factory Reset | Restore the default settings. Usage: Turn on the router (ACT LED is blinking). Press the hole and keep for more than 5 seconds.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

1.3 Hardware Installation

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

1. Connect Line port to land line jack with a RJ-11 cable (Vn model).
2. Connect this device to a modem with a RJ-45 cable.
3. Connect one port of 4-port switch to your computer with a RJ-45 cable. This device allows you to connect 4 PCs directly.
4. Connect Phone port to a conventional analog telephone.
5. Connect detachable antennas to the router for Vigor2110 series (n model).
6. Connect one end of the power cord to the power port of this device. Connect the other end to the wall outlet of electricity.
7. Power on the router.
8. Check the **ACT** and **WAN**, **LAN** LEDs to assure network connections.



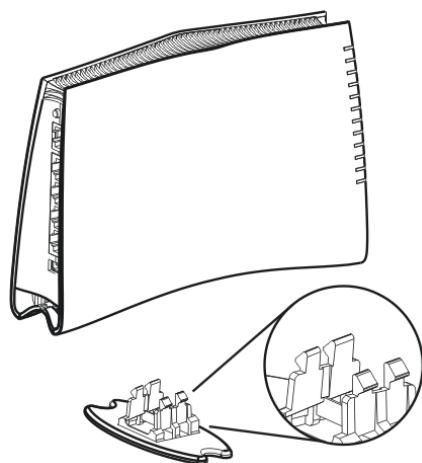
Caution: Caution:

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

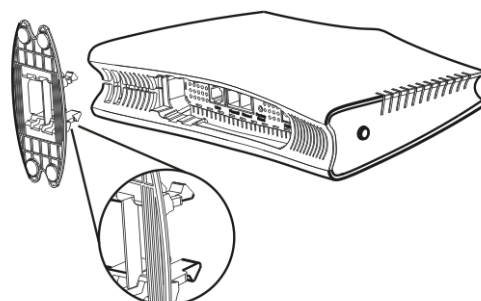
Stand Installation

The Vigor2110 must be placed erectly. Therefore you have to install a stand onto the router to make it standing firmly. Please follow the figures listed below to finish the installation.

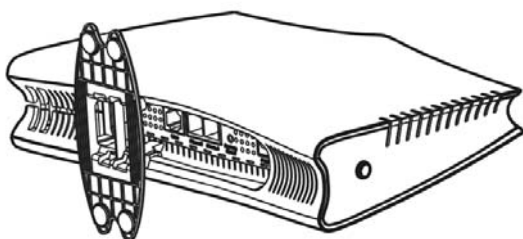
①



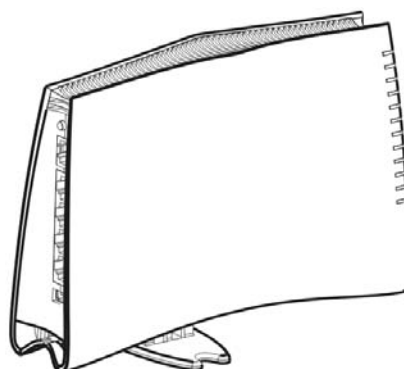
②



③

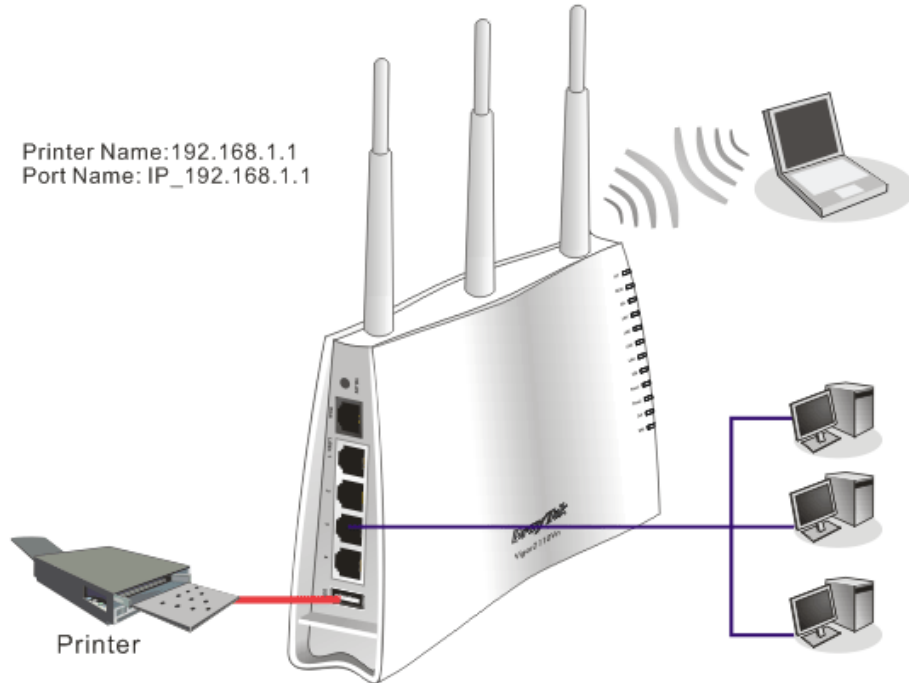


④



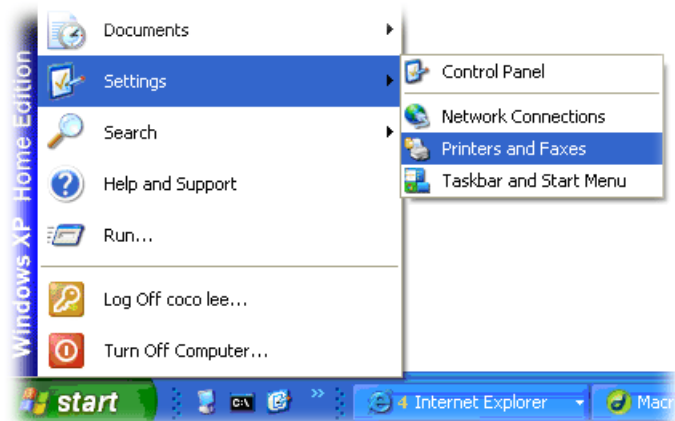
1.4 Printer Installation

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

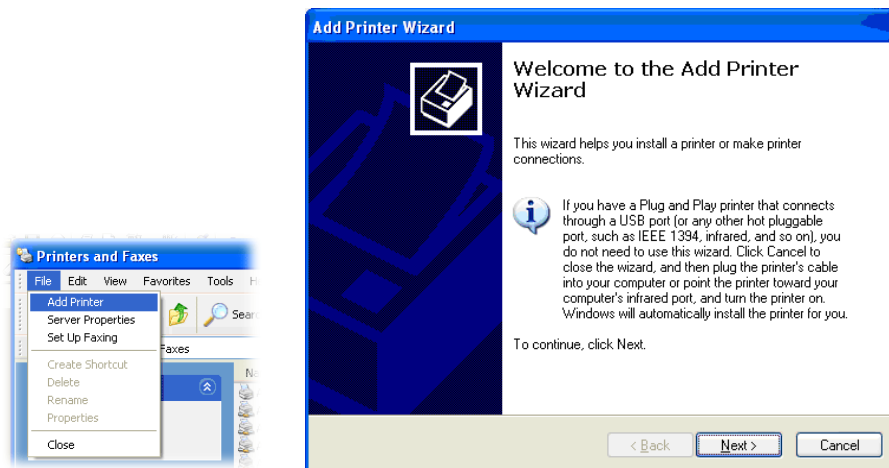


Before using it, please follow the steps below to configure settings for connected computers (or wireless clients).

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



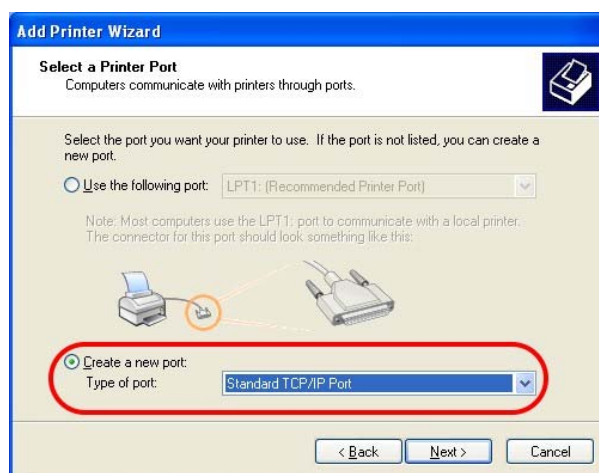
3. Open **File->Add a New Computer**. A welcome dialog will appear. Please click **Next**.



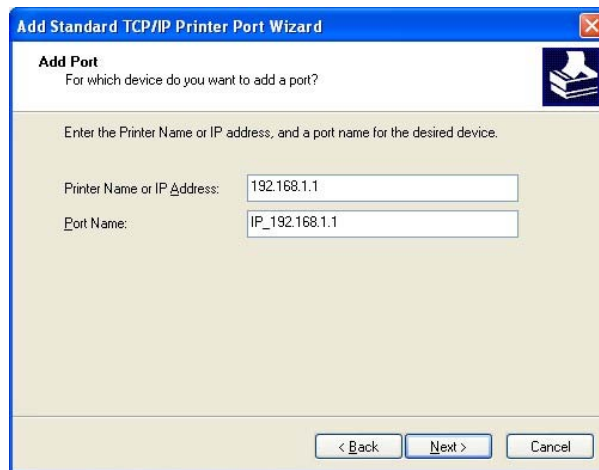
4. Click Local printer attached to this computer and click Next.



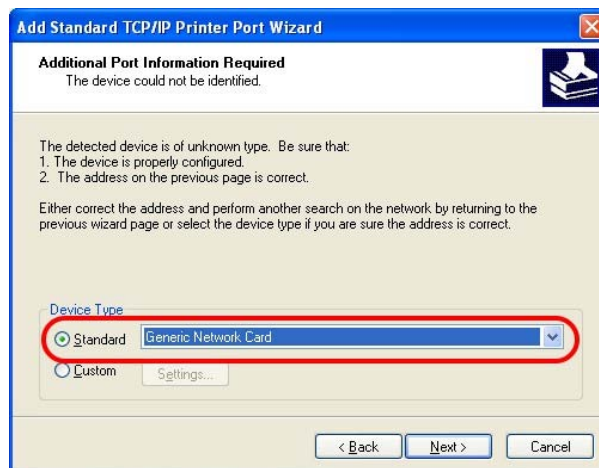
5. In this dialog, choose **Create a new port Type of port** and use the drop down list to select **Standard TCP/IP Port**. Click Next.



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



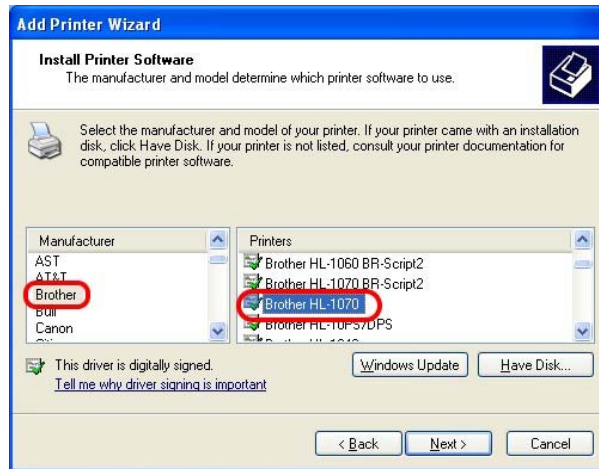
7. Click **Standard** and choose **Generic Network Card**.



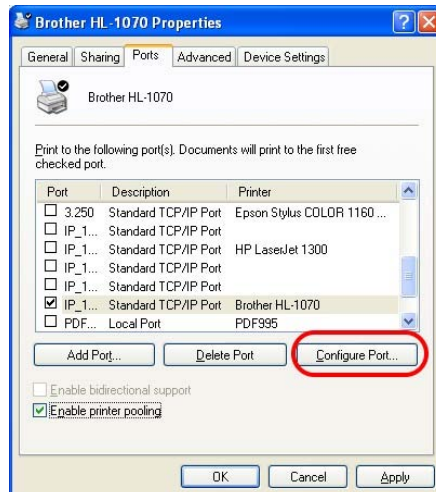
8. Then, in the following dialog, click **Finish**.



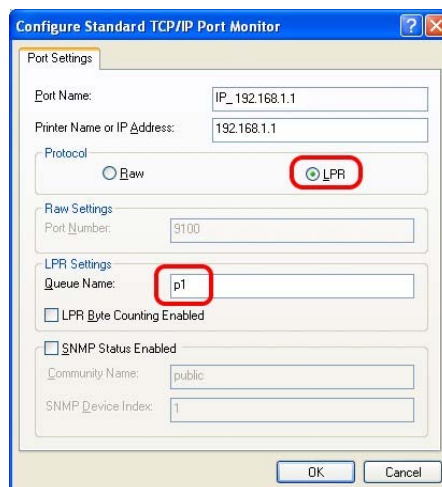
9. Now, your system will ask you to choose right name of the printer that you installed onto the router. Such step can make correct driver loaded onto your PC. When you finish the selection, click **Next**.



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



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



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

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

The screenshot shows the Draytek website's Support Center. At the top, there is a navigation bar with links: "Support Center" (selected), "Contact us", "Corporate", "Products Center", and "Info". Below this, a dropdown menu for "Support Center" is open, showing options: "FAQ" (highlighted in red), "Application Notes", "Contact Tech Support", "Trouble Shooting", and "Downloads". The main content area is titled "Support Center > FAQ". Under this, there is a sub-section "FAQ" with a list of links: "ISDN FAQ (2008/03/20)", "IP Filter FAQ (2007/05/31)", "Printer Server FAQ (2008/03/14)" (highlighted), and "USB ISDN TA FAQ". Below this, another navigation bar is visible with links: "Corporate", "Products Center", "Information Center", "Support Center" (selected), and "Contact us". The final section is titled "Support Center > FAQ > Print Server FAQ" and contains a list of numbered questions and answers:

- 04 [How do I configure LPR printing on Mac OSX ?](#) (2008/04/17)
- 05 [Why there are some strange print-outs when I try to print my documents through Vigor2104P / 2300](#)
- 06 [What types of printers are compatible with Vigor router ?](#) (2008/03/14)
- 07 [What are the limitations in the USB Printer Port of Vigor Router ?](#)

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

2

Configuring Basic Settings

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

2.1 Two-Level Management

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

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

2.2 Accessing Web Page

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



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

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

Username

Password

Login

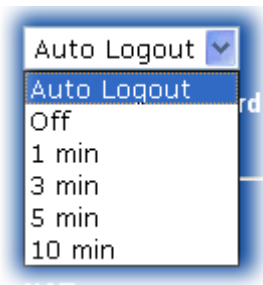
Copyright©, DrayTek Corp. All Rights Reserved. **DrayTek**

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



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

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



2.3 Changing Password

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

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

Vigor2110 Series
Broadband Firewall Router

DrayTek
www.draytek.com

Off

Quick Start Wizard
Online Status

Internet Access
LAN
NAT
Firewall
Objects Setting
CSM
Bandwidth Management
Applications
VPN and Remote Access
Certificate Management
VoIP
Wireless LAN
System Maintenance
Diagnostics

Logout

All Rights Reserved.

Admin mode
Status: Ready

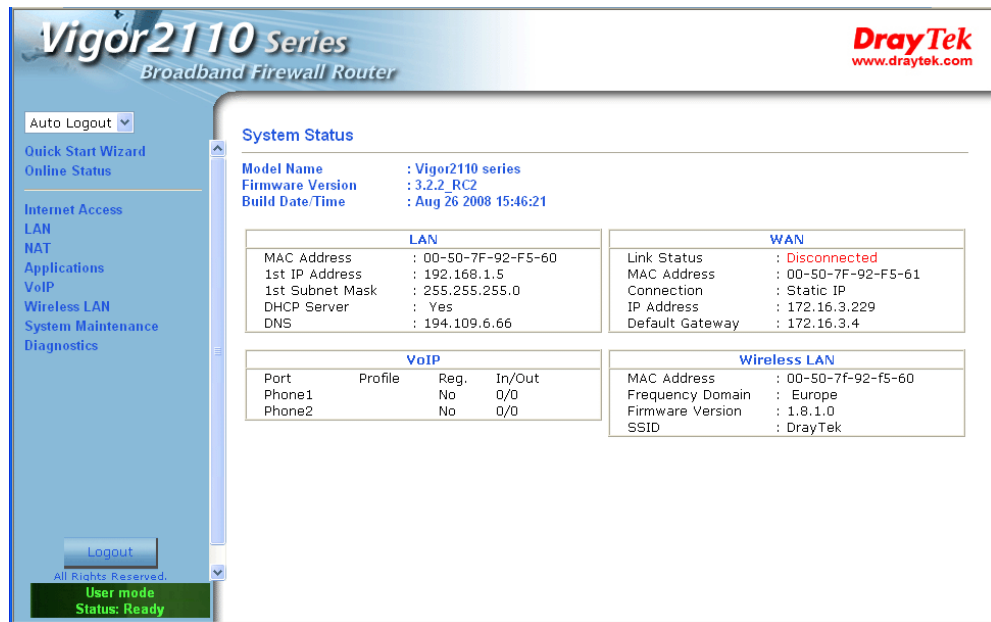
System Status

Model Name : Vigor2110 series
Firmware Version : 3.2.2_RC2
Build Date/Time : Aug 26 2008 15:46:21

| LAN | | WAN | |
|-----------------|---------------------|-----------------|-----------------------|
| MAC Address | : 00-50-7F-92-F5-60 | Link Status | : Disconnected |
| 1st IP Address | : 192.168.1.5 | MAC Address | : 00-50-7F-92-F5-61 |
| 1st Subnet Mask | : 255.255.255.0 | Connection | : Static IP |
| DHCP Server | : Yes | IP Address | : 172.16.3.229 |
| DNS | : 194.109.6.66 | Default Gateway | : 172.16.3.4 |

| VoIP | | | | Wireless LAN | |
|--------|---------|------|--------|------------------|---------------------|
| Port | Profile | Reg. | In/Out | MAC Address | : 00-50-7f-92-f5-60 |
| Phone1 | | No | 0/0 | Frequency Domain | : Europe |
| Phone2 | | No | 0/0 | Firmware Version | : 1.8.1.0 |
| | | | | SSID | : DrayTek |

Main screen for admin mode operation (full configuration)



Main screen for user mode operation (simple configuration)

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

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

System Maintenance >> Administrator Password Setup

Administrator Password

| | |
|------------------|----------------------|
| Old Password | <input type="text"/> |
| New Password | <input type="text"/> |
| Confirm Password | <input type="text"/> |

OK

or

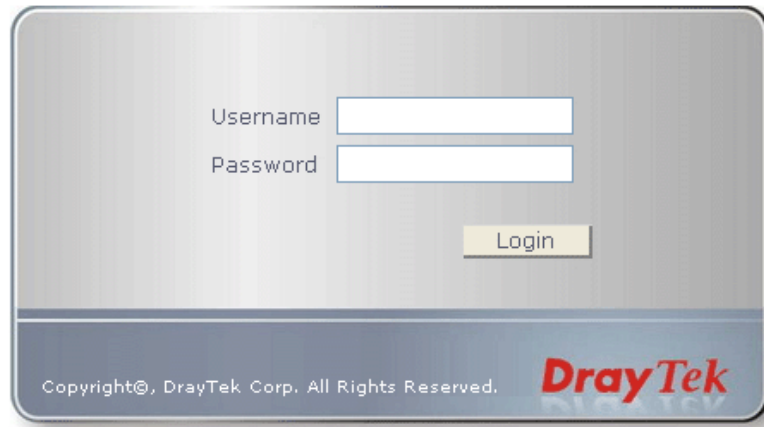
System Maintenance >> User Password

User Password

| | |
|------------------|----------------------|
| Old Password | <input type="text"/> |
| New Password | <input type="text"/> |
| Confirm Password | <input type="text"/> |

OK

5. Enter the login password (the default is blank) on the field of **Old Password**. Type **New Password**. Then click **OK** to continue.
6. Now, the password has been changed. Next time, use the new password to access the Web Configurator for this router.

A login screen with a grey gradient background. It features two input fields: 'Username' and 'Password'. Below the 'Password' field is a 'Login' button. At the bottom, there is a dark blue bar containing the text 'Copyright©, DrayTek Corp. All Rights Reserved.' and the 'DrayTek' logo in red.

2.4 Quick Start Wizard



Notice: Quick Start Wizard for user mode operation is the same as for admin mode operation.

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

Quick Start Wizard

Enter login password

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

Old Password

New Password

Confirm Password

< Back

Next >

Finish

Cancel

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

Quick Start Wizard

Connect to Internet

WAN 1
Select one of the following Internet Access types provided by your ISP.
☒ PPPoE
☐ PPTP
☐ Static IP
☐ DHCP

< Back Next > Finish Cancel

2.4.2 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.

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

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

Quick Start Wizard

PPPoE Client Mode

WAN 1
Enter the user name and password provided by your ISP.
User Name 123
Password ●●●
Confirm Password ●●●

< Back Next > Finish Cancel

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

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

Quick Start Wizard

Please confirm your settings:

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

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

< Back

Next >

Finish

Cancel

Click **Finish**. Then, the system status of this protocol will be shown.

2.4.3 PPTP

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

Quick Start Wizard

PPTP Client Mode

WAN 1

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

User Name

Password

Confirm Password

WAN IP Configuration

☐ Obtain an IP address automatically

☒ Specify an IP address

IP Address

Subnet Mask

PPTP Server IP

< Back

Next >

Finish

Cancel

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

Quick Start Wizard

Please confirm your settings:

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

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

[< Back](#)[Next >](#)[Finish](#)[Cancel](#)

Click **Finish**. Then, the system status of this protocol will be shown.

2.4.4 Static IP

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

Quick Start Wizard

Static IP Client Mode

WAN 1

Enter the Static IP configuration provided by your ISP.

| | |
|---------------|---|
| WAN IP | <input type="text" value="172.16.3.229"/> |
| Subnet Mask | <input type="text" value="255.255.0.0"/> |
| Gateway | <input type="text" value="172.16.3.4"/> |
| Primary DNS | <input type="text"/> |
| Secondary DNS | <input type="text"/> (optional) |

[< Back](#)[Next >](#)[Finish](#)[Cancel](#)

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

Quick Start Wizard

Please confirm your settings:

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

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

< Back

Next >

Finish

Cancel

Click **Finish**. Then, the system status of this protocol will be shown.

2.4.5 DHCP

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

Quick Start Wizard

DHCP Client Mode

WAN 1

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

Host Name (optional)

MAC - - - - - (optional)

< Back

Next >

Finish

Cancel

2.5 Online Status

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

Online status for PPPoE

Online Status

| | | | | | |
|---------------|------------|---------------------------|--------------|---------------------------|--------------|
| System Status | | | | System Uptime: 4:32:33 | |
| LAN Status | | Primary DNS: 194.109.6.66 | | Secondary DNS: 168.95.1.1 | |
| IP Address | TX Packets | RX Packets | | | |
| 192.168.1.5 | 3854 | 4731 | | | |
| WAN Status | | | | | |
| Enable | Line | Name | Mode | Up Time | |
| Yes | Ethernet | | Static IP | 00:00:00 | |
| IP | GW IP | TX Packets | TX Rate(Bps) | RX Packets | RX Rate(Bps) |
| 172.16.3.229 | 172.16.3.4 | 0 | 0 | 1 | 0 |

Detailed explanation is shown below:

Primary DNS Displays the IP address of the primary DNS.

Secondary DNS Displays the IP address of the secondary DNS.

LAN Status

IP Address Displays the IP address of the LAN interface.

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

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

WAN Status

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

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

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

Up Time Displays the total uptime of the interface.

IP Displays the IP address of the WAN interface.

GW IP Displays the IP address of the default gateway.

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

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

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

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

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

2.6 Saving Configuration

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

Status: Ready

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

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

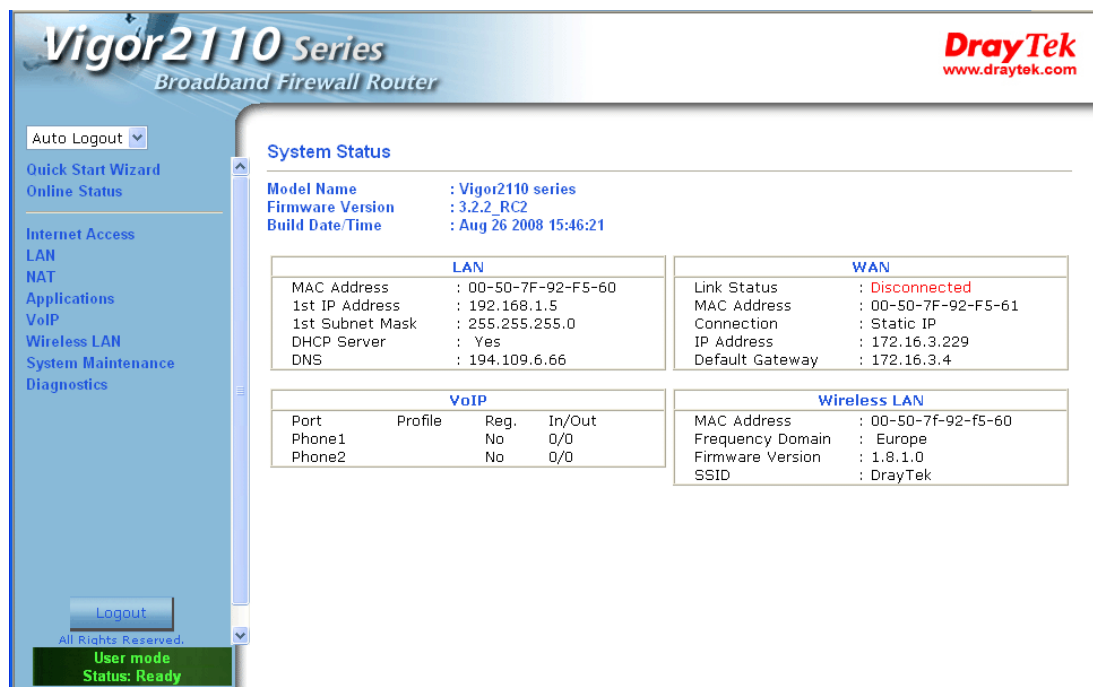
3

User Mode Operation

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

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

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



3.1 Internet Access

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

3.1.1 Basics of Internet Protocol (IP) Network

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

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

What are Public IP Address and Private IP Address

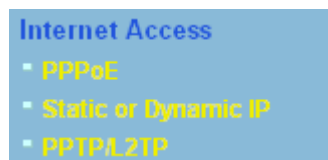
As the router plays a role to manage and further protect its LAN, it interconnects groups of host PCs. Each of them has a private IP address assigned by the built-in DHCP server of the Vigor router. The router itself will also use the default **private IP** address: 192.168.1.1 to communicate with the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

Get Your Public IP Address from ISP

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

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

Below shows the menu items for Internet Access.



3.1.2 PPPoE

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.

PPPoE Client Mode

| | |
|--|--|
| PPPoE Setup PPPoE Link <input checked="" type="radio"/> Enable <input type="radio"/> Disable | |
| ISP Access Setup Username <input type="text" value="123"/> Password <input type="password" value="..."/> Index(1-15) in Schedule Setup: => <input type="text"/> , <input type="text"/> , <input type="text"/> , <input type="text"/> | |
| PPP/MP Setup PPP Authentication <input type="text" value="PAP or CHAP"/> <input checked="" type="checkbox"/> Always On Idle Timeout <input type="text" value="-1"/> second(s) | |
| IP Address Assignment Method (IPCP) <input type="button" value="WAN IP Alias"/> Fixed IP <input type="radio"/> Yes <input checked="" type="radio"/> No (Dynamic IP) Fixed IP Address <input type="text"/> | |
| <input checked="" type="radio"/> Default MAC Address <input type="radio"/> Specify a MAC Address MAC Address: <input type="text" value="00"/> <input type="text" value="50"/> <input type="text" value="7F"/> <input type="text" value="92"/> <input type="text" value="F5"/> <input type="text" value="61"/> | |
| <input type="button" value="OK"/> | |

Enable/Disable

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

ISP Access Setup

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

PPP/MP Setup

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

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

IP Address Assignment Method (IPCP)

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

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

| Index | Enable | Aux. WAN IP | Join NAT IP Pool |
|-------|--------------------------|----------------------|--------------------------|
| 1. | v | 172.16.3.229 | v |
| 2. | <input type="checkbox"/> | <input type="text"/> | <input type="checkbox"/> |
| 3. | <input type="checkbox"/> | <input type="text"/> | <input type="checkbox"/> |
| 4. | <input type="checkbox"/> | <input type="text"/> | <input type="checkbox"/> |
| 5. | <input type="checkbox"/> | <input type="text"/> | <input type="checkbox"/> |
| 6. | <input type="checkbox"/> | <input type="text"/> | <input type="checkbox"/> |
| 7. | <input type="checkbox"/> | <input type="text"/> | <input type="checkbox"/> |
| 8. | <input type="checkbox"/> | <input type="text"/> | <input type="checkbox"/> |

OK Clear All Close

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

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

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

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

3.1.3 Static or Dynamic IP

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

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

Static or Dynamic IP (DHCP Client)

| | | | |
|---|--|--|--|
| Access Control Broadband Access <input checked="" type="radio"/> Enable <input type="radio"/> Disable | | WAN IP Network Settings WAN IP Alias | |
| Keep WAN Connection <input type="checkbox"/> Enable PING to keep alive PING to the IP <input type="text" value="0.0.0.0"/> PING Interval <input type="text" value="0"/> minute(s) | | <input type="radio"/> Obtain an IP address automatically Router Name <input type="text"/> * Domain Name <input type="text"/> * <small>* : Required for some ISPs</small> | |
| WAN physical type <input type="button" value="Auto negotiation"/> | | <input checked="" type="radio"/> Specify an IP address IP Address <input type="text" value="172.16.3.229"/> Subnet Mask <input type="text" value="255.255.0.0"/> Gateway IP Address <input type="text" value="172.16.3.4"/> | |
| RIP Protocol <input type="checkbox"/> Enable RIP | | <input checked="" type="radio"/> Default MAC Address <input type="radio"/> Specify a MAC Address MAC Address: <input type="text" value="00"/> <input type="text" value="50"/> <input type="text" value="7F"/> <input type="text" value="92"/> <input type="text" value="F5"/> <input type="text" value="61"/> | |
| | | DNS Server IP Address Primary IP Address <input type="text"/> Secondary IP Address <input type="text"/> | |

OK

Access Control

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

Keep WAN Connection

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

PING to the IP - If you enable the PING function, please specify the IP address for the system to PING it for keeping alive.

PING Interval - Enter the interval for the system to execute the PING operation.

WAN Physical Type

Choose **Auto negotiation** as the physical type for your router.

RIP Protocol

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

WAN IP Network Settings

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

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

| Index | Enable | Aux. WAN IP | Join NAT IP Pool |
|-------|--------------------------|----------------------|--------------------------|
| 1. | v | 172.16.3.229 | v |
| 2. | <input type="checkbox"/> | <input type="text"/> | <input type="checkbox"/> |
| 3. | <input type="checkbox"/> | <input type="text"/> | <input type="checkbox"/> |
| 4. | <input type="checkbox"/> | <input type="text"/> | <input type="checkbox"/> |
| 5. | <input type="checkbox"/> | <input type="text"/> | <input type="checkbox"/> |
| 6. | <input type="checkbox"/> | <input type="text"/> | <input type="checkbox"/> |
| 7. | <input type="checkbox"/> | <input type="text"/> | <input type="checkbox"/> |
| 8. | <input type="checkbox"/> | <input type="text"/> | <input type="checkbox"/> |

OK Clear All Close

Obtain an IP address automatically – Click this button to obtain the IP address automatically if you want to use **Dynamic IP** mode.

Router Name: Type in the router name provided by ISP.

Domain Name: Type in the domain name that you have assigned.

Specify an IP address – Click this radio button to specify some data if you want to use **Static IP** mode.

IP Address: Type the IP address.

Subnet Mask: Type the subnet mask.

Gateway IP Address: Type the gateway IP address.

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

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

DNS Server IP Address

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

3.1.4 PPTP/L2TP

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

PPTP Client Mode

| | | |
|---|--|--|
| PPTP Setup PPTP Link <input type="radio"/> Enable <input checked="" type="radio"/> Disable PPTP Server <input type="text"/> ISP Access Setup Username <input type="text" value="123"/> Password <input type="password" value="..."/> Index(1-15) in Schedule Setup: => <input type="text"/> , <input type="text"/> , <input type="text"/> , <input type="text"/> | | PPP Setup PPP Authentication <input type="text" value="PAP or CHAP"/> <input checked="" type="checkbox"/> Always On Idle Timeout <input type="text" value="-1"/> second(s) IP Address Assignment Method (IPCP) Fixed IP <input type="radio"/> Yes <input checked="" type="radio"/> No (Dynamic IP) Fixed IP Address <input type="text"/> WAN IP Network Settings <input type="radio"/> Obtain an IP address automatically <input checked="" type="radio"/> Specify an IP address IP Address <input type="text" value="172.16.3.229"/> Subnet Mask <input type="text" value="255.255.0.0"/> |
| <input type="button" value="OK"/> | | |

PPTP Setup

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

Disable – Click this radio button to close the connection through PPTP.

PPTP Server - Specify the IP address of the PPTP/L2TP server if you enable PPTP/L2TP client mode.

ISP Access Setup

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

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

Index (1-15) in Schedule Setup - You can type in four sets of time schedule for your request. All the schedules can be set previously in **Application – Schedule** web page and you can use the number that you have set in that web page.

PPP Setup

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

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

IP Address Assignment Method(IPCP)

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

Fixed IP Address -Type a fixed IP address.

WAN IP Network 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.

3.2 LAN

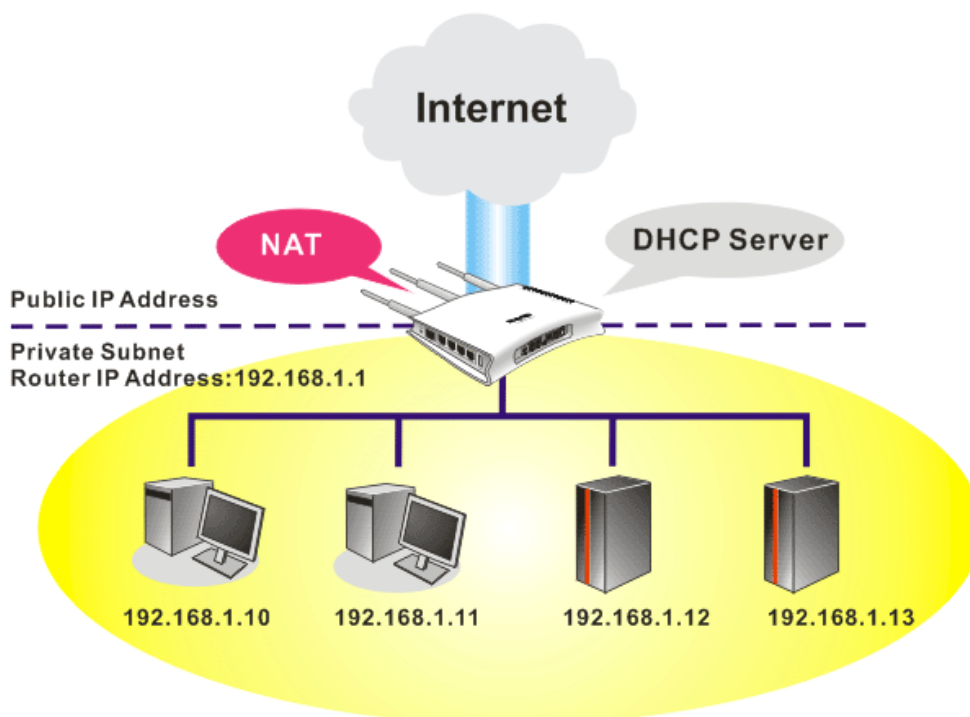
Local Area Network (LAN) is a group of subnets regulated and ruled by router. The design of network structure is related to what type of public IP addresses coming from your ISP.

LAN

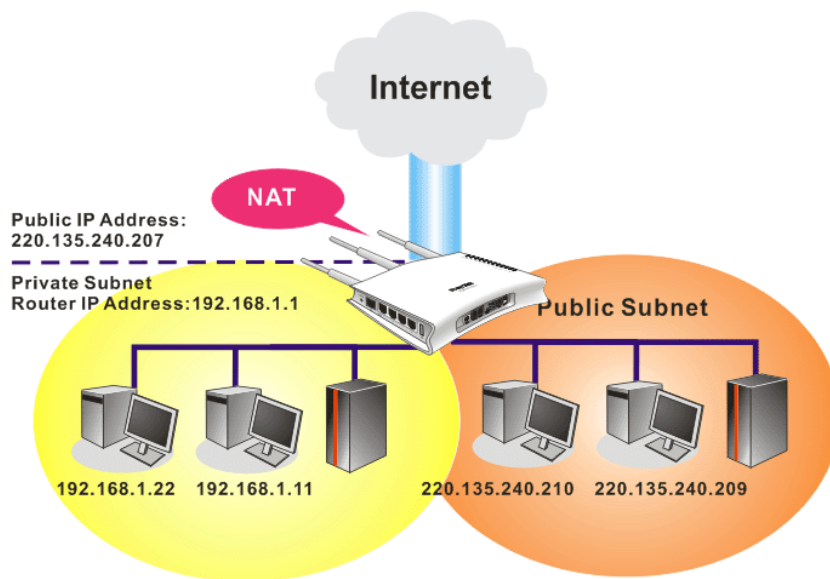
General Setup

3.2.1 Basics of LAN

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



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



What is Routing Information Protocol (RIP)

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

3.2.2 General Setup

This page provides you the general settings for LAN.

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

[LAN >> General Setup](#)

Ethernet TCP / IP and DHCP Setup

LAN IP Network Configuration

For NAT Usage

1st IP Address

1st Subnet Mask

For IP Routing Usage ☐ Enable ☒ Disable

2nd IP Address

2nd Subnet Mask

RIP Protocol Control

DHCP Server Configuration

☒ Enable Server ☐ Disable Server

Relay Agent: ☐ 1st Subnet ☐ 2nd Subnet

Start IP Address

IP Pool Counts

Gateway IP Address

DHCP Server IP Address for Relay Agent

DNS Server IP Address

☐ Force DNS manual setting

Primary IP Address

Secondary IP Address

1st IP Address

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

1st Subnet Mask

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

- For IP Routing Usage** Click **Enable** to invoke this function. The default setting is **Disable**.
- 2nd IP Address** Type in secondary IP address for connecting to a subnet.
(Default: 192.168.2.1/ 24)
- 2nd Subnet Mask** An address code that determines the size of the network.
(Default: 255.255.255.0/ 24)
- 2nd DHCP Server** You can configure the router to serve as a DHCP server for the 2nd subnet.

The screenshot shows the '2nd DHCP Server' configuration window in a Microsoft Internet Explorer browser. The window title is 'http://192.168.1.5 - Router Web Configurator - Microsoft Internet Explorer'. The page has a title '2nd DHCP Server'. It contains two input fields: 'Start IP Address' and 'IP Pool Counts' (with a value of 0 and a note '(max. 10)'). Below these is a table with three columns: 'Index', 'Matched MAC Address', and 'given IP Address'. The table is currently empty. Below the table is a 'MAC Address' input field with a dropdown menu. At the bottom of the table area are buttons 'Add', 'Delete', 'Edit', and 'Cancel'. At the bottom of the window are buttons 'OK', 'Clear All', and 'Close'.

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

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

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

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

RIP Protocol Control

The screenshot shows a dropdown menu for 'RIP Protocol Control'. The menu is open, showing three options: 'Disable' (which is highlighted), '1st Subnet', and '2nd Subnet'.

1st Subnet - Select the router to change the RIP information of the

1st subnet with neighboring routers.

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

DHCP Server Configuration

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

If you want to use another DHCP server in the network other than the Vigor Router's, you can let Relay Agent help you to redirect the DHCP request to the specified location.

Enable Server - Let the router assign IP address to every host in the LAN.

Disable Server - Let you manually assign IP address to every host in the LAN.

Relay Agent - (1st subnet/2nd subnet) Specify which subnet that DHCP server is located the relay agent should redirect the DHCP request to.

Start IP Address - Enter a value of the IP address pool for the DHCP server to start with when issuing IP addresses. If the 1st IP address of your router is 192.168.1.1, the starting IP address must be 192.168.1.2 or greater, but smaller than 192.168.1.254.

IP Pool Counts - Enter the maximum number of PCs that you want the DHCP server to assign IP addresses to. The default is 50 and the maximum is 253.

Gateway IP Address - Enter a value of the gateway IP address for the DHCP server. The value is usually as same as the 1st IP address of the router, which means the router is the default gateway.

DHCP Server IP Address for Relay Agent - Set the IP address of the DHCP server you are going to use so the Relay Agent can help to forward the DHCP request to the DHCP server.

DNS Server Configuration

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

Force DNS manual setting - Force Vigor router to use DNS servers in this page instead of DNS servers given by the Internet Access server (PPPoE, PPTP, L2TP or DHCP server).

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

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

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

| | | | |
|---------------|------------|---------------------------|---------------------------|
| System Status | | System Uptime: 5:11:9 | |
| LAN Status | | Primary DNS: 194.109.6.66 | Secondary DNS: 168.95.1.1 |
| IP Address | TX Packets | RX Packets | |
| 192.168.1.5 | 9326 | 9487 | |

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

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

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

3.3 NAT

Usually, the router serves as an NAT (Network Address Translation) router. NAT is a mechanism that one or more private IP addresses can be mapped into a single public one. Public IP address is usually assigned by your ISP, for which you may get charged. Private IP addresses are recognized only among internal hosts.

When the outgoing packets destined to some public server on the Internet reach the NAT router, the router will change its source address into the public IP address of the router, select the available public port, and then forward it. At the same time, the router shall list an entry in a table to memorize this address/port-mapping relationship. When the public server response, the incoming traffic, of course, is destined to the router's public IP address and the router will do the inversion based on its table. Therefore, the internal host can communicate with external host smoothly.

The benefit of the NAT includes:

- **Save cost on applying public IP address and apply efficient usage of IP address.** NAT allows the internal IP addresses of local hosts to be translated into one public IP address, thus you can have only one IP address on behalf of the entire internal hosts.
- **Enhance security of the internal network by obscuring the IP address.** There are many attacks aiming victims based on the IP address. Since the attacker cannot be aware of any private IP addresses, the NAT function can protect the internal network.

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

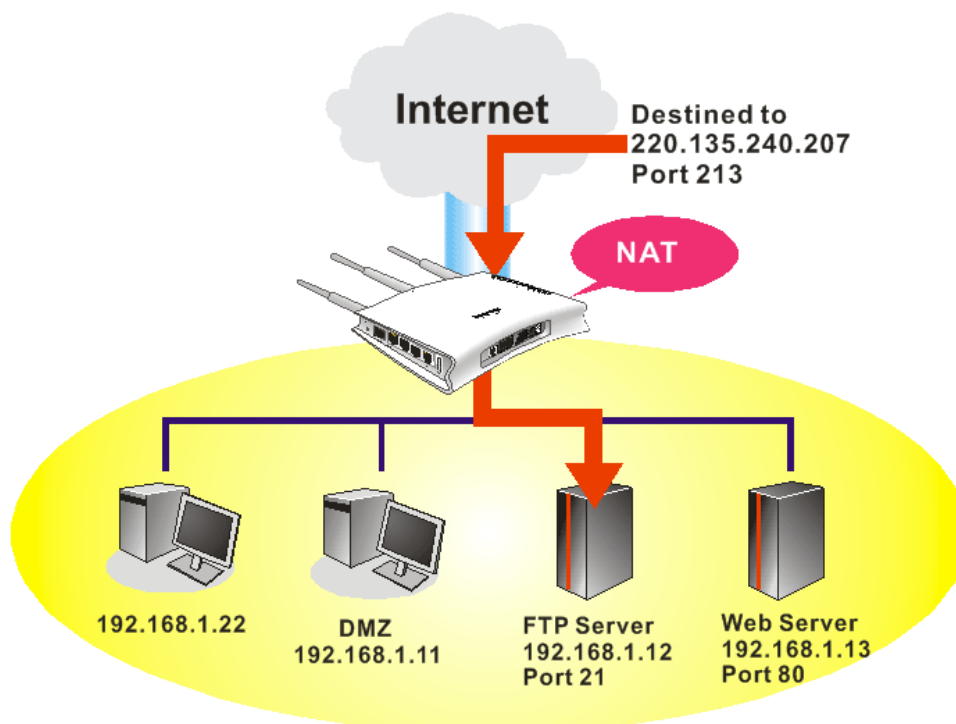
Below shows the menu items for NAT.



3.3.1 Port Redirection

Port Redirection is usually set up for server related service inside the local network (LAN), such as web servers, FTP servers, E-mail servers etc. Most of the case, you need a public IP address for each server and this public IP address/domain name are recognized by all users. Since the server is actually located inside the LAN, the network well protected by NAT of

the router, and identified by its private IP address/port, the goal of Port Redirection function is to forward all access request with public IP address from external users to the mapping private IP address/port of the server.



The port redirection can only apply to incoming traffic.

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

[NAT >> Port Redirection](#)

Port Redirection

[Set to Factory Default](#)

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

<< [1-10](#) | [11-20](#) >>

[Next](#) >>

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

Index No. 1

| | |
|---------------------------------|--------|
| <input type="checkbox"/> Enable | |
| Mode | Single |
| Service Name | Single |
| Protocol | --- |
| WAN IP | 1.All |
| Public Port | 0 |
| Private IP | |
| Private Port | 0 |

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

OK Clear Cancel

Enable

Check this box to enable such port redirection setting.

Mode

Two options (Single and Range) are provided here for you to choose. To set a range for the specific service, select **Range**. In Range mode, if the public port (start port and end port) and the starting IP of private IP had been entered, the system will calculate and display the ending IP of private IP automatically.

Service Name

Enter the description of the specific network service.

Protocol

Select the transport layer protocol (TCP or UDP).

WAN IP

Select the WAN IP used for port redirection. There are eight WAN IP alias that can be selected and used for port redirection. The default setting is **All** which means all the incoming data from any port will be redirected to specified range of IP address and port.

Public Port

Specify which port can be redirected to the specified **Private IP and Port** of the internal host. If you choose **Range** as the port redirection mode, you will see two boxes on this field. Simply type the required number on the first box. The second one will be assigned automatically later.

Private IP

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

Private Port

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

Active

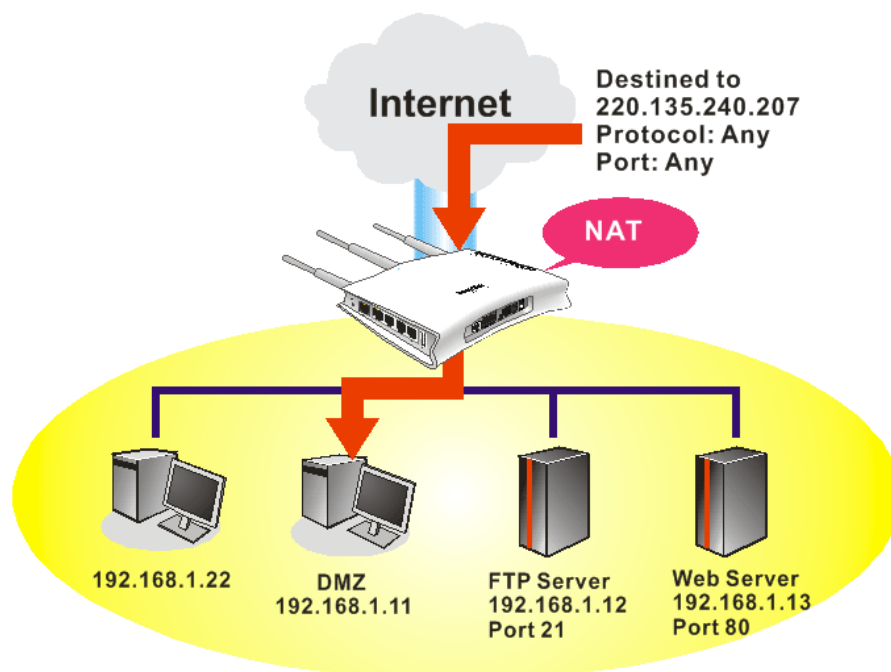
Check this box to activate the port-mapping entry you have defined.

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

3.3.2 DMZ Host

As mentioned above, **Port Redirection** can redirect incoming TCP/UDP or other traffic on particular ports to the specific private IP address/port of host in the LAN. However, other IP

protocols, for example Protocols 50 (ESP) and 51 (AH), do not travel on a fixed port. Vigor router provides a facility **DMZ Host** that maps ALL unsolicited data on any protocol to a single host in the LAN. Regular web surfing and other such Internet activities from other clients will continue to work without inappropriate interruption. **DMZ Host** allows a defined internal user to be totally exposed to the Internet, which usually helps some special applications such as Netmeeting or Internet Games etc.



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

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

[NAT >> DMZ Host Setup](#)

DMZ Host Setup

WAN 1

None

Private IP

MAC Address of the True IP DMZ Host

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

OK

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

NAT >> DMZ Host Setup

DMZ Host Setup

| WAN 1 | | | | |
|-------|--------------------------|--------------|----------------------|--|
| Index | Enable | Aux. WAN IP | Private IP | |
| 1. | <input type="checkbox"/> | 172.16.3.229 | <input type="text"/> | <input type="button" value="Choose PC"/> |
| 2. | <input type="checkbox"/> | 162.168.1.55 | <input type="text"/> | <input type="button" value="Choose PC"/> |

Enable

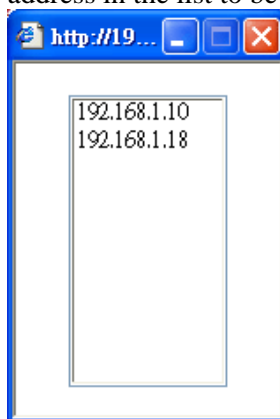
Check to enable the DMZ Host function.

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.



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

NAT >> DMZ Host Setup

DMZ Host Setup

| WAN 1 | | | | |
|-------|-------------------------------------|--------------|----------------------|--|
| Index | Enable | Aux. WAN IP | Private IP | |
| 1. | <input checked="" type="checkbox"/> | 172.16.3.229 | 192.168.1.10 | <input type="button" value="Choose PC"/> |
| 2. | <input type="checkbox"/> | 162.168.1.55 | <input type="text"/> | <input type="button" value="Choose PC"/> |

3.3.3 Open Ports

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

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

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

[NAT >> Open Ports](#)

| Open Ports Setup | | | | Set to Factory Default |
|---------------------|---------|-------------|------------------|--|
| 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 |

<< [1-10](#) | [11-20](#) >> [Next](#) >>

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

| | | | | | | |
|---|--|--------------|--|--|-----------|--|
| <input checked="" type="checkbox"/> Enable Open Ports | | | | | | |
| Comment | | P2P | | | | |
| WAN IP | | 172.16.3.229 | | | | |
| Local Computer | | 192.168.1.10 | | | Choose PC | |

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

OK Clear Cancel

Enable Open Ports

Check to enable this entry.

Comment

Make a name for the defined network application/service.

WAN Interface

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

Local Computer

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

Choose PC

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

Protocol

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

Start Port

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

End Port

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

3.4 Applications

Below shows the menu items for Applications.



3.4.1 Dynamic DNS

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

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

Enable the Function and Add a Dynamic DNS Account

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

[Applications >> Dynamic DNS Setup](#)

Dynamic DNS Setup

[Set to Factory Default](#)

☐ Enable Dynamic DNS Setup

[View Log](#)
[Force Update](#)

Accounts:

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

OK

Clear All

Set to Factory Default

Clear all profiles and recover to factory settings.

Enable Dynamic DNS Setup

Check this box to enable DDNS function.

Index

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

Domain Name

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

Active

Display if this account is active or inactive.

View Log

Display DDNS log status.

Force Update

Force the router updates its information to DDNS server.

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

Index : 1

| | | |
|--|----------------------------------|--------------|
| <input checked="" type="checkbox"/> Enable Dynamic DNS Account | | |
| Service Provider | dyndns.org (www.dyndns.org) ▼ | |
| Service Type | Dynamic ▼ | |
| Domain Name | chronic6853 | dyndns.org ▼ |
| Login Name | chronic6853 (max. 64 characters) | |
| Password | •••••••• (max. 23 characters) | |
| <input type="checkbox"/> Wildcards | | |
| <input type="checkbox"/> Backup MX | | |
| Mail Extender | | |

OK Clear Cancel

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 or Static). If you choose Custom, you can modify the domain that is chosen in the Domain Name field.

Domain Name

Type in one domain name that you applied previously. Use the drop down list to choose the desired domain.

Login Name

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

Password

Type in the password that you set for applying domain.

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

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

Disable the Function and Clear all Dynamic DNS Accounts

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

Delete a Dynamic DNS Account

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

3.4.2 UPnP

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

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

Applications >> UPnP

UPnP

- ☒ Enable UPnP Service
- ☐ Enable Connection control Service
- ☐ Enable Connection Status Service

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

OK

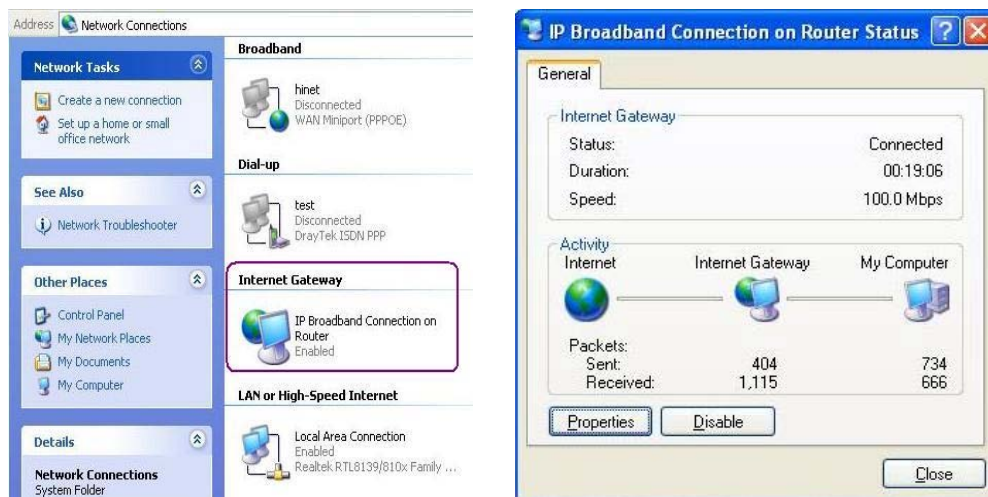
Clear

Cancel

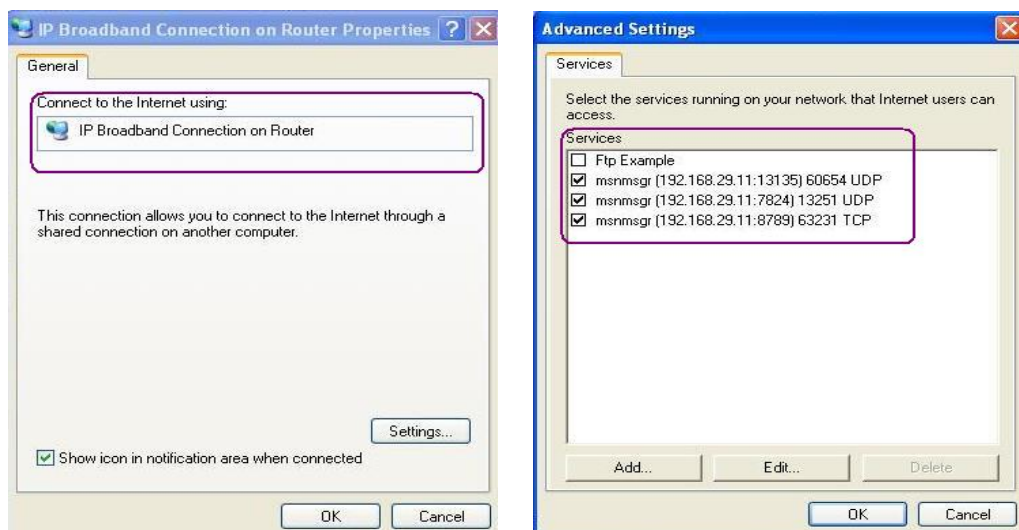
Enable UPNP Service

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

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



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



The reminder as regards concern about Firewall and UPnP

Can't work with Firewall Software

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

Security Considerations

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

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

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

3.5 Wireless LAN

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

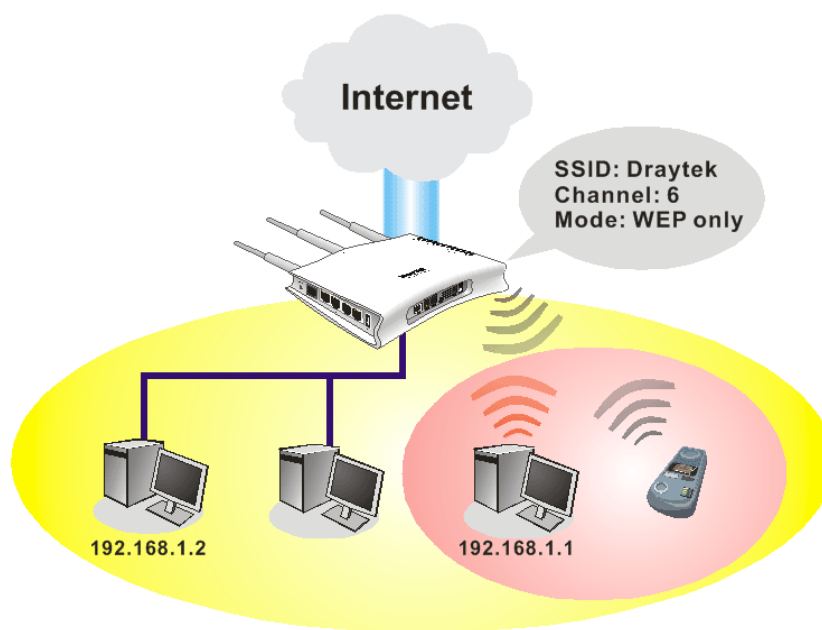
3.5.1 Basic Concepts

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 “n” model, a.k.a. Vigor wireless router, is designed for maximum flexibility and efficiency of a small office/home. Any authorized staff can bring a built-in WLAN client PDA or notebook into a meeting room for conference without laying a clot of LAN cable or drilling holes everywhere. Wireless LAN enables high mobility so WLAN users can simultaneously access all LAN facilities just like on a wired LAN as well as Internet access.

The Vigor wireless routers are equipped with a wireless LAN interface compliant with the standard IEEE 802.11n draft 2 protocol. To boost its performance further, the Vigor Router is also loaded with advanced wireless technology to lift up data rate up to 300 Mbps*. Hence, you can finally smoothly enjoy stream music and video.

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

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



Security Overview

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

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

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

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

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

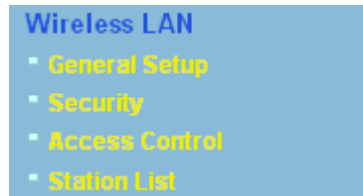
Since WEP has been proved vulnerable, you may consider using WPA for the most secure connection. You should select the appropriate security mechanism according to your needs. No matter which security suite you select, they all will enhance the over-the-air data protection and /or privacy on your wireless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

Separate the Wireless and the Wired LAN- WLAN Isolation enables you to isolate your wireless LAN from wired LAN for either quarantine or limit access reasons. To isolate

means neither of the parties can access each other. To elaborate an example for business use, you may set up a wireless LAN for visitors only so they can connect to Internet without hassle of the confidential information leakage. For a more flexible deployment, you may add filters of MAC addresses to isolate users' access from wired LAN.

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

Below shows the menu items for Wireless LAN.



3.5.2 General Setup

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

Wireless LAN >> General Setup

General Setting (IEEE 802.11)

☒ Enable Wireless LAN

Mode :

Mixed(11b+11g+11n) ▼

Index(1-15) in [Schedule](#) Setup:

, , ,

Only schedule profiles that have the action "Force Down" are applied to the WLAN, all other actions are ignored.

SSID:

DrayTek

Channel :

Channel 6, 2437MHz ▼

Packet-OVERDRIVE™

☐ Tx Burst

Note:

The same technology must also be supported in clients to boost WLAN performance.

☐ Hide SSID

☐ Long Preamble

Hide SSID: prevent SSID from being scanned.

Long Preamble: necessary for some older 802.11b devices only (lowers performance).

OK

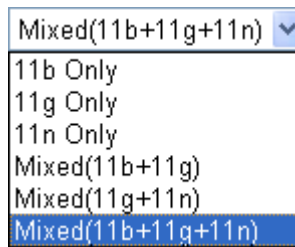
Cancel

Enable Wireless LAN

Check the box to enable wireless function.

Mode

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



Note: You should also set **RADIUS Server** simultaneously if 11g Only, 11b Only or 11n Only mode is selected.

Index(1-15)

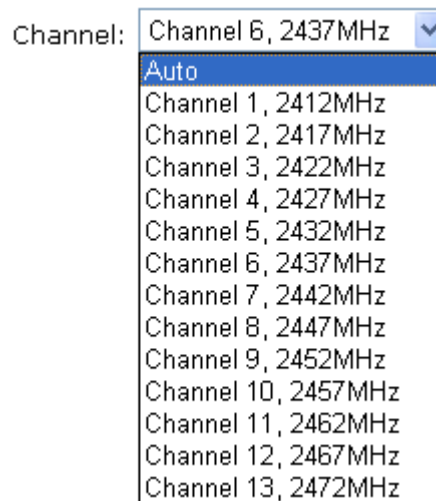
Set the wireless LAN to work at certain time interval only. You may choose up to 4 schedules out of the 15 schedules pre-defined in **Applications >> Schedule** setup. The default setting of this field is blank and the function will always work.

SSID

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

Channel

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

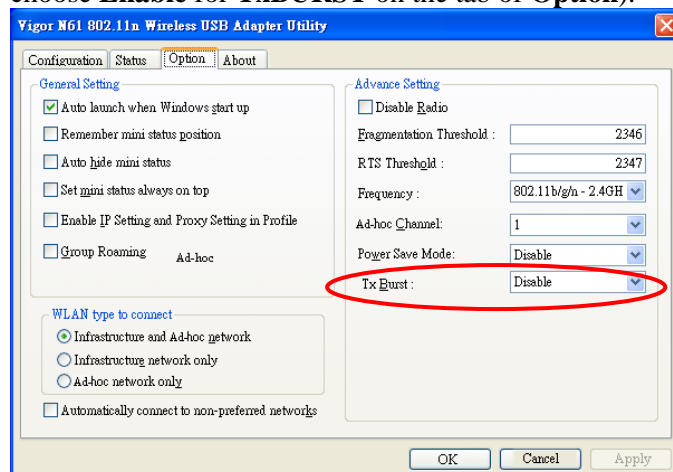


Packet-OVERDRIVE

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

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

choose **Enable** for **TxBURST** on the tab of **Option**).



Hide SSID

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

Long Preamble

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

3.5.3 Security

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

[Wireless LAN >> Security Settings](#)

Security Settings

Mode: Disable

WPA:

Encryption Mode: TKIP

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

☒ 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".

OK Cancel

Mode

There are several modes provided for you to choose.

Mode: Disable

- Disable
- WEP
- WPA/PSK
- WPA2/PSK
- Mixed(WPA+WPA2)/PSK

Disable - Turn off the encryption mechanism.

WEP-Accepts only WEP clients and the encryption key should be entered in WEP Key.

WPA/PSK-Accepts only WPA clients and the encryption key should be entered in PSK.

WPA2/PSK-Accepts only WPA2 clients and the encryption key should be entered in PSK.

Mixed (WPA+ WPA2)/PSK - Accepts WPA and WPA2 clients simultaneously and the encryption key should be entered in PSK.

WPA

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

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

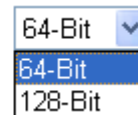
WEP

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

64-Bit - For 64 bits WEP key, either **5** ASCII characters, such as 12345 (or 10 hexadecimal digitals leading by 0x, such as 0x4142434445.)

128-Bit - For 128 bits WEP key, either **13** ASCII characters, such as ABCDEFGHIJKLM (or 26 hexadecimal digits leading by 0x, such as 0x4142434445464748494A4B4C4D).

Encryption Mode:

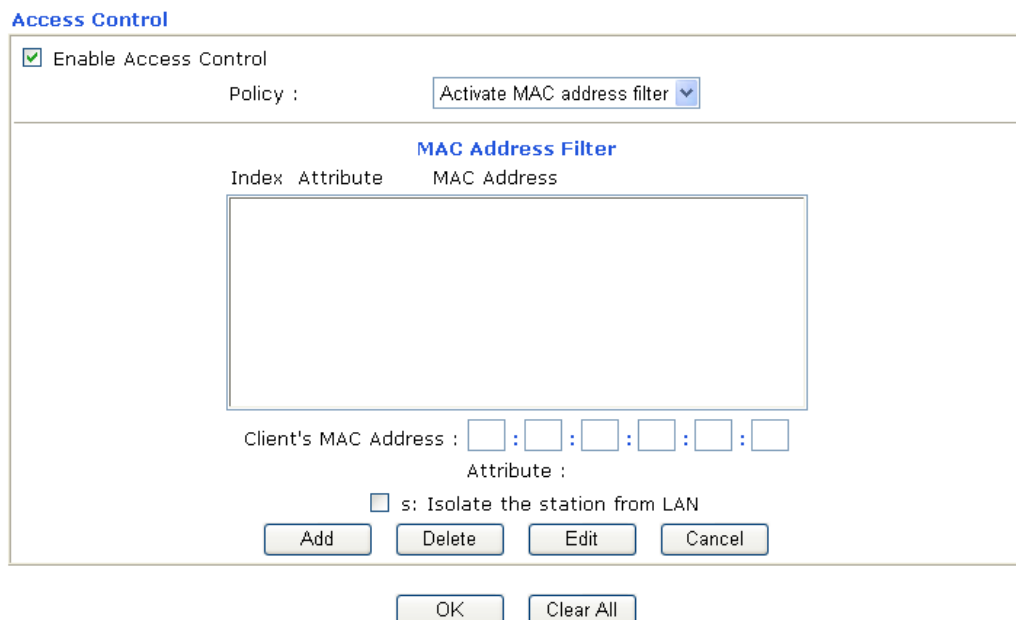


All wireless devices must support the same WEP encryption bit size and have the same key. **Four** keys can be entered here, but only one key can be selected at a time. The keys can be entered in ASCII or Hexadecimal. Check the key you wish to use.

3.5.4 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.

[Wireless LAN >> Access Control](#)



Enable Max Access Filter

Select to enable the MAC Address filter for wireless LAN identified with SSID 1 to 4 respectively. All the clients (expressed by MAC addresses) listed in the box can be grouped under different wireless LAN. For example, they can be grouped under SSID 1 and SSID 2 at the same time if you check SSID 1 and SSID 2.

| | |
|-----------------------------|--|
| MAC Address Filter | Display all MAC addresses that are edited before. |
| Client's MAC Address | Manually enter the MAC address of wireless client. |
| Attribute | s: Isolate the station from LAN - select to isolate the wireless connection of the wireless client of the MAC address from LAN. |
| Add | Add a new MAC address into the list. |
| Delete | Delete the selected MAC address in the list. |
| Edit | Edit the selected MAC address in the list. |
| Cancel | Give up the access control set up. |
| OK | Click it to save the access control list. |
| Clear All | Clean all entries in the MAC address list. |

3.5.5 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.

[Wireless LAN >> Station List](#)

Station List

| Status | MAC Address | Associated with |
|--------|-------------|-----------------|
| | | |

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 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 : : : : :

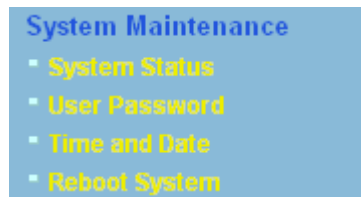
Add

| | |
|----------------|---|
| Refresh | Click this button to refresh the status of station list. |
| Add | Click this button to add current typed MAC address into Access Control . |

3.6 System Maintenance

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

Below shows the menu items for System Maintenance.



3.6.1 System Status

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

System Status

Model Name : Vigor2110 series
Firmware Version : 3.2.2_RC2
Build Date/Time : Aug 26 2008 15:46:21

| LAN | | WAN | |
|-----------------|---------------------|-----------------|-----------------------|
| MAC Address | : 00-50-7F-92-F5-60 | Link Status | : Disconnected |
| 1st IP Address | : 192.168.1.5 | MAC Address | : 00-50-7F-92-F5-61 |
| 1st Subnet Mask | : 255.255.255.0 | Connection | : Static IP |
| DHCP Server | : Yes | IP Address | : 172.16.3.229 |
| DNS | : 194.109.6.66 | Default Gateway | : 172.16.3.4 |

| Wireless LAN | |
|------------------|---------------------|
| MAC Address | : 00-50-7f-92-f5-60 |
| Frequency Domain | : Europe |
| Firmware Version | : 1.8.1.0 |
| SSID | : DrayTek |

| | |
|-----------------------------------|---|
| Model Name | Display the model name of the router. |
| Firmware Version | Display the firmware version of the router. |
| Build Date/Time | Display the date and time of the current firmware build. |
| LAN----- | |
| MAC Address | Display the MAC address of the LAN Interface. |
| 1st IP Address | Display the IP address of the LAN interface. |
| 1st Subnet Mask | Display the subnet mask address of the LAN interface. |
| DHCP Server | Display the current status of DHCP server of the LAN interface. |
| DNS | Display the assigned IP address of the primary DNS. |
| WAN----- | |
| Link Status | Display current connection status. |
| MAC Address | Display the MAC address of the WAN Interface. |
| Connection | Display the connection type. |
| IP Address | Display the IP address of the WAN interface. |
| Default Gateway | Display the assigned IP address of the default gateway. |

Wireless LAN-----

| | |
|-------------------------|--|
| MAC Address | Display the MAC address of the wireless LAN. |
| Frequency Domain | It can be Europe (13 usable channels), USA (11 usable channels) etc. The available channels supported by the wireless products in different countries are various. |
| Firmware Version | It indicates information about equipped WLAN miniPCi card. This also helps to provide availability of some features that are bound with some WLAN miniPCi. |
| SSID | Display the SSID of the router. |

3.6.2 User Password

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

[System Maintenance >> User Password](#)

User Password

| | |
|------------------|----------------------|
| Old Password | <input type="text"/> |
| New Password | <input type="text"/> |
| Confirm Password | <input type="text"/> |

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

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

3.6.3 Time and Date

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

[System Maintenance >> Time and Date](#)

Time Information

| | | |
|---------------------|----------------------------|---|
| Current System Time | 2000 Jan 2 Sun 2 : 57 : 33 | <input type="button" value="Inquire Time"/> |
|---------------------|----------------------------|---|

Time Setup

| | |
|---|---|
| <input type="radio"/> Use Browser Time | |
| <input checked="" type="radio"/> Use Internet Time Client | |
| Server IP Address | <input type="text" value="pool.ntp.org"/> |
| Time Zone | <input type="text" value="(GMT) Greenwich Mean Time : Dublin"/> |
| Enable Daylight Saving | <input type="checkbox"/> |
| Automatically Update Interval | <input type="text" value="30 min"/> |

| | |
|----------------------------|---|
| Current System Time | Click Inquire Time to get the current time. |
| Use Browser Time | Select this option to use the browser time from the remote administrator PC host as router's system time. |

| | |
|--------------------------------------|--|
| Use Internet Time | Select to inquire time information from Time Server on the Internet using assigned protocol. |
| Time Protocol | Select a time protocol. |
| Server IP Address | Type the IP address of the time server. |
| Time Zone | Select the time zone where the router is located. |
| Enable Daylight Saving | Check the box to activate daylight saving function. Such feature is useful for some areas. |
| Automatically Update Interval | Select a time interval for updating from the NTP server. |

Click **OK** to save these settings.

3.6.4 Reboot System

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

[System Maintenance >> Reboot System](#)

Reboot System

Do you want to reboot your router ?

☒ Using current configuration

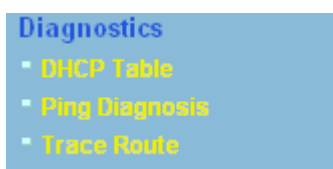
Click **OK**. The router will take 5 seconds to reboot the system.

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

3.7 Diagnostics

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

Below shows the menu items for Diagnostics.



3.7.1 DHCP Table

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

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

DHCP IP Assignment Table | [Refresh](#) |

| DHCP server: Running | | | | |
|----------------------|--------------|-------------------|-------------|---------|
| Index | IP Address | MAC Address | Leased Time | HOST ID |
| 1 | 192.168.1.12 | 00-1D-4F-D5-C1-39 | 4:16:43.820 | iPod-3 |

| | |
|--------------------|--|
| Index | It displays the connection item number. |
| IP Address | It displays the IP address assigned by this router for specified PC. |
| MAC Address | It displays the MAC address for the specified PC that DHCP assigned IP address for it. |
| Leased Time | It displays the leased time of the specified PC. |
| HOST ID | It displays the host ID name of the specified PC. |
| Refresh | Click it to reload the page. |

3.7.2 Ping Diagnosis

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

[Diagnostics >> Ping Diagnosis](#)

Ping Diagnosis

Note: If you want to ping a LAN PC or you don't want to specify which WAN to ping through, please select "Unspecified".

Ping to: IP Address:

Result | [Clear](#) |

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

Clear

Click this link to remove the result on the window.

3.7.3 Trace Route

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

[Diagnostics >> Trace Route](#)

Trace Route

Protocol: ICMP

Host / IP Address:

Run

Result | [Clear](#) |

Protocol

Use the drop down list to choose the interface that you want to ping through.

Host/IP Address

It indicates the IP address of the host.

Run

Click this button to start route tracing work.

Clear

Click this link to remove the result on the window.

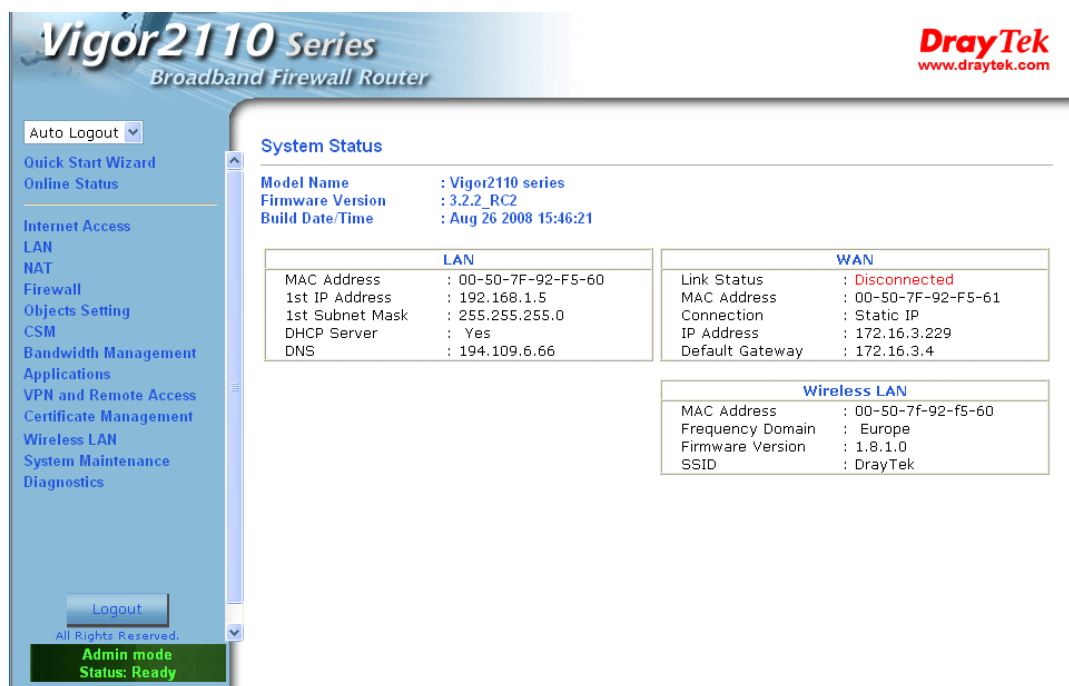
4

Admin Mode Operation

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

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

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



4.1 Internet Access

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

4.1.1 Basics of Internet Protocol (IP) Network

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

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

What are Public IP Address and Private IP Address

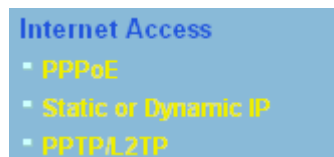
As the router plays a role to manage and further protect its LAN, it interconnects groups of host PCs. Each of them has a private IP address assigned by the built-in DHCP server of the Vigor router. The router itself will also use the default **private IP** address: 192.168.1.1 to communicate with the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

Get Your Public IP Address from ISP

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

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

Below shows the menu items for Internet Access.



4.1.2 PPPoE

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.

PPPoE Client Mode

| | |
|--|--|
| PPPoE Setup PPPoE Link <input checked="" type="radio"/> Enable <input type="radio"/> Disable | |
| ISP Access Setup Username <input type="text" value="123"/> Password <input type="password" value="..."/> Index(1-15) in Schedule Setup: => <input type="text"/> , <input type="text"/> , <input type="text"/> , <input type="text"/> | |
| PPP/MP Setup PPP Authentication <input type="text" value="PAP or CHAP"/> <input checked="" type="checkbox"/> Always On Idle Timeout <input type="text" value="-1"/> second(s) | |
| IP Address Assignment Method (IPCP) <input type="button" value="WAN IP Alias"/> Fixed IP <input type="radio"/> Yes <input checked="" type="radio"/> No (Dynamic IP) Fixed IP Address <input type="text"/> | |
| <input checked="" type="radio"/> Default MAC Address <input type="radio"/> Specify a MAC Address MAC Address: <input type="text" value="00"/> <input type="text" value="50"/> <input type="text" value="7F"/> <input type="text" value="92"/> <input type="text" value="F5"/> <input type="text" value="61"/> | |
| <input type="button" value="OK"/> | |

Enable/Disable

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

ISP Access Setup

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

PPP/MP Setup

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

IP Address Assignment Method (IPCP)

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

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

| Index | Enable | Aux. WAN IP | Join NAT IP Pool |
|-------|--------------------------|----------------------|--------------------------|
| 1. | v | 172.16.3.229 | v |
| 2. | <input type="checkbox"/> | <input type="text"/> | <input type="checkbox"/> |
| 3. | <input type="checkbox"/> | <input type="text"/> | <input type="checkbox"/> |
| 4. | <input type="checkbox"/> | <input type="text"/> | <input type="checkbox"/> |
| 5. | <input type="checkbox"/> | <input type="text"/> | <input type="checkbox"/> |
| 6. | <input type="checkbox"/> | <input type="text"/> | <input type="checkbox"/> |
| 7. | <input type="checkbox"/> | <input type="text"/> | <input type="checkbox"/> |
| 8. | <input type="checkbox"/> | <input type="text"/> | <input type="checkbox"/> |

OK Clear All Close

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

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

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

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

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

Static or Dynamic IP (DHCP Client)

| | | | |
|---|--|--|--|
| Access Control Broadband Access <input checked="" type="radio"/> Enable <input type="radio"/> Disable | | WAN IP Network Settings WAN IP Alias | |
| Keep WAN Connection <input type="checkbox"/> Enable PING to keep alive PING to the IP <input type="text" value="0.0.0.0"/> PING Interval <input type="text" value="0"/> minute(s) | | <input type="radio"/> Obtain an IP address automatically Router Name <input type="text"/> * Domain Name <input type="text"/> * <small>* : Required for some ISPs</small> | |
| WAN physical type <input type="button" value="Auto negotiation"/> | | <input checked="" type="radio"/> Specify an IP address IP Address <input type="text" value="172.16.3.229"/> Subnet Mask <input type="text" value="255.255.0.0"/> Gateway IP Address <input type="text" value="172.16.3.4"/> | |
| RIP Protocol <input type="checkbox"/> Enable RIP | | <input checked="" type="radio"/> Default MAC Address <input type="radio"/> Specify a MAC Address MAC Address: <input type="text" value="00"/> <input type="text" value="50"/> <input type="text" value="7F"/> <input type="text" value="92"/> <input type="text" value="F5"/> <input type="text" value="61"/> | |
| | | DNS Server IP Address Primary IP Address <input type="text"/> Secondary IP Address <input type="text"/> | |

OK

Access Control

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

Keep WAN Connection

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

PING to the IP - If you enable the PING function, please specify the IP address for the system to PING it for keeping alive.

PING Interval - Enter the interval for the system to execute the PING operation.

WAN Physical Type

Choose **Auto negotiation** as the physical type for your router.

RIP Protocol

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

WAN IP Network Settings

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

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

| Index | Enable | Aux. WAN IP | Join NAT IP Pool |
|-------|--------------------------|----------------------|--------------------------|
| 1. | v | 172.16.3.229 | v |
| 2. | <input type="checkbox"/> | <input type="text"/> | <input type="checkbox"/> |
| 3. | <input type="checkbox"/> | <input type="text"/> | <input type="checkbox"/> |
| 4. | <input type="checkbox"/> | <input type="text"/> | <input type="checkbox"/> |
| 5. | <input type="checkbox"/> | <input type="text"/> | <input type="checkbox"/> |
| 6. | <input type="checkbox"/> | <input type="text"/> | <input type="checkbox"/> |
| 7. | <input type="checkbox"/> | <input type="text"/> | <input type="checkbox"/> |
| 8. | <input type="checkbox"/> | <input type="text"/> | <input type="checkbox"/> |

OK Clear All Close

Obtain an IP address automatically – Click this button to obtain the IP address automatically if you want to use **Dynamic IP** mode.

Router Name: Type in the router name provided by ISP.

Domain Name: Type in the domain name that you have assigned.

Specify an IP address – Click this radio button to specify some data if you want to use **Static IP** mode.

IP Address: Type the IP address.

Subnet Mask: Type the subnet mask.

Gateway IP Address: Type the gateway IP address.

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

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

DNS Server IP Address

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

4.1.4 PPTP/L2TP

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

PPTP Client Mode

| | | |
|---|--|--|
| PPTP Setup PPTP Link <input type="radio"/> Enable <input checked="" type="radio"/> Disable PPTP Server <input type="text"/> ISP Access Setup Username <input type="text" value="123"/> Password <input type="password" value="..."/> Index(1-15) in Schedule Setup: => <input type="text"/> , <input type="text"/> , <input type="text"/> , <input type="text"/> | | PPP Setup PPP Authentication <input type="text" value="PAP or CHAP"/> <input checked="" type="checkbox"/> Always On Idle Timeout <input type="text" value="-1"/> second(s) IP Address Assignment Method (IPCP) Fixed IP <input type="radio"/> Yes <input checked="" type="radio"/> No (Dynamic IP) Fixed IP Address <input type="text"/> WAN IP Network Settings <input type="radio"/> Obtain an IP address automatically <input checked="" type="radio"/> Specify an IP address IP Address <input type="text" value="172.16.3.229"/> Subnet Mask <input type="text" value="255.255.0.0"/> |
| <input type="button" value="OK"/> | | |

PPTP Setup

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

Disable – Click this radio button to close the connection through PPTP.

PPTP Server - Specify the IP address of the PPTP/L2TP server if you enable PPTP/L2TP client mode.

ISP Access Setup

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

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

Index (1-15) in Schedule Setup - You can type in four sets of time schedule for your request. All the schedules can be set previously in **Application – Schedule** web page and you can use the number that you have set in that web page.

PPP Setup

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

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

IP Address Assignment Method(IPCP)

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

Fixed IP Address -Type a fixed IP address.

WAN IP Network 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.

4.2 LAN

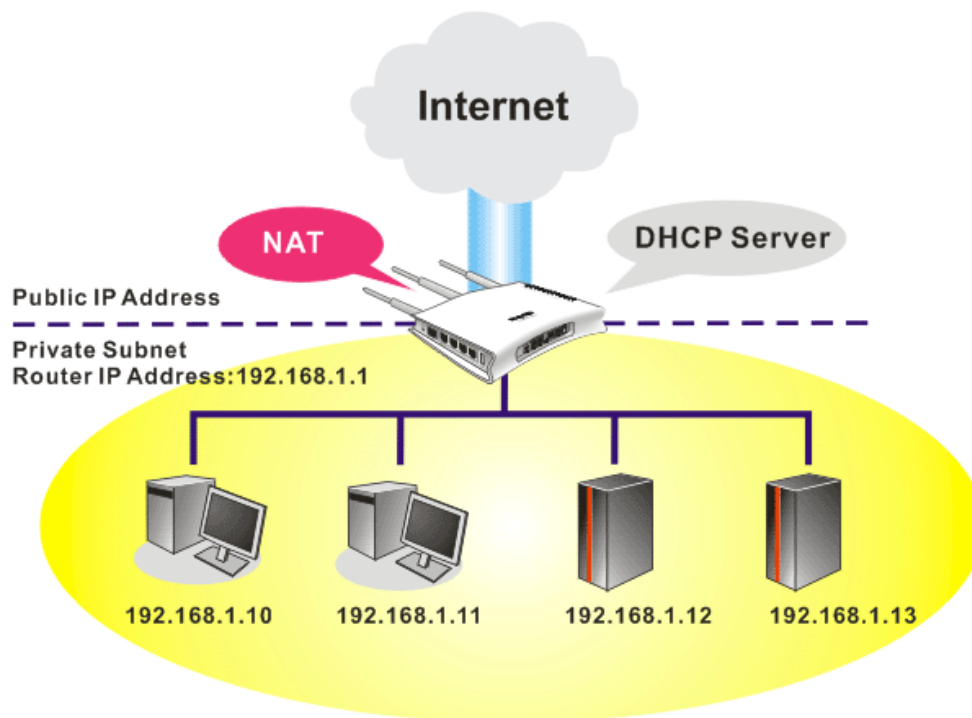
Local Area Network (LAN) is a group of subnets regulated and ruled by router. The design of network structure is related to what type of public IP addresses coming from your ISP.

LAN

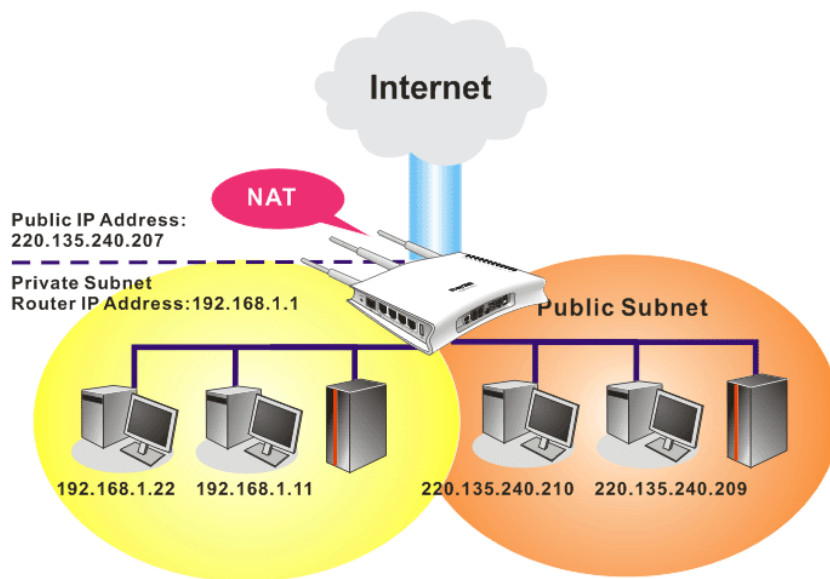
- General Setup
- Static Route
- VLAN
- Bind IP to MAC

4.2.1 Basics of LAN

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



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



What is Routing Information Protocol (RIP)

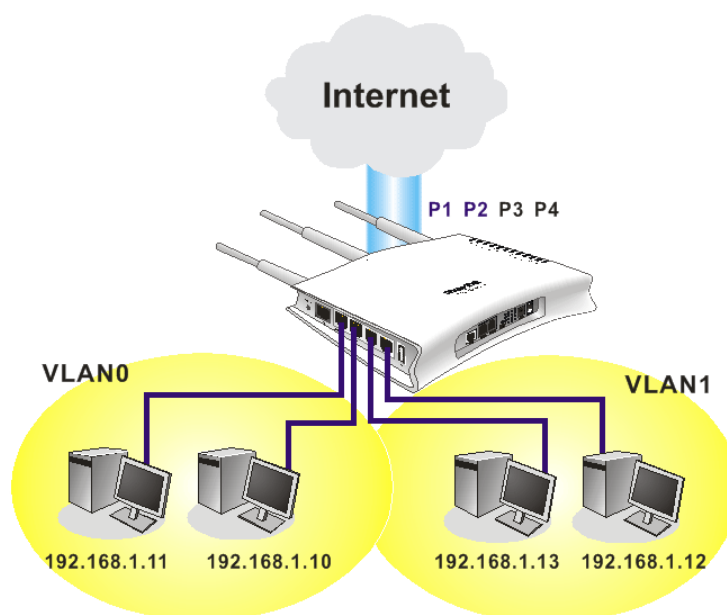
Vigor router will exchange routing information with neighboring routers using the RIP to accomplish IP routing. This allows users to change the information of the router such as IP address and the routers will automatically inform for each other.

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 and Rate Control

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



4.2.2 General Setup

This page provides you the general settings for LAN.

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

[LAN >> General Setup](#)

Ethernet TCP / IP and DHCP Setup

| LAN IP Network Configuration | DHCP Server Configuration |
|--|---|
| For NAT Usage | <input checked="" type="radio"/> Enable Server <input type="radio"/> Disable Server |
| 1st IP Address <input type="text" value="192.168.1.5"/> | Relay Agent: <input type="radio"/> 1st Subnet <input type="radio"/> 2nd Subnet |
| 1st Subnet Mask <input type="text" value="255.255.255.0"/> | Start IP Address <input type="text" value="192.168.1.10"/> |
| For IP Routing Usage <input type="radio"/> Enable <input checked="" type="radio"/> Disable | IP Pool Counts <input type="text" value="50"/> |
| 2nd IP Address <input type="text" value="192.168.2.1"/> | Gateway IP Address <input type="text" value="192.168.1.5"/> |
| 2nd Subnet Mask <input type="text" value="255.255.255.0"/> | DHCP Server IP Address for Relay Agent <input type="text"/> |
| <input checked="" type="checkbox"/> 2nd Subnet DHCP Server | |
| RIP Protocol Control <input type="text" value="Disable"/> | DNS Server IP Address |
| | <input type="checkbox"/> Force DNS manual setting |
| | Primary IP Address <input type="text"/> |
| | Secondary IP Address <input type="text"/> |

OK

- | | |
|-----------------------------------|---|
| 1st IP Address | Type in private IP address for connecting to a local private network (Default: 192.168.1.1). |
| 1st Subnet Mask | Type in an address code that determines the size of the network. (Default: 255.255.255.0/ 24) |
| For IP Routing Usage | Click Enable to invoke this function. The default setting is Disable . |
| 2nd IP Address | Type in secondary IP address for connecting to a subnet. (Default: 192.168.2.1/ 24) |
| 2nd Subnet Mask | An address code that determines the size of the network. (Default: 255.255.255.0/ 24) |
| 2nd DHCP Server | You can configure the router to serve as a DHCP server for the 2nd subnet. |

2nd DHCP Server

Start IP Address:

IP Pool Counts: (max. 10)

| Index | Matched MAC Address | given IP Address |
|-------|---------------------|------------------|
| | | |

MAC Address :

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

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

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

RIP Protocol Control

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

RIP Protocol Control

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

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

DHCP Server Configuration

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

If you want to use another DHCP server in the network other than the Vigor Router's, you can let Relay Agent help you to redirect the DHCP request to the specified location.

Enable Server - Let the router assign IP address to every host in the LAN.

Disable Server – Let you manually assign IP address to every host in the LAN.

Relay Agent – (1st subnet/2nd subnet) Specify which subnet that DHCP server is located the relay agent should redirect the DHCP request to.

Start IP Address - Enter a value of the IP address pool for the DHCP server to start with when issuing IP addresses. If the 1st IP address of your router is 192.168.1.1, the starting IP address must be 192.168.1.2 or greater, but smaller than 192.168.1.254.

IP Pool Counts - Enter the maximum number of PCs that you want the DHCP server to assign IP addresses to. The default is 50 and the maximum is 253.

Gateway IP Address - Enter a value of the gateway IP address for the DHCP server. The value is usually as same as the 1st IP address of the router, which means the router is the default gateway.

DHCP Server IP Address for Relay Agent - Set the IP address of the DHCP server you are going to use so the Relay Agent can help to forward the DHCP request to the DHCP server.

DNS Server Configuration

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

Force DNS manual setting - Force Vigor router to use DNS servers in this page instead of DNS servers given by the Internet Access server (PPPoE, PPTP, L2TP or DHCP server).

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

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

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

| System Status | | | System Uptime: 5:11:9 | |
|---------------|------------|---------------------------|-----------------------|---------------------------|
| LAN Status | | Primary DNS: 194.109.6.66 | | Secondary DNS: 168.95.1.1 |
| IP Address | TX Packets | RX Packets | | |
| 192.168.1.5 | 9326 | 9487 | | |

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.

4.2.3 Static Route

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

[LAN >> Static Route Setup](#)

| Static Route Configuration | | | Set to Factory Default | View Routing Table | |
|----------------------------|---------------------|--------|--|------------------------------------|--------|
| Index | Destination Address | Status | Index | Destination Address | Status |
| 1. | ??? | ? | 6. | ??? | ? |
| 2. | ??? | ? | 7. | ??? | ? |
| 3. | ??? | ? | 8. | ??? | ? |
| 4. | ??? | ? | 9. | ??? | ? |
| 5. | ??? | ? | 10. | ??? | ? |

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

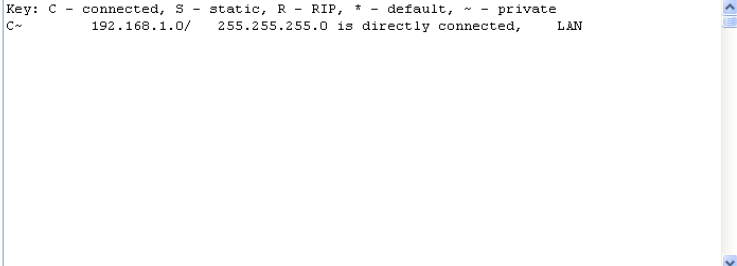
Index The number (1 to 10) under Index allows you to open next page to set up static route.

Destination Address Displays the destination address of the static route.

Status Displays the status of the static route.

Viewing Routing Table Displays the routing table for your reference.

[Diagnostics >> View Routing Table](#)

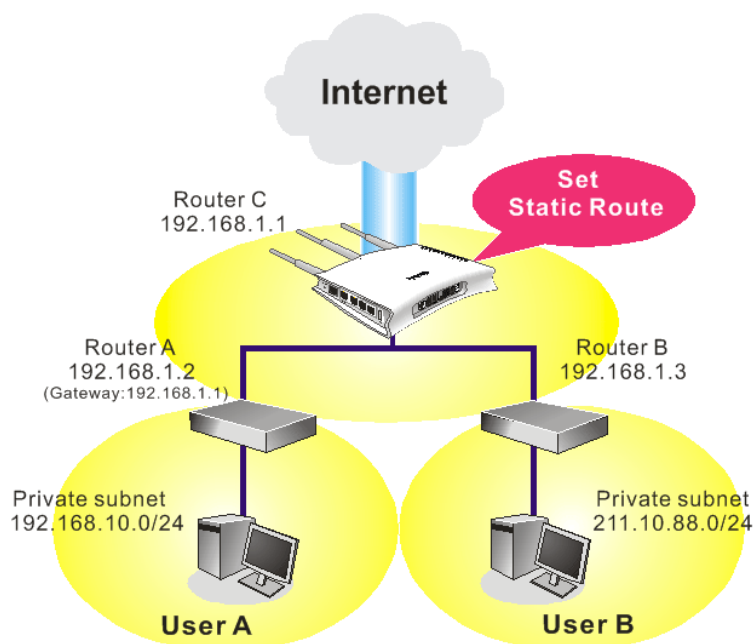
| Current Running Routing Table | | Refresh |
|---|--|-------------------------|
| Key: C - connected, S - static, R - RIP, * - default, ~ - private C~ 192.168.1.0/ 255.255.255.0 is directly connected, LAN | | |
|  | | |

Add Static Routes to Private and Public Networks

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

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

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



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

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

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

[LAN >> Static Route Setup](#)

Index No. 1

| | |
|--|---------------|
| <input checked="" type="checkbox"/> Enable | |
| Destination IP Address | 192.168.10.0 |
| Subnet Mask | 255.255.255.0 |
| Gateway IP Address | 192.168.1.2 |
| Network Interface | LAN |

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

LAN >> Static Route Setup

Index No. 1

| | |
|--|--|
| <input checked="" type="checkbox"/> Enable | |
| Destination IP Address | <input type="text" value="211.100.88.0"/> |
| Subnet Mask | <input type="text" value="255.255.255.0"/> |
| Gateway IP Address | <input type="text" value="192.168.1.3"/> |
| Network Interface | <input type="text" value="LAN"/> |

OK

Cancel

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

Diagnostics >> View Routing Table

Current Running Routing Table

| [Refresh](#) |

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


4.2.4 VLAN

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

LAN >> VLAN Configuration

VLAN Configuration

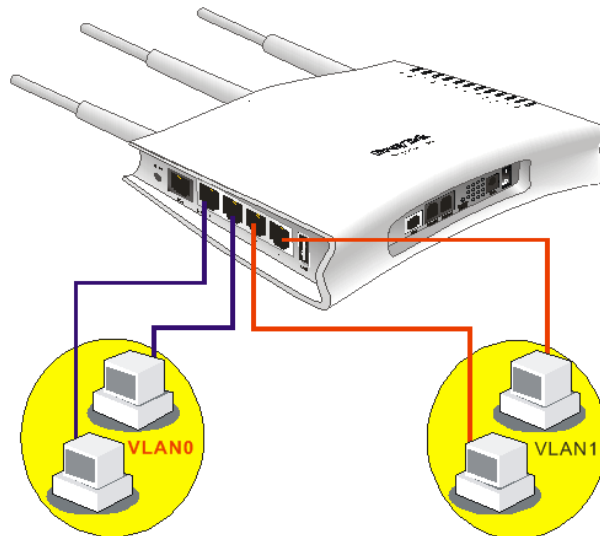
☒ Enable

| | P1 | P2 | P3 | P4 |
|-------|--------------------------|--------------------------|--------------------------|--------------------------|
| VLAN0 | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| VLAN1 | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| VLAN2 | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| VLAN3 | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |

OK Clear Cancel

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

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



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

LAN >> VLAN Configuration

VLAN Configuration

☒ Enable

| | P1 | P2 | P3 | P4 |
|-------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|
| VLAN0 | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| VLAN1 | <input type="checkbox"/> | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |
| VLAN2 | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| VLAN3 | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |

OK Clear Cancel

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

4.2.5 Bind IP to MAC

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

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

[LAN >> Bind IP to MAC](#)

Bind IP to MAC
Note: IP-MAC binding presets DHCP Allocations.
If you select Strict Bind, unspecified LAN clients cannot access the Internet.
☒ **Enable** ☐ **Disable** ☐ **Strict Bind**

ARP Table | [Select All](#) | [Sort](#) | [Refresh](#) |

| IP Address | Mac Address |
|--------------|-------------------|
| 192.168.1.1 | 00-50-7F-DD-15-18 |
| 192.168.1.10 | 00-0E-A6-2A-D5-A1 |

IP Bind List | [Select All](#) | [Sort](#) |

| Index | IP Address | Mac Address |
|-------|------------|-------------|
|-------|------------|-------------|

Add and Edit
IP Address
Mac Address :::::

Enable

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

Disable

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

Strict Bind

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

ARP Table

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

Add and Edit

IP Address – Type the IP address that will be used for the specified MAC address.

Mac Address – Type the MAC address that is used to bind with the assigned IP address.

Refresh

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

IP Bind List

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

| | |
|---------------|---|
| Add | It allows you to add the one you choose from the ARP table or the IP/MAC address typed in Add and Edit to the table of IP Bind List . |
| Edit | It allows you to edit and modify the selected IP address and MAC address that you create before. |
| Remove | You can remove any item listed in IP Bind List . Simply click and select the one, and click Remove . The selected item will be removed from the IP Bind List . |

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

4.3 NAT

Usually, the router serves as an NAT (Network Address Translation) router. NAT is a mechanism that one or more private IP addresses can be mapped into a single public one. Public IP address is usually assigned by your ISP, for which you may get charged. Private IP addresses are recognized only among internal hosts.

When the outgoing packets destined to some public server on the Internet reach the NAT router, the router will change its source address into the public IP address of the router, select the available public port, and then forward it. At the same time, the router shall list an entry in a table to memorize this address/port-mapping relationship. When the public server response, the incoming traffic, of course, is destined to the router's public IP address and the router will do the inversion based on its table. Therefore, the internal host can communicate with external host smoothly.

The benefit of the NAT includes:

- **Save cost on applying public IP address and apply efficient usage of IP address.** NAT allows the internal IP addresses of local hosts to be translated into one public IP address, thus you can have only one IP address on behalf of the entire internal hosts.
- **Enhance security of the internal network by obscuring the IP address.** There are many attacks aiming victims based on the IP address. Since the attacker cannot be aware of any private IP addresses, the NAT function can protect the internal network.

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

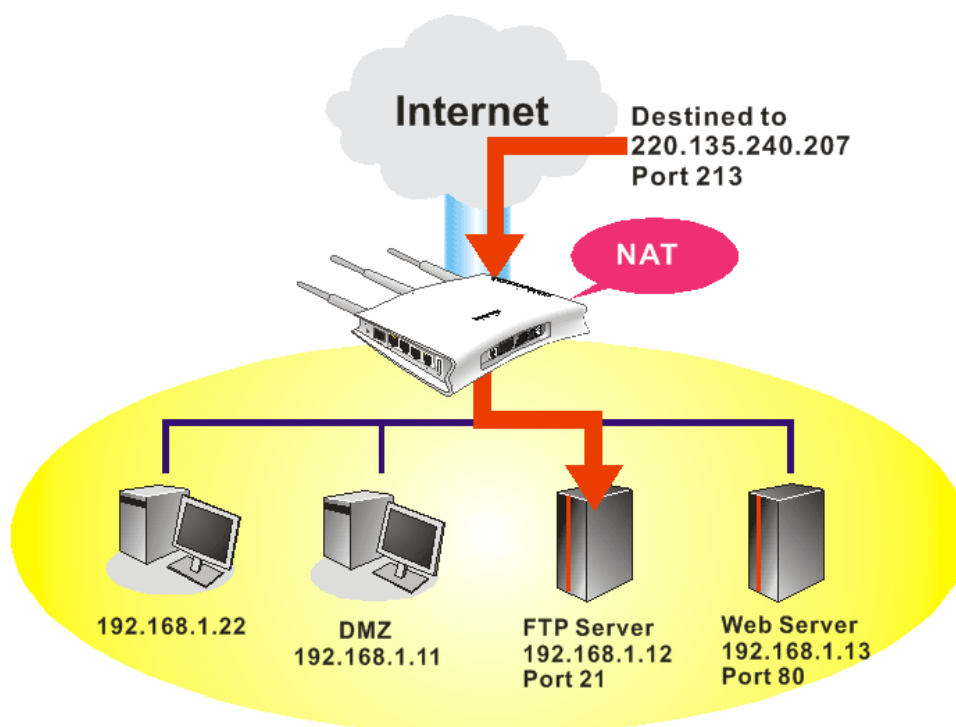
Below shows the menu items for NAT.



4.3.1 Port Redirection

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

is to forward all access request with public IP address from external users to the mapping private IP address/port of the server.



The port redirection can only apply to incoming traffic.

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

[NAT >> Port Redirection](#)

Port Redirection

[Set to Factory Default](#)

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

<< [1-10](#) | [11-20](#) >>

[Next](#) >>

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

Index No. 1

| | |
|---------------------------------|--------|
| <input type="checkbox"/> Enable | |
| Mode | Single |
| Service Name | Single |
| Protocol | --- |
| WAN IP | 1.All |
| Public Port | 0 |
| Private IP | |
| Private Port | 0 |

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

OK Clear Cancel

Enable

Check this box to enable such port redirection setting.

Mode

Two options (Single and Range) are provided here for you to choose. To set a range for the specific service, select **Range**. In Range mode, if the public port (start port and end port) and the starting IP of private IP had been entered, the system will calculate and display the ending IP of private IP automatically.

Service Name

Enter the description of the specific network service.

Protocol

Select the transport layer protocol (TCP or UDP).

WAN IP

Select the WAN IP used for port redirection. There are eight WAN IP alias that can be selected and used for port redirection. The default setting is **All** which means all the incoming data from any port will be redirected to specified range of IP address and port.

Public Port

Specify which port can be redirected to the specified **Private IP and Port** of the internal host. If you choose **Range** as the port redirection mode, you will see two boxes on this field. Simply type the required number on the first box. The second one will be assigned automatically later.

Private IP

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

Private Port

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

Active

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

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

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

conflict, such as 8080. This can be set in the **System Maintenance >>Management Setup**. You then will access the admin screen of by suffixing the IP address with 8080, e.g., http://192.168.1.1:8080 instead of port 80.

[System Maintenance >> Management](#)

Management Setup

Management Access Control

☐ Allow management from the Internet

☐ FTP Server
 ☒ HTTP Server
 ☒ HTTPS Server
 ☒ Telnet Server
 ☐ SSH Server

☒ Disable PING from the Internet

Access List

| List | IP | Subnet Mask |
|------|----------------------|------------------------|
| 1 | <input type="text"/> | <input type="text"/> ▼ |
| 2 | <input type="text"/> | <input type="text"/> ▼ |
| 3 | <input type="text"/> | <input type="text"/> ▼ |

Management Port Setup

☒ User Define Ports
 ☐ Default Ports

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

SNMP Setup

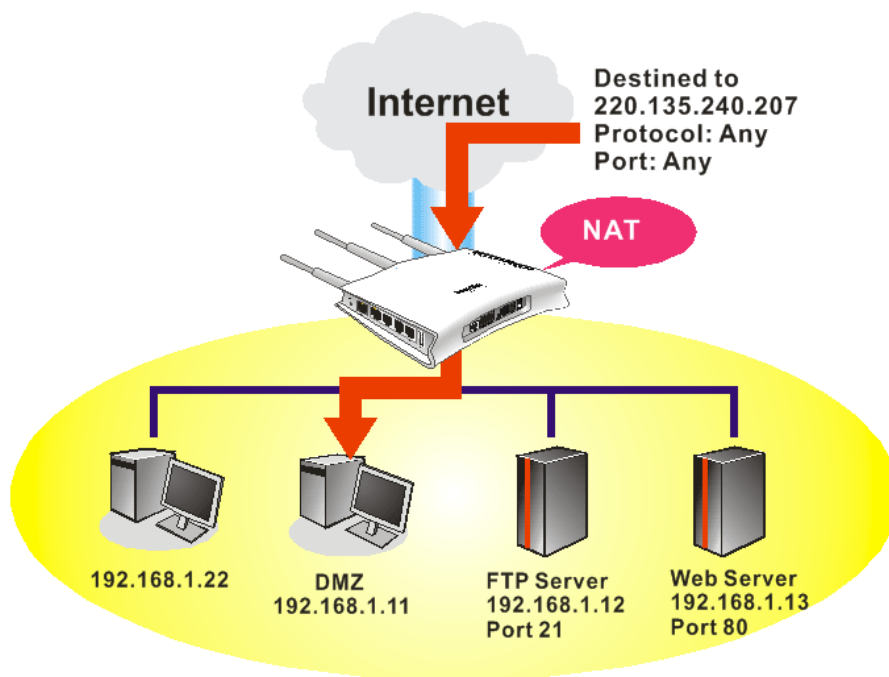
☐ Enable SNMP Agent

Get Community
 Set Community
 Manager Host IP
 Trap Community
 Notification Host IP
 Trap Timeout seconds

OK

4.3.2 DMZ Host

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



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

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

[NAT >> DMZ Host Setup](#)

DMZ Host Setup

WAN 1

None

Private IP

Choose PC

MAC Address of the True IP DMZ Host

00 . 00 . 00 . 00 . 00 . 00

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

OK

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

[NAT >> DMZ Host Setup](#)

DMZ Host Setup

WAN 1

| Index | Enable | Aux. WAN IP | Private IP | |
|-------|--------------------------|--------------|------------|-----------|
| 1. | <input type="checkbox"/> | 172.16.3.229 | | Choose PC |
| 2. | <input type="checkbox"/> | 162.168.1.55 | | Choose PC |

OK

Clear

Enable

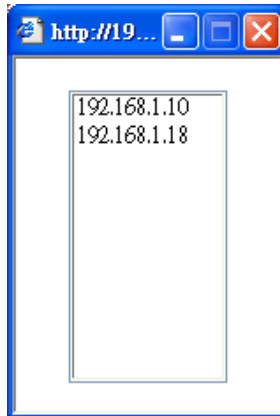
Check to enable the DMZ Host function.

Private IP

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

Choose PC

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



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

[NAT >> DMZ Host Setup](#)

DMZ Host Setup

| WAN 1 | | | | |
|-------|-------------------------------------|--------------|--------------|---------------------------|
| Index | Enable | Aux. WAN IP | Private IP | |
| 1. | <input checked="" type="checkbox"/> | 172.16.3.229 | 192.168.1.10 | Choose PC |
| 2. | <input type="checkbox"/> | 162.168.1.55 | | Choose PC |

[OK](#) [Clear](#)

4.3.3 Open Ports

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

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

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

[NAT >> Open Ports](#)

Open Ports Setup

[Set to Factory Default](#)

| 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 |

<< [1-10](#) | [11-20](#) >>

[Next](#) >>

| | |
|-------------------------|---|
| Index | Indicate the relative number for the particular entry that you want to offer service in a local host. You should click the appropriate index number to edit or clear the corresponding entry. |
| Comment | Specify the name for the defined network service. |
| Local IP Address | Display the private IP address of the local host offering the service. |
| Status | Display the state for the corresponding entry. X or V is to represent the Inactive or Active state. |

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

NAT >> Open Ports >> Edit Open Ports

Index No. 1

☒ Enable Open Ports

Comment

WAN IP

Local Computer

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

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

4.4 Firewall

4.4.1 Basics for Firewall

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

Firewall Facilities

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

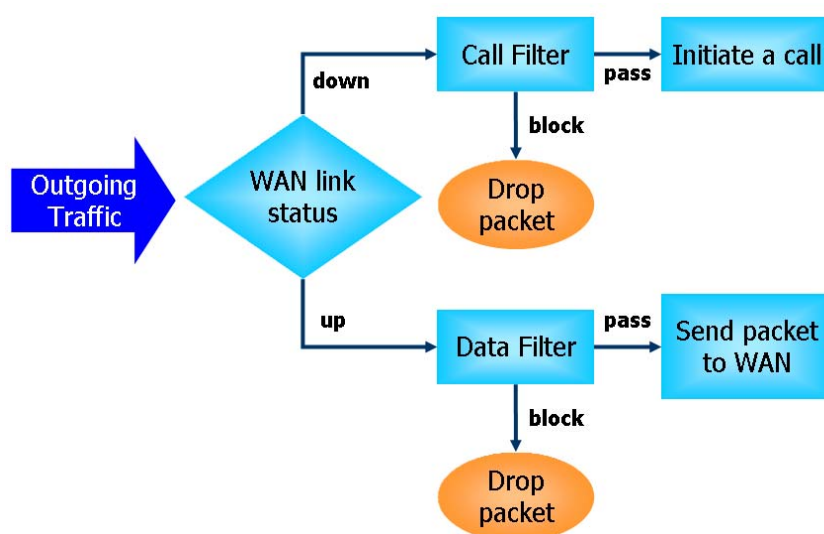
- User-configurable IP filter (Call Filter/ Data Filter).
- Stateful Packet Inspection (SPI): tracks packets and denies unsolicited incoming data
- Selectable Denial of Service (DoS) /Distributed DoS (DDoS) attacks protection

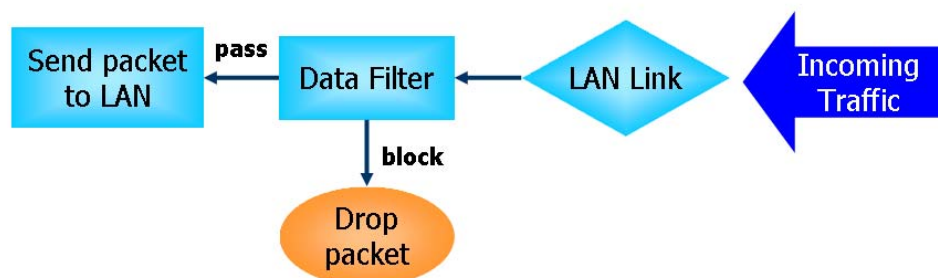
IP Filters

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

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

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





Stateful Packet Inspection (SPI)

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

Denial of Service (DoS) Defense

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

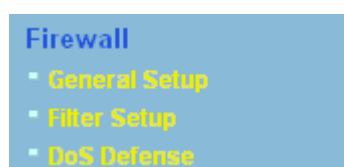
The **DoS Defense** function enables the Vigor router to inspect every incoming packet based on the attack signature database. Any malicious packet that might duplicate itself to paralyze the host in the secure LAN will be strictly blocked and a Syslog message will be sent as warning, if you set up Syslog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

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

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

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

Below shows the menu items for Firewall.



4.4.2 General Setup

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

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

Firewall >> General Setup

General Setup

Call Filter
☒ Enable
☐ Disable

Start Filter Set Set#1

Data Filter
☒ Enable
☐ Disable

Start Filter Set Set#2

Actions for default rule:

| Application | Action/Profile | Syslog |
|---------------------------|-------------------|--------------------------|
| Filter | Pass | <input type="checkbox"/> |
| IM/P2P Filter | None | <input type="checkbox"/> |
| URL Content Filter | None | <input type="checkbox"/> |
| Web Content Filter | None | <input type="checkbox"/> |

Advance Setting Edit

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

OK Cancel

Call Filter

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

Data Filter

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

Filter

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

Pass

Pass

Block

IM/P2P Filter

Select a CSM profile for global IM/P2P application blocking. All the hosts in LAN must follow the standard configured in the CSM profile selected here. For detailed information, refer to the section of CSM profile setup. For troubleshooting needs, you can specify to record information for IM/P2P by checking the Log box. It will be sent to Syslog server. Please refer to section 4.14.4 **Syslog/Mail Alert** for more detailed information.

URL Content Filter

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

box. It will be sent to Syslog server. Please refer to section 4.14.4 **Syslog/Mail Alert** for more detailed information.

Web Content Filter

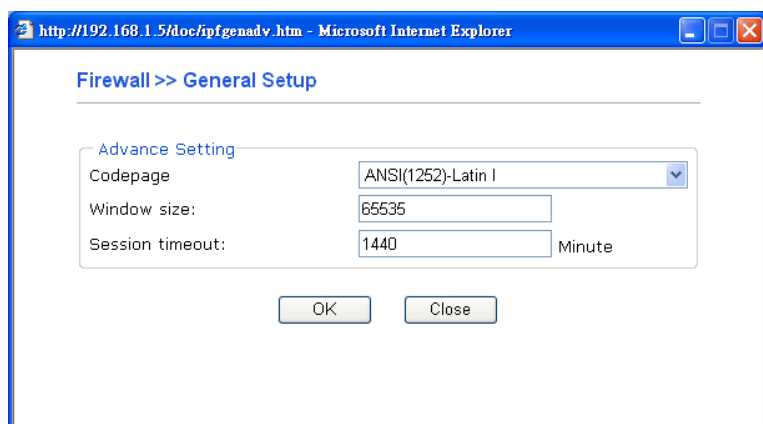
Select one of the **Web Content Filter** profile settings (created in **CSM>> Web Content Filter**) for applying with this router. Please set at least one profile for anti-virus in **CSM>> Web Content Filter** web page first. For troubleshooting needs, you can specify to record information for **Web Content Filter** by checking the Log box. It will be sent to Syslog server. Please refer to section 4.14.4 **Syslog/Mail Alert** for more detailed information.

Syslog

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

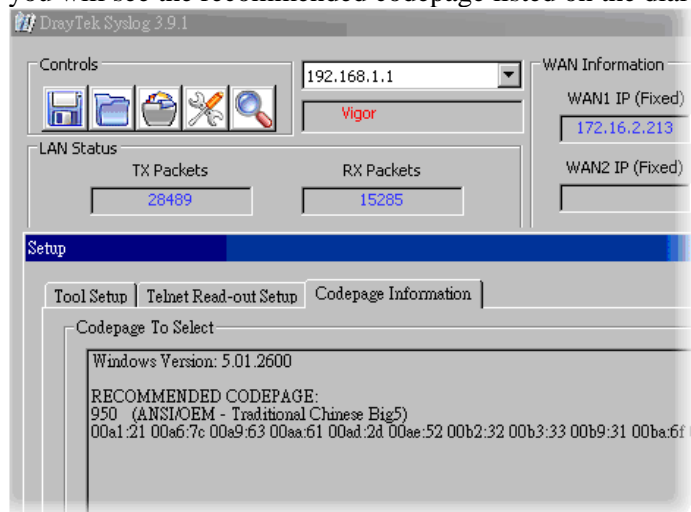
Advance Setting

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



Codepage - This function is used to compare the characters among different languages. Choose correct codepage can help the system obtaining correct ASCII after decoding data from URL and enhance the correctness of URL Content Filter. The default value for this setting is ANSI 1252 Latin I. If you do not choose any codepage, no decoding job of URL will be processed. Please use the drop-down list to choose a codepage.

If you do not have any idea of choosing suitable codepage, please open Syslog. From Codepage Information of Setup dialog, you will see the recommended codepage listed on the dialog box.



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

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

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

4.4.3 Filter Setup

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

[Firewall >> Filter Setup](#)

| Filter Setup Set to Factory Default | | | |
|--|---------------------|---------------------|----------|
| Set | Comments | Set | Comments |
| 1. | Default Call Filter | 7. | |
| 2. | Default Data Filter | 8. | |
| 3. | | 9. | |
| 4. | | 10. | |
| 5. | | 11. | |
| 6. | | 12. | |

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

[Firewall >> Filter Setup >> Edit Filter Set](#)

Filter Set 1

Comments :

| Filter Rule | Active | Comments | Move Up | Move Down |
|----------------------------------|-------------------------------------|---------------|--------------------|----------------------|
| <input type="button" value="1"/> | <input checked="" type="checkbox"/> | Block NetBios | | Down |
| <input type="button" value="2"/> | <input type="checkbox"/> | | UP | Down |
| <input type="button" value="3"/> | <input type="checkbox"/> | | UP | Down |
| <input type="button" value="4"/> | <input type="checkbox"/> | | UP | Down |
| <input type="button" value="5"/> | <input type="checkbox"/> | | UP | Down |
| <input type="button" value="6"/> | <input type="checkbox"/> | | UP | Down |
| <input type="button" value="7"/> | <input type="checkbox"/> | | UP | |

Next Filter Set None

Filter Rule

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

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

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

[Firewall >> Edit Filter Set >> Edit Filter Rule](#)

Filter Set 1 Rule 1

☒ Check to enable the Filter Rule

Comments:

Index(1-15) in [Schedule](#) Setup: , , ,

Direction:

Source IP:

Destination IP:

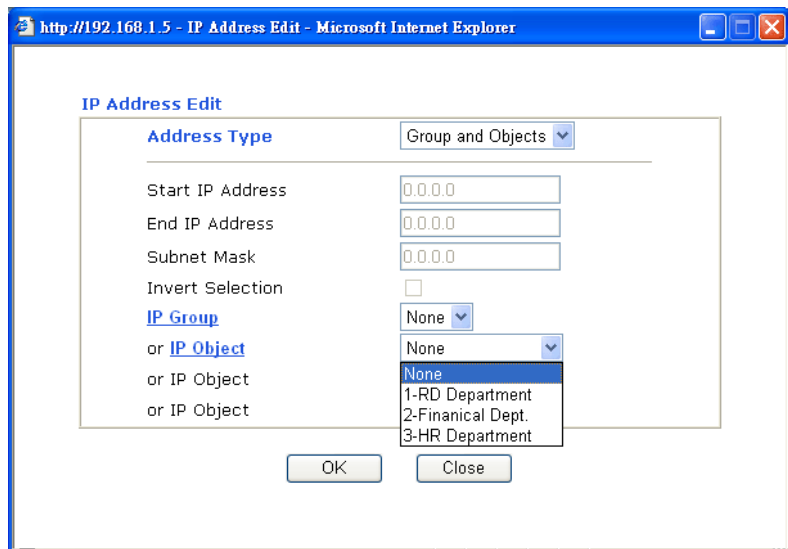
Service Type:

Fragments:

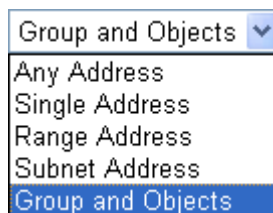
| Application | Action/Profile | Syslog |
|------------------------------------|--|--------------------------|
| Filter: | <input type="text" value="Block Immediately"/> | <input type="checkbox"/> |
| Branch to Other Filter Set: | <input type="text" value="None"/> | |
| IM/P2P Filter: | <input type="text" value="None"/> | <input type="checkbox"/> |
| URL Content Filter | <input type="text" value="None"/> | <input type="checkbox"/> |
| Web Content Filter | <input type="text" value="None"/> | <input type="checkbox"/> |

Advance Setting

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



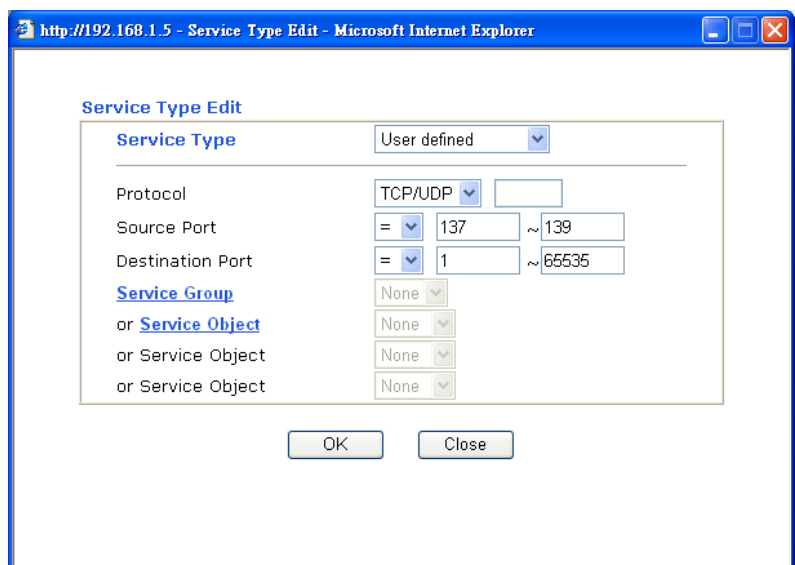
To set the IP address manually, please choose **Any Address/Single Address/Range Address/Subnet Address** as the Address Type and type them in this dialog. In addition, if you want to use the IP range from defined groups or objects, please choose **Group and Objects** as the Address Type.



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

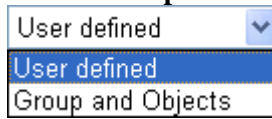
Service Type

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



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

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



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

Source/Destination Port -

(=) – when the first and last value are the same, it indicates one port; when the first and last values are different, it indicates a range for the port and available for this service type.

(!=) – when the first and last value are the same, it indicates all the ports except the port defined here; when the first and last values are different, it indicates that all the ports except the range defined here are available for this service type.

(>) – the port number greater than this value is available.

(<) – the port number less than this value is available for this profile.

Service Group/Object - Use the drop down list to choose the one that you want.

Fragments

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

Don't care -No action will be taken towards fragmented packets.

Unfragmented -Apply the rule to unfragmented packets.

Fragmented - Apply the rule to fragmented packets.

Too Short - Apply the rule only to packets that are too short to contain a complete header.

Filter

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

Block Immediately - Packets matching the rule will be dropped immediately.

Pass Immediately - Packets matching the rule will be passed immediately.

Block If No Further Match - A packet matching the rule, and that does not match further rules, will be dropped.

Pass If No Further Match - A packet matching the rule, and that does not match further rules, will be passed through.

Branch to other Filter Set

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

Content Security Management

All the packets/connections within the range configured in the above conditions must follow the standard configured in the CSM profile selected here. For detailed information, refer to the section of CSM profile setup.

SysLog

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

Example

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

The screenshot illustrates the configuration steps for the Firewall:

- Firewall >> General Setup:** Shows the 'Start Filter Set' dropdown menu for both Call Filter and Data Filter, with 'Set#1' and 'Set#2' selected respectively. The 'Actions for default rule' section shows 'Filter' set to 'Pass' and 'Application' set to 'None'. The 'Advance Setting' section has a checkbox for 'Accept large incoming fragmented UDP or ICMP packets'.
- Firewall >> Filter Setup:** Shows a table of filter sets. The first set is 'Set#1' with 'Default Call Filter' and 'Default Data Filter'.
- Firewall >> Filter Setup >> Edit Filter Set:** Shows a table of filter rules for 'Filter Set 1'. The first rule is 'Block NetBios'.
- Firewall >> Edit Filter Set >> Edit Filter Rule:** Shows the configuration for 'Filter Set 1 Rule 1'. The 'Direction' is 'LAN -> WAN', 'Source IP' is 'Any', 'Destination IP' is 'Any', 'Service Type' is 'TCP/UDP, Port: from 137-139 to undefined', and 'Fragments' is 'Don't Care'. The 'Action/Profile' is 'Block Immediately'.

Red arrows indicate the workflow: from 'General Setup' to 'Filter Setup', then to 'Edit Filter Set', and finally to 'Edit Filter Rule'.

4.4.4 DoS Defense

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

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

[Firewall >> DoS defense Setup](#)

DoS defense Setup

☒ Enable DoS Defense

| | | | |
|---|-----------|----------------------------------|---------------|
| <input type="checkbox"/> Enable SYN flood defense | Threshold | <input type="text" value="50"/> | packets / sec |
| | Timeout | <input type="text" value="10"/> | sec |
| <input type="checkbox"/> Enable UDP flood defense | Threshold | <input type="text" value="150"/> | packets / sec |
| | Timeout | <input type="text" value="10"/> | sec |
| <input type="checkbox"/> Enable ICMP flood defense | Threshold | <input type="text" value="50"/> | packets / sec |
| | Timeout | <input type="text" value="10"/> | sec |
| <input type="checkbox"/> Enable Port Scan detection | Threshold | <input type="text" value="150"/> | packets / sec |

☐ Block IP options
☐ Block Land
☐ Block Smurf
☐ Block trace route
☐ Block SYN fragment
☐ Block Fraggle Attack

☐ Block TCP flag scan
☐ Block Tear Drop
☐ Block Ping of Death
☐ Block ICMP fragment
☐ Block UnknownProtocol

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

OK

Clear All

Cancel

Enable Dos Defense

Check the box to activate the DoS Defense Functionality.

Enable SYN flood defense

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

Enable UDP flood defense

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

Enable ICMP flood defense

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

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

Block Unknown Protocol

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

Warning Messages

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

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

[System Maintenance >> SysLog / Mail Alert Setup](#)

SysLog / Mail Alert Setup

| SysLog Access Setup | Mail Alert Setup |
|--|---|
| <input checked="" type="checkbox"/> Enable | <input checked="" type="checkbox"/> Enable Send a test e-mail |
| Server IP Address: 192.168.1.5 | SMTP Server: <input type="text"/> |
| Destination Port: 514 | Mail To: <input type="text"/> |
| Enable syslog message: | Return-Path: <input type="text"/> |
| <input checked="" type="checkbox"/> Firewall Log | <input type="checkbox"/> Authentication |
| <input checked="" type="checkbox"/> VPN Log | User Name: <input type="text"/> |
| <input checked="" type="checkbox"/> User Access Log | Password: <input type="text"/> |
| <input checked="" type="checkbox"/> Call Log | Enable E-Mail Alert: |
| <input checked="" type="checkbox"/> WAN Log | <input checked="" type="checkbox"/> DoS Attack |
| <input checked="" type="checkbox"/> Router/DSL information | <input checked="" type="checkbox"/> IM-P2P |

OK Clear Cancel

DrayTek Syslog 3.7.0

Controls: 192.168.1.1 **Vigor Series**

LAN Status

| TX Packets | RX Packets |
|------------|------------|
| 4175 | 3668 |

WAN Status

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

Firewall Log | VPN Log | User Access Log | Call Log | WAN Log | Others | Network Information | NetState | Traffic Graph

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

ADSL Status

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

4.5 Objects Settings

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

Objects Setting

- IP Object
- IP Group
- Service Type Object
- Service Type Group
- Keyword Object
- Keyword Group
- File Extension Object
- IM Object
- P2P Object
- Misc Object

4.5.1 IP Object

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

[Objects Setting >> IP Object](#)

IP Object Profiles:

[Set to Factory Default](#)

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

<< [1-32](#) | [33-64](#) | [65-96](#) | [97-128](#) | [129-160](#) | [161-192](#) >>

[Next >>](#)

Set to Factory Default Clear all profiles.

Click the number under Index column for settings in detail.

Profile Index : 1

| | |
|-------------------|--------------------------|
| Name: | RD Department |
| Interface: | Any |
| Address Type: | Range Address |
| Start IP Address: | 192.168.1.64 |
| End IP Address: | 192.168.1.75 |
| Subnet Mask: | 0.0.0.0 |
| Invert Selection: | <input type="checkbox"/> |

OK Clear Cancel

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

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

Interface:

| | |
|-----|---|
| Any | ▼ |
| Any | |
| LAN | |
| WAN | |

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

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

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

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

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

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

Below is an example of IP objects settings.

Objects Setting >> IP Object

IP Object Profiles:

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

4.5.2 IP Group

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

Objects Setting >> IP Group

IP Group Table:

[Set to Factory Default](#)

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

Set to Factory Default Clear all profiles.

Click the number under Index column for settings in detail.

Profile Index : 1

Name:

Interface: Any ▼

Available IP Objects

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

Selected IP Objects

>> <<

OK Clear Cancel

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

4.5.3 Service Type Object

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

[Objects Setting >> Service Type Object](#)

Service Type Object Profiles: | [Set to Factory Default](#) |

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

<< [1-32](#) | [33-64](#) | [65-96](#) >> [Next](#) >>

Set to Factory Default Clear all profiles.

Click the number under Index column for settings in detail.

[Objects Setting >> Service Type Object Setup](#)

Profile Index : 1

Name

www

Protocol

TCP

6

Source Port

=

1

~

65535

Destination Port

=

1

~

65535

OK

Clear

Cancel

Name Type a name for this profile.

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

TCP

6

Any

ICMP

IGMP

TCP

UDP

TCP/UDP

Other

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

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

Below is an example of service type objects settings.

Objects Setting >> Service Type Object

Service Type Object Profiles:

| Index | Name |
|--------------------|------|
| 1. | SIP |
| 2. | RTP |
| 3. | |

4.5.4 Service Type Group

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

Objects Setting >> Service Type Group

Service Type Group Table:

[Set to Factory Default](#)

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

Set to Factory Default

Clear all profiles.

Click the number under Index column for settings in detail.

Profile Index : 1

Name:

Available Service Type Objects

1-SIP
2-RTP

Selected Service Type Objects

>>
<<

OK Clear Cancel

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

4.5.5 Keyword Object

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

Objects Setting >> Keyword Object

Keyword Object Profiles: [Set to Factory Default](#)

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

<< [1-32](#) | [33-64](#) | [65-96](#) | [97-128](#) | [129-160](#) | [161-192](#) | [193-200](#) >> [Next](#) >>

- Set to Factory Default** Clear all profiles.
- Click the number under Index column for setting in detail.

Objects Setting >> Keyword Object Setup

Profile Index : 1

| | |
|----------|--|
| Name | <input type="text"/> |
| Contents | <input type="text"/> (Max 63 characters) |

Name

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

Contents

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

4.5.6 Keyword Group

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

Objects Setting >> Keyword Group

Keyword Group Table:

[Set to Factory Default](#)

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

Set to Factory Default

Clear all profiles.

Click the number under Index column for setting in detail.

Objects Setting >> Keyword Group Setup

Profile Index : 1

Name:

Available Keyword Objects

1-Keyword-1
2-keyword-2

Selected Keyword Objects(Max 16 Objects)

>>

<<

OK

Clear

Cancel


Name

Type a name for this group.

Available Keyword Objects

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

Selected Keyword Objects

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

4.5.7 File Extension Object

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

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

Objects Setting >> File Extension Object

| File Extension Object Profiles: | | | | Set to Factory Default | |
|---------------------------------|------|--------------------|------|--|--|
| Profile | Name | Profile | Name | | |
| 1. | | 5. | | | |
| 2. | | 6. | | | |
| 3. | | 7. | | | |
| 4. | | 8. | | | |

Set to Factory Default

Clear all profiles.

Click the number under Profile column for configuration in details.

Objects Setting >> File Extension Object Setup

Profile Index: 1 Profile Name:

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

Profile Name Type a name for this profile.

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

4.5.8 IM Object

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

[Objects Setting >> IM Object Profile](#)

IM Profile Table: [Set to Factory Default](#)

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

Set to Factory Default Clear all profiles.

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

[Objects Setting >> IM Object Profile](#)

Profile Index: **1**

Profile Name:

Check for Disallow:

| IM Application | | | | VoIP |
|------------------------------|----------------------------------|--|-------------------------------------|--------------------------------|
| <input type="checkbox"/> MSN | <input type="checkbox"/> YahooIM | <input type="checkbox"/> AIM | <input type="checkbox"/> ICQ | <input type="checkbox"/> Skype |
| <input type="checkbox"/> QQ | <input type="checkbox"/> iChat | <input type="checkbox"/> Jabber/GoogleTalk | <input type="checkbox"/> GoogleChat | <input type="checkbox"/> SIP |

| Web IM (* = more than one address) | | | | | |
|-------------------------------------|------------------------------|----------------------------------|----------------------------|-------------------------|------------------------------|
| <input type="checkbox"/> WebIM URLs | eMessenger | WebMSN | meebo* | eBuddy | ILoveIM* |
| | ICQ Java* | ICQ Flash* | goowy* | IMhaha* | getMessenger |
| | IMUnitive* | WabJet* | mabber* | MSN2GO* | KoolIM |
| | MessengerFX* | MessengerAdictos | WebYahooIM | | |

Profile Name Type a name for this profile.

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

4.5.9 P2P Object

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

[Objects Setting >> P2P Object Profile](#)

P2P Profile Table: [Set to Factory Default](#)

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

Set to Factory Default Clear all profiles.

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

[Objects Setting >> P2P Object Profile](#)

Profile Index: 1

Profile Name:

Check for Disallow:

| Protocol | Applications |
|-------------------------------------|-------------------------------------|
| <input type="checkbox"/> SoulSeek | SoulSeek |
| <input type="checkbox"/> eDonkey | eDonkey, eMule, Shareaza |
| <input type="checkbox"/> FastTrack | Kazaa, BearShare, iMesh |
| <input type="checkbox"/> OpenFT | KCeasy, FilePipe |
| <input type="checkbox"/> Gnutella | BearShare, Limewire, Shareaza, Foxy |
| <input type="checkbox"/> OpenNap | Lopster, XNap, WinLop |
| <input type="checkbox"/> BitTorrent | BitTorrent, BitSpirit, BitComet |
| <input type="checkbox"/> Winny | Winny, WinMX, Share |

Profile Name Type a name for this profile.

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

4.5.10 Misc Object

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

[Objects Setting >> Misc Object Profile](#)

Misc Profile Table:

[Set to Factory Default](#)

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

Set to Factory Default Clear all profiles.

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

[Objects Setting >> Misc Object Profile](#)

Profile Index: 1

Profile Name:

Check for Disallow:

| Streaming | | | |
|------------------------------------|----------------------------------|----------------------------------|-------------------------------------|
| <input type="checkbox"/> MMS | <input type="checkbox"/> RTSP | <input type="checkbox"/> TVAnts | <input type="checkbox"/> PPStream |
| <input type="checkbox"/> PPLive | <input type="checkbox"/> FeiDian | <input type="checkbox"/> UUSee | <input type="checkbox"/> NSPlayer |
| <input type="checkbox"/> PCAST | <input type="checkbox"/> TVKoo | <input type="checkbox"/> SopCast | <input type="checkbox"/> UDLiveX |
| <input type="checkbox"/> TVUPlayer | <input type="checkbox"/> MySee | <input type="checkbox"/> Joost | <input type="checkbox"/> FlashVideo |

Profile Name Type a name for this profile.

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

4.6 CSM Profile

Content Security Management (CSM)

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

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

IM/P2P Filter

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

URL Content Filter

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

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

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

Web Content Filter

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

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

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

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

CSM

- [IM/P2P Filter Profile](#)
- [URL Content Filter Profile](#)
- [Web Content Filter Profile](#)

4.6.1 IM/P2P Filter Profile

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

[CSM >> IM/P2P Filter Profile](#)

IM/P2P Filter Profile Table:

[Set to Factory Default](#)

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

Set to Factory Default

Clear all profiles.

Click the number under Index column for settings in detail.

[CSM >> IM/P2P Filter Profile](#)

Profile Index: **1**

Profile Name:

[IM Object](#)

None ▾

[P2P Object](#)

None ▾

[Misc Object](#)

None ▾

OK

Cancel

Profile Name Type a name for the CSM profile.

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

4.6.2 URL Content Filter Profile

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

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

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

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

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

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

CSM >> URL Content Filter Profile

URL Content Filter Profile Table:

| [Set to Factory Default](#) |

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

Administration Message (Max 255 characters)

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

OK

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

Profile Index: 1

| | |
|--|------------------------|
| Profile Name: <input type="text"/> | |
| Priority: Both : Pass | Log: None |
| 1.URL Access Control <input type="checkbox"/> Enable URL Access Control <input type="checkbox"/> Prevent web access from IP address Action: Pass Group/Object Selections: <input type="text"/> Edit | |
| 2.Web Feature <input type="checkbox"/> Enable Restrict Web Feature Action: Pass <input type="checkbox"/> Cookie <input type="checkbox"/> Proxy <u>File Extension Profile:</u> None | |
| <div>OK Clear Cancel</div> | |

Profile Name

Type the name for such profile.

Priority

It determines the action that this router will apply.

Both: Pass – The router will let all the packages that match with the conditions specified in URL Access Control and Web Feature below passing through. When you choose this setting, both configuration set in this page for URL Access Control and Web Feature will be inactive.

Both:Block –The router will block all the packages that match with the conditions specified in URL Access Control and Web Feature below. When you choose this setting, both configuration set in this page for URL Access Control and Web Feature will be inactive.

Either: URL Access Control First – When all the packages matching with the conditions specified in URL Access Control and Web Feature below, such function can determine the priority for the actions executed. For this one, the router will process the packages with the conditions set below for URL first, then Web feature second.

Either: Web Feature First –When all the packages matching with the conditions specified in URL Access Control and Web Feature below, such function can determine the priority for the actions executed. For this one, the router will process the packages with the conditions set below for web feature first, then URL second.

Both : Pass

Both : Pass

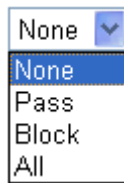
Both : Block

Either : URL Access Control First

Either : Web Feature First

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

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



URL Access Control

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

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

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

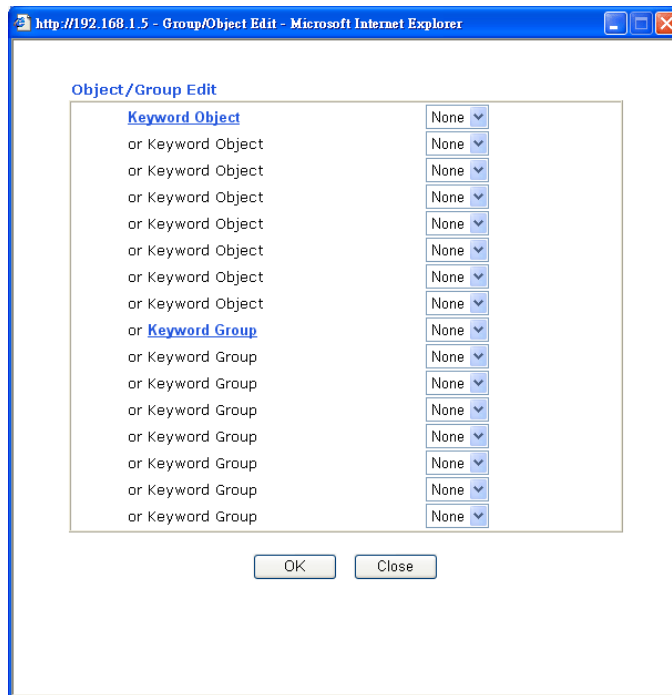
Block - Restrict accessing into the corresponding webpage with the keywords listed on the box below.

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

Action:



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



Web Feature

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

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

Pass - Allow accessing into the corresponding webpage with the keywords listed on the box below.

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

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

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

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

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

File Extension Profile: None ▼
None
1-default

4.6.3 Web Content Filter Profile

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

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

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

[CSM >> Web Content Filter Profile](#)

Web Content Filter Profile Table:

[Set to Factory Default](#)

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

Web Content Filter Setup

Select a server:

[Test a site to verify whether it is categorized](#)

Administration Message (Max 255 characters)

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

OK

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

Profile Index : 1

Profile Name:

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

Action

Pass - allow accessing into the corresponding webpage with the categories listed on the box below.

Block - restrict accessing into the corresponding webpage with the categories listed on the box below.

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

Log

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

Pass – Only the log about Pass will be recorded in Syslog.

Block – Only the log about Block will be recorded in Syslog.

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

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

4.7 Bandwidth Management

Below shows the menu items for Bandwidth Management.



4.7.1 Sessions Limit

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

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

[Bandwidth Management >> Sessions Limit](#)

Sessions Limit

☒ **Enable** ☐ **Disable**

Default Max Sessions:

Limitation List

| Index | Start IP | End IP | Max Sessions |
|-------|----------|--------|--------------|
|-------|----------|--------|--------------|

Specific Limitation

Start IP: End IP:

Maximum Sessions:

Time Schedule

Index(1-15) in [Schedule](#) Setup: , , ,

Note: Action and Idle Timeout settings will be ignored.

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

Enable

Click this button to activate the function of limit session.

Disable

Click this button to close the function of limit session.

Default session limit

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

Limitation List

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

Start IP

Defines the start IP address for limit session.

End IP

Defines the end IP address for limit session.

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

4.7.2 Bandwidth Limit

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

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

[Bandwidth Management >> Bandwidth Limit](#)

Bandwidth Limit

☐ Enable ☒ Disable

Default TX Limit: Kbps Default RX Limit: Kbps

Limitation List

| Index | Start IP | End IP | TX limit | RX limit |
|-------|----------|--------|----------|----------|
|-------|----------|--------|----------|----------|

Specific Limitation

Start IP: End IP:

TX Limit: Kbps RX Limit: Kbps

Time Schedule

Index(1-15) in [Schedule](#) Setup: , , ,

Note: Action and Idle Timeout settings will be ignored.

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

| | |
|-------------------------|---|
| Enable | Click this button to activate the function of limit bandwidth. |
| Disable | Click this button to close the function of limit bandwidth. |
| Default TX limit | Define the default speed of the upstream for each computer in LAN. |
| Default RX limit | Define the default speed of the downstream for each computer in LAN. |
| Limitation List | Display a list of specific limitations that you set on this web page. |
| Start IP | Define the start IP address for limit bandwidth. |
| End IP | Define the end IP address for limit bandwidth. |
| TX limit | Define the limitation for the speed of the upstream. If you do not set the limit in this field, the system will use the default speed for the specific limitation you set for each index. |
| RX limit | Define the limitation for the speed of the downstream. If you do not set the limit in this field, the system will use the default speed for the specific limitation you set for each index. |

| | |
|---------------------------------------|---|
| Add | Add the specific speed limitation onto the list above. |
| Edit | Allows you to edit the settings for the selected limitation. |
| Delete | Remove the selected settings existing on the limitation list. |
| Index (1-15) in Schedule Setup | You can type in four sets of time schedule for your request. All the schedules can be set previously in Application – Schedule web page and you can use the number that you have set in that web page. |

4.7.3 Quality of Service

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

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

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

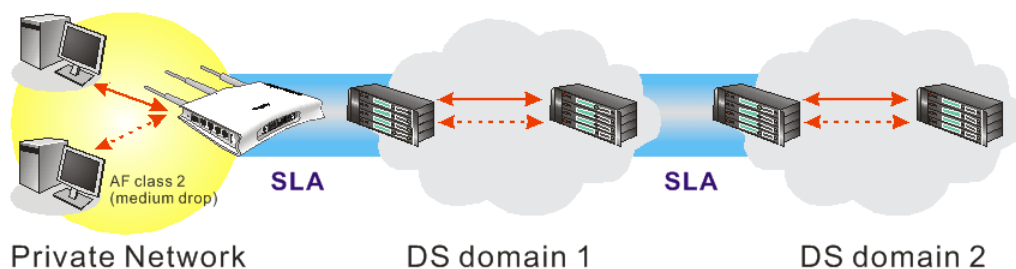
There are two components within Primary configuration of QoS deployment:

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

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

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

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



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

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

[Bandwidth Management >> Quality of Service](#)

| General Setup | | | | | | | Set to Factory Default |
|---------------|---------------------|-----------|---------|---------|---------|--------|--|
| Status | Bandwidth | Direction | Class 1 | Class 2 | Class 3 | Others | UDP Bandwidth Control |
| Enable | 10000Kbps/10000Kbps | Outbound | 25% | 25% | 25% | 25% | Inactive Setup |

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

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

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

General Setup for WAN Interface

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

General Setup

☒ Enable the QoS Control OUTWAN Inbound Bandwidth KbpsWAN Outbound Bandwidth Kbps

| Index | Class Name | Reserved_bandwidth Ratio |
|---------|------------|-----------------------------------|
| Class 1 | | <input type="text" value="25"/> % |
| Class 2 | | <input type="text" value="25"/> % |
| Class 3 | | <input type="text" value="25"/> % |
| | Others | <input type="text" value="25"/> % |

☐ Enable UDP Bandwidth ControlLimited_bandwidth Ratio %☐ Outbound TCP ACK Prioritize[Online Statistics](#)

OK

Clear

Cancel

Enable the QoS Control

The factory default for this setting is checked.

Please also define which traffic the QoS Control settings will apply to.

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

It allows you to set the connecting rate of data input for WAN. For example, if your ADSL supports 1M of downstream and 256K upstream, please set 1000kbps for this box. The default value is 10000kbps.

WAN Outbound Bandwidth

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

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

Reserved Bandwidth Ratio

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

Enable UDP Bandwidth Control

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

Outbound TCP ACK Prioritize

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

network traffic.

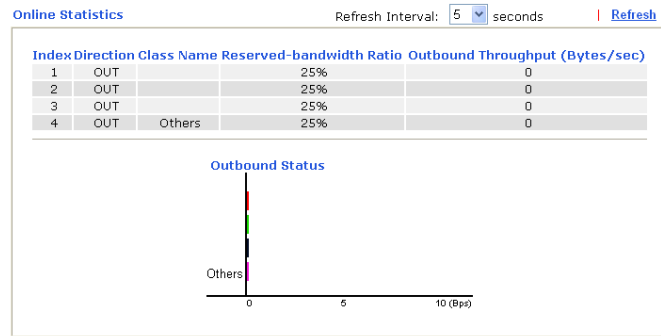
Limited_bandwidth Ratio

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

Online Statistics

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

[Bandwidth Management >> Quality of Service](#)



Edit the Class Rule for QoS

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

[Bandwidth Management >> Quality of Service](#)

[General Setup](#) | [Set to Factory Default](#) |

| Status | Bandwidth | Direction | Class 1 | Class 2 | Class 3 | Others | UDP Bandwidth Control |
|--------|---------------------|-----------|---------|---------|---------|--------|--------------------------------|
| Enable | 10000Kbps/10000Kbps | Outbound | 25% | 25% | 25% | 25% | Inactive Setup |

[Class Rule](#)

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

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

[Bandwidth Management >> Quality of Service](#)

[Class Index #1](#)

Name

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

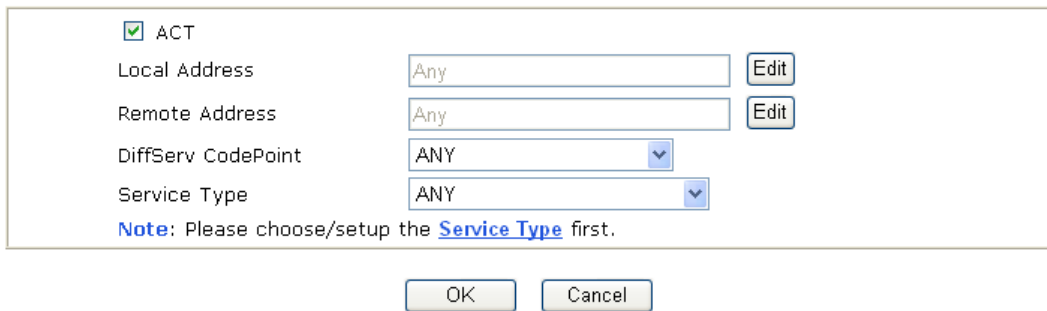
[Add](#) [Edit](#) [Delete](#)

[OK](#) [Cancel](#)

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

[Bandwidth Management >> Quality of Service](#)

Rule Edit



The 'Rule Edit' dialog box contains the following fields and controls:

- ☒ ACT
- Local Address:
- Remote Address:
- DiffServ CodePoint:
- Service Type:
- Note:** Please choose/setup the [Service Type](#) first.
-

ACT

Check this box to invoke these settings.

Local Address

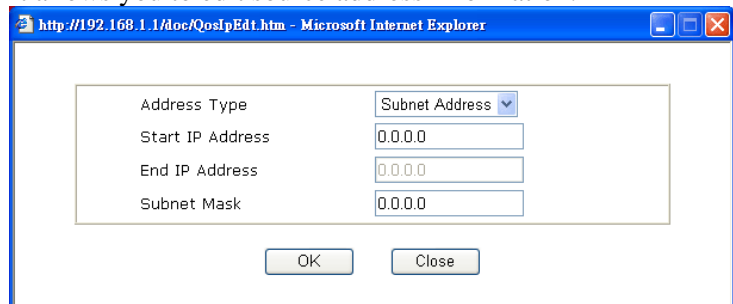
Click the **Edit** button to set the local IP address (on LAN) for the rule.

Remote Address

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

Edit

It allows you to edit source address information.



The 'Edit source address' dialog box, titled 'http://192.168.1.1/doc/QosIpEdit.htm - Microsoft Internet Explorer', contains the following fields and controls:

- Address Type:
- Start IP Address:
- End IP Address:
- Subnet Mask:
-

Address Type – Determine the address type for the source address.

For **Single Address**, you have to fill in Start IP address.

For **Range Address**, you have to fill in Start IP address and End IP address.

For **Subnet Address**, you have to fill in Start IP address and Subnet Mask.

DiffServ CodePoint

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

Service Type

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

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

Bandwidth Management >> Quality of Service

Class Index #1

Name

| NO | Status | Local Address | Remote Address | DiffServ CodePoint | Service Type |
|----------------------------|--------|---------------|----------------|--------------------|--------------|
| 1 | Active | Any | Any | IP precedence 2 | TFTP(UDP:69) |
| <div>Add Edit Delete</div> | | | | | |

OK Cancel

Edit the Service Type for Class Rule

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

Bandwidth Management >> Quality of Service

General Setup

[Set to Factory Default](#)

| Status | Bandwidth | Direction | Class 1 | Class 2 | Class 3 | Others | UDP Bandwidth Control |
|--------|---------------------|-----------|---------|---------|---------|--------|--------------------------------|
| Enable | 10000Kbps/10000Kbps | Outbound | 25% | 25% | 25% | 25% | Inactive Setup |

Class Rule

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

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

Bandwidth Management >> Quality of Service

User Defined Service Type

| NO | Name | Protocol | Port |
|----------------------------|-------|----------|------|
| 1 | Empty | - | - |
| <div>Add Edit Delete</div> | | | |

Cancel

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

[Bandwidth Management >> Quality of Service](#)

Service Type Edit

| | |
|--------------------|---|
| Service Name | <input type="text"/> |
| Service Type | TCP <input type="button" value="v"/> <input type="text" value="6"/> |
| Port Configuration | |
| Type | <input checked="" type="radio"/> Single <input type="radio"/> Range |
| Port Number | <input type="text" value="0"/> - <input type="text" value="0"/> |

OK

Cancel

Service Name

Type in a new service for your request.

Service Type

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

Port Configuration

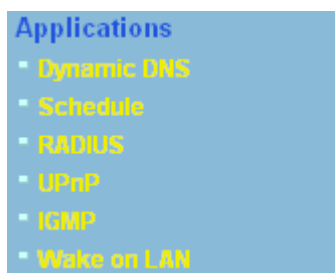
Click **Single** or **Range** as the **Type**. If you select Range, you have to type in the starting port number and the end porting number on the boxes below.

Port Number – Type in the starting port number and the end porting number here if you choose Range as the type.

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

4.8 Applications

Below shows the menu items for Applications.



4.8.1 Dynamic DNS

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

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

Enable the Function and Add a Dynamic DNS Account

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

[Applications >> Dynamic DNS Setup](#)

A screenshot of the 'Dynamic DNS Setup' configuration page. At the top, there is a title 'Dynamic DNS Setup' and a link 'Set to Factory Default'. Below the title, there is a checkbox labeled 'Enable Dynamic DNS Setup' which is checked. To the right of the checkbox are two buttons: 'View Log' and 'Force Update'. Below this is a section titled 'Accounts:' containing a table with three columns: 'Index', 'Domain Name', and 'Active'. The table has three rows, each with a blue underlined index (1, 2, 3), a domain name ending in a period, and an 'x' in the 'Active' column. At the bottom of the page are two buttons: 'OK' and 'Clear All'.

Set to Factory Default

Clear all profiles and recover to factory settings.

Enable Dynamic DNS Setup

Check this box to enable DDNS function.

Index

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

Domain Name

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

| | |
|---------------------|--|
| Active | Display if this account is active or inactive. |
| View Log | Display DDNS log status. |
| Force Update | Force the router updates its information to DDNS server. |

- 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*.

[Applications >> Dynamic DNS Setup >> Dynamic DNS Account Setup](#)

Index : 1

☒ Enable Dynamic DNS Account

Service Provider

Service Type

Domain Name

Login Name (max. 64 characters)

Password (max. 23 characters)

☐ Wildcards

☐ Backup MX

Mail Extender

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

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

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

Disable the Function and Clear all Dynamic DNS Accounts

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

Delete a Dynamic DNS Account

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

4.8.2 Schedule

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

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

[Applications >> Schedule](#)

| Schedule: | | Set to Factory Default | |
|--------------------|--------|--|--------|
| Index | Status | Index | Status |
| 1. | x | 9. | x |
| 2. | x | 10. | x |
| 3. | x | 11. | x |
| 4. | x | 12. | x |
| 5. | x | 13. | x |
| 6. | x | 14. | x |
| 7. | x | 15. | x |
| 8. | x | | |

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

Set to Factory Default

Clear all profiles and recover to factory settings.

Index

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

Status

Display if this schedule setting is active or inactive.

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

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

[Applications >> Schedule](#)

Index No. 1

☒ Enable Schedule Setup

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

Start Time (hh:mm) 0 : 0

Duration Time (hh:mm) 0 : 0

Action Force On

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

How Often

☐ Once

☒ Weekdays

☐ Sun ☒ Mon ☒ Tue ☒ Wed ☒ Thu ☒ Fri ☐ Sat

OK Clear Cancel

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

Example

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

Office

Hour:

(Force On)



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

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

4.8.3 RADIUS

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

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

Applications >> RADIUS

RADIUS Setup

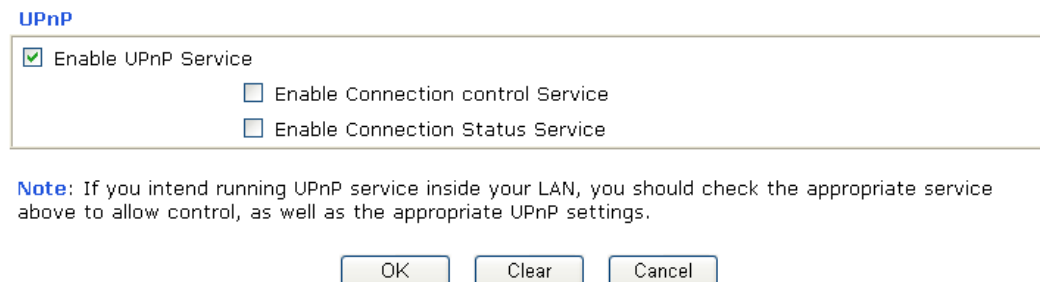
| | |
|--|-----------------------------------|
| <input checked="" type="checkbox"/> Enable | |
| Server IP Address | <input type="text"/> |
| Destination Port | <input type="text" value="1812"/> |
| Shared Secret | <input type="text"/> |
| Confirm Shared Secret | <input type="text"/> |

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

4.8.4 UPnP

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

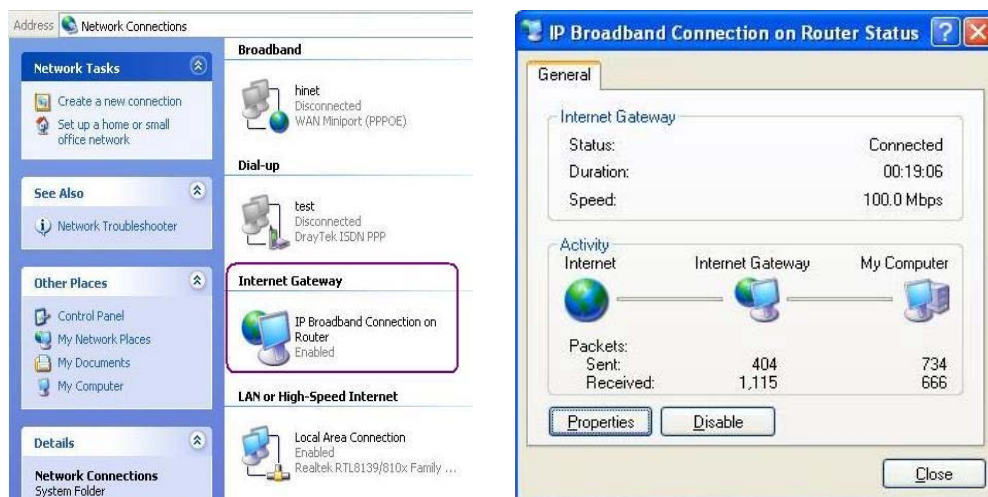
Applications >> UPnP



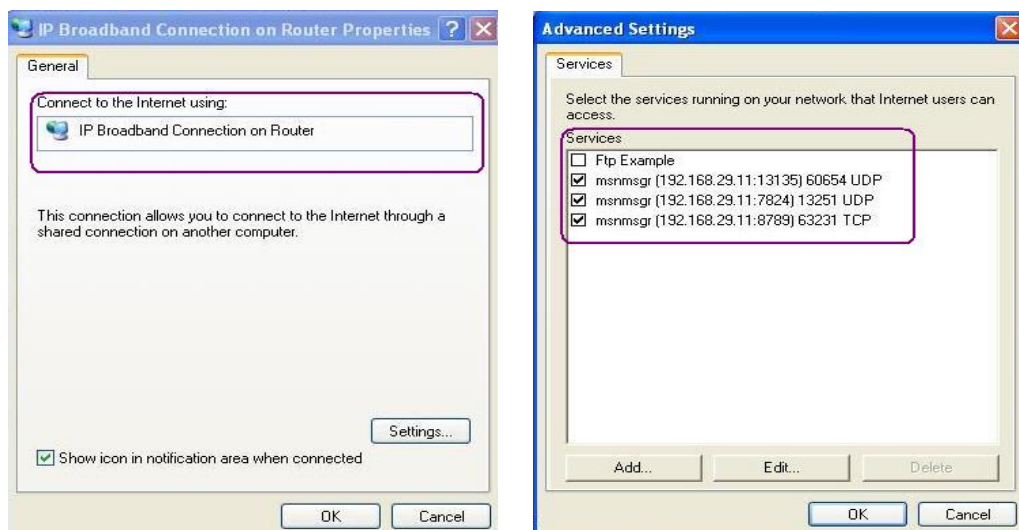
Enable UPNP Service

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

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



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



The reminder as regards concern about Firewall and UPnP

Can't work with Firewall Software

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

Security Considerations

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

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

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

4.8.5 IGMP

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

[Applications >> IGMP](#)

IGMP

☐ Enable IGMP Proxy

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

☐ Enable IGMP Snooping

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

OK

Cancel

[Refresh](#)

| Working Multicast Groups | | | | | |
|--------------------------|----------|----|----|----|----|
| Index | Group ID | P1 | P2 | P3 | P4 |

Enable IGMP Proxy

Check this box to enable this function. The application of multicast will be executed through WAN port. In addition, such function is available in NAT mode.

Enable IGMP Snooping

Check this box to enable this function. Multicast traffic will be forwarded to ports that have members of that group. Disabling IGMP snooping will make multicast traffic treated in the same manner as broadcast traffic.

Group ID

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

P1 to P4

It indicates the LAN port used for the multicast group.

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

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

4.8.6 Wake on LAN

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

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

Application >> Wake on LAN

Wake on LAN

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

Wake by:

IP Address:

MAC Address:

Result

| | | | | | |
|------------------------|------------|------------|--------|--|--|
| Valid subcommands are: | | | | | |
| admin | cfg | cmdlog | | | |
| ftpd | domainname | iface | name | | |
| passwd | reboot | autoreboot | commit | | |

Wake by

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

Wake by:

IP Address

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

MAC Address

Type any one of the MAC address of the bound PCs.

Wake Up

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

Application >> Wake on LAN

Wake on LAN

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

Wake by:

IP Address:

MAC Address:

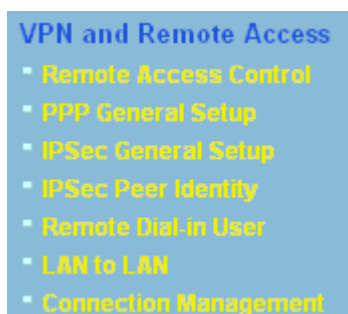
Result

Send command to client done.

4.9 VPN and Remote Access

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

Below shows the menu items for VPN and Remote Access.



4.9.1 Remote Access Control

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

[VPN and Remote Access >> Remote Access Control Setup](#)

Remote Access Control Setup

| | |
|-------------------------------------|--------------------------|
| <input checked="" type="checkbox"/> | Enable PPTP VPN Service |
| <input checked="" type="checkbox"/> | Enable IPSec VPN Service |
| <input checked="" type="checkbox"/> | Enable L2TP VPN Service |

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

OK Clear Cancel

4.9.2 PPP General Setup

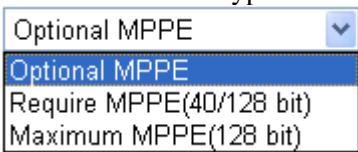
This submenu only applies to PPP-related VPN connections, such as PPTP, L2TP, L2TP over IPSec.

[VPN and Remote Access >> PPP General Setup](#)

PPP General Setup

| | | | |
|-------------------------------|---|--|---------------|
| PPP/MP Protocol | | IP Address Assignment for Dial-In Users (When DHCP Disable set) | |
| Dial-In PPP Authentication | PAP or CHAP | Start IP Address | 192.168.1.200 |
| Dial-In PPP Encryption (MPPE) | Optional MPPE | | |
| Mutual Authentication (PAP) | <input type="radio"/> Yes <input checked="" type="radio"/> No | | |
| Username | | | |
| Password | | | |

OK

| | |
|--|--|
| Dial-In PPP Authentication PAP Only PAP or CHAP | <p>Select this option to force the router to authenticate dial-in users with the PAP protocol.</p> <p>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.</p> |
| Dial-In PPP Encryption (MPPE Optional MPPE) | <p>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.</p>  <p>Require MPPE (40/128bits) - Selecting this option will force the router to encrypt packets by using the MPPE encryption algorithm. In addition, the remote dial-in user will use 40-bit to perform encryption prior to using 128-bit for encryption. In other words, if 128-bit MPPE encryption method is not available, then 40-bit encryption scheme will be applied to encrypt the data.</p> <p>Maximum MPPE - This option indicates that the router will use the MPPE encryption scheme with maximum bits (128-bit) to encrypt the data.</p> |
| Mutual Authentication (PAP) | <p>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.</p> |
| Start IP Address | <p>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.</p> |

4.9.3 IPSec General Setup

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

There are two phases of IPSec.

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

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

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

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

VPN and Remote Access >> IPSec General Setup

VPN IKE/IPSec General Setup

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

IKE Authentication Method
Pre-Shared Key
Confirm Pre-Shared Key

IPSec Security Method
☒ Medium (AH)
Data will be authentic, but will not be encrypted.

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

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

Pre-Shared Key -Currently only support Pre-Shared Key authentication.

Pre-Shared Key- Specify a key for IKE authentication

Confirm Pre-Shared Key- Retype the characters to confirm the pre-shared key.

IPSec Security Method

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

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

4.9.4 IPSec Peer Identity

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

X509 Peer ID Accounts:

[Set to Factory Default](#)

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

Set to Factory Default

Click it to clear all indexes.

Index

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

Name

Display the profile name of that index.

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

Profile Index : 1

| | |
|--|---|
| Profile Name | <input data-bbox="507 1346 689 1377" type="text" value="???"/> |
| <input checked="" type="checkbox"/> Enable this account | |
| <input checked="" type="radio"/> Accept Any Peer ID | |
| <input type="radio"/> Accept Subject Alternative Name | |
| Type | <input data-bbox="735 1541 887 1572" type="text" value="IP Address"/> |
| IP | <input data-bbox="735 1576 917 1608" type="text"/> |
| <input type="radio"/> Accept Subject Name | |
| Country (C) | <input data-bbox="735 1675 807 1706" type="text"/> |
| State (ST) | <input data-bbox="735 1713 1121 1744" type="text"/> |
| Location (L) | <input data-bbox="735 1751 1121 1783" type="text"/> |
| Organization (O) | <input data-bbox="735 1789 1121 1821" type="text"/> |
| Organization Unit (OU) | <input data-bbox="735 1827 1121 1859" type="text"/> |
| Common Name (CN) | <input data-bbox="735 1865 1121 1897" type="text"/> |
| Email (E) | <input data-bbox="735 1904 1121 1935" type="text"/> |

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

4.9.5 Remote Dial-in User

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

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

VPN and Remote Access >> Remote Dial-in User

Remote Access User Accounts:

[Set to Factory Default](#)

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

Set to Factory Default

Click to clear all indexes.

Index

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

User

Display the username for the specific dial-in user of the LAN-to-LAN profile. The symbol ??? represents that the profile is empty.

Status

Display the access state of the specific dial-in user. The symbol V and X represent the specific dial-in user to be active and inactive, respectively.

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

Index No. 1

| | | |
|---|--|--|
| User account and Authentication <input checked="" type="checkbox"/> Enable this account Idle Timeout <input type="text" value="300"/> second(s) | | Username <input type="text" value="???"/> Password <input type="password"/> |
| Allowed Dial-In Type <input checked="" type="checkbox"/> PPTP <input checked="" type="checkbox"/> IPSec Tunnel <input checked="" type="checkbox"/> L2TP with IPSec Policy <input type="text" value="None"/> | | IKE Authentication Method <input checked="" type="checkbox"/> Pre-Shared Key IKE Pre-Shared Key <input type="text"/> <input type="checkbox"/> Digital Signature(X.509) <input type="text" value="None"/> |
| | | IPSec Security Method <input checked="" type="checkbox"/> Medium(AH) High(ESP) <input checked="" type="checkbox"/> DES <input checked="" type="checkbox"/> 3DES <input checked="" type="checkbox"/> AES Local ID (optional) <input type="text"/> |

OK Clear Cancel

Enable this account

Check the box to enable this function.

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

PPTP

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

IPSec Tunnel

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

L2TP

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

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

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

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

User Name

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

Password

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

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

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

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

IPSec Security Method

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

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

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

4.9.6 LAN to LAN

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

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

VPN and Remote Access >> LAN to LAN

LAN-to-LAN Profiles: [Set to Factory Default](#)

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

Set to Factory Default

Click to clear all indexes.

Name

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

Status

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

inactive, respectively.

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

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

VPN and Remote Access >> LAN to LAN

Profile Index : 1

1. Common Settings

| | |
|---|---|
| Profile Name <input data-bbox="587 555 810 589" type="text" value="???"/> | Call Direction <input checked="" type="radio"/> Both <input type="radio"/> Dial-Out <input type="radio"/> Dial-In |
| <input type="checkbox"/> Enable this profile | <input type="checkbox"/> Always on |
| Netbios Naming Packet <input checked="" type="radio"/> Pass <input type="radio"/> Block | Idle Timeout <input data-bbox="1098 629 1169 663" type="text" value="300"/> second(s) |
| | <input type="checkbox"/> Enable PING to keep alive |
| | PING to the IP <input data-bbox="1098 701 1321 734" type="text"/> |

2. Dial-Out Settings

| | |
|--|--|
| Type of Server I am calling <input type="radio"/> PPTP <input type="radio"/> IPsec Tunnel <input type="radio"/> L2TP with IPsec Policy <input data-bbox="611 898 746 931" type="text" value="None"/> | Username <input data-bbox="1114 790 1337 824" type="text" value="???"/> Password <input data-bbox="1114 835 1337 869" type="text"/> PPP Authentication <input data-bbox="1114 880 1249 913" type="text" value="PAP/CHAP"/> VJ Compression <input checked="" type="radio"/> On <input type="radio"/> Off |
| Server IP/Host Name for VPN. (such as draytek.com or 123.45.67.89) <input data-bbox="331 1014 647 1048" type="text"/> | IKE Authentication Method <input checked="" type="radio"/> Pre-Shared Key IKE Pre-Shared Key <input data-bbox="1114 1037 1321 1070" type="text"/> <input type="radio"/> Digital Signature(X.509) <input data-bbox="850 1115 930 1149" type="text" value="None"/> |
| | IPsec Security Method <input checked="" type="radio"/> Medium(AH) <input type="radio"/> High(ESP) <input data-bbox="986 1238 1265 1272" type="text" value="DES without Authentication"/> <input data-bbox="850 1272 962 1305" type="button" value="Advanced"/> |
| | Index(1-15) in Schedule Setup: <input data-bbox="850 1361 914 1395" type="text"/> , <input data-bbox="938 1361 1002 1395" type="text"/> , <input data-bbox="1026 1361 1090 1395" type="text"/> , <input data-bbox="1114 1361 1177 1395" type="text"/> |

Profile Name

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

Enable this profile

Check here to activate this profile.

Netbios Naming Packet

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

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

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 be no where to know this situation. To resolve this dilemma, by continuously sending PING packets to the remote host, the Vigor router can know the true existence of this VPN connection and react accordingly. This is independent of DPD (dead peer detection).

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

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

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

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

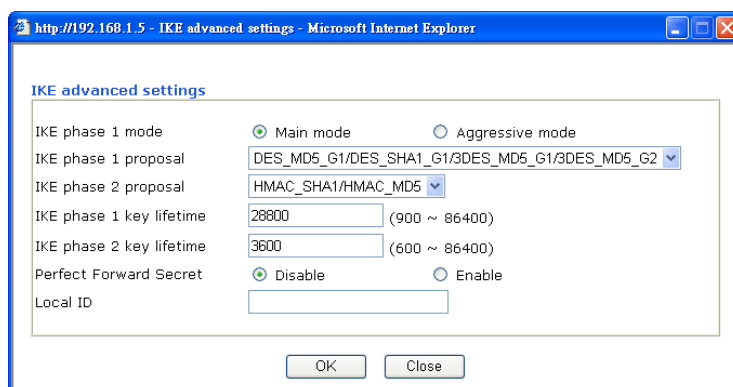
Password This field is applicable when you select PPTP or L2TP with or without IPSec policy above.

PPP Authentication This field is applicable when you select, PPTP or L2TP with or without IPSec policy above. PAP/CHAP is the most common selection due to wide compatibility.

VJ compression This field is applicable when you select PPTP or L2TP with or without IPSec policy above. VJ Compression is used for TCP/IP protocol header compression. Normally set to **Yes** to improve bandwidth utilization.

IKE Authentication This group of fields is applicable for IPSec Tunnels and L2TP

| | |
|------------------------------|--|
| Method | with IPSec Policy. Pre-Shared Key - Input 1-63 characters as pre-shared key. Digital Signature (X.509) - Select one predefined Profiles set in the VPN and Remote Access >>IPSec Peer Identity . |
| IPSec Security Method | This group of fields is a must for IPSec Tunnels and L2TP with IPSec Policy. |
| Medium | Authentication Header (AH) means data will be authenticated, but not be encrypted. By default, this option is active. High (ESP-Encapsulating Security Payload) - means payload (data) will be encrypted and authenticated. Select from below: DES without Authentication -Use DES encryption algorithm and not apply any authentication scheme. DES with Authentication -Use DES encryption algorithm and apply MD5 or SHA-1 authentication algorithm. 3DES without Authentication -Use triple DES encryption algorithm and not apply any authentication scheme. 3DES with Authentication -Use triple DES encryption algorithm and apply MD5 or SHA-1 authentication algorithm. AES without Authentication -Use AES encryption algorithm and not apply any authentication scheme. AES with Authentication -Use AES encryption algorithm and apply MD5 or SHA-1 authentication algorithm. |
| Advanced | Specify mode, proposal and key life of each IKE phase, Gateway, etc. The window of advance setup is shown as below: |



IKE phase 1 mode -Select from **Main** mode and **Aggressive** mode. The ultimate outcome is to exchange security proposals to create a protected secure channel. **Main** mode is more secure than **Aggressive** mode since more exchanges are done in a secure channel to set up the IPSec session. However, the **Aggressive** mode is faster. The default value in Vigor router is Main mode.

IKE phase 1 proposal-To propose the local available authentication schemes and encryption algorithms to the VPN peers, and get its feedback to find a match. Two combinations are available for Aggressive mode and nine for **Main** mode. We suggest you select the combination that covers the most schemes.

IKE phase 2 proposal-To propose the local available

algorithms to the VPN peers, and get its feedback to find a match. Three combinations are available for both modes. We suggest you select the combination that covers the most algorithms.

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

IKE phase 2 key lifetime-For security reason, the lifetime of key should be defined. The default value is 3600 seconds. You may specify a value in between 600 and 86400 seconds.

Perfect Forward Secret (PFS)-The IKE Phase 1 key will be reused to avoid the computation complexity in phase 2. The default value is inactive this function.

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

3. Dial-In Settings

| | | |
|--|--|---|
| Allowed Dial-In Type <input checked="" type="checkbox"/> PPTP <input checked="" type="checkbox"/> IPSec Tunnel <input checked="" type="checkbox"/> L2TP with IPSec Policy None | | Username ??? Password VJ Compression On Off |
| <input type="checkbox"/> Specify Remote VPN Gateway Peer VPN Server IP or Peer ID | | IKE Authentication Method <input checked="" type="checkbox"/> Pre-Shared Key IKE Pre-Shared Key <input type="checkbox"/> Digital Signature(X.509) None |
| IPSec Security Method <input checked="" type="checkbox"/> Medium(AH) High(ESP) <input checked="" type="checkbox"/> DES <input checked="" type="checkbox"/> 3DES <input checked="" type="checkbox"/> AES | | |

4. TCP/IP Network Settings

| | |
|---|---|
| My WAN IP 0.0.0.0 Remote Gateway IP 0.0.0.0 Remote Network IP 0.0.0.0 Remote Network Mask 255.255.255.0 More | RIP Direction Disable From first subnet to remote network, you have to do Route <input type="checkbox"/> Change default route to this VPN tunnel (Only single WAN supports this) |
|---|---|

OK Clear Cancel

Allowed Dial-In Type

Determine the dial-in connection with different types.

PPTP

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

IPSec Tunnel

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

L2TP

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

| | |
|-----------------------------------|--|
| | <p>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.</p> <p>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.</p> <p>Must - Specify the IPsec policy to be definitely applied on the L2TP connection.</p> |
| Specify Remote VPN Gateway | <p>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. Also, you should further specify the corresponding security methods on the right side.</p> <p>If you uncheck the checkbox, the connection type you select above will apply the authentication methods and security methods in the general settings.</p> |
| User Name | This field is applicable when you select PPTP or L2TP with or without IPsec policy above. |
| Password | This field is applicable when you select PPTP or L2TP with or without IPsec policy above. |
| VJ Compression | VJ Compression is used for TCP/IP protocol header compression. This field is applicable when you select PPTP or L2TP with or without IPsec policy above. |
| IKE Authentication Method | <p>This group of fields is applicable for IPsec Tunnels and L2TP with IPsec Policy when you specify the IP address of the remote node. The only exception is Digital Signature (X.509) can be set when you select IPsec tunnel either with or without specify the IP address of the remote node.</p> <p>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.</p> <p>Digital Signature (X.509) - Check the box of Digital Signature to invoke this function and select one predefined Profiles set in the VPN and Remote Access >>IPsec Peer Identity.</p> |
| IPsec Security Method | <p>This group of fields is a must for IPsec Tunnels and L2TP with IPsec Policy when you specify the remote node.</p> <p>Medium- Authentication Header (AH) means data will be authenticated, but not be encrypted. By default, this option is active.</p> <p>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.</p> |
| My WAN IP | This field is only applicable when you select PPTP or L2TP with or without IPsec policy above. The default value is 0.0.0.0, which means the Vigor router will get a PPP IP address from the remote router during the IPCP negotiation phase. If the PPP IP address is fixed by remote side, specify the fixed IP address here. Do not change the default value if you do not select PPTP or L2TP. |

| | |
|--|---|
| Remote Gateway IP | This field is only applicable when you select PPTP or L2TP with or without IPSec policy above. The default value is 0.0.0.0, which means the Vigor router will get a remote Gateway PPP IP address from the remote router during the IPCP negotiation phase. If the PPP IP address is fixed by remote side, specify the fixed IP address here. Do not change the default value if you do not select PPTP or L2TP. |
| Remote Network IP/ Remote Network Mask | Add a static route to direct all traffic destined to this Remote Network IP Address/Remote Network Mask through the VPN connection. For IPSec, this is the destination clients IDs of phase 2 quick mode. |
| More | Add a static route to direct all traffic destined to more Remote Network IP Addresses/ Remote Network Mask through the VPN connection. This is usually used when you find there are several subnets behind the remote VPN router. |
| RIP Direction | The option specifies the direction of RIP (Routing Information Protocol) packets. You can enable/disable one of direction here. Herein, we provide four options: TX/RX Both, TX Only, RX Only, and Disable. |
| From first subnet to remote network, you have to do | If the remote network only allows you to dial in with single IP, please choose NAT , otherwise choose Route . |
| Change default route to this VPN tunnel | Check this box to change the default route with this VPN tunnel. |

4.9.7 Connection Management

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

[VPN and Remote Access >> Connection Management](#)

Dial-out Tool

Refresh Seconds : 10 Refresh

Dial

VPN Connection Status

Current Page: 1Page No. Go >>

| VPN | Type | Remote IP | Virtual Network | Tx Pkts | Tx Rate (Bps) | Rx Pkts | Rx Rate (Bps) | UpTime |
|----------------------------------|------|-----------|-----------------|---------|---------------|---------|---------------|--------|
| xxxxxxxx : Data is encrypted. | | | | | | | | |
| xxxxxxxx : Data isn't encrypted. | | | | | | | | |

- Dial

Click this button to execute dial out function.
- Refresh Seconds

Choose the time for refresh the dial information among 5, 10, and 30.
- Refresh

Click this button to refresh the whole connection status.

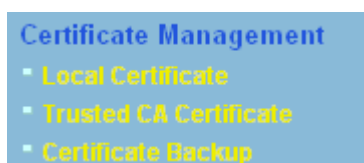
4.10 Certificate Management

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

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

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

Below shows the menu items for Certificate Management.



4.10.1 Local Certificate

[Certificate Management >> Local Certificate](#)

X509 Local Certificate Configuration

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

[GENERATE](#) [IMPORT](#) [REFRESH](#)

X509 Local Certificate

Generate

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

Generate Certificate Request

| | |
|---------------------------------|----------------------|
| Subject Alternative Name | |
| Type | IP Address |
| IP | <input type="text"/> |
| Subject Name | |
| Country (C) | <input type="text"/> |
| State (ST) | <input type="text"/> |
| Location (L) | <input type="text"/> |
| Organization (O) | <input type="text"/> |
| Organization Unit (OU) | <input type="text"/> |
| Common Name (CN) | <input type="text"/> |
| Email (E) | <input type="text"/> |
| Key Type | RSA |
| Key Size | 1024 Bit |

Generate

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

Import

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

Refresh

Click this button to refresh the information listed below.

View

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

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

Certificate Management >> Local Certificate

X509 Local Certificate Configuration

| Name | Subject | Status | Modify |
|-------|---------------------------------|------------|---|
| Local | /C=TW/ST=HC/L=HC/O=Draytek/O... | Requesting | <input type="button" value="View"/> <input type="button" value="Delete"/> |

X509 Local Certificate

```

-----BEGIN CERTIFICATE REQUEST-----
MIIBqjCCARMCAQAwajELMAkGA1UEBhMCVFcxZzAJBgNVBAGTAkhDMQswCQYDVQQH
EwJlQzEQMA4GA1UEChMHRHJheXRlay5jb20wgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJ
CQEW3N1cHBvcnRAZHJheXRlay5jb20wgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJ
AoGBALMjdTsqfF97FEpYy+IqeJVJGuSrtqG6EtW8yTU5HQvXpAzcrgJBGr1kTUBX
a1X//fgnEccQA2LPsQIQ85Qychwq07BmOEDf10wHwCa1A2QoGvIiODMC7f5w9xA8
m6+0f4xZ4QqnjXXgcIC0Bj1iAa6MLScelsynZhkgmQ1QN5uFgMBAAGGADANBgkq
hkiG9w0BAQUFAA0BgQCq3sdwVc21t9qn4U6X2BJsVzu7JHafSSeUnaYDZefCmGfX
9yojHpstNsmWsmRuAwGeKCWc8S/gLtHhr6iccMoToQFv/LWdaEPU5LqryBKKgC9t
eorpDa1/rC9ZwCraOt8XUmPqNoiytq8BxStTE8vULiIxmwaBvc1hWFSXKVLU7g==
-----END CERTIFICATE REQUEST-----

```

4.10.2 Trusted CA Certificate

Trusted CA certificate lists three sets of trusted CA certificate.

[Certificate Management >> Trusted CA Certificate](#)

X509 Trusted CA Certificate Configuration

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

[IMPORT](#)

[REFRESH](#)

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

[Certificate Management >> Trusted CA Certificate](#)

Import X509 Trusted CA Certificate

Select a trusted CA certificate file.

[Browse...](#)

Click [Import](#) to upload the certification.

[Import](#)

[Cancel](#)

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



4.10.3 Certificate Backup

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

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

[Certificate Management >> Certificate Backup](#)

Certificate Backup / Restoration

Backup

Encrypt password:

Confirm password:

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

Restoration

Select a backup file to restore.

Decrypt password:

Click to upload the file.

4.11 Wireless LAN

This function is used for “n” models only.

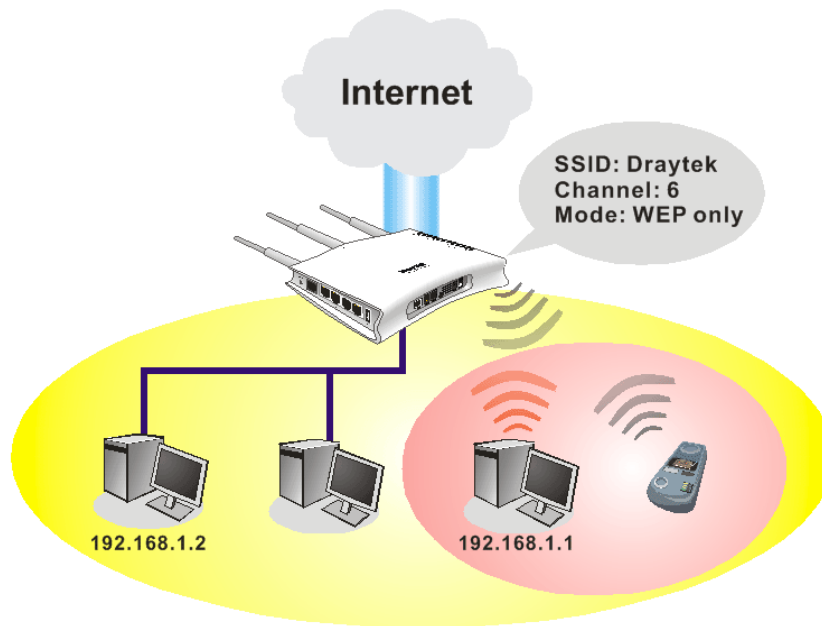
4.11.1 Basic Concepts

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

The Vigor wireless routers are equipped with a wireless LAN interface compliant with the standard IEEE 802.11n draft 2 protocol. To boost its performance further, the Vigor Router is also loaded with advanced wireless technology to lift up data rate up to 300 Mbps*. Hence, you can finally smoothly enjoy stream music and video.

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

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



Multiple SSIDs

Vigor router supports four SSID settings for wireless connections. Each SSID can be defined with different name and download/upload rate for selecting by stations connected to the router wirelessly.

Security Overview

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

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

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

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

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

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

Separate the Wireless and the Wired LAN- WLAN Isolation enables you to isolate your wireless LAN from wired LAN for either quarantine or limit access reasons. To isolate means neither of the parties can access each other. To elaborate an example for business use, you may set up a wireless LAN for visitors only so they can connect to Internet without

hassle of the confidential information leakage. For a more flexible deployment, you may add filters of MAC addresses to isolate users' access from wired LAN.

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

Below shows the menu items for Wireless LAN.



4.11.2 General Setup

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

General Setting (IEEE 802.11)

☒ Enable Wireless LAN

Mode :

Mixed(11b+11g+11n)

Index(1-15) in [Schedule](#) Setup: , , ,

Only schedule profiles that have the action "Force Down" are applied to the WLAN, all other actions are ignored.

| | Enable | Hide SSID | SSID | Isolate | LAN | Member |
|---|--------------------------|--------------------------|---------|--------------------------|--------------------------|--------------------------|
| 1 | <input type="checkbox"/> | <input type="checkbox"/> | DrayTek | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 2 | <input type="checkbox"/> | <input type="checkbox"/> | | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 3 | <input type="checkbox"/> | <input type="checkbox"/> | | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 4 | <input type="checkbox"/> | <input type="checkbox"/> | | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |

Hide SSID: Prevent SSID from being scanned.
Isolate Member: Wireless clients (stations) with the same SSID cannot access for each other.
Isolate LAN: Wireless clients (stations) with the same SSID cannot access wired PCs on LAN.

Channel:

Channel 6, 2437MHz

 Long Preamble: ☐
Long Preamble: necessary for some old 802.11 b devices only(lower performance)

Packet-OVERDRIVE™
☐ Tx Burst
Note:
The same technology must also be supported in clients to boost WLAN performance.

Rate Control

| | Enable | Upload | Download |
|--------|--------------------------|-----------------------|-----------------------|
| SSID 1 | <input type="checkbox"/> | <div>30000</div> kbps | <div>30000</div> kbps |
| SSID 2 | <input type="checkbox"/> | <div>30000</div> kbps | <div>30000</div> kbps |
| SSID 3 | <input type="checkbox"/> | <div>30000</div> kbps | <div>30000</div> kbps |
| SSID 4 | <input type="checkbox"/> | <div>30000</div> kbps | <div>30000</div> kbps |

Note: range 100~50,000 kbps

OK

Cancel

Enable Wireless LAN

Mode

Check the box to enable wireless function.

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

Mixed(11b+11g+11n)

11b Only

11g Only

11n Only

Mixed(11b+11g)

Mixed(11g+11n)

Mixed(11b+11g+11n)

Note: You should also set **RADIUS Server** simultaneously if 11g Only, 11b Only or 11n Only mode is selected.

Index(1-15)

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

Hide SSID

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

SSID

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

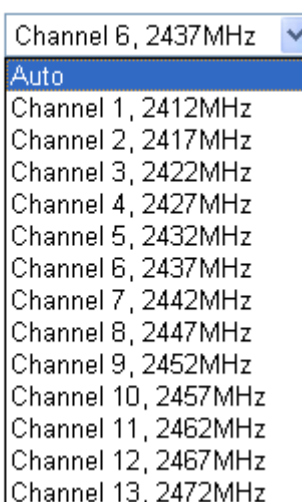
Isolate

LAN – Check this box to make the wireless clients (stations) with the same SSID cannot access wired PCs on LAN.

Member – Check this box to make the wireless clients (stations) with the same SSID not accessing for each other.

Channel

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

Channel: 

| |
|---------------------|
| Channel 6, 2437MHz |
| Auto |
| Channel 1, 2412MHz |
| Channel 2, 2417MHz |
| Channel 3, 2422MHz |
| Channel 4, 2427MHz |
| Channel 5, 2432MHz |
| Channel 6, 2437MHz |
| Channel 7, 2442MHz |
| Channel 8, 2447MHz |
| Channel 9, 2452MHz |
| Channel 10, 2457MHz |
| Channel 11, 2462MHz |
| Channel 12, 2467MHz |
| Channel 13, 2472MHz |

Long Preamble

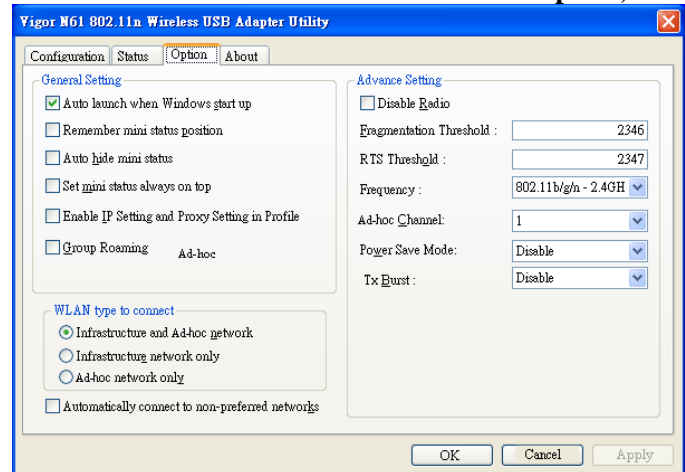
This option is to define the length of the sync field in an 802.11 packet. Most modern wireless network uses short preamble with 56 bit sync field instead of long preamble with 128 bit sync field. However, some original 11b wireless network devices only support long preamble.

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

Packet-OVERDRIVE

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

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



Rate Control

It controls the data transmission rate through wireless connection.

Upload – Check Enable and type the transmitting rate for data upload. Default value is 30,000 kbps.

Download – Type the transmitting rate for data download. Default value is 30,000 kbps.

4.11.3 Security

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

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

| SSID 1 | SSID 2 | SSID 3 | SSID 4 |
|--|--------|--------|--------|
| Mode: Disable | | | |
| WPA: Encryption Mode: TKIP Pre-Shared Key(PSK): ***** Type 8~63 ASCII character or 64 Hexadecimal digits leading by "0x", for example "cfigs01a2..." or "0x655abcd....". | | | |
| WEP: Encryption Mode: 64-Bit <input checked="" type="radio"/> Key 1 : ***** <input type="radio"/> Key 2 : ***** <input type="radio"/> Key 3 : ***** <input type="radio"/> Key 4 : ***** | | | |
| For 64 bit WEP key Type 5 ASCII character or 10 Hexadecimal digits leading by "0x", for example "A8312" or "0x4142333132". For 128 bit WEP key Type 13 ASCII character or 26 Hexadecimal digits leading by "0x", for example "0123456789abc" or "0x30313233343536373839414243". | | | |
| <div>OK Cancel</div> | | | |

Mode

There are several modes provided for you to choose.

Mode:

Disable

Disable
 WEP
 WPA/PSK
 WPA2/PSK
 Mixed(WPA+WPA2)/PSK

Disable - Turn off the encryption mechanism.

WEP-Accepts only WEP clients and the encryption key should be entered in WEP Key.

WPA/PSK-Accepts only WPA clients and the encryption key should be entered in PSK.

WPA2/PSK-Accepts only WPA2 clients and the encryption key should be entered in PSK.

Mixed (WPA+ WPA2)/PSK - Accepts WPA and WPA2 clients simultaneously and the encryption key should be entered in PSK.

WPA

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

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

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

WEP

64-Bit - For 64 bits WEP key, either **5** ASCII characters, such as 12345 (or 10 hexadecimal digitals leading by 0x, such as 0x4142434445.)

128-Bit - For 128 bits WEP key, either **13** ASCII characters, such as ABCDEFGHIJKLM (or 26 hexadecimal digits leading by 0x, such as 0x4142434445464748494A4B4C4D).

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.

4.11.4 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.

Wireless LAN >> Access Control

Access Control

Enable Mac Address Filter

☐ SSID 1
 ☐ SSID 2
 ☐ SSID 3
 ☐ SSID 4

MAC Address Filter

| Index | Attribute | MAC Address |
|-------|-----------|-------------|
| | | |

Client's MAC Address : : : : : :

Attribute :

☐ s: Isolate the station from LAN

Add

Delete

Edit

Cancel

OK

Clear All

Enable Max Access Filter

Select to enable the MAC Address filter for wireless LAN identified with SSID 1 to 4 respectively. All the clients (expressed by MAC addresses) listed in the box can be grouped under different wireless LAN. For example, they can be grouped under SSID 1 and SSID 2 at the same time if you check SSID 1 and SSID 2.

MAC Address Filter

Display all MAC addresses that are edited before.

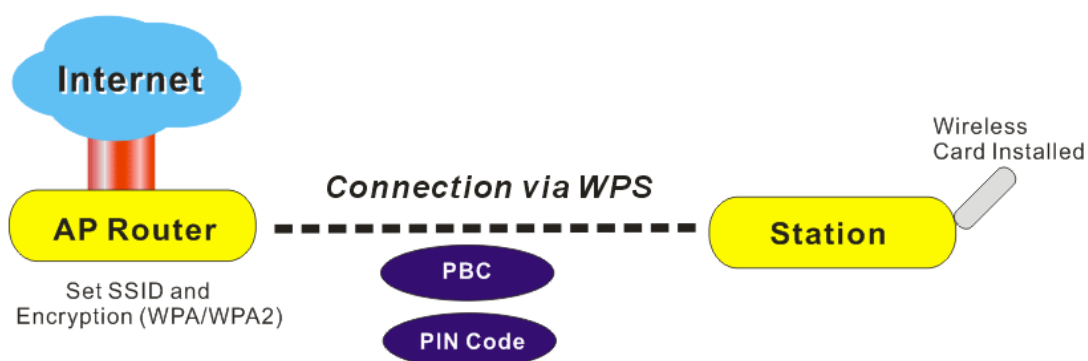
Client's MAC Address

Manually enter the MAC address of wireless client.

| | |
|------------------|--|
| Attribute | s: Isolate the station from LAN - select to isolate the wireless connection of the wireless client of the MAC address from LAN. |
| Add | Add a new MAC address into the list. |
| Delete | Delete the selected MAC address in the list. |
| Edit | Edit the selected MAC address in the list. |
| Cancel | Give up the access control set up. |
| OK | Click it to save the access control list. |
| Clear All | Clean all entries in the MAC address list. |

4.11.5 WPS

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

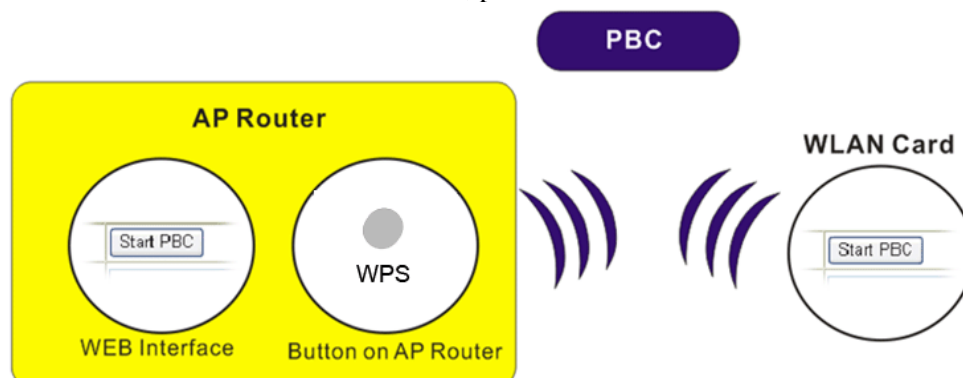


Note: Such function is available for the wireless station with WPS supported.

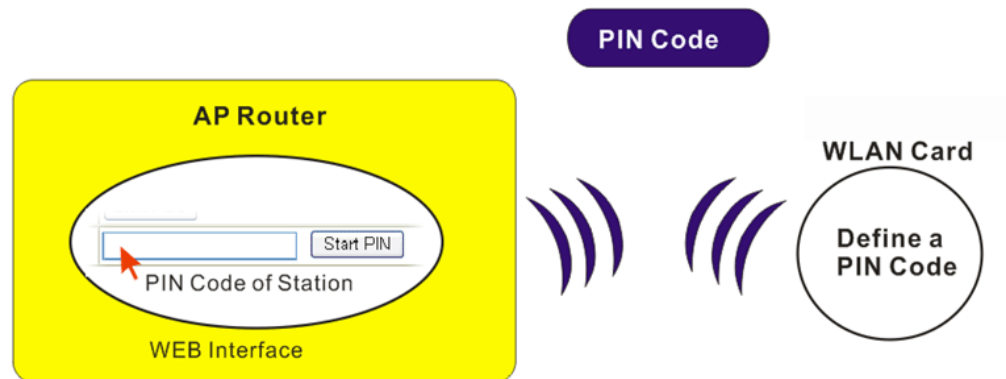
It is the simplest way to build connection between wireless network clients and vigor router. Users do not need to select any encryption mode and type any long encryption passphrase to setup a wireless client every time. He/she only needs to press a button on wireless client, and WPS will connect for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

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

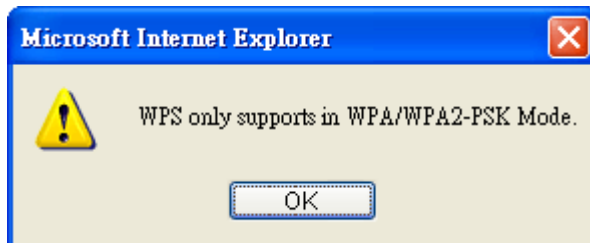
- On the side of Vigor 2110 series which served as an AP, press **WPS** button once on the front panel of the router or click **Start PBC** on web configuration interface. On the side of a station with network card installed, press **Start PBC** button of network card.



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



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



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

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

Wireless LAN >> WPS (Wi-Fi Protected Setup)

☒ Enable WPS 

Wi-Fi Protected Setup Information


| | |
|---------------------|------------|
| WPS Status | Configured |
| SSID | DrayTek |
| Authentication Mode | Disable |


Device Configure

| | |
|------------------------------|---|
| Configure via Push Button | <input type="button" value="Start PBC"/> |
| Configure via Client PinCode | <input type="text"/> <input type="button" value="Start PIN"/> |

Status: The Authentication Mode is NOT WPA/WPA2 PSK!!

Note: WPS can help your wireless client automatically connect to the Access point.

 : WPS is Disabled.

 : WPS is Enabled.

 : Waiting for WPS requests from wireless clients.

Enable WPS

Check this box to enable WPS setting.

WPS Status

Display related system information for WPS. If the wireless security (encryption) function of the router is properly configured, you can see 'Configured' message here.

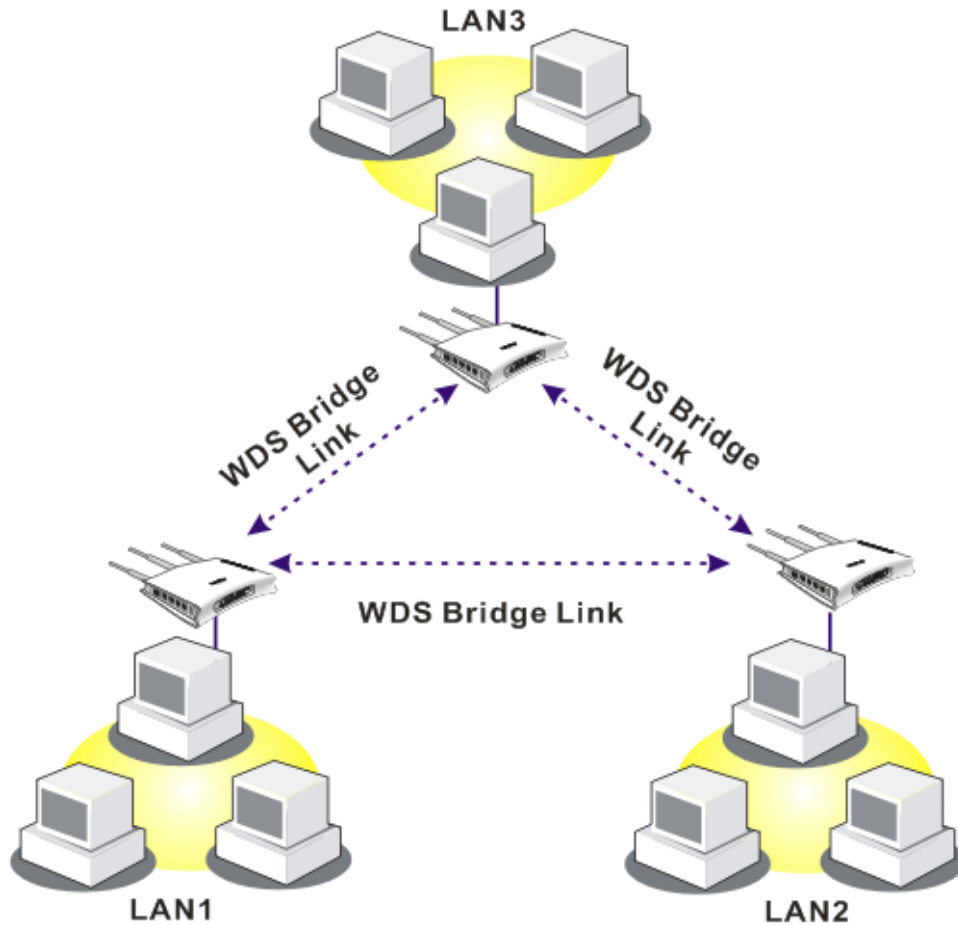
| | |
|-------------------------------------|---|
| SSID | Display the SSID1 of the router. WPS is supported by SSID1 only. |
| Authentication Mode | Display current authentication mode of the router. Only WPA2/PSK and WPA/PSK support WPS. |
| Configure via Push Button | Click Start PBC to invoke Push-Button style WPS setup procedure. The router will wait for WPS requests from wireless clients about two minutes. The WLAN LED on the router will blink fast when WPS is in progress. It will return to normal condition after two minutes. (You need to setup WPS within two minutes) |
| Configure via Client PinCode | Please input the PIN code specified in wireless client you wish to connect, and click Start PIN button. The WLAN LED on the router will blink fast when WPS is in progress. It will return to normal condition after two minutes. (You need to setup WPS within two minutes) |

4.11.6 WDS

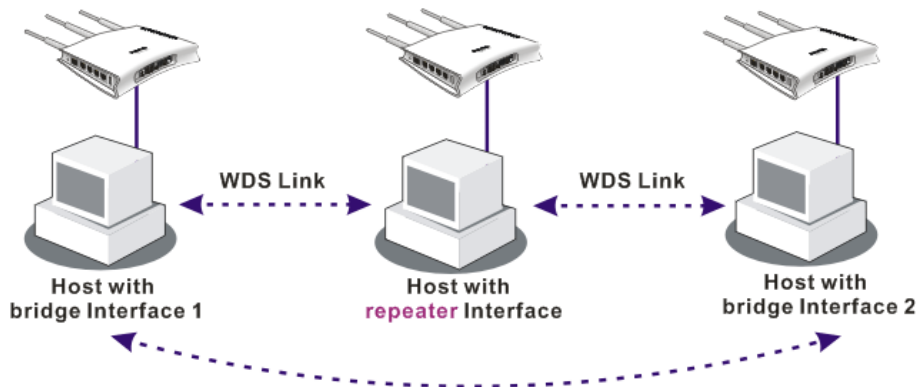
WDS means Wireless Distribution System. It is a protocol for connecting two access points (AP) wirelessly. Usually, it can be used for the following application:

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

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

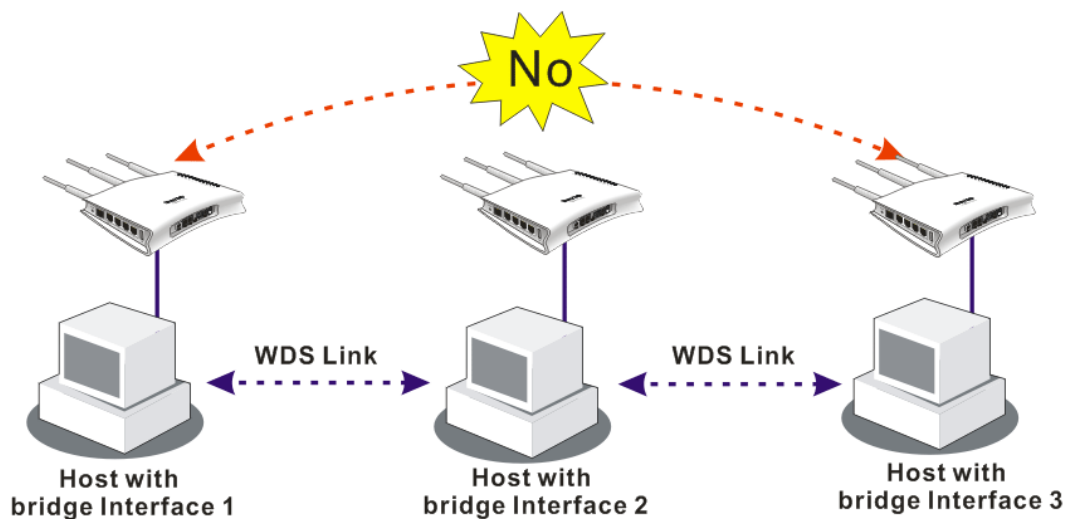


The application for the WDS-Repeater mode is depicted as below:



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

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



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

Wireless LAN >> WDS Settings

WDS Settings
[Set to Factory Default](#)

Mode: Bridge

Security:

☒ Disable ☐ WEP ☐ Pre-shared Key

WEP:

Use the same WEP key set in [Security Settings](#).

Pre-shared Key:

Type : TKIP

Key : *****

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

Bridge

Enable ☐ Peer MAC Address

| | | | | | | |
|--------------------------|----------------------|----------------------|----------------------|----------------------|----------------------|----------------------|
| <input type="checkbox"/> | <input type="text"/> | <input type="text"/> | <input type="text"/> | <input type="text"/> | <input type="text"/> | <input type="text"/> |
| <input type="checkbox"/> | <input type="text"/> | <input type="text"/> | <input type="text"/> | <input type="text"/> | <input type="text"/> | <input type="text"/> |
| <input type="checkbox"/> | <input type="text"/> | <input type="text"/> | <input type="text"/> | <input type="text"/> | <input type="text"/> | <input type="text"/> |
| <input type="checkbox"/> | <input type="text"/> | <input type="text"/> | <input type="text"/> | <input type="text"/> | <input type="text"/> | <input type="text"/> |

Note: Disable unused links to get better performance.

Repeater

Enable ☐ Peer MAC Address

| | | | | | | |
|--------------------------|----------------------|----------------------|----------------------|----------------------|----------------------|----------------------|
| <input type="checkbox"/> | <input type="text"/> | <input type="text"/> | <input type="text"/> | <input type="text"/> | <input type="text"/> | <input type="text"/> |
| <input type="checkbox"/> | <input type="text"/> | <input type="text"/> | <input type="text"/> | <input type="text"/> | <input type="text"/> | <input type="text"/> |
| <input type="checkbox"/> | <input type="text"/> | <input type="text"/> | <input type="text"/> | <input type="text"/> | <input type="text"/> | <input type="text"/> |
| <input type="checkbox"/> | <input type="text"/> | <input type="text"/> | <input type="text"/> | <input type="text"/> | <input type="text"/> | <input type="text"/> |

Access Point Function:

☒ Enable ☐ Disable

Status:

☐ Send "Hello" message to peers.

Link Status

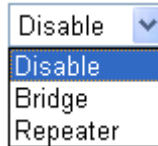
Note: The status is valid only when the peer also supports this function.

OK
Cancel

Mode

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

one.



| | |
|------------------------------|---|
| Security | There are three types for security, Disable , WEP and Pre-shared key . The setting you choose here will make the following WEP or Pre-shared key field valid or not. Choose one of the types for the router. |
| WEP | Check this box to use the same key set in Security Settings page. If you did not set any key in Security Settings page, this check box will be dimmed. |
| Pre-shared Key | Type 8 ~ 63 ASCII characters or 64 hexadecimal digits leading by "0x". |
| Bridge | If you choose Bridge as the connecting mode, please type in the peer MAC address in these fields. Four peer MAC addresses are allowed to be entered in this page at one time. Yet please disable the unused link to get better performance. If you want to invoke the peer MAC address, remember to check Enable box in the front of the MAC address after typing. |
| Repeater | If you choose Repeater as the connecting mode, please type in the peer MAC address in these fields. Four peer MAC addresses are allowed to be entered in this page at one time. Similarly, if you want to invoke the peer MAC address, remember to check Enable box in the front of the MAC address after typing. |
| Access Point Function | Click Enable to make this router serving as an access point; click Disable to cancel this function. |
| Status | It allows user to send "hello" message to peers. Yet, it is valid only when the peer also supports this function. |

4.11.7 AP Discovery

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

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

Access Point List

| BSSID | Channel | SSID |
|-------|---------|------|
| | | |

See [Statistics](#).

Note: During the scanning process (~5 seconds), no station is allowed to connect with the router.

Add to [WDS Settings](#) :

AP's MAC address : : : : :

☒ Bridge ☐ Repeater

Scan

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

Statistics

It displays the statistics for the channels used by APs.

[Wireless LAN >> Site Survey Statistics](#)

Recommended channels for usage:
1 2 3 4 5 6 7 8 9 10 11 12 13

| AP number v.s. Channel | | | | | | | | | | | | | |
|------------------------|---|---|---|---|---|---|---|---|----|----|----|----|----|
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 |

Channel

Add to

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

4.11.8 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 | Associated with |
|-------------|-------------|-----------------|
| <div></div> | | |

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 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 : : : : :

Add

Refresh

Click this button to refresh the status of station list.

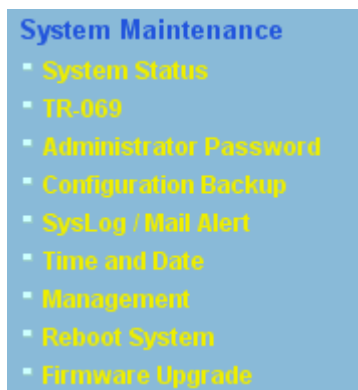
Add

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

4.12 System Maintenance

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

Below shows the menu items for System Maintenance.



4.12.1 System Status

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

System Status

Model Name : Vigor2110 series
Firmware Version : 3.2.2_RC2
Build Date/Time : Aug 26 2008 15:46:21

| LAN | | WAN | |
|-----------------|---------------------|-----------------|-----------------------|
| MAC Address | : 00-50-7F-92-F5-60 | Link Status | : Disconnected |
| 1st IP Address | : 192.168.1.5 | MAC Address | : 00-50-7F-92-F5-61 |
| 1st Subnet Mask | : 255.255.255.0 | Connection | : Static IP |
| DHCP Server | : Yes | IP Address | : 172.16.3.229 |
| DNS | : 194.109.6.66 | Default Gateway | : 172.16.3.4 |

| Wireless LAN | |
|------------------|---------------------|
| MAC Address | : 00-50-7f-92-f5-60 |
| Frequency Domain | : Europe |
| Firmware Version | : 1.8.1.0 |
| SSID | : DrayTek |

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

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

4.12.2 TR-069

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

System Maintenance >> TR-069 Setting

ACS and CPE Settings

ACS Server On
Internet
Internet

ACS Server

URL

Username

Password

CPE Client

☐ Enable
☒ Disable

URL

Port
8069

Username
vigor

Password

Periodic Inform Settings

☐ Disable
☒ Enable

Interval Time
900
second(s)

OK

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

| | |
|---------------------------------|--|
| ACS Server | URL/Username/Password – Such data must be typed according to the ACS (Auto Configuration Server) you want to link. Please refer to Auto Configuration Server user’s manual for detailed information. |
| CPE Client | It is not necessary for you to type them. Such information is useful for Auto Configuration Server. Enable/Disable – Sometimes, port conflict might be occurred. To solve such problem, you might want to change port number for CPE. Please click Enable and change the port number. |
| Periodic Inform Settings | The default setting is Enable . Please set interval time or schedule time for the router to send notification to CPE. Or click Disable to close the mechanism of notification. |

4.12.3 Administrator Password

This page allows you to set new password.

[System Maintenance >> Administrator Password Setup](#)

Administrator Password

| | |
|------------------|--------------------------|
| Old Password | <input type="password"/> |
| New Password | <input type="password"/> |
| Confirm Password | <input type="password"/> |

| | |
|-------------------------|---|
| Old Password | Type in the old password. The factory default setting for password is “ admin ”. |
| New Password | Type in new password in this field. |
| Confirm Password | Type in the new password again. |

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

4.12.4 Configuration Backup

Backup the Configuration

Follow the steps below to backup your configuration.

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

System Maintenance >> Configuration Backup

Configuration Backup / Restoration

Restoration

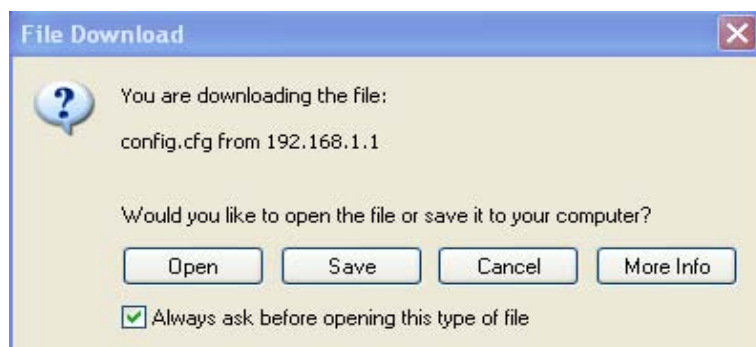
Select a configuration file.

Click Restore to upload the file.

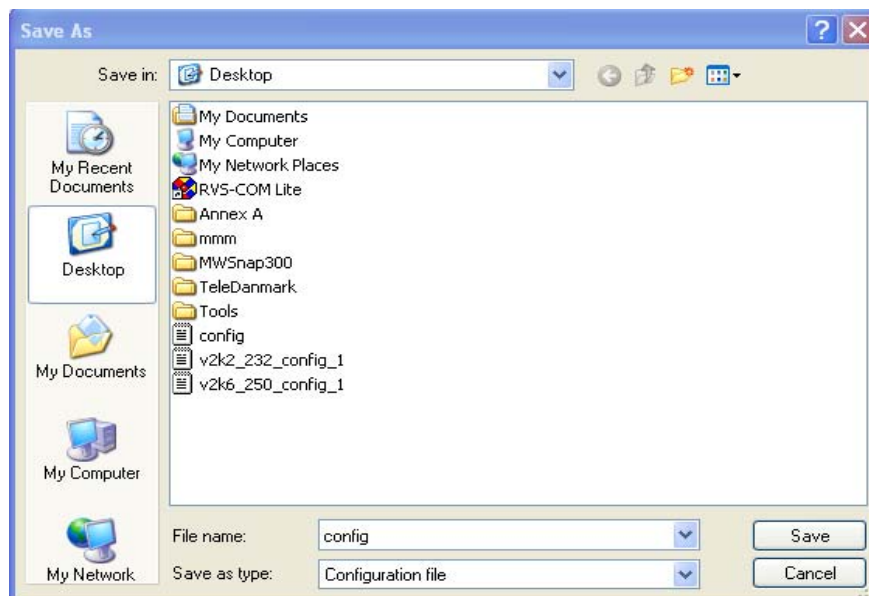
Backup

Click Backup to download current running configurations as a file.

- Click **Backup** button to get into the following dialog. 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.



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

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

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

Restore Configuration

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

System Maintenance >> Configuration Backup

Configuration Backup / Restoration

Restoration

Select a configuration file.

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.

4.12.5 Syslog/Mail Alert

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

System Maintenance >> SysLog / Mail Alert Setup

SysLog / Mail Alert Setup

SysLog Access Setup

☒ Enable

Server IP Address

Destination Port

Enable syslog message:

☒ Firewall Log

☒ VPN Log

☒ User Access Log

☒ Call Log

☒ WAN Log

☒ Router/DSL information

Mail Alert Setup

☐ Enable

SMTP Server

Mail To

Return-Path

☐ Authentication

User Name

Password

Enable E-Mail Alert:

☒ DoS Attack

☒ IM-P2P

Enable (Syslog Access...)

Check “**Enable**” to activate function of syslog.

Syslog Server IP

The IP address of the Syslog server.

Destination Port

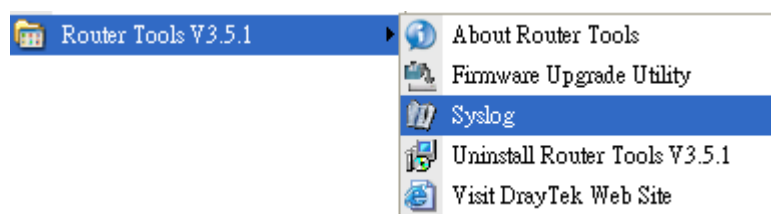
Assign a port for the Syslog protocol.

| | |
|--------------------------------|---|
| Enable syslog message | Check the box listed on this web page to send the corresponding message of firewall, VPN, User Access, Call, WAN, Router/DSL information to Syslog. |
| Enable (Alert Setup...) | Check “ Enable ” to activate function of mail alert. |
| Send a test e-mail | Make a simple test for the e-mail address specified in this page. Please assign the mail address first and click this button to execute a test for verify the mail address is available or not. |
| SMTP Server | The IP address of the SMTP server. |
| Mail To | Assign a mail address for sending mails out. |
| Return-Path | Assign a path for receiving the mail from outside. |
| Authentication | Check this box to activate this function while using e-mail application. |
| User Name | Type the user name for authentication. |
| Password | Type the password for authentication. |
| Enable E-mail Alert | Check the box to send alert message to the e-mail box while the router detecting the item(s) you specify here. |

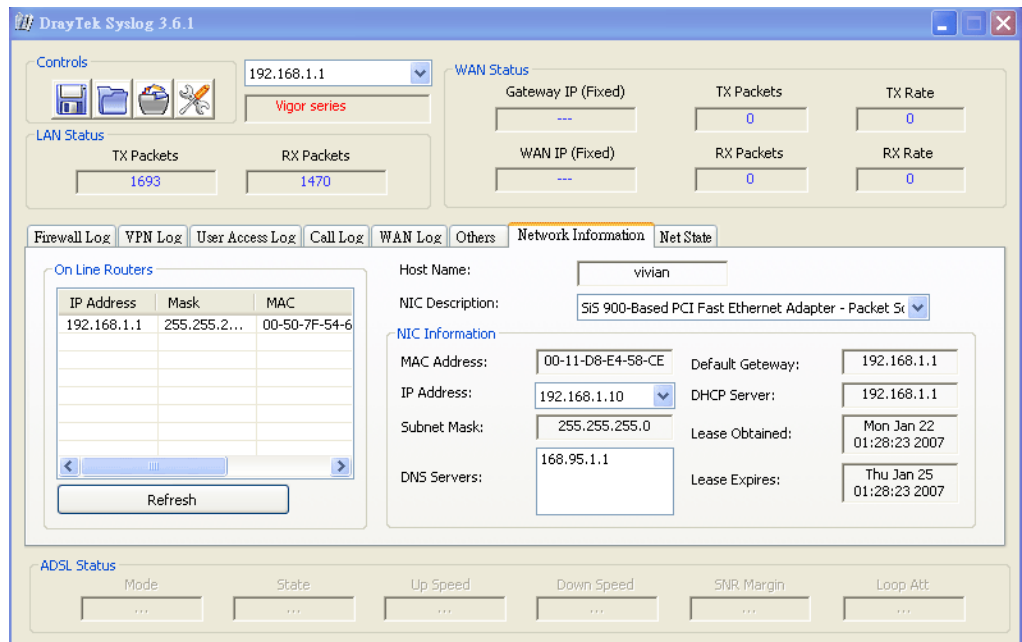
Click **OK** to save these settings.

For viewing the Syslog, please do the following:

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



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



4.12.6 Time and Date

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

System Maintenance >> Time and Date

Time Information

| | | |
|---------------------|----------------------------|--------------|
| Current System Time | 2000 Jan 2 Sun 3 : 31 : 21 | Inquire Time |
|---------------------|----------------------------|--------------|

Time Setup

| | |
|---|------------------------------------|
| <input type="radio"/> Use Browser Time <input checked="" type="radio"/> Use Internet Time Client | |
| Server IP Address | pool.ntp.org |
| Time Zone | (GMT) Greenwich Mean Time : Dublin |
| Enable Daylight Saving | <input type="checkbox"/> |
| Automatically Update Interval | 30 min |

| | |
|----|--------|
| OK | Cancel |
|----|--------|

Current System Time

Click **Inquire Time** to get the current time.

Use Browser Time

Select this option to use the browser time from the remote administrator PC host as router's system time.

Use Internet Time

Select to inquire time information from Time Server on the Internet using assigned protocol.

Time Protocol

Select a time protocol.

Server IP Address

Type the IP address of the time server.

Time Zone

Select the time zone where the router is located.

Automatically Update Interval

Select a time interval for updating from the NTP server.

Click **OK** to save these settings.

4.12.7 Management

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

[System Maintenance >> Management](#)

Management Setup

Management Access Control
☒ Allow management from the Internet
☐ FTP Server
☒ HTTP Server
☒ HTTPS Server
☒ Telnet Server
☐ SSH Server
☒ Disable PING from the Internet

Access List

| List | IP | Subnet Mask |
|------|----------------------|----------------------|
| 1 | <input type="text"/> | <input type="text"/> |
| 2 | <input type="text"/> | <input type="text"/> |
| 3 | <input type="text"/> | <input type="text"/> |

Management Port Setup
☒ User Define Ports ☐ Default Ports
Telnet Port (Default: 23)
HTTP Port (Default: 80)
HTTPS Port (Default: 443)
FTP Port (Default: 21)
SSH Port (Default: 22)

SNMP Setup
☐ Enable SNMP Agent
Get Community
Set Community
Manager Host IP
Trap Community
Notification Host IP
Trap Timeout seconds

OK

Allow management from the Internet

Enable the checkbox to allow system administrators to login from the Internet. There are several servers provided by the system to allow you managing the router from Internet. Check the box(es) to specify.

Disable PING from the Internet

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

Access List

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

List IP - Indicate an IP address allowed to login to the router.

Subnet Mask - Represent a subnet mask allowed to login to the router.

Default Ports

Check to use standard port numbers for the Telnet and HTTP servers.

User Defined Ports

Check to specify user-defined port numbers for the Telnet, HTTP and FTP servers.

Enable SNMP Agent

Check it to enable this function.

Get Community

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

| | |
|-----------------------------|--|
| Set Community | Set community by typing a proper name. The default setting is private . |
| Manager Host IP | Set one host as the manager to execute SNMP function. Please type in IP address to specify certain host. |
| Trap Community | Set trap community by typing a proper name. The default setting is public . |
| Notification Host IP | Set the IP address of the host that will receive the trap community. |
| Trap Timeout | The default setting is 10 seconds. |

4.12.8 Reboot System

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

[System Maintenance >> Reboot System](#)

Reboot System

Do you want to reboot your router ?

☒ Using current configuration
☐ Using factory default configuration

OK

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

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

4.12.9 Firmware Upgrade

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

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

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

System Maintenance >> Firmware Upgrade

Web Firmware Upgrade

Select a firmware file.

Click Upgrade to upload the file.

TFTP Firmware Upgrade from LAN

Current Firmware Version: 3.2.2_RC2


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 complete, 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.

System Maintenance >> Firmware Upgrade

 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 5.

4.13 Diagnostics

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

Below shows the menu items for Diagnostics.



4.13.1 Dial-out Trigger

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

[Diagnostics >> Dial-out Trigger](#)

Dial-out Triggered Packet Header

| [Refresh](#) |

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)

Decoded Format

It shows the source IP address (local), destination IP (remote) address, the protocol and length of the package.

Refresh

Click it to reload the page.

4.13.2 Routing Table

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

[Diagnostics >> View Routing Table](#)

| Current Running Routing Table | | | Refresh |
|---|---------------|--------------------------------------|-------------------------|
| Key: C - connected, S - static, R - RIP, * - default, ~ - private | | | |
| S~ | 192.168.10.0/ | 255.255.255.0 via 192.168.1.2, | LAN |
| C~ | 192.168.1.0/ | 255.255.255.0 is directly connected, | LAN |
| S~ | 211.100.88.0/ | 255.255.255.0 via 192.168.1.3, | LAN |

Refresh

Click it to reload the page.

4.13.3 ARP Cache Table

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

[Diagnostics >> View ARP Cache Table](#)

| Ethernet ARP Cache Table | | | Clear | Refresh |
|--------------------------|-------------------|-----------------|-----------------------|-------------------------|
| IP Address | MAC Address | Netbios Name | | |
| 192.168.1.1 | 00-50-7F-C2-80-20 | | | |
| 192.168.1.10 | 00-0E-A6-2A-D5-A1 | USER-6A0E182CE8 | | |

Refresh

Click it to reload the page.

Clear

Click it to clear the whole table.

4.13.4 DHCP Table

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

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

[Diagnostics >> View DHCP Assigned IP Addresses](#)

| DHCP IP Assignment Table | | | | | Refresh |
|--------------------------|------------|-------------|-------------|---------|-------------------------|
| DHCP server: Running | | | | | |
| Index | IP Address | MAC Address | Leased Time | HOST ID | |
| | | | | | |

| | |
|--------------------|--|
| Index | It displays the connection item number. |
| IP Address | It displays the IP address assigned by this router for specified PC. |
| MAC Address | It displays the MAC address for the specified PC that DHCP assigned IP address for it. |
| Leased Time | It displays the leased time of the specified PC. |
| HOST ID | It displays the host ID name of the specified PC. |
| Refresh | Click it to reload the page. |

4.13.5 NAT Sessions Table

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

[Diagnostics >> NAT Sessions Table](#)

| NAT Active Sessions Table | | | | Refresh |
|---------------------------|--------------|---------------|-----------|-------------------------|
| Private IP :Port | #Pseudo Port | Peer IP :Port | Interface | |
| | | | | |

| | |
|-----------------------|---|
| TX rate (kbps) | Display the transmission speed of the monitored device. |
| RX rate (kbps) | Display the receiving speed of the monitored device. |
| Sessions | Display the session number that you specified in Limit Session web page. |
| Action | Block - can prevent specified PC accessing into Internet within 5 minutes. |

Page: 1 | Refresh |

| | Sessions | Action |
|--|----------|-----------------------|
| | 7 | Block |
| | | |
| | | |

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

Page: 1 | Refresh |

| | Sessions | Action |
|--|---------------|-------------------------|
| | blocked / 298 | Unblock |
| | | |
| | | |

4.13.7 Ping Diagnosis

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

[Diagnostics >> Ping Diagnosis](#)

Ping Diagnosis

Note: If you want to ping a LAN PC or you don't want to specify which WAN to ping through, please select "Unspecified".

Ping to: Host / IP IP Address:

Host / IP
Gateway
DNS

Run

Result | Clear |

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

Clear

Click this link to remove the result on the window.

4.13.8 Trace Route

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

[Diagnostics >> Trace Route](#)

Trace Route

| | | |
|--------------------|------|------------------------------------|
| Protocol: | ICMP | |
| Host / IP Address: | ICMP | <input type="text"/> |
| | UDP | |
| | | <input type="button" value="Run"/> |

Result [Clear](#)

Protocol

Use the drop down list to choose the interface that you want to ping through.

Host/IP Address

It indicates the IP address of the host.

Run

Click this button to start route tracing work.

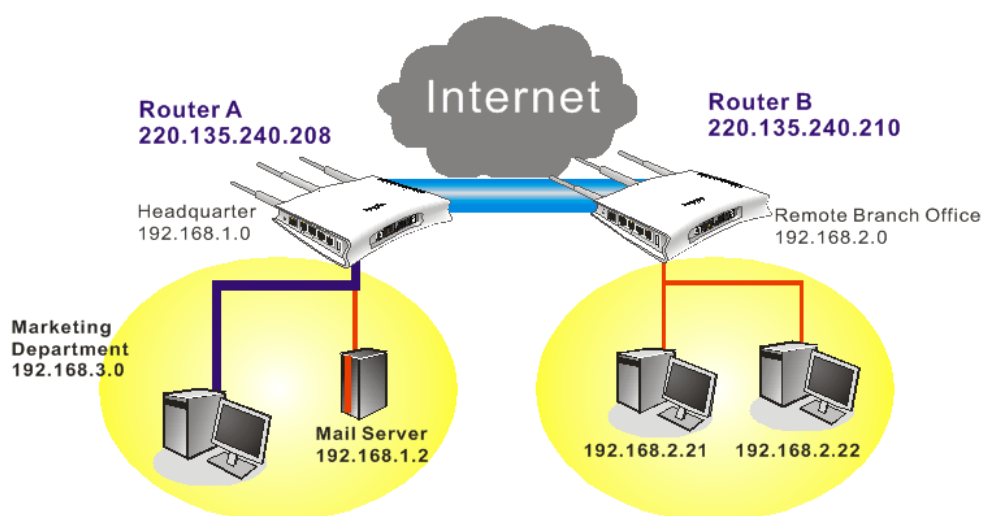
Clear

Click this link to remove the result on the window.

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

VPN and Remote Access >> PPP General Setup

| PPP General Setup | |
|--|---|
| PPP/MP Protocol | |
| Dial-In PPP Authentication | PAP or CHAP |
| Dial-In PPP Encryption (MPPE) | Optional MPPE |
| Mutual Authentication (PAP) | <input type="radio"/> Yes <input checked="" type="radio"/> No |
| Username | <input type="text"/> |
| Password | <input type="text"/> |
| IP Address Assignment for Dial-In Users (When DHCP Disable set) | |
| Start IP Address | 192.168.1.200 |

OK

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

parties have known.

VPN and Remote Access >> IPSec General Setup

VPN IKE/IPSec General Setup

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

| | |
|---|--|
| IKE Authentication Method | |
| Pre-Shared Key | |
| Confirm Pre-Shared Key | |
| IPSec Security Method | |
| <input checked="" type="checkbox"/> Medium (AH) | Data will be authentic, but will not be encrypted. |
| High (ESP) | <input checked="" type="checkbox"/> DES <input checked="" type="checkbox"/> 3DES <input checked="" type="checkbox"/> AES |
| Data will be encrypted and authentic. | |
| OK Cancel | |

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

VPN and Remote Access >> LAN to LAN

Profile Index : 1

1. Common Settings

| | | | |
|--|---|--|--|
| Profile Name | Branch1 | Call Direction | <input checked="" type="radio"/> Both <input type="radio"/> Dial-Out <input type="radio"/> Dial-In |
| <input type="checkbox"/> Enable this profile | | <input type="checkbox"/> Always on | |
| Netbios Naming Packet | <input checked="" type="radio"/> Pass <input type="radio"/> Block | Idle Timeout | 300 second(s) |
| | | <input type="checkbox"/> Enable PING to keep alive | |
| | | PING to the IP | |

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

2. Dial-Out Settings

| | | |
|---|--|---|
| Type of Server I am calling <input type="radio"/> PPTP <input checked="" type="radio"/> IPSec Tunnel <input type="radio"/> L2TP with IPSec Policy None | | Username ??? Password PPP Authentication PAP/CHAP VJ Compression <input checked="" type="radio"/> On <input type="radio"/> Off |
| Server IP/Host Name for VPN. (such as draytek.com or 123.45.67.89) 220.135.240.210 | | IKE Authentication Method <input checked="" type="radio"/> Pre-Shared Key IKE Pre-Shared Key <input type="radio"/> Digital Signature(X.509) None |
| | | IPSec Security Method <input checked="" type="radio"/> Medium(AH) <input type="radio"/> High(ESP) DES without Authentication Advanced |
| | | Index(1-15) in Schedule Setup: , , , |

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

2. Dial-Out Settings

| | | |
|---|--|--|
| Type of Server I am calling <input checked="" type="radio"/> PPTP <input type="radio"/> IPSec Tunnel <input type="radio"/> L2TP with IPSec Policy None | | Username draytek Password •••••• PPP Authentication PAP/CHAP VJ Compression <input checked="" type="radio"/> On <input type="radio"/> Off |
| Server IP/Host Name for VPN. (such as draytek.com or 123.45.67.89) 220.135.240.210 | | IKE Authentication Method <input type="radio"/> Pre-Shared Key IKE Pre-Shared Key <input type="radio"/> Digital Signature(X.509) None |
| | | IPSec Security Method <input checked="" type="radio"/> Medium(AH) <input type="radio"/> High(ESP) DES without Authentication Advanced |
| | | Index(1-15) in Schedule Setup: , , , |

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

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

3. Dial-In Settings

| | |
|--|--|
| Allowed Dial-In Type <input type="checkbox"/> PPTP <input checked="" type="checkbox"/> IPSec Tunnel <input type="checkbox"/> L2TP with IPSec Policy None <input checked="" type="checkbox"/> Specify Remote VPN Gateway Peer VPN Server IP <input type="text" value="220.135.240.210"/> or Peer ID <input type="text"/> | Username <input type="text" value="???"/> Password <input type="text"/> VJ Compression <input checked="" type="radio"/> On <input type="radio"/> Off IKE Authentication Method <input checked="" type="checkbox"/> Pre-Shared Key IKE Pre-Shared Key <input type="text"/> <input type="checkbox"/> Digital Signature(X.509) None IPSec Security Method <input checked="" type="checkbox"/> Medium(AH) High(ESP) <input checked="" type="checkbox"/> DES <input checked="" type="checkbox"/> 3DES <input checked="" type="checkbox"/> AES |
|--|--|

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

3. Dial-In Settings

| | |
|--|--|
| Allowed Dial-In Type <input checked="" type="checkbox"/> PPTP <input type="checkbox"/> IPSec Tunnel <input type="checkbox"/> L2TP with IPSec Policy None <input checked="" type="checkbox"/> Specify Remote VPN Gateway Peer VPN Server IP <input type="text" value="220.135.240.210"/> or Peer ID <input type="text"/> | Username <input type="text" value="draytek"/> Password <input type="text" value="*****"/> VJ Compression <input checked="" type="radio"/> On <input type="radio"/> Off IKE Authentication Method <input checked="" type="checkbox"/> Pre-Shared Key IKE Pre-Shared Key <input type="text"/> <input type="checkbox"/> Digital Signature(X.509) None IPSec Security Method <input checked="" type="checkbox"/> Medium(AH) High(ESP) <input checked="" type="checkbox"/> DES <input checked="" type="checkbox"/> 3DES <input checked="" type="checkbox"/> AES |
|--|--|

- 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 <input type="text" value="0.0.0.0"/> Remote Gateway IP <input type="text" value="0.0.0.0"/> Remote Network IP <input type="text" value="192.168.2.0"/> Remote Network Mask <input type="text" value="255.255.255.0"/> <input type="button" value="More"/> | RIP Direction Disable From first subnet to remote network, you have to do Route <input type="checkbox"/> Change default route to this VPN tunnel (Only single WAN supports this) |
|---|---|

Settings in Router B in the remote office:

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

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

[VPN and Remote Access >> PPP General Setup](#)

PPP General Setup

| | |
|---|--|
| <p>PPP/MP Protocol</p> <p>Dial-In PPP Authentication <input type="text" value="PAP or CHAP"/></p> <p>Dial-In PPP Encryption (MPPE) <input type="text" value="Optional MPPE"/></p> <p>Mutual Authentication (PAP) <input type="radio"/> Yes <input checked="" type="radio"/> No</p> <p>Username <input type="text"/></p> <p>Password <input type="text"/></p> | <p>IP Address Assignment for Dial-In Users (When DHCP Disable set)</p> <p>Start IP Address <input type="text" value="192.168.2.200"/></p> |
|---|--|

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

[VPN and Remote Access >> IPSec General Setup](#)

VPN IKE/IPSec General Setup

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

| | |
|--|--|
| <p>IKE Authentication Method</p> <p>Pre-Shared Key <input type="text" value="....."/></p> <p>Confirm Pre-Shared Key <input type="text" value="....."/></p> | |
| <p>IPSec Security Method</p> <p><input checked="" type="checkbox"/> Medium (AH) Data will be authentic, but will not be encrypted.</p> <p>High (ESP) <input checked="" type="checkbox"/> DES <input checked="" type="checkbox"/> 3DES <input checked="" type="checkbox"/> AES Data will be encrypted and authentic.</p> | |

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

[VPN and Remote Access >> LAN to LAN](#)

Profile Index : 1

1. Common Settings

| | |
|---|--|
| <p>Profile Name <input type="text" value="Branch1"/></p> <p><input type="checkbox"/> Enable this profile</p> <p>Netbios Naming Packet <input checked="" type="radio"/> Pass <input type="radio"/> Block</p> | <p>Call Direction <input checked="" type="radio"/> Both <input type="radio"/> Dial-Out <input type="radio"/> Dial-In</p> <p><input type="checkbox"/> Always on</p> <p>Idle Timeout <input type="text" value="300"/> second(s)</p> <p><input type="checkbox"/> Enable PING to keep alive</p> <p>PING to the IP <input type="text"/></p> |
|---|--|

- 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 <input type="radio"/> PPTP <input checked="" type="radio"/> IPSec Tunnel <input type="radio"/> L2TP with IPSec Policy None | | Username ??? Password PPP Authentication PAP/CHAP VJ Compression <input checked="" type="radio"/> On <input type="radio"/> Off |
| Server IP/Host Name for VPN. (such as draytek.com or 123.45.67.89) 220.135.240.208 | | IKE Authentication Method <input checked="" type="radio"/> Pre-Shared Key IKE Pre-Shared Key <input type="radio"/> Digital Signature(X.509) None |
| | | IPSec Security Method <input checked="" type="radio"/> Medium(AH) <input type="radio"/> High(ESP) DES without Authentication Advanced |
| | | Index(1-15) in Schedule Setup: , , , |

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

2. Dial-Out Settings

| | | |
|---|--|---|
| Type of Server I am calling <input checked="" type="radio"/> PPTP <input type="radio"/> IPSec Tunnel <input type="radio"/> L2TP with IPSec Policy None | | Username draytek Password ***** PPP Authentication PAP/CHAP VJ Compression <input checked="" type="radio"/> On <input type="radio"/> Off |
| Server IP/Host Name for VPN. (such as draytek.com or 123.45.67.89) 220.135.240.208 | | IKE Authentication Method <input checked="" type="radio"/> Pre-Shared Key IKE Pre-Shared Key <input type="radio"/> Digital Signature(X.509) None |
| | | IPSec Security Method <input checked="" type="radio"/> Medium(AH) <input type="radio"/> High(ESP) DES without Authentication Advanced |
| | | Index(1-15) in Schedule Setup: , , , |

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

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

3. Dial-In Settings

| | |
|--|--|
| Allowed Dial-In Type <input type="checkbox"/> PPTP <input checked="" type="checkbox"/> IPSec Tunnel <input type="checkbox"/> L2TP with IPSec Policy None ▼ | Username ??? Password VJ Compression <input checked="" type="radio"/> On <input type="radio"/> Off |
| <input checked="" type="checkbox"/> Specify Remote VPN Gateway Peer VPN Server IP 220.135.240.208 or Peer ID | IKE Authentication Method <input checked="" type="checkbox"/> Pre-Shared Key IKE Pre-Shared Key <input type="checkbox"/> Digital Signature(X.509) None ▼ |
| | IPSec Security Method <input checked="" type="checkbox"/> Medium(AH) High(ESP) <input checked="" type="checkbox"/> DES <input checked="" type="checkbox"/> 3DES <input checked="" type="checkbox"/> AES |

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

3. Dial-In Settings

| | |
|--|--|
| Allowed Dial-In Type <input checked="" type="checkbox"/> PPTP <input type="checkbox"/> IPSec Tunnel <input type="checkbox"/> L2TP with IPSec Policy None ▼ | Username draytek Password •••••• VJ Compression <input checked="" type="radio"/> On <input type="radio"/> Off |
| <input checked="" type="checkbox"/> Specify Remote VPN Gateway Peer VPN Server IP 220.135.240.208 or Peer ID | IKE Authentication Method <input checked="" type="checkbox"/> Pre-Shared Key IKE Pre-Shared Key <input type="checkbox"/> Digital Signature(X.509) None ▼ |
| | IPSec Security Method <input checked="" type="checkbox"/> Medium(AH) High(ESP) <input checked="" type="checkbox"/> DES <input checked="" type="checkbox"/> 3DES <input checked="" type="checkbox"/> AES |

- 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.

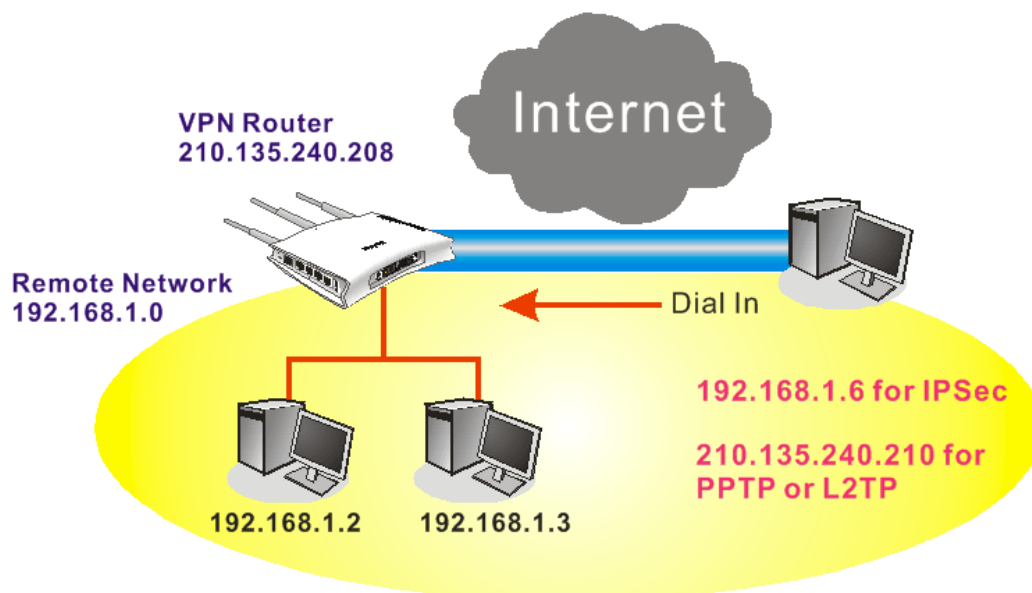
4. TCP/IP Network Settings

| | |
|--|--|
| My WAN IP 0.0.0.0 | RIP Direction Disable ▼ |
| Remote Gateway IP 0.0.0.0 | From first subnet to remote network, you have to do |
| Remote Network IP 192.168.1.0 | Route ▼ |
| Remote Network Mask 255.255.255.0 | <input type="checkbox"/> Change default route to this VPN tunnel (Only single WAN supports this) |
| More | |

OK Clear Cancel

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

VPN and Remote Access >> PPP General Setup

| PPP General Setup | |
|--|--|
| PPP/MP Protocol | IP Address Assignment for Dial-In Users (When DHCP Disable set) |
| Dial-In PPP Authentication: PAP or CHAP | Start IP Address: 192.168.1.200 |
| Dial-In PPP Encryption (MPPE): Optional MPPE | |
| Mutual Authentication (PAP): <input type="radio"/> Yes <input checked="" type="radio"/> No | |
| Username: <input type="text"/> | |
| Password: <input type="text"/> | |
| <input type="button" value="OK"/> | |

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

VPN and Remote Access >> IPSec General Setup

VPN IKE/IPSec General Setup

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

| | |
|---|--|
| IKE Authentication Method | |
| Pre-Shared Key | |
| Confirm Pre-Shared Key | |
| IPSec Security Method | |
| <input checked="" type="checkbox"/> Medium (AH) | Data will be authentic, but will not be encrypted. |
| High (ESP) | <input checked="" type="checkbox"/> DES <input checked="" type="checkbox"/> 3DES <input checked="" type="checkbox"/> AES |
| Data will be encrypted and authentic. | |
| OK Cancel | |

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

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

VPN and Remote Access >> Remote Dial-in User

Index No. 1

| | | |
|--|----------|-----------|
| User account and Authentication | Username | ??? |
| <input checked="" type="checkbox"/> Enable this account | Password | |
| Idle Timeout | 300 | second(s) |
| Allowed Dial-In Type | | |
| <input type="checkbox"/> PPTP | | |
| <input checked="" type="checkbox"/> IPSec Tunnel | | |
| <input type="checkbox"/> L2TP with IPSec Policy | | |
| None | | |
| IKE Authentication Method | | |
| <input checked="" type="checkbox"/> Pre-Shared Key | | |
| IKE Pre-Shared Key | | |
| <input type="checkbox"/> Digital Signature(X.509) | | |
| None | | |
| IPSec Security Method | | |
| <input checked="" type="checkbox"/> Medium(AH) | | |
| High(ESP) | | |
| <input checked="" type="checkbox"/> DES <input checked="" type="checkbox"/> 3DES <input checked="" type="checkbox"/> AES | | |
| Local ID (optional) | | |
| OK Clear Cancel | | |

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.

Index No. 1

| | | |
|---|--|--|
| User account and Authentication <input checked="" type="checkbox"/> Enable this account Idle Timeout <input type="text" value="300"/> second(s) | | Username <input type="text" value="???"/> Password <input type="password"/> |
| Allowed Dial-In Type <input checked="" type="checkbox"/> PPTP <input type="checkbox"/> IPSec Tunnel <input type="checkbox"/> L2TP with IPSec Policy <input type="text" value="None"/> | | IKE Authentication Method <input checked="" type="checkbox"/> Pre-Shared Key IKE Pre-Shared Key <input type="text"/> <input type="checkbox"/> Digital Signature(X.509) None <input type="text"/> |
| | | IPSec Security Method <input checked="" type="checkbox"/> Medium(AH) High(ESP) <input checked="" type="checkbox"/> DES <input checked="" type="checkbox"/> 3DES <input checked="" type="checkbox"/> AES Local ID (optional) <input type="text"/> |

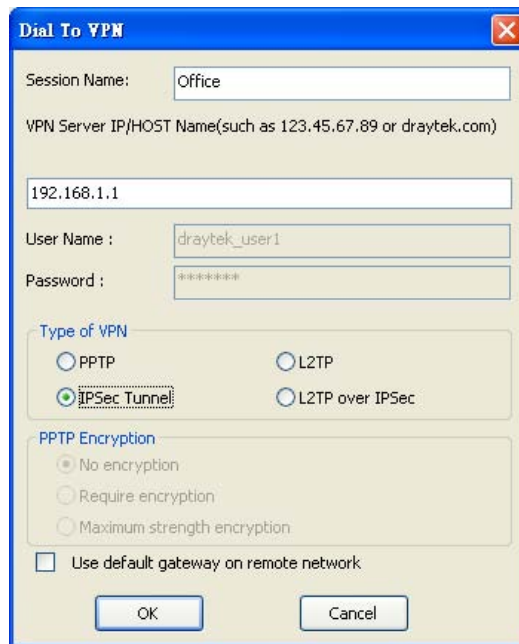
Settings in the remote host:

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



- 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,



Dial To VPN

Session Name: Office

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

192.168.1.1

User Name : draytek_user1

Password : *****

Type of VPN

☐ PPTP ☐ L2TP

☒ IPsec Tunnel ☐ L2TP over IPsec

PPTP Encryption

☒ No encryption

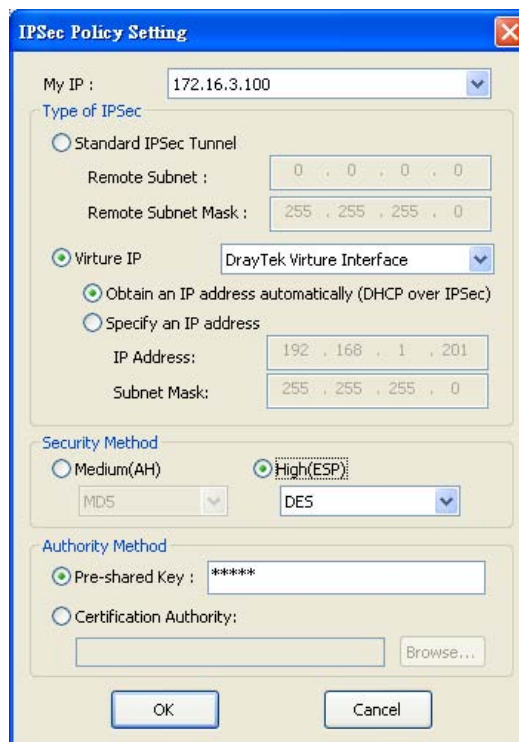
☐ Require encryption

☐ Maximum strength encryption

☐ Use default gateway on remote network

OK Cancel

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 : 172.16.3.100

Type of IPSec

☐ Standard IPSec Tunnel

Remote Subnet : 0 . 0 . 0 . 0

Remote Subnet Mask : 255 . 255 . 255 . 0

☒ Virture IP

DrayTek Virture Interface

☒ Obtain an IP address automatically (DHCP over IPSec)

☐ Specify an IP address

IP Address: 192 . 168 . 1 . 201

Subnet Mask: 255 . 255 . 255 . 0

Security Method

☐ Medium(AH)

☒ High(ESP)

MD5 DES

Authority Method

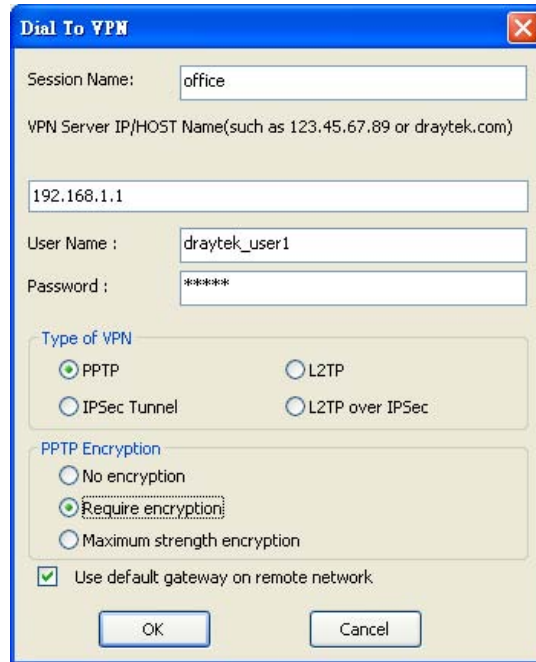
☒ Pre-shared Key : *****

☐ Certification Authority:

Browse...

OK Cancel

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.



The image shows a 'Dial To VPN' configuration window. It includes fields for Session Name (office), VPN Server IP/Host Name (192.168.1.1), User Name (draytek_user1), and Password (masked with asterisks). Under 'Type of VPN', PPTP is selected. Under 'PPTP Encryption', 'Require encryption' is selected. A checkbox for 'Use default gateway on remote network' is checked. OK and Cancel buttons are at the bottom.

- 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 headquarter office downtown via either HTTPS or VPN to check email and access internal database. Meanwhile, children may chat on Skype in the restroom.

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

Bandwidth Management >> Quality of Service

| General Setup | | | | | | | Set to Factory Default |
|---------------|---------------------|-----------|---------|---------|---------|--------|--|
| Status | Bandwidth | Direction | Class 1 | Class 2 | Class 3 | Others | UDP Bandwidth Control |
| Enable | 10000Kbps/10000Kbps | Outbound | 25% | 25% | 25% | 25% | Inactive Setup |

| Class Rule | | | |
|------------|------|----------------------|----------------------|
| Index | Name | Rule | Service Type |
| Class 1 | Test | Edit | Edit |
| Class 2 | | Edit | |
| Class 3 | | Edit | |

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

Bandwidth Management >> Quality of Service

General Setup

☒ **Enable the QoS Control** OUT ▼

WAN Inbound Bandwidth IN

WAN Outbound Bandwidth OUT

BOTH

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

Bandwidth Management >> Quality of Service

Class Index #1

Name

| NO | Status | Local Address | Remote Address | DiffServ CodePoint | Service Type |
|-------------------------|--------|---------------|----------------|--------------------|--------------|
| 1 <input type="radio"/> | Active | Any | Any | IP precedence 2 | TFTP(UDP:69) |

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

Bandwidth Management >> Quality of Service

General Setup

☒ **Enable the QoS Control** BOTH ▼

WAN Inbound Bandwidth Kbps

WAN Outbound Bandwidth Kbps

| Index | Class Name | Reserved_bandwidth Ratio |
|----------------|------------|-----------------------------------|
| Class 1 | E-mail | <input type="text" value="25"/> % |
| Class 2 | | <input type="text" value="25"/> % |
| Class 3 | | <input type="text" value="25"/> % |
| | Others | <input type="text" value="25"/> % |

☐ Enable UDP Bandwidth Control Limited_bandwidth Ratio %

☐ Outbound TCP ACK Prioritize [Online Statistics](#)

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

[Bandwidth Management >> Quality of Service](#)

Class Index #2

Name

| NO | Status | Local Address | Remote Address | DiffServ CodePoint | Service Type |
|----|--------|---------------|----------------|--------------------|--------------|
| 1 | Active | Any | Any | ANY | TFTP(UDP:69) |

6. Click **Setup** link for WAN.

[Bandwidth Management >> Quality of Service](#)

General Setup [Set to Factory Default](#)

| Status | Bandwidth | Direction | Class 1 | Class 2 | Class 3 | Others | UDP Bandwidth Control |
|--------|---------------------|-----------|---------|---------|---------|--------|--|
| Enable | 10000Kbps/10000Kbps | Both | 25% | 25% | 25% | 25% | Inactive Setup |

Class Rule

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

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

[Bandwidth Management >> Quality of Service](#)

General Setup

☒ **Enable the QoS Control** BOTH

WAN Inbound Bandwidth Kbps

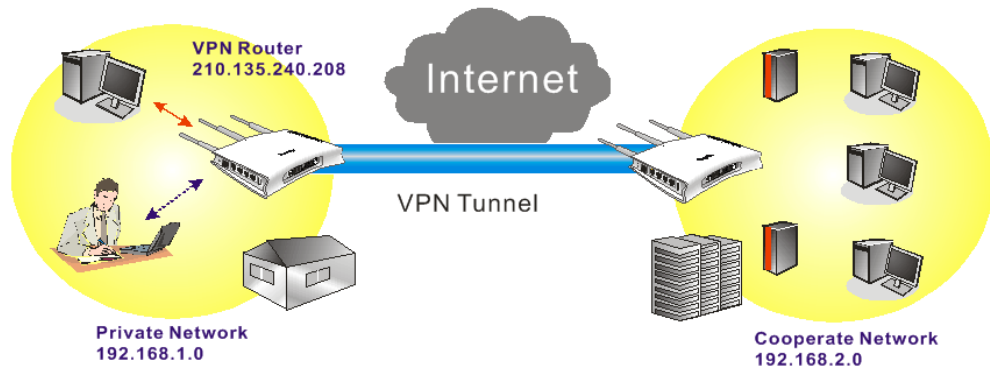
WAN Outbound Bandwidth Kbps

| Index | Class Name | Reserved_bandwidth Ratio |
|---------|------------|-----------------------------------|
| Class 1 | E-mail | <input type="text" value="25"/> % |
| Class 2 | HTTPS | <input type="text" value="25"/> % |
| Class 3 | | <input type="text" value="25"/> % |
| | Others | <input type="text" value="25"/> % |

☒ **Enable UDP Bandwidth Control** Limited_bandwidth Ratio %

☐ Outbound TCP ACK Prioritize [Online Statistics](#)

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



Bandwidth Management >> Quality of Service

Class Index #3

Name

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

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

Bandwidth Management >> Quality of Service

Rule Edit

☒ ACT

Local Address

Remote Address

DiffServ CodePoint

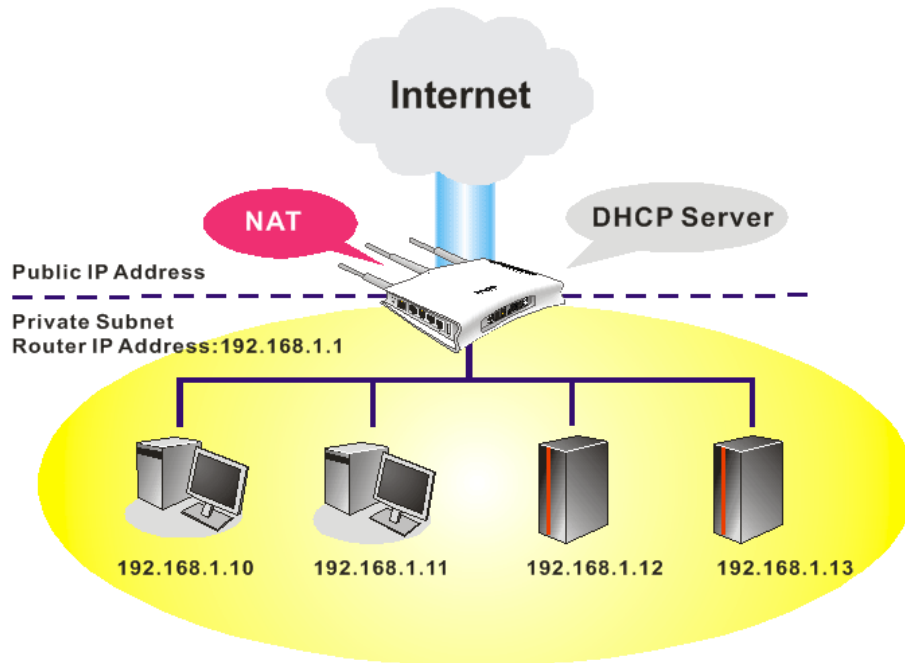
Service Type

Note: Please choose/setup the [Service Type](#) first.

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

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.

LAN >> General Setup

Ethernet TCP / IP and DHCP Setup

LAN IP Network Configuration

For NAT Usage

1st IP Address
 1st Subnet Mask

For IP Routing Usage ☐ Enable ☒ Disable

2nd IP Address
 2nd Subnet Mask

RIP Protocol Control

DHCP Server Configuration

☒ Enable Server ☐ Disable Server

Relay Agent: ☐ 1st Subnet ☐ 2nd Subnet

Start IP Address

IP Pool Counts

Gateway IP Address

DHCP Server IP Address

for Relay Agent

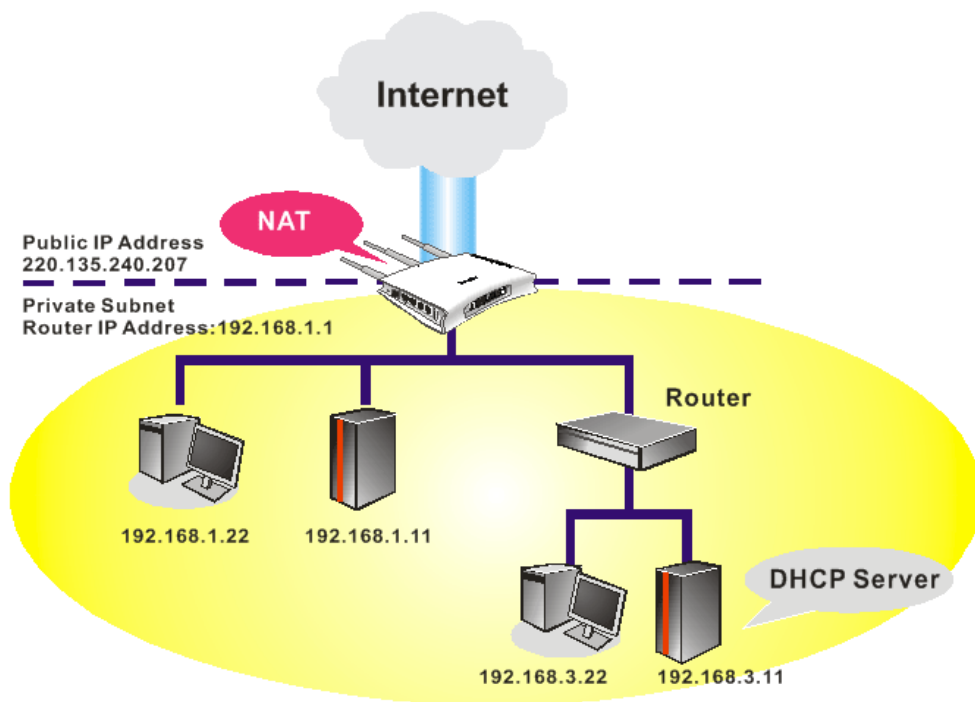
DNS Server IP Address

☐ Force DNS manual setting

Primary IP Address

Secondary IP Address

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



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

LAN >> General Setup

Ethernet TCP / IP and DHCP Setup

LAN IP Network Configuration

For NAT Usage

1st IP Address

1st Subnet Mask

For IP Routing Usage ☐ Enable ☒ Disable

2nd IP Address

2nd Subnet Mask

RIP Protocol Control

DHCP Server Configuration

☐ Enable Server ☒ Disable Server

Relay Agent: ☐ 1st Subnet ☐ 2nd Subnet

Start IP Address

IP Pool Counts

Gateway IP Address

DHCP Server IP Address for Relay Agent

DNS Server IP Address

☐ Force DNS manual setting

Primary IP Address

Secondary IP Address

4.5 Upgrade Firmware for Your Router

Before upgrading your router firmware, you need to install the Router Tools. The **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 :

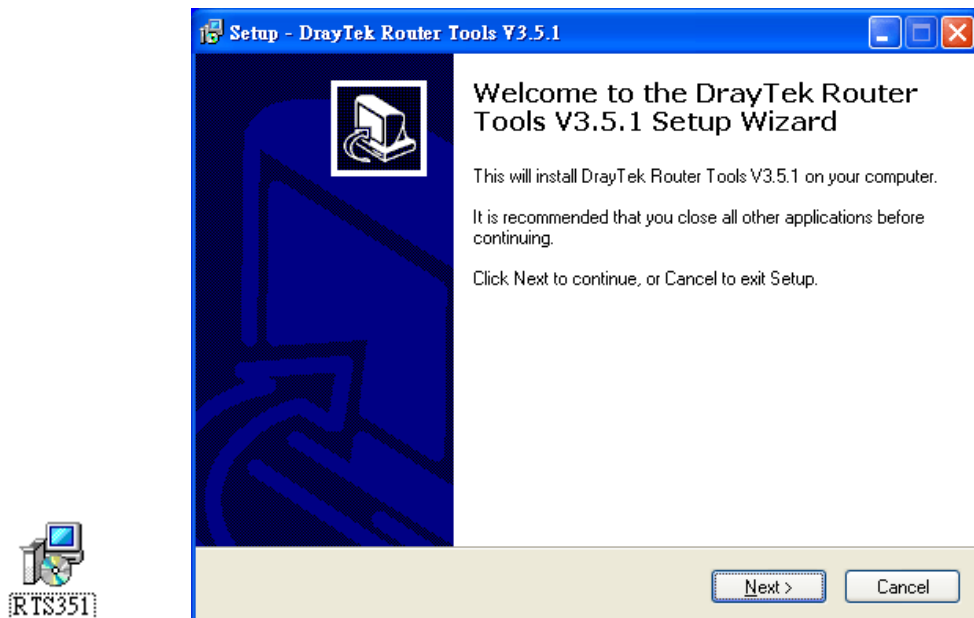
- Server IP Address : IP address of the PC that runs the Syslog
- Port Number : Default value 514



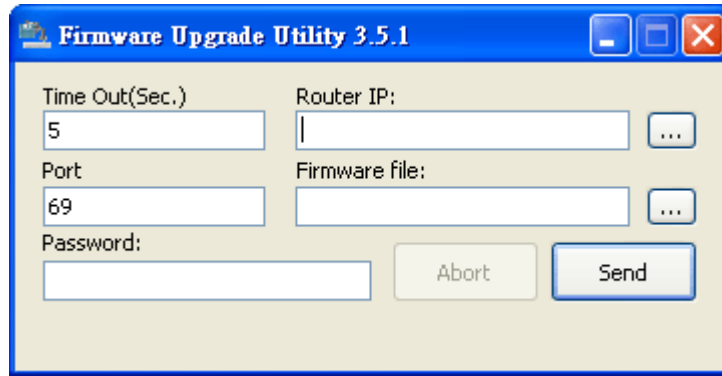
4. The file **RTSxxx.exe** will be asked to copy onto your computer. Remember the place of storing the execution file.
5. Go to **www.draytek.com** to find out the newly update firmware for your router.
6. Access into **Support Center >> Downloads**. Find out the model name of the router and click the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

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

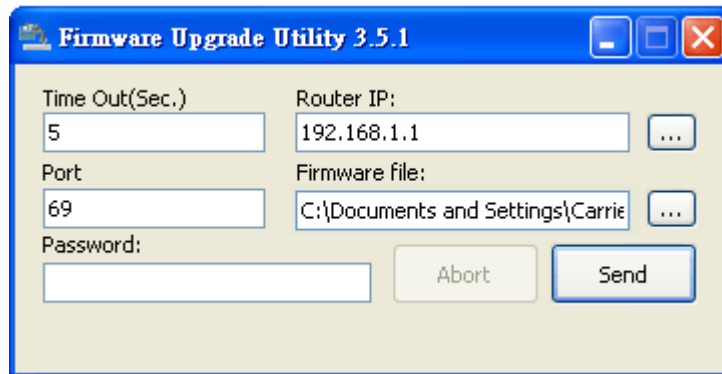
7. Choose the one that matches with your operating system and click the corresponding link to download correct firmware (zip file).
8. Next, decompress the zip file.
9. Double click on the icon of router tool. The setup wizard will appear.



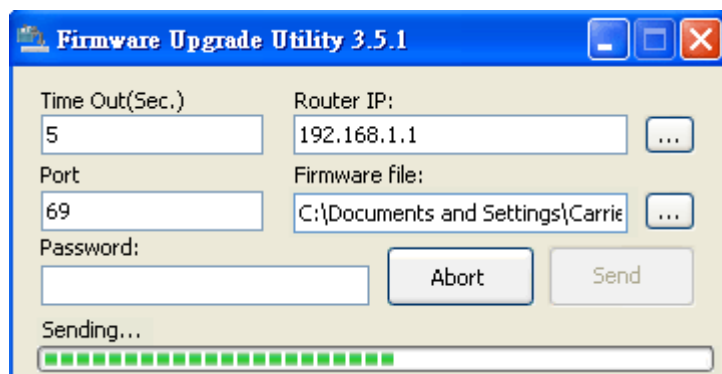
10. Follow the onscreen instructions to install the tool. Finally, click **Finish** to end the installation.
11. From the **Start** menu, open **Programs** and choose **Router Tools XXX >> Firmware Upgrade Utility**.



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

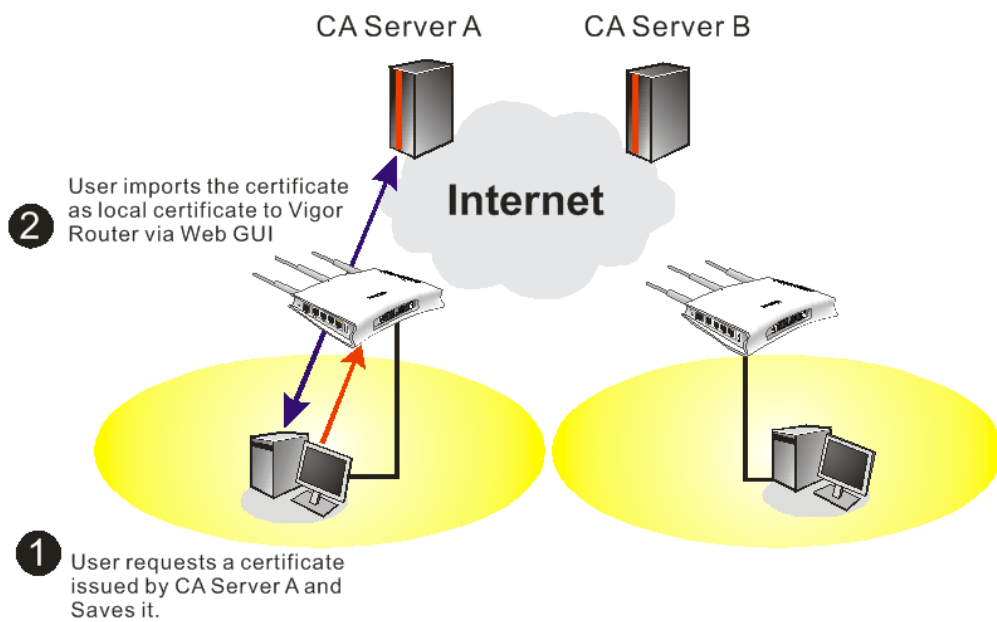


14. Click **Send**.



15. Now the firmware update is finished.

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



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

[Certificate Management >> Local Certificate](#)

X509 Local Certificate Configuration

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

[GENERATE](#) [IMPORT](#) [REFRESH](#)

X509 Local Certificate

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

[Certificate Management >> Local Certificate](#)

Generate Certificate Request

Subject Alternative Name

Type
IP

Subject Name

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

Key Type
Key Size

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

[Certificate Management >> Local Certificate](#)

X509 Local Certificate Configuration

| Name | Subject | Status | Modify |
|-------|---------------------------------|------------|---|
| Local | /C=TW/ST=HC/L=HC/O=Draytek/O... | Requesting | <input type="button" value="View"/> <input type="button" value="Delete"/> |

X509 Local Certificate

```
-----BEGIN CERTIFICATE REQUEST-----
MIIBqjCCARMCAQAwajELMAkGA1UEBhMCVFcxZzAJBgNVBAGTAkhDMQswCQYDVQQH
EwJlQzEQMA4GA1UEChMHRRHJheXR1azELMAkGA1UECzMCUkQxIjAgBgkqhkiG9w0B
CQEWE3N1cHBvcnRAZHJheXR1ay5jb20wgZ8wDQYJKoZIhvcNAQEBBQADgYOAMIGJ
AoGBALMjdTsqqfF97FEpYy+IqeJVJGuSRtqG6Etw8yTU5HQvXpAzcrGJBGr1kTUBX
a1X//fgnEccQA2LPSQIQ85Qychwq07Bm0EDf10wHwCa1A2QoGvIiODMC7f5w9xA8
m6+Of4xZ4QQnjXXgcicOBj1iAa6MLScelSynZhkgNq1QN5uFagMBAAGgADANBgkq
hkiG9w0BAQUFAAOBgQCq3sdwVc21t9qn4U6X2BJSVzu7JHafSSeUnaYDZefCmGfX
9yojHpstNsmWsmRuAwGeKCWc8S/gLtHhr6iccMoToQFv/LWdaEPUSLqrYBKKGc9t
eorpDa1/rC9ZwCraOt8XUmPqNoiytq8BxStTE8vULiIxmwaBvc1hWFSXKVLU7g==
-----END CERTIFICATE REQUEST-----
```

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

Microsoft Certificate Services - vigor Home

Welcome

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

Select a task:

- ☐ Retrieve the CA certificate or certificate revocation list
- ☒ Request a certificate
- ☐ Check on a pending certificate

Select **Advanced request**.

The screenshot shows the 'Choose Request Type' page. At the top, there is a breadcrumb 'Microsoft Certificate Services -- vigor' and a 'Home' link. The main heading is 'Choose Request Type'. Below it, a message says 'Please select the type of request you would like to make:'. There are two radio buttons: 'User certificate request' (which is selected) and 'Advanced request'. Under 'User certificate request', there is a button labeled 'User Certificate'. At the bottom right, there is a 'Next >' button.

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

The screenshot shows the 'Advanced Certificate Requests' page. At the top, there is a breadcrumb 'Microsoft Certificate Services -- vigor' and a 'Home' link. The main heading is 'Advanced Certificate Requests'. Below it, a message says 'You can request a certificate for yourself, another user, or a computer using one of the following methods. Note that the policy of the certification authority (CA) will determine the certificates that you can obtain.' There are three radio buttons: 'Submit a certificate request to this CA using a form.', 'Submit a certificate request using a base64 encoded PKCS #10 file or a renewal request using a base64 encoded PKCS #7 file.' (which is selected), and 'Request a certificate for a smart card on behalf of another user using the Smart Card Enrollment Station.' Below the third option, there is a note: 'You must have an enrollment agent certificate to submit a request for another user.' At the bottom right, there is a 'Next >' button.

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

The screenshot shows the 'Submit A Saved Request' page. At the top, there is a breadcrumb 'Microsoft Certificate Services -- vigor' and a 'Home' link. The main heading is 'Submit A Saved Request'. Below it, a message says 'Paste a base64 encoded PKCS #10 certificate request or PKCS #7 renewal request generated by an external application (such as a web server) into the request field to submit the request to the certification authority (CA)'. There is a text area labeled 'Saved Request:' containing a base64 encoded certificate request. Below the text area, there is a 'Browse for a file to insert.' button. There is a 'Certificate Template:' dropdown menu with 'Administrator' selected. Below it, there is an 'Additional Attributes' section with a list of attributes: 'Authenticated Session', 'Basic EFS', 'EFS Recovery Agent', 'User', 'IPSEC (Offline request)', 'Router (Offline request)' (which is selected), 'Subordinate Certification Authority', and 'Web Server'. At the bottom right, there is a 'Submit >' button.

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

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

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

Certificate Management >> Local Certificate

X509 Local Certificate Configuration

| Name | Subject | Status | Modify |
|-------|---------------------------------|------------|---|
| Local | /C=TW/ST=HC/L=HC/O=Draytek/O... | Requesting | View Delete |

[GENERATE](#)
[IMPORT](#)
[REFRESH](#)

X509 Local Certificate

```

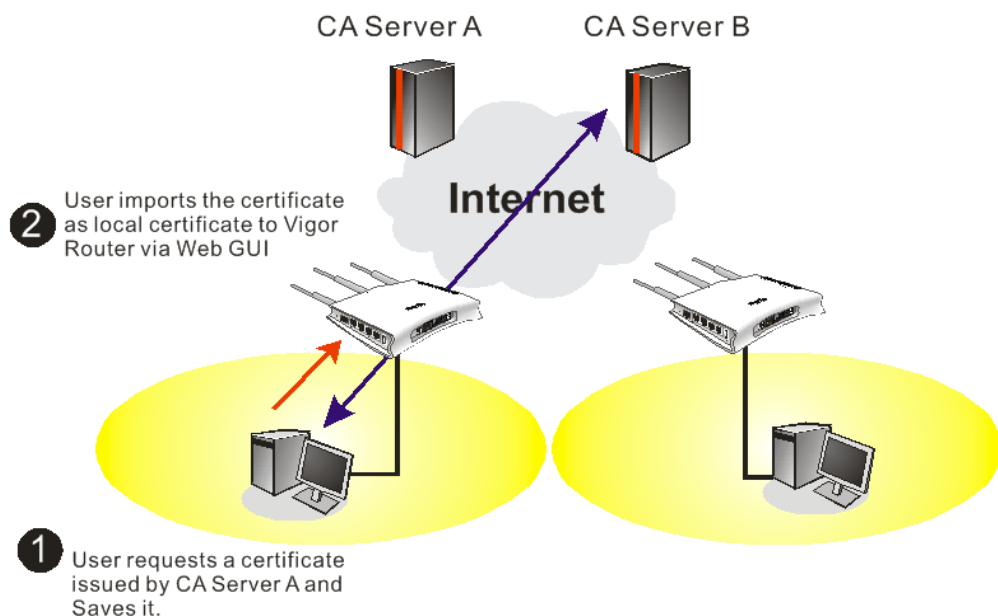
-----BEGIN CERTIFICATE REQUEST-----
MIIBqjCCARMCQAQAwajELMAkGA1UEBhMCVFcxHzAJBgNVBAGTAkhDMQswCQYDVQQH
EwJlQzEQMA4GA1UEChMHRRHJheXRlay5jb20wgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJ
AoGBALMjdTsqqfF97FEpYy+IqeJVJGuSRtqG6Etw8yTUSHQvXpAzcrqJBGrIkTUBX
a1X//fgnEccQA2LPSQIQ85Qychwq07BmOEDf10wHwCalAZQoGvIiODMC7f5w9xA8
m6+Of4xZ4QOnjXXGciC0Bj1iAa6MLScelsynZhkgQ1QN5uFAGMBAAGGADANBgkq
hkiG9w0BAQUFAAOBgQCq3sdwVc21t9qn4U6X2BjsVzu7JHafSSeUnaYDZefCmGfX
9yojHpstNsmWsmRuAwGeKCWc8S/gLtHhr6iccMoToQFv/LWdaEPu5LqryBKKgC9t
eorpDa1/rC9ZwCra0t8XUmPqNoiytq8BxStTE8vULiIxmwabVclhWFSXKVLU7g==
-----END CERTIFICATE REQUEST-----

```

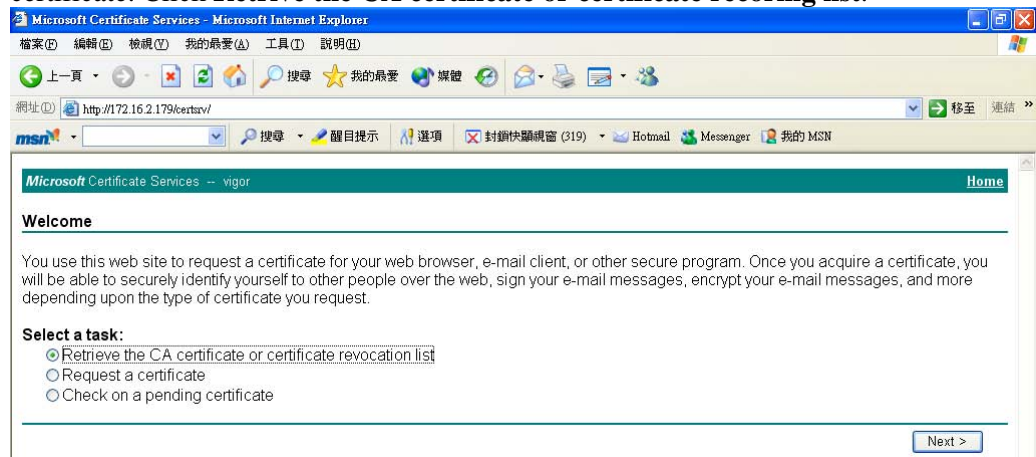
- You may review the detail information of the certificate by clicking **View** button.

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

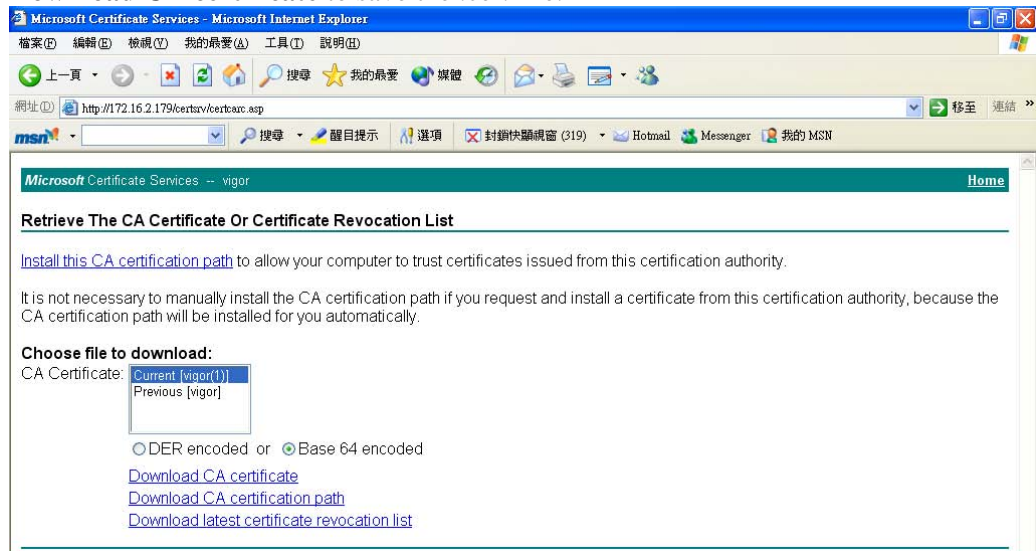
5.7 Request a CA Certificate and Set as Trusted on Windows CA Server



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



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



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

[Certificate Management >> Trusted CA Certificate](#)

X509 Trusted CA Certificate Configuration

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

[IMPORT](#)

[REFRESH](#)

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

| | |
|----------------------------|--------------------------|
| Name : | Trusted CA-1 |
| Issuer : | /C=US/CN=vigor |
| Subject : | /C=US/CN=vigor |
| Subject Alternative Name : | DNS:draytek.com |
| Valid From : | Aug 30 23:08:43 2005 GMT |
| Valid To : | Aug 30 23:17:47 2007 GMT |

[Close](#)

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

6 Troubleshooting

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

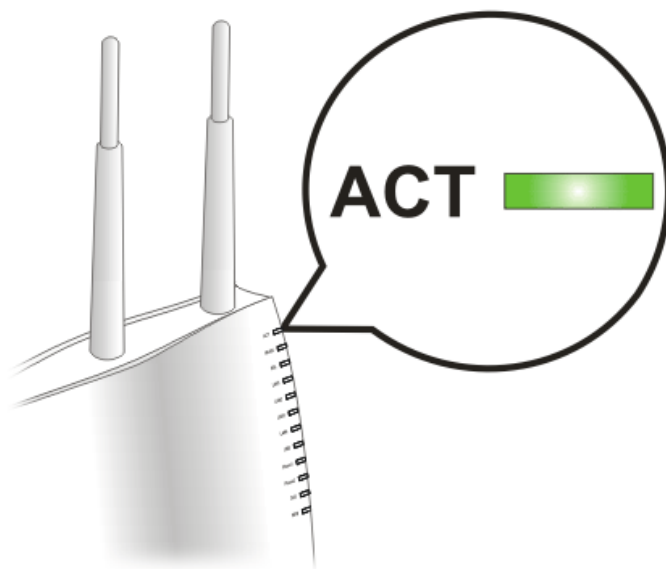
- Checking if the hardware status is OK or not.
- Checking if the network connection settings on your computer are OK or not.
- Pinging the router from your computer.
- Checking if the ISP settings are OK or not.
- Backing to factory default setting if necessary.

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

6.1 Checking If the Hardware Status Is OK or Not

Follow the steps below to verify the hardware status.

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



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

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

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

For Windows

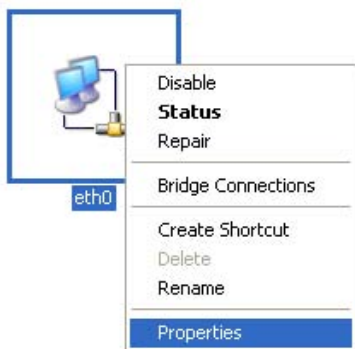


The example is based on Windows XP. As to the examples for other operation systems, please refer to the similar steps or find support notes in www.draytek.com.

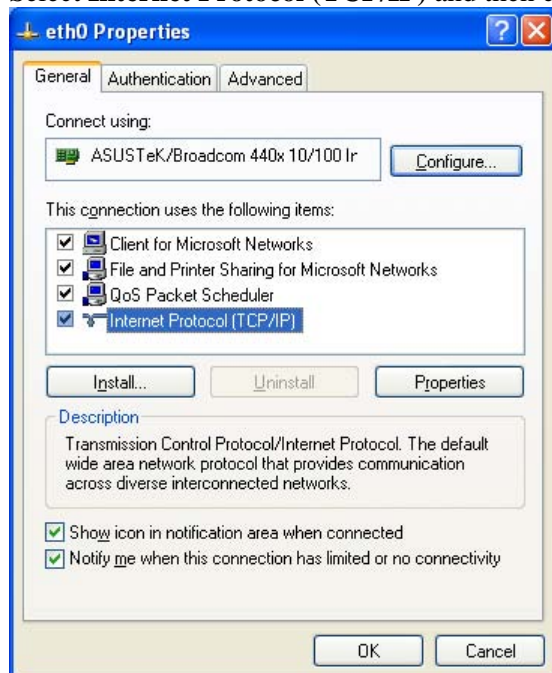
1. Go to **Control Panel** and then double-click on **Network Connections**.



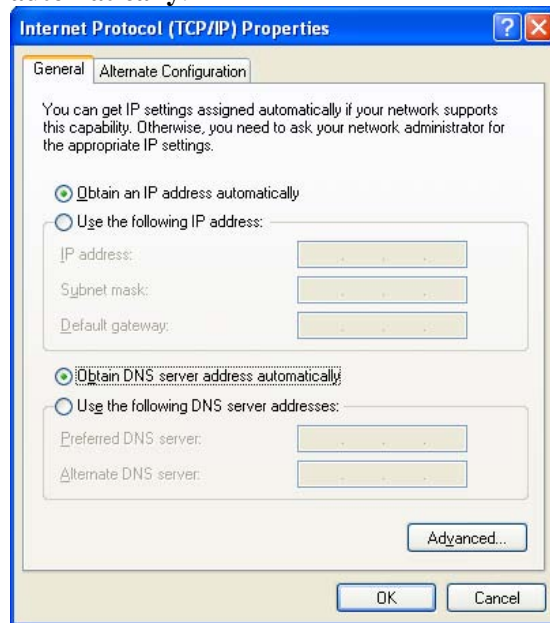
2. Right-click on **Local Area Connection** and click on **Properties**.



3. Select **Internet Protocol (TCP/IP)** and then click **Properties**.

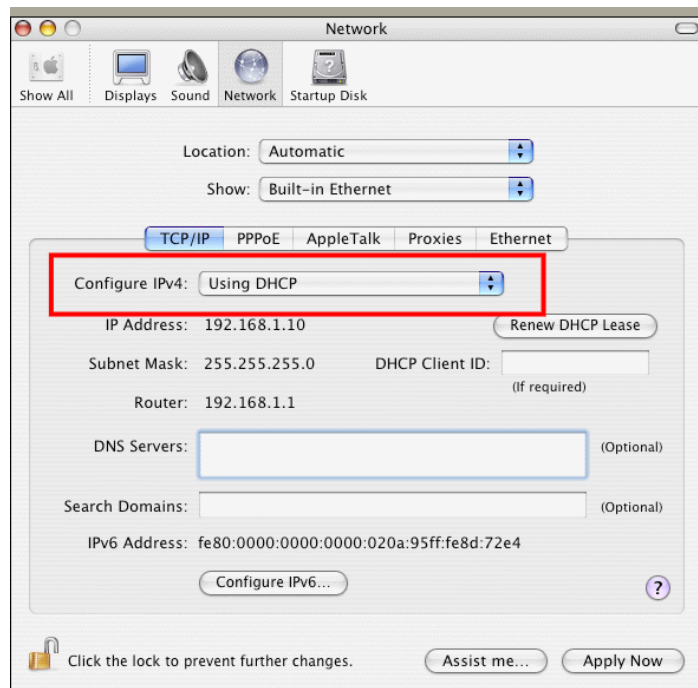


4. Select **Obtain an IP address automatically** and **Obtain DNS server address automatically**.



For MacOs

1. Double click on the current used MacOs on the desktop.
2. Open the **Application** folder and get into **Network**.
3. On the **Network** screen, select **Using DHCP** from the drop down list of Configure IPv4.



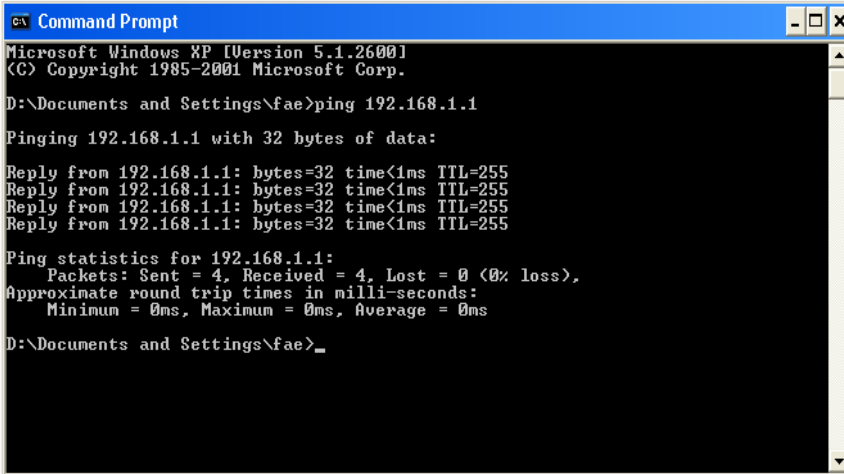
6.3 Pinging the Router from Your Computer

The default gateway IP address of the router is 192.168.1.1. For some reason, you might need to use “ping” command to check the link status of the router. **The most important thing is that the computer will receive a reply from 192.168.1.1.** If not, please check the IP address of your computer. We suggest you setting the network connection as **get IP automatically**. (Please 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.



```

C:\ Command Prompt
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

D:\Documents and Settings\fae>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:

Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

D:\Documents and Settings\fae>_

```

3. Type **ping 192.168.1.1** and press [Enter]. If the link is OK, the line of “**Reply from 192.168.1.1:bytes=32 time<1ms TTL=255**” will appear.
4. If the line does not appear, please check the IP address setting of your computer.

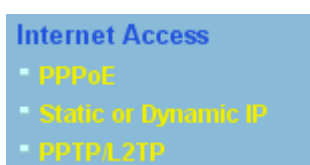
For MacOs (Terminal)

1. Double click on the current used MacOs on the desktop.
2. Open the **Application** folder and get into **Utilities**.
3. Double click **Terminal**. The Terminal window will appear.
4. Type **ping 192.168.1.1** and press [Enter]. If the link is OK, the line of “**64 bytes from 192.168.1.1: icmp_seq=0 ttl=255 time=xxxx ms**” will appear.

```
Terminal — bash — 80x24
Last login: Sat Jan  3 02:24:18 on ttyt1
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.



For PPPoE Users

1. Check if the **Enable** option is selected.
2. Check if **Username** and **Password** are entered with correct values that you **got from** your **ISP**.

[Internet Access >> PPPoE](#)

The image shows a web-based configuration interface for a network device. The main heading is "PPPoE Client Mode". Underneath, there's a "PPPoE Setup" section which is highlighted with a red rectangular box. Inside this box, the "PPPoE Link" is set to "Enable" (indicated by a selected radio button), the "Username" field contains "123", and the "Password" field contains three dots. Below the red box, there's a "Schedule Setup" section with a label "Index(1-15) in" followed by four empty input boxes. To the right of the "PPPoE Setup" section, there's a "PPP/MP Setup" section. It includes "PPP Authentication" set to "PAP or CHAP" via a dropdown menu, an "Always On" checkbox that is checked, and an "Idle Timeout" set to "-1" seconds. Below that is the "IP Address Assignment Method (IPCP)" section, where "WAN IP Alias" is selected. It also has "Fixed IP" set to "No (Dynamic IP)" and an empty "Fixed IP Address" field. At the bottom of the right column is a "MAC Address" section with "Default MAC Address" selected and a "Specify a MAC Address" option. The "MAC Address" field shows the value "00 . 50 . 7F . 92 . F5 . 61". At the very bottom of the form, there is an "OK" button.

For Static Users

1. Check if the **Enable** option for Broadband Access is selected.

Internet Access >> Static or Dynamic IP

Static or Dynamic IP (DHCP Client)

Access Control
 Broadband Access ☒ Enable ☐ Disable

Keep WAN Connection
☐ Enable PING to keep alive
 PING to the IP
 PING Interval minute(s)

WAN physical type
 Auto negotiation

RIP Protocol
☐ Enable RIP

WAN IP Network Settings WAN IP Alias

☐ Obtain an IP address automatically

Router Name *

Domain Name *

* : Required for some ISPs

☒ **Specify an IP address**

IP Address
 Subnet Mask
 Gateway IP Address

☒ Default MAC Address
☐ Specify a MAC Address
 MAC Address:

DNS Server IP Address
 Primary IP Address
 Secondary IP Address

OK

2. Check if **WAN IP Network Settings** is set appropriately.
3. Check if **IP Address**, **Subnet Mask** and **Gateway** are set correctly (must identify with the values from your ISP) if you choose **Specify an IP address**.

For PPTP Users

1. Check if the **Enable** option for **PPTP Link** is selected.

Internet Access >> PPTP

PPTP Client Mode

PPTP Setup

PPTP Link ☒ Enable ☐ Disable

PPTP Server

ISP Access Setup

Username
 Password

Index(1-15) in [Schedule Setup](#).
 => , , ,

PPP Setup

PPP Authentication PAP or CHAP

☒ Always On

Idle Timeout second(s)

IP Address Assignment Method (IPCP)

Fixed IP ☐ Yes ☒ No (Dynamic IP)

Fixed IP Address

WAN IP Network Settings

☐ Obtain an IP address automatically
☒ Specify an IP address

IP Address
 Subnet Mask

OK

2. Check if **PPTP Server**, **Username**, and **Password** are set correctly (must identify with the values from your ISP).
3. Check if **WAN IP Network Settings** are set properly. If you select **Specify an IP address**, you have to type in the values of **IP Address** and **Subnet Mask** manually. Be sure the values that you type identify with the values from your ISP.

6.5 Backing to Factory Default Setting If Necessary

Sometimes, a wrong connection can be improved by returning to the default settings. Try to reset the router by software or hardware. Such function is available in **Admin Mode** only.



Warning: After pressing **factory default setting**, you will lose all settings you did before. Make sure you have recorded all useful settings before you pressing. The password of factory default is null.

Software Reset

You can reset the router to factory default via Web page.

Go to **System Maintenance** and choose **Reboot System** on the web page. The following screen will appear. Choose **Using factory default configuration** and click **OK**. After few seconds, the router will return all the settings to the factory settings.

[System Maintenance >> Reboot System](#)

Reboot System

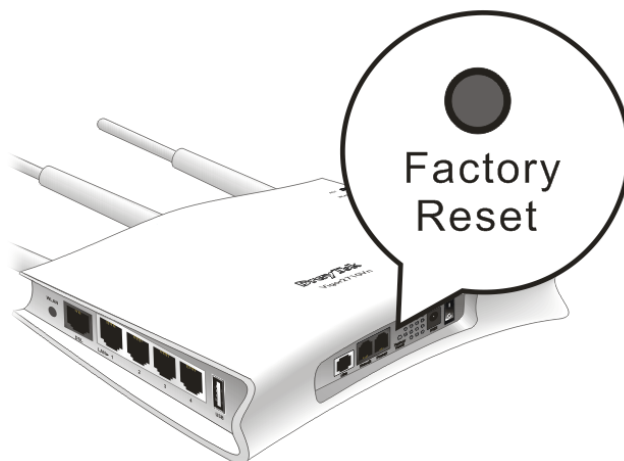
Do you want to reboot your router ?

- ☒ Using current configuration
- ☐ Using factory default configuration

OK

Hardware Reset

While the router is running (ACT LED blinking), press the **Factory Reset** button and hold for more than 5 seconds. When you see the **ACT LED** blinks rapidly, please release the button. Then, the router will restart with the default configuration.



After restore the factory default setting, you can configure the settings for the router again to fit your personal request.

6.6 Contacting Your Dealer

If the router still cannot work correctly after trying many efforts, please contact your dealer for further help right away. For any questions, please feel free to send e-mail to support@draytek.com.