

Vigor2710 Series ADSL2/2+ Firewall Router User's Guide

Version: 1.0 Date: 2008/09/12

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 |
|-----------------------------|--|
| Warranty | conservation of the environment. We warrant to the original end user (purchaser) that the router will be free from any defects in workmanship or materials for a period of two (2) years from the date of purchase from the dealer. Please keep your purchase receipt in a safe place as it serves as proof of date of purchase. During the warranty period, and upon proof of purchase, should the product have indications of failure due to faulty workmanship and/or materials, we will, at our discretion, repair or replace the defective products or components, without charge for either parts or labor, to whatever extent we deem necessary tore-store the product to proper operating condition. Any replacement will consist of a new or re-manufactured functionally equivalent product of equal value, and will be offered solely at our discretion. This warranty will not apply if the product is modified, misused, tampered with, damaged by an act of God, or subjected to abnormal working conditions. The warranty does not cover the bundled or licensed software of other vendors. Defects which do not significantly affect the usability of the product will not be covered by the warranty. We reserve the right to revise the manual and online documentation and to make changes from time to time in the contents hereof without obligation to notify any person of such revision or changes. |
| Be a Registered Owner | Web registration is preferred. You can register your Vigor router via http://www.draytek.com. |
| Firmware & Tools Updates | Due to the continuous evolution of DrayTek technology, all routers will be regularly upgraded. Please consult the DrayTek web site for more information on newest firmware, tools and documents. |
| | http://www.draytek.com |

European Community Declarations

Manufacturer: DrayTek Corp.

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

DrayTek Corp. declares that Vigor2820 Series of routers are in compliance with the following essential requirements and other relevant provisions of R&TTE Directive 1999/5/EEC.

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

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

Regulatory Information

Federal Communication Commission Interference Statement

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

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

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

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

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

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



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

Table of Contents



| Preface | 1 |
|---|--------|
| 1.1 Web Configuration Buttons Explanation | 1 |
| 1.2 LED Indicators and Connectors | 2 |
| 1.2.1 For Vigor2710 1.2.2 For Vigor2710n | 2 4 |
| 1.2.3 For Vigor2710Vn | 6 |
| 1.3 Hardware Installation | 8 |
| 1.4 Printer Installation | 9 |



| 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 |
| 2.4.1 Adjusting Protocol/Encapsulation 2.4.2 PPPoE/PPPoA 2.4.3 1483 Bridged IP 2.4.4 1483 Routed IP | 19 20 21 22 |
| 2.5 Online Status | 23 |
| 2.6 Saving Configuration | 25 |
| | |



| User Mode Operation | 27 |
|---|----------|
| 3.1 Internet Access | 27 |
| 3.1.1 Basics of Internet Protocol (IP) Network 3.1.2 PPPoE/PPPoA | 27 28 |
| 3.2 LAN | 33 |
| 3.2.1 Basics of LAN 3.2.2 General Setup | 33 34 |
| 3.3 NAT | 37 |
| 3.3.1 Port Redirection 3.3.2 DMZ Host 3.3.3 Open Ports | 39 |
| 3.4 Applications | 43 |
| 3.4.1 Dynamic DNS 3.4.2 UPnP | 45 |
| 3.5 Wireless LAN | 47 |

| 3.5.1 Basic Concepts | |
|------------------------|--|
| 3.5.2 General Setup | |
| 3.5.3 Security | |
| 3.5.4 Access Control | |
| 3.5.5 Station List | |
| | |
| 3.6 System Maintenance | |
| 3.6.1 System Status | |
| 3.6.2 User Password | |
| 3.6.3 Time and Date | |
| | |
| • | |
| 3.7 Diagnostics | |
| 3.7.1 DHCP Table | |
| 3.7.2 Ping Diagnosis | |
| 3.7.3 Trace Route | |
| | |



| Admin Mode Operation | 61 |
|--|-----|
| 4.1 Internet Access | 61 |
| 4.1.1 Basics of Internet Protocol (IP) Network 4.1.2 PPPoE/PPPoA 4.1.3 Multi-PVCs | |
| 4.2 LAN | 71 |
| 4.2.1 Basics of LAN 4.2.2 General Setup 4.2.3 Static Route 4.2.4 VLAN 4.2.5 Bind IP to MAC | |
| 4.3 NAT | |
| 4.3.1 Port Redirection4.3.2 DMZ Host4.3.3 Open Ports | |
| 4.4 Firewall | |
| 4.4.1 Basics for Firewall4.4.2 General Setup4.4.3 Filter Setup4.4.4 DoS Defense | |
| 4.5 Objects Settings | 100 |
| 4.5.1 IP Object 4.5.2 IP Group 4.5.3 Service Type Object 4.5.4 Service Type Group 4.5.5 Keyword Object | |
| 4.5.6 Keyword Group 4.5.7 File Extension Object | |
| 4.5.10 Misc Object | 112 |
| 4.6 CSM Profile | |
| 4.6.1 IM/P2P Filter Profile | 114 |

| 4.6.2 URL Content Filter Profile 4.6.3 Web Content Filter Profile | |
|--|-----|
| 4.7 Bandwidth Management | 121 |
| 4.7.1 Sessions Limit | 121 |
| 4.7.2 Bandwidth Limit | |
| 4.7.3 Quality of Service | 124 |
| 4.8 Applications | 131 |
| 4.8.1 Dynamic DNS | |
| 4.8.2 Schedule | |
| 4.8.3 RADIUS 4.8.4 UPnP | |
| 4.8.5 IGMP | |
| 4.8.6 Wake on LAN | |
| 4.9 VPN and Remote Access | 140 |
| 4.9.1 Remote Access Control | 140 |
| 4.9.2 PPP General Setup | |
| 4.9.3 IPSec General Setup | |
| 4.9.4 IPSec Peer Identity | |
| 4.9.5 Remote Dial-in User 4.9.6 LAN to LAN | |
| 4.9.7 Connection Management | |
| C C C C C C C C C C C C C C C C C C C | |
| 4.10 Certificate Management | |
| 4.10.1 Local Certificate | |
| 4.10.2 Trusted CA Certificate 4.10.3 Certificate Backup | |
| | |
| 4.11 Wireless LAN | |
| 4.11.1 Basic Concepts | |
| 4.11.2 General Setup 4.11.3 Security | |
| 4.11.3 Security | |
| 4.11.5 WPS | |
| 4.11.6 WDS | |
| 4.11.7 AP Discovery | |
| 4.11.8 Station List | 1/1 |
| 4.12 System Maintenance | 173 |
| 4.12.1 System Status | |
| 4.12.2 TR-069 | |
| 4.12.3 Administrator Password | |
| 4.12.4 Configuration Backup 4.12.5 Syslog/Mail Alert | |
| 4.12.6 Time and Date | |
| 4.12.7 Management | |
| 4.12.8 Reboot System | |
| 4.12.9 Firmware Upgrade | 182 |
| 4.13 Diagnostics | 183 |
| 4.13.1 Dial-out Trigger | |
| 4.13.2 Routing Table | |
| 4.13.3 ARP Cache Table 4.13.4 DHCP Table | |
| 4.13.5 NAT Sessions Table | |
| 4.13.6 Data Flow Monitor | |
| 4.13.7 Traffic Graph | |
| 4.13.8 Ping Diagnosis | 188 |



| Application and Examples | 191 |
|--|-------|
| 5.1 Create a LAN-to-LAN Connection Between Remote Office and Headquarter | . 191 |
| 5.2 Create a Remote Dial-in User Connection Between the Teleworker and Headquarter | . 198 |
| 5.3 QoS Setting Example | . 202 |
| 5.4 LAN – Created by Using NAT | . 206 |
| 4.5 Upgrade Firmware for Your Router | . 207 |
| 5.6 Request a certificate from a CA server on Windows CA Server | . 210 |
| 5.7 Request a CA Certificate and Set as Trusted on Windows CA Server | . 214 |



| Trouble Shooting | 217 |
|---|-----|
| 6.1 Checking If the Hardware Status Is OK or Not | 217 |
| 6.2 Checking If the Network Connection Settings on Your Computer Is OK or Not | 218 |
| 6.3 Pinging the Router from Your Computer | 220 |
| 6.4 Checking If the ISP Settings are OK or Not | 221 |
| 6.5 Backing to Factory Default Setting If Necessary | 222 |
| 6.6 Contacting Your Dealer | 223 |



Vigor2710 series is an ADSL 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, Vigor2710 series supports USB interface for connecting USB printer to share printer or USB storage device for sharing files. Vigor2710 series provides two-level management to simplify the configuration of network connection. The user operation allows user accessing into WEB interface via simple configuration. However, if users want to have advanced configurations, they can access into WEB interface through administration operation.

1.1 Web Configuration Buttons Explanation

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

| OK | Save and apply current settings. |
|--|--|
| Cancel | Cancel current settings and recover to the previous saved settings. |
| Clear | Clear all the selections and parameters settings, including selection from drop-down list. All the values must be reset with factory default settings. |
| Add | Add new settings for specified item. |
| Edit | Edit the settings for the selected item. |
| Delete | Delete the selected item with the corresponding settings. |
| Note: For the other buttons shown on the web pages, please refer to Chapter 4 for detailed | |

explanation.

1.2 LED Indicators and Connectors

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

1.2.1 For Vigor2710



| LED | Status | Explanation |
|-------------|------------|--|
| ACT | Blinking | The router is powered on and running |
| (Activity) | U | normally. |
| | Off | The router is powered off. |
| CSM | On | The profile(s) of CSM (Content Security |
| | | Management) for IM/P2P, URL/Web |
| | | Content Filter application can be enabled |
| | | from Firewall >> General Setup . (Such |
| | | profile must be established under CSM menu). |
| DSL | On | The router is ready to access Internet |
| DSE | 011 | through DSL link. |
| | Blinking | Slowly: The modem is ready. |
| | U | Quickly: The connection is training. |
| | On | The port is connected. |
| LAN 1/2/3/4 | 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 | Descripti | |
| DSL | | for accessing the Internet through ADSL2/2+. |
| LAN (1-4) | | s for local networked devices. |
| USB | | for USB storage device (Pen Driver/Mobile |
| | HD) or pri | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |





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

1.2.2 For Vigor2710n



| LED | Statua | Evaluation |
|-------------|------------|--|
| | Status | Explanation |
| ACT | Blinking | The router is powered on and running |
| (Activity) | Off | normally. The router is powered off. |
| WLAN | On | Wireless access point is ready. |
| W LAIN | Blinking | It will blink while wireless traffic goes |
| | Dinking | through. |
| DSL | On | The router is ready to access Internet |
| 2.52 | 0.11 | through DSL link. |
| | Blinking | Slowly: The modem is ready. |
| | Ũ | Quickly: The connection is training. |
| | On | The port is connected. |
| LAN 1/2/3/4 | 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 |
| | Dillikilig | for connection about two minutes. |
| Interface | Descripti | |
| WLAN | | utton once to enable (WLAN LED on) or |
| | disable (W | LAN LED off) wireless connection. |
| DSL | Connecter | for accessing the Internet through ADSL2/2+. |
| LAN (1-4) | | s for local networked devices. |
| USB | Connecter | for USB storage (Pen Driver Mobile/HD) or |
| | printer. | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |





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

1.2.3 For Vigor2710Vn



| LED | Status | Explanation |
|---------------|-----------|--|
| ACT | Blinking | The router is powered on and running |
| (Activity) | | normally. |
| | Off | The router is powered off. |
| WLAN | On | Wireless access point is ready. |
| | Blinking | It will blink while wireless traffic goes |
| | | through. |
| DSL | On | The router is ready to access Internet |
| | | through DSL link. |
| | Blinking | Slowly: The modem is ready. |
| | | Quickly: The connection is training. |
| T ANT 1/0/0/4 | On | The port is connected. |
| LAN 1/2/3/4 | 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/ | On | The phone connected to this port is off-hook. |
| Phone2 | 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 | Descripti | |
| WLAN | | utton once to enable (WLAN LED on) or |
| WLAN | | LAN LED off) wireless connection. |
| DSL | ` | , |
| LAN (1-4) | | for accessing the Internet through ADSL2/2+. |
| | | |
| USB | printer. | for USB storage (Pen Driver Mobile/HD) or |
| | printer. | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |





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

1.3 Hardware Installation

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

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



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

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



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

1.4 Printer Installation

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



Printer

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.

| Add Printer Wizard |
|--|
| Local or Network Printer The wizard needs to know which type of printer to set up. |
| Select the option that describes the printer you want to use: |
| Local printer attached to this computer |
| Automatically detect and install my Plug and Play printer |
| A network printer, or a printer attached to another computer To set up a network printer that is not attached to a print server, use the "Local printer" option. |
| < <u>Back</u> <u>Next</u> Cancel |

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**.

| | our printers arrough poils. | can create a |
|-----------|----------------------------------|--------------|
| new port. | LPT1: (Recommended Printer Port) | |
| 600 | | |
| | | - |

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

| Add Standard TCP/IP Printer | Port Wizard 🛛 🔀 |
|---|---|
| Add Port For which device do you wan | t to add a port? |
| Enter the Printer Name or IP a | ddress, and a port name for the desired device. |
| Printer Name or IP <u>A</u> ddress: | 192.168.1.1 |
| Port Name: | IP_192.168.1.1 |
| | |
| | |
| | |
| | |
| | |
| | < <u>B</u> ack Next > Cancel |

7. Click Standard and choose Generic Network Card.

| ldd Standard TCP/IP Printer Port Wizard 🛛 🛛 🔀 |
|--|
| Additional Port Information Required The device could not be identified. |
| The detected device is of unknown type. Be sure that: 1. The device is properly configured. 2. The address on the previous page is correct. Either correct the address and perform another search on the network by returning to the previous wizard page or select the device type if you are sure the address is correct. Device Type |
| Standard Generic Network Card |
| < <u>B</u> ack Next Cancel |

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.

| 💕 Brother HL-1070 Properti | es 🔹 🛛 🛛 🛛 |
|--|------------------------------------|
| General Sharing Ports Advar | nced Device Settings |
| Brother HL-1070 | |
| Print to the following port(s). Docur checked port. | ments will print to the first free |
| Port Description | Printer 🔥 |
| □ 3.250 Standard TCP/IP P □ IP_1 Standard TCP/IP P | |
| □ IP_1 Standard TCP/IP P □ IP_1 Standard TCP/IP P | ort |
| IP_1 Standard TCP/IP P | |
| IP_1 Standard TCP/IP P | |
| PDF Local Port | PDF995 |
| Add Port | elete Port |
| Enable bidirectional support ✓ Enable printer pooling | |
| | OK Cancel Apply |

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.

| ort Name: | IP 192,168.1.1 |
|----------------------------------|----------------|
| rinter Name or IP <u>A</u> ddres | s: 192.168.1.1 |
| Protocol O <u>R</u> aw | (O LPR |
| Raw Settings | |
| Port Number: | 9100 |
| LPR Settings | |
| Queue Name: | p1 |
| LPR Byte Counting E | nabled |
| SNMP Status Enable | ed |
| Community Name: | public |
| SNMP Device Index: | 1 |

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

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



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

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.
 - V

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. | Dray Tek |

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



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

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

| ſ | Auto Logout 🔽 |
|---|---------------|
| ſ | Auto Loqout 💦 |
| ſ | Off 👘 |
| l | 1 min |
| l | 3 min 🗧 |
| l | 5 min |
| l | 10 min |

2.3 Changing Password

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

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

| Vigor271 ADSL2/2 | 0 Series + Firewall Router | | Dray Tek www.draytek.com | |
|---|---|---|--|---|
| Auto Logout V Quick Start Wizard Online Status Internet Access LAN NAT Firewall Objects Setting CSM Bandwidth Management Applications VPN and Remote Access Certificate Management Wireless LAN System Maintenance Diagnostics | MAC Address 1st IP Address 1st Subnet Mask DHCP Server | : Vigo12710 series : 3.2.1_RC11 : Aug 5 2008 18:07:02 : 211801_A Annex A : 00-50-7F-92-F5-00 : 192.166.1.5 : 255.255.255.0 : Yes : 194.109.6.66 | Link Status MAC Address Connection IP Address Default Gateway MAC Address Frequency Domain Firmware Version SSID | WAN : Disconnected : 00-50-7F-92-F5-01 : PPPoE : |
| Logout All Rights Reserved. v Admin mode Status: Ready | 2 | | | |

Main screen for admin mode operation (full configuration)

| Auto Logout 👻 | System Status | | | |
|---|--|--|---|--|
| Quick Start Wizard Online Status Internet Access I AN | Model Name Firmware Version Build Date/Time ADSL Firmware Version | : Vigor2710 series : 3.2.1_RC11 : Aug 6 2008 18:07:02 : 211801_A Annex A | | |
| NAT | | LAN | i | WAN |
| Applications Wireless LAN System Maintenance Diagnostics | MAC Address 1st IP Address 1st Subnet Mask DHCP Server DNS | : 00-50-7F-92-F5-00 : 192.168.1.5 : 255.255.255.0 : Yes : 194.109.6.66 | Link Status MAC Address Connection IP Address Default Gateway | : Disconnected : 00-50-7F-92-F5-01 : PPPoE : : |
| | | | Wir | eless LAN |
| | | | MAC Address Frequency Domain Firmware Version SSID | : 00-50-7f-92-f5-00 : Europe : 1.8.1.0 : DrayTek |

Main screen for user mode operation (simple configuration)

System Maintenance >> Administrator Password Setup

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.

| | Old Password | | | |
|-------------------------------|--------------------------------------|----|-------------|--|
| | New Password | | | |
| | Confirm Password | | | |
| | | 0 | K | |
| | | | | |
| | | or | | |
| ystem Mainter | nance >> User Passwo | | ······ | |
| | nance >> User Passwo | | ·· <u>·</u> | |
| | nance >> User Passwo Old Password | | | |
| ystem Mainter ser Password | | | | |

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

| Username Password | |
|--|-----------------|
| | Login |
| Copyright©, DrayTek Corp. All Rights Reserved. | Dray Tek |

2.4 Quick Start Wizard

Notice: Quick Start Wizard for user operation is the same as for administrator's 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

| ig as your Password (Max 23 characters). |
|--|
| |
| ••• |
| ••• |
| |
| |
| |
| |
| |
| |
| |
| _ |

In the **Quick Start Wizard**, you can configure the router to access the Internet with different protocol/modes such as **PPPoE**, **PPPoA**, **Bridged IP**, **or Routed IP**. The router supports the

2.4.1 Adjusting Protocol/Encapsulation

In the **Quick Start Wizard**, you can configure the router to access the Internet with different protocol/modes such as **PPPoE**, **PPPoA**, **Bridged IP**, **or Routed IP**. The router supports the ADSL WAN interface for Internet access.

| nnect to Internet | |
|--------------------------|----------------------|
| VPI | 0 Auto detect |
| VCI | 35 |
| Protocol / Encapsulation | PPPoA VC MUX |
| Fixed IP | ○Yes ④No(Dynamic IP) |
| IP Address | |
| Subnet Mask | |
| Default Gateway | |
| Primary DNS | |
| Second DNS | |

Now, you have to select an appropriate WAN connection type for connecting to the Internet through this router according to the settings that your ISP provided.

| VPI | Stands for Virtual Path Identifier . It is an 8-bit header inside each ATM cell that indicates where the cell should be routed. The ATM, is a method of sending data in small packets of fixed sizes. It is used for transferring data to client computers. | | |
|------------------------|---|--|--|
| VCI | Stands for Virtual Channel Identifier. It is a 16-1 ATM cell's header that indicates the cell's next de travels through the network. A virtual channel is a connection between two end devices on the netwo | | |
| Protocol/Encapsulation | Select an IP mode for this WA available modes for Internet ac Bridged IP and Routed IP . | | |
| | Protocol / Encapsulation | 1483 Bridged IP LLC | |
| | ·····, _···p·· | PPPoE LLC/SNAP | |
| | Fixed IP | PPP0E VC MUX PPP0A LLC/SNAP | |
| | IP Address | PPPoA VC MUX | |
| | Subnet Mask | 1483 Bridged IP LLC 1483 Routed IP LLC | |
| | | 1483 Bridged IP VC-Mux | |
| | Default Gateway | 1483 Routed IP VC-Mux (IPoA) 1483 Bridged IP (IPoE) | |
| | Primary DNS | | |
| Fixed IP | (Dynamic IP) to allow the rou | for the router. Otherwise, click No ter choosing a dynamic IP. If you ddress, Subnet Mask and Default | |
| IP Address | Assign an IP address for the protocol that you select. | | |
| Subnet Mask | | r the protocol of Routed IP and | |

| Default Gateway | Assign an IP address to the gateway for the protocol of Routed IP and Bridged IP . |
|-----------------|--|
| Primary DNS | Assign an IP address to the primary DNS. |
| Second DNS | Assign an IP address to the secondary DNS. |

2.4.2 PPPoE/PPPoA

Quick Start Wizard

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:

| Set PPPoE / PPPoA | | | | | |
|-------------------|---------------|---------------------|-------------|--------------|--------|
| User Name | | | | | |
| Password | | | | | |
| Confirm Password | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | < Back | Next > | Finish | Cancel |
| User Name | Assign a spec | cific valid user na | ame provide | ed by the IS | SP. |
| Password | Assign a vali | d password prov | ided by the | ISP. | |

Confirm Password Retype the password.

Click Next for viewing summary of such connection.

Quick Start Wizard

| se confirm your settings: | |
|---------------------------|---|
| VPI: | 0 |
| VCI: | 33 |
| Protocol / Encapsulation: | PPPoE / LLC |
| Fixed IP: | No |
| Primary DNS: | |
| Secondary DNS: | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | <pre>< Back Next > Finish Can</pre> |

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

2.4.3 1483 Bridged IP

Quick Start Wizard

Click **1483 Bridged IP** as the protocol. Type in all the information that your ISP provides for this protocol.

| nnect to Internet | |
|--------------------------|------------------------|
| VPI | 0 Auto detect |
| VCI | 35 |
| Protocol / Encapsulation | 1483 Bridged IP LLC |
| Fixed IP | ◯ Yes ③ No(Dynamic IP) |
| IP Address | |
| Subnet Mask | |
| Default Gateway | |
| Primary DNS | |
| Second DNS | |

Click Next for viewing summary of such connection.

Quick Start Wizard

| e confirm your settings: | |
|---------------------------|--|
| VPI: | 0 |
| VCI: | 33 |
| Protocol / Encapsulation: | 1483 Bridge LLC |
| Fixed IP: | No |
| Primary DNS: | |
| Secondary DNS: | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | <pre>< Back Next > Finish Ca</pre> |

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

2.4.4 1483 Routed IP

Click **1483 Routed IP** as the protocol. Type in all the information that your ISP provides for this protocol.

| Quick Start Wizard | |
|--------------------------|-----------------------------|
| Connect to Internet | |
| VPI | 0 Auto detect |
| VCI | 33 |
| Protocol / Encapsulation | 1483 Routed IP LLC |
| Fixed IP | |
| | ⊙Yes ⊙No(Dynamic IP) |
| IP Address | |
| Subnet Mask | |
| Default Gateway | |
| Primary DNS | |
| Second DNS | |
| | |
| 2 | |
| | < Back Next > Finish Cancel |

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

Quick Start Wizard

| e confirm your settings: | |
|---------------------------|----------------|
| VPI: | 0 |
| VCI: | 33 |
| Protocol / Encapsulation: | 1483 Route LLC |
| Fixed IP: | No |
| Primary DNS: | |
| Secondary DNS: | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |

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

2.5 Online Status

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

Online status for PPPoE

Online Status

| System Status | | | | | Syster | n Uptime: 0:1:58 |
|------------------|-----------|------------|--------------|--------------|-------------------|----------------------|
| Primary | 1 | Secondary | | | | |
| LAN Status | | Primary | DNS: 168.95 | .192.1 | Secondary DN | S: 168.95.1.1 |
| IP Address | ТХ Р | ackets | RX Pac | kets | | |
| 192.168.1.5 | 404 | | 391 | | | |
| WAN 1 Status | | | | | | >> Drop PPPoE |
| Enable | Line | | Name | Mode | Up Time | |
| Yes | ADSL | | | PPPoE | 0:01:29 | |
| IP | GW IP | | TX Packets | TX Rate(Bps) | RX Packets | RX Rate(Bps) |
| 61.230.203.119 | 61.230.19 | 2.254 | 38 | 15 | 39 | 40 |
| ADSL Information | (ADSL | . Firmware | Version: 211 | 801_A) | | |
| ATM Statistics | TX Blocks | R | X Blocks | Corrected | Blocks Unco | rrected Blocks |
| | 63 | 3 | 53 | 6 | 1 | |
| ADSL Status Mo | de Stat | e | Up Speed | Down Speed | SNR Margin | Loop Att. |
| G.D | MT SHO | WTIME | 256000 | 2048000 | 23 | 31 |

Online status for Static IP

Online Status

| System Status | | | | System | 1 Uptime: 0:1:10 |
|-----------------|---------------------------|-------------------|--------------|-------------------|-------------------|
| Prima | ry | Second | ary | | |
| LAN Status | Prin | nary DNS: 194.10 | 9.6.66 | Secondary DNS | 168.95.1.1 |
| IP Address | TX Packe | ts RX Pac | kets | | |
| 192.168.1.5 | 585 | 500 | | | |
| WAN 1 Status | | | | | |
| Enable | Line | Name | Mode | Up Time | |
| Yes | ADSL | | Static IP | 0:00:28 | |
| IP | GW IP | TX Packets | TX Rate(Bps) | RX Packets | RX Rate(Bps) |
| 192.168.33.12 | 192.168.33.1 | 2 | 4 | 1 | 9 |
| ADSL Informatio | n (ADSL Firm | ware Version: 211 | .801_A) | | |
| ATM Statistics | TX Blocks | RX Blocks | Corrected | l Blocks Unco | rrected Blocks |
| | 6 | 9 | 0 | 18 | |
| ADSL Status M | ode State | Up Speed | Down Speed | SNR Margin | Loop Att. |
| | OSL2+ S.992.5) SHOWTIM | IE 1026000 | 22215000 | 6 | 0 |

Online status for DHCP

Online Status

| System Status | | | | | Syste | m Uptime: 0:6:32 |
|------------------|---------------------|-----------|--------------|--------------|-------------------|----------------------|
| Primary | Secondary | | | | | |
| LAN Status | | Primary I | DNS: 192.16 | 8.33.1 | Secondary DN | S: 168.95.1.1 |
| IP Address | TX P | ackets | RX Pac | kets | | |
| 192.168.1.5 | 3710 | | 2863 | | | |
| WAN 1 Status | | | | | | >> <u>Release</u> |
| Enable | Line | | Name | Mode | Up Time | |
| Yes | ADSL | | | DHCP Client | 0:00:00 | |
| IP | GW IP | | TX Packets | TX Rate(Bps) | RX Packets | RX Rate(Bps) |
| 192.168.33.12 | 192.168.33 | 3.1 | 1 | 9 | 1 | 35 |
| ADSL Information | (ADSL | Firmware | Version: 211 | 801_A) | | |
| ATM Statistics | TX Blocks | R | (Blocks | Corrected | d Blocks Unc | orrected Blocks |
| | 19 | 21 | L | 0 | 8 | |
| ADSL Status Mo | de Stat | e | Up Speed | Down Speed | SNR Margin | Loop Att. |
| | 5L2+ 992.5) SHOV | NTIME | 1036000 | 22448000 | 6 | 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. |
| WAN1 Status | |
| Line | Displays the physical connection (Ethernet) of this interface. |
| Name | Displays the name set in WAN1/WAN web page. |

| Mode | Displays the type of WAN connection (e.g., PPPoE). | | | |
|--|---|--|--|--|
| Up Time | Displays the total uptime of the interface. | | | |
| IP | Displays the IP address of the WAN interface. | | | |
| GW IP | Displays the IP address of the default gateway. | | | |
| TX Packets | Displays the total transmitted packets at the WAN interface. | | | |
| TX Rate | Displays the speed of transmitted octets at the WAN interface. | | | |
| RX Packets | Displays the total number of received packets at the WAN interface. | | | |
| RX Rate | Displays the speed of received octets at the WAN interface. | | | |
| Note: The words in green mean that the WAN connection of that interface (WAN1) is ready for accessing Internet; the words in red mean that the WAN connection of that interface (WAN1) is not ready for accessing Internet. | | | | |

2.6 Saving Configuration

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

Admin mode 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.

| Vigor271 ADSL2/2 | O Series + Firewall Router | | | Dray Tek www.draytek.com |
|--|--|--|---|--|
| Auto Logout 👻 | System Status | | | |
| Quick Start Wizard down of the Status down of the S | Model Name Firmware Version Build Date/Time ADSL Firmware Version | : Vigo12710 series : 3.2.1_RC11 : Aug 6 2008 18:07:02 : 211801_A Annex A | | |
| NAT | | LAN | | WAN |
| Applications Wireless LAN System Maintenance Diagnostics | MAC Address 1st IP Address 1st Subnet Mask DHCP Server DNS | : 00-50-7F-92-F5-00 : 192.168.1.5 : 255.255.255.0 : Yes : 194.109.6.66 | Link Status MAC Address Connection IP Address Default Gateway | : Disconnected : 00-50-7F-92-F5-01 : PPPoE : : |
| | | | Wir | eless LAN |
| | | | MAC Address Frequency Domain Firmware Version SSID | : 00-50-7f-92-f5-00 : Europe : 1.8.1.0 : DrayTek |
| Logout All Rights Reserved. User mode Status: Ready | | | | |

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.

Internet Access

PPPoE / PPPoA

MPoA (RFC1483/2684)

3.1.2 PPPoE/PPPoA

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

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

Internet Access >> PPPoE / PPPoA

| DDDoE | / PPPoA | Ollowt | Mode |
|--------|---------|--------|------|
| PPPUE, | / PPPUA | Glient | Moue |

| PPPoE/PPPoA Client | 💿 Enable i 🔘 Disable | ISP Access Setup | [] |
|--|--|--|-----------------|
| VPI VCI Encapsulating Type Protocol | Channel 1 🖌 0 33 LLC/SNAP 🔨 PPPoE 💙 Multimode 💙 | ISP Name Username Password PPP Authentication ✓ Always On Idle Timeout IP Address From ISP Fixed IP | .7F :92 .F5 .01 |

ΟK

| Enable/Disable | Click Enable for activating this function. If you click Disable , this function will be closed and all the settings that you adjusted in this page will be invalid. |
|--------------------|--|
| DSL Modem Settings | Set up the DSL parameters required by your ISP. These are vital for building DSL connection to your ISP. Multi-PVC channel - The selections displayed here are determined by the page of Internet Access – Multi PVCs. Select M-PVCs Channel means no selection will be chosen. VPI - Type in the value provided by ISP. VCI - Type in the value provided by ISP. Encapsulating Type - Drop down the list to choose the type provided by ISP. Protocol - Drop down the list to choose the one provided by ISP. If you have already used Quick Start Wizard to set the protocol, then it is not necessary for you to change any settings in this group. |
| PPPoE Pass-through | The router offers PPPoE dial-up connection. Besides, you also can establish the PPPoE connection directly from local clients to your ISP via the Vigor router. When PPPoA protocol is selected, the PPPoE package transmitted by PC will be transformed into PPPoA package and sent to WAN server. Thus, the PC can access Internet through such direction. For Wired LAN – If you check this box, PCs on the same network can use another set of PPPoE session (different with the Host PC) to access into Internet. For Wireless LAN – If you check this box, PCs on the same wireless network can use another set of PPPoE session (different with the Host PC) to access into Internet. |

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

Username – Type in the username provided by ISP in this field. **Password** – Type in the password provided by ISP in this field. **PPP Authentication** – Select **PAP only** or **PAP or CHAP** for PPP.

Idle Timeout – Set the timeout for breaking down the Internet after passing through the time without any action. This setting is active only when the **Active on demand** option for Active Mode is selected in **WAN>> General Setup** page.

IP Address From ISP Usually ISP dynamically assigns IP address to you each time you connect to it and request. In some case, your ISP provides service to always assign you the same IP address whenever you request. In this case, you can fill in this IP address in the Fixed IP field. Please contact your ISP before you want to use this function. 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. Type the additional WAN IP address and check the Enable box. Then click OK to exit the dialog.



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

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

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

Index (1-15) in Schedule Setup - You can type in four sets of time schedule for your request. All the schedules can be set previously in **Applications – Schedule** web page and you can use the number that you have set in that web page.
After finishing all the settings here, please click **OK** to activate them.

MPoA

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

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

| MPoA (RFC1483/2684) 🔿 Enable 💿 Disable | | WAN IP Network Settings | | | |
|--|--------------------|-------------------------|---------------------------|--|--|
| | | — Obtain an IP addres | ss automatically | | |
| DSL Modem Setting | | Router Name | , | | |
| Multi-PVC channel Channel 1 💌 Encapsulation | | Domain Name | | | |
| | | *: Required for some I | *: Required for some ISPs | | |
| | 483 Bridged IP LLC | Specify an IP addre | ss VVAN IP Alias | | |
| VPI | 0 | IP Address | 0.0.0.0 | | |
| VCI | 33 | Subnet Mask | 0.0.0.0 | | |
| Modulation | Multimode 💙 | Gateway IP Address | 0.0.0.0 | | |
| RIP Protocol | | | | | |
| Enable RIP | | O Default MAC Address | Oefault MAC Address | | |
| | | — 🔘 Specify a MAC Addro | ess | | |
| Bridge Mode | | MAC Address: 00 .5 | D .7F 92 .F5 .01 | | |
| 📃 Enable Bridge Moo | de | | | | |
| | | DNS Server IP Address | 5 | | |
| | | Primary IP Address | | | |
| | | Secondary IP Address | | | |

Internet Access >> MPoA (RFC1483/2684)

MPoA (RFC1483/2684) Click Enable for activating this function. If you click Disable, this function will be closed and all the settings that you adjusted in this page will be invalid.

| DSL Modem Settings | Set up the DSL parameters required by your ISP. These are vital for building DSL connection to your ISP. Multi-PVC channel - The selections displayed here are determined by the page of Internet Access – Multi PVCs. Select M-PVCs Channel means no selection will be chosen. Encapsulating Type - Drop down the list to choose the type provided by ISP. VPI - Type in the value provided by ISP. VCI - Type in the value provided by ISP. |
|--------------------|--|
| RIP Protocol | Routing Information Protocol is abbreviated as RIP (RFC1058) specifying how routers exchange routing tables information. Click Enable RIP for activating this function. |
| Bridge Mode | If you choose Bridged IP as the protocol, you can check this box to invoke the function. The router will work as a bridge modem. |

WAN IP Network Settings

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

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

Router Name – Type in the router name provided by ISP. **Domain Name** – Type in the domain name that you have assigned. **Specify an IP address** – Click this radio button to specify some data.

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. Type the additional WAN IP address and check the Enable box. Then click OK to exit the dialog.



IP Address – Type in the private IP address.

Subnet Mask – Type in the subnet mask.

Gateway IP Address – Type in gateway IP address.

Default MAC Address Type in MAC address for the router. You can use **Default MAC Address** or specify another MAC address for your necessity.

MAC Address – Type in the MAC address for the router manually.

DNS Server IPType in the primary IP address for the router. If necessary, type in
secondary IP address for necessity in the future.

3.2 LAN

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



3.2.1 Basics of LAN

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



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

| LAN IP Network Configuration | | DHCP Server Configura | DHCP Server Configuration | | |
|------------------------------|------------------------|-------------------------|----------------------------------|--|--|
| For NAT Usage | | 💿 Enable Server 🔘 Disa | ⊙ Enable Server ◯ Disable Server | | |
| 1st IP Address | 192.168.1.1 | Relay Agent: 🔘 1st Subr | net 🔾 2nd Subnet | | |
| 1st Subnet Mask | 255.255.255.0 | Start IP Address | 192.168.1.10 | | |
| For IP Routing Usage 🔘 | Enable 💿 Disable | IP Pool Counts | 50 | | |
| 2nd IP Address | 192.168.2.1 | Gateway IP Address | 192.168.1.1 | | |
| 2nd Subnet Mask | 255.255.255.0 | DHCP Server IP Address | | | |
| | 2nd Subnet DHCP Server | for Relay Agent | | | |
| | | DNS Server IP Address | | | |
| RIP Protocol Control | Disable 💙 | 🔲 Force DNS manual se | tting | | |
| | | Primary IP Address | | | |
| | | Secondary IP Address | | | |

1st IP AddressType in private IP address for connecting to a local private network
(Default: 192.168.1.1).1st Subnet MaskType 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 . |
|-----------------------------|--|
| 2 nd IP Address | Type in secondary IP address for connecting to a subnet. (Default: 192.168.2.1/24) |
| 2 nd Subnet Mask | An address code that determines the size of the network. (Default: 255.255.255.0/24) |
| 2 nd DHCP Server | You can configure the router to serve as a DHCP server for the |

2nd subnet.

| nd DHCP Se Start IP A IP Pool Co | ddress | |
|--|--------------------------------------|--|
| Index | Matched MAC Address given IP Address | |
| | | |
| | | |
| | | |
| MAC Addre | Add Delete Edit Cancel | |
| | OK Clear All 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

| Disable 🛛 👻 |
|-------------|
| Disable |
| 1st Subnet |
| 2nd Subnet |

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

| l. The etwork so l user |
|--|
| l that you t have a |
| o other than o redirect the ery host in o every host subnet that the DHCP |
| for the f the 1st IP dress must 54. hat you efault is 50 address for st IP address eway. P address of ent can help |
| host must friendly, DNS nt IP |
| e DNS e Internet IP address more than uter will 4.109.6.66 NS server IP e than one will address: |
| o suth ff d 5 h ff as seven h f I n e III 1 u 4 N e w |

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

| System Status | | | System Uptime: 0:54:34 |
|---------------|------------|------------------|---------------------------|
| Primary | | Secondary | |
| LAN Status | Primary D | NS: 194.109.6.66 | Secondary DNS: 168.95.1.1 |
| IP Address | TX Packets | RX Packets | |
| 192.168.1.1 | 1311 | 1221 | |

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

| Index | Service Name | Public Port | Private IP | Status |
|------------|--------------|-------------|------------|--------|
| <u>1.</u> | | | | x |
| <u>2.</u> | | | | х |
| <u>3.</u> | | | | х |
| <u>4.</u> | | | | x |
| <u>5.</u> | | | | × |
| <u>6.</u> | | | | х |
| <u>7.</u> | | | | х |
| <u>8.</u> | | | | х |
| <u>9.</u> | | | | × |
| <u>10.</u> | | | | × |

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

NAT >> Port Redirection

| Index No. 1 | |
|--------------|--------------|
| 🗌 Enable | |
| Mode | Single 💌 |
| Service Name | Single Range |
| 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.

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

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

| NAT | >> | DMZ | Host | Setup |
|-----|----|-----|-------|-------|
| | | | 11000 | outap |

NAT >> DMZ Host Setup

| AN 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 turne be always on. | d on, it will force the router's WAN connection to |

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

ΟK

| MZ Host | Setup | | | |
|---------|--------|--------------|------------|-----------|
| WAN 1 | | | | |
| Index | Enable | Aux. WAN IP | Private IP | |
| 1. | | 192.168.1.55 | | 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.

| WAN 1 Index | Enable | Aux. WAN IP | Private IP | |
|----------------|---------------------|--------------|--------------|-----------|
| 1. | ✓ | 192.168.1.55 | 192.168.1.10 | 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

| Index | Comment | Local IP Address | Status |
|-----------|---------|------------------|--------|
| <u>1.</u> | | | × |
| <u>2.</u> | | | × |
| <u>3.</u> | | | × |
| <u>4.</u> | | | × |
| <u>5.</u> | | | × |
| <u>6.</u> | | | × |
| <u>7.</u> | | | × |
| <u>8.</u> | | | × |
| <u>9.</u> | | | × |
| 10. | | | × |

| 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 | | | P2P | P2P | | | |
| 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 |
| з. | 💙 | 0 | 0 | 8. | 💙 | 0 | 0 |
| 4. | 💌 | 0 | 0 | 9. | 🚩 | 0 | 0 |
| 5. | 💙 | 0 | 0 | 10. | 💙 | 0 | 0 |

Clear

Cancel

OK

| 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.

| Applications | |
|--------------|--|
| Dynamic DNS | |
| ▶ UPnP | |

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 Enable Dynamic DNS S | etup | View Log | t to Factory Default Force Update |
|--|--------------|----------|--------------------------------------|
| Accounts: | | | |
| Index | Domain Name | | Active |
| <u>1.</u> | | | × |
| <u>2.</u> | | | × |
| <u>3.</u> | | | × |
| | | | |
| | 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*.

| ndex : 1 | 2 Account |
|----------------------|-------------------------------------|
| Z Enable Dynamic DNS | Account |
| Service Provider | dyndns.org (www.dyndns.org) 🛛 👻 |
| Service Type | Dynamic 💌 |
| Domain Name | chronic6853 dyndns.info dyndns.info |
| Login Name | chronic6853 (max. 64 characters) |
| Password | (max. 23 characters) |
| 🔲 Wildcards | |
| 🔲 Backup MX | |
| Mail Extender | |

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

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

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

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

Disable the Function and Clear all Dynamic DNS Accounts

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

Delete a Dynamic DNS Account

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

3.4.2 UPnP

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

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.

| eneral | Services |
|--|--|
| Connect to the Internet using: | Select the services running on your network that Internet users can access. |
| IP Broadband Connection on Router | Services |
| This connection allows you to connect to the Internet through a shared connection on another computer. | □ Ftp Example ☑ msnmsgr (192.168.29.11:13135) 60654 UDP ☑ msnmsgr (192.168.29.11:7824) 13251 UDP ☑ msnmsgr (192.168.29.11:8789) 63231 TCP |
| Settings | Add Edit Delete |

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 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.

| Wireless LAN | |
|----------------|--|
| General Setup | |
| Security | |
| Access Control | |
| Station List | |

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

| Gener | al Setting (IEEE 802.11) | |
|-------|--|--|
| 🗹 En | able Wireless LAN | |
| | Mode : | Mixed(11b+11g+11n) 💌 |
| | Index(1-15) in <u>Schedule</u> Setup: | |
| | | e action "Force Down" are applied to the WLAN, all |
| | 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 bein Long Preamble: necessary for son | ng scanned. ne older 802.11b devices only (lowers performance). |
| | | OK Cancel |

| Enable Wireless LAN | Che |
|---------------------|-----|
| Mode | Atr |

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) |
|-------------|---|
| Index(1-15) | Set the wireless LAN to work at certain time interval only. You may choose up to 4 schedules out of the 15 schedules pre-defined in Applications >> Schedule setup. The default setting of this filed is blank and the function will always work. |
| 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. |
| | Channel: Channel 6, 2437MHz Auto Channel 1, 2412MHz Channel 2, 2417MHz Channel 3, 2422MHz Channel 4, 2427MHz Channel 6, 2437MHz Channel 6, 2437MHz Channel 7, 2442MHz Channel 8, 2447MHz |

Packet-OVERDRIVEThis 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,

Channel 9, 2452MHz Channel 10, 2457MHz Channel 11, 2462MHz Channel 12, 2467MHz Channel 13, 2472MHz

| Figor N61 802.11n Wireless USB Adapter Utility | | | X |
|---|--|---|---|
| Configuration Status Option About General Setting ✓ Auto launch when Windows start up Remember mini status gostion Auto hide mini status Set mini status always on top Enable IP Setting and Proxy Setting in Profile Group Roaming Ad-hoc | Advance Setting Disable Radio Eragmentation Threshold : RTS Threshold : Frequency : Ad-hoc Channel: Poyer Save Mode: | 2346 2347 802.11b/g/n - 2.4GH ♥ 1 ♥ Disable ♥ | |
| WLAN type to connect Infrastructure and Ad-hoc network Infrastructure network only Ad-hoc network only Ad-hoc network only Automatically connect to non-preferred networks | Tx <u>B</u> ust : | Distor | |

Hide SSIDCheck 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 PreambleThis option is to define the length of the sync field in an
002.11

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.

| urity Settings | | |
|------------------|--|--|
| Mode: | Disable | ¥ |
| WPA: | | |
| Encryption Mode: | ТКІР | |
| Pre-Shared K | (ey(PSK): | |
| | SCII character or 64 Hexadeo ' or "0x655abcd". | cimal digits leading by "Ox", for example |
| WEP: | | |
| Encryption M | 1ode: 64-Bit 🔽 | |
| | ******** | |
| | ******* | |
| ○Key 2 : | | |
| ○Кеу 3 : | ********** | |
| ○Кеу 4: | ********* | |
| | | s leading by "0x", for example +14243". |
| | | Cancel |
| le | There are seve | eral modes provided for you to choose. |
| | Mode: | Disable |
| | | Disable WEP WPA/PSK WPA2/PSK Mixed(WPA+WPA2)/PSK |
| | Disable - Tur | WEP WPA/PSK WPA2/PSK <u>Mixed(WPA+WPA2)/PSK</u> n off the encryption mechanism. |
| | Disable - Tur WEP- Accept | WEP WPA/PSK WPA2/PSK <u>Mixed(WPA+WPA2)/PSK</u> n off the encryption mechanism. s only WEP clients and the encryption k |
| | Disable - Tur WEP- Accept should be ente | WEP WPA/PSK WPA2/PSK <u>Mixed(WPA+WPA2)/PSK</u> n off the encryption mechanism. s only WEP clients and the encryption k ered in WEP Key. |
| | Disable - Tur WEP- Accept should be ente WPA/PSK- A | WEP WPA/PSK WPA2/PSK <u>Mixed(WPA+WPA2)/PSK</u> n off the encryption mechanism. s only WEP clients and the encryption k ered in WEP Key. |
| | Disable - Tur WEP- Accept should be ente WPA/PSK- A key should be | WEP WPA/PSK WPA2/PSK <u>Mixed(WPA+WPA2)/PSK</u> n off the encryption mechanism. s only WEP clients and the encryption k ered in WEP Key. Accepts only WPA clients and the encryp |
| | Disable - Tur WEP-Accept should be ente WPA/PSK-A key should be WPA2/PSK-, encryption ke | WEP WPA/PSK WPA2/PSK Mixed(WPA+WPA2)/PSK s only WEP clients and the encryption k ered in WEP Key. Accepts only WPA clients and the encryp entered in PSK. Accepts only WPA2 clients and the sy should be entered in PSK. |
| | Disable - Tur WEP-Accept should be ente WPA/PSK-A key should be WPA2/PSK- encryption ke Mixed (WPA | WEP WPA/PSK WPA2/PSK Mixed(WPA+WPA2)/PSK n off the encryption mechanism. s only WEP clients and the encryption k ered in WEP Key. Accepts only WPA clients and the encrypt entered in PSK. Accepts only WPA2 clients and the sy should be entered in PSK. Accepts WPA and WF |
| | Disable - Tur WEP-Accept should be ente WPA/PSK-A key should be WPA2/PSK- encryption ke Mixed (WPA | WEP WPA/PSK WPA2/PSK Mixed(WPA+WPA2)/PSK n off the encryption mechanism. s only WEP clients and the encryption ke ered in WEP Key. Accepts only WPA clients and the encrypt entered in PSK. Accepts only WPA2 clients and the should be entered in PSK. Accepts WPA and WF aneously and the encryption key should be |

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:

| 64-Bit | * |
|----------|-----|
| 64-Bit | |
| 128-Bit | |
| a como V | UD. |

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

Wireless LAN >> 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.

| s Control | | | |
|----------------------------|-----------------|----------------|--|
| Policy : | Activate MAC ad | dress filter 👻 | |
| | MAC Address Fi | lter | |
| Index Attribut | e MAC Address | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| Client's MAC / | Address : : : : | | |
| Client's MAC / | Address : : : : | | |
| Client's MAC / | | | |
| Client's MAC / [Add | Attribute : | on from LAN | |

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

WEP

Policy

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

3.5.5 Station List

Add

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

| | Status | MAC Address | Associated with | |
|-------|---------------------------------------|-----------------------------|---|---------|
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | Refresh | | |
| _ | t atus Codes : : Connected, | No encryption. | | |
| | Connected, ' Connected, ' | | | |
| A | Connected, | | | |
| N | : Connecting. | NPA/PSK authentication. | | |
| | | | | |
| tu | | ut notice. In that case, it | iter successfully, it may be will still be on the list until the | |
| A | dd to <u>Access</u> | Control : | | |
| cl | ient's MAC ad | dress :::: | | |
| | | Add |] | |
| fresh | | Click | this button to refresh the status of | of stat |

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.

| System Maintenance |
|--------------------|
| System Status |
| User Password |
| Time and Date |
| Reboot System |

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 Firmware Version Build Date/Time ADSL Firmware Version : Vigor2710 series : 3.2.1_RC7 : Jul 11 2008 17:03:59 : 211801_A Annex A

| | LAN | | WAN |
|-----------------|---------------------|-----------------|---------------------|
| MAC Address | : 00-50-7F-92-F5-00 | Link Status | : Disconnected |
| 1st IP Address | : 192.168.1.5 | MAC Address | : 00-50-7F-92-F5-01 |
| 1st Subnet Mask | : 255.255.255.0 | Connection | : PPPoE |
| DHCP Server | : Yes | IP Address | : |
| DNS | : 194.109.6.66 | Default Gateway | : |

| Wireless LAN | | |
|------------------|---------------------|--|
| MAC Address | : 00-50-7f-92-f5-00 | |
| 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. |
| 1 st IP Address | Display the IP address of the LAN interface. |
| 1 st 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

| Old Password | |
|------------------|--|
| New Password | |
| Confirm Password | |

ΟK

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

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

3.6.3 Time and Date

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

System Maintenance >> Time and Date

| Current System Time 20 | 000 Jan 1 Sat 1 : 54 : 44 Inquire Time |
|----------------------------|---|
| Time Setup | |
| O Use Browser Time | |
| ⊙ Use Internet Time Client | |
| Time Protocol | NTP (RFC-1305) 💌 |
| Server IP Address | pool.ntp.org |
| Time Zone | (GMT) Greenwich Mean Time : Dublin 🛛 🔽 |
| Enable Daylight Saving | |
| Automatically Update Inter | rval 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. |
| Fime 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 Inte | rval 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 | | |
|---|-----------------------------|--|
| | | |
| | Osing current configuration | |
| 1 | ОК | |

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.

Diagnostics DHCP Table
Ping Diagnosis
Trace Route

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.

Diagnostics >> View DHCP Assigned IP Addresses

| DHCP ser | ver: Stop | | | | ~ |
|----------|-----------|-------------|-------------|---------|---|
| | | 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. |

3.7.2 Ping Diagnosis

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

```
Diagnostics >> Ping Diagnosis
```

| | If you want to ping a WAN to ping through | | don't want to specify Unspecified". |
|-------|--|-------------|--|
| Pir | ng to: Host / IP 💌 Host / IP Gateway | IP Address: | |
| Resul | | | <u>Clear</u> |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | <u>~</u> |

| 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.

| ice Rout | e | | |
|----------|--------------------|--------------|--|
| | Protocol: | | |
| | | | |
| | Host / IP Address: | ICMP Run | |
| | Result | <u>Clear</u> | |
| | | ~ | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |

| 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. |

Click this link to remove the result on the window.

Clear

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.

- 3. Open a web browser on your PC and type http://192.168.1.1. The window will ask for typing username and password.
- 4. 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/PPPoA

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

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

Internet Access >> PPPoE / PPPoA

| PPPoF | / PPPoA | Client | Mode |
|-------|---------|--------|------|
| | | | |

| PPPoE/PPPoA Client Enable | 🔘 Disable | ISP Access Setup | |
|--|-----------|--|-----------------|
| DSL Modem Settings Multi-PVC channel VPI 0 VCI 34 Encapsulating Type Protocol PPPoE Modulation Multimode PPPoE Pass-through For Wireless LAN | | ISP Name Username Password PPP Authentication ✓ Always On Idle Timeout IP Address From ISP Fixed IP | .7F :92 .F5 .01 |

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. |
|--------------------|--|
| DSL Modem Settings | Set up the DSL parameters required by your ISP. These are vital for building DSL connection to your ISP. Multi-PVC channel - The selections displayed here are determined by the page of Internet Access – Multi PVCs. Select M-PVCs Channel means no selection will be chosen. VPI - Type in the value provided by ISP. VCI - Type in the value provided by ISP. Encapsulating Type - Drop down the list to choose the type provided by ISP. Protocol - Drop down the list to choose the one provided by ISP. If you have already used Quick Start Wizard to set the protocol, then it is not necessary for you to change any settings in this group. |
| PPPoE Pass-through | The router offers PPPoE dial-up connection. Besides, you also can establish the PPPoE connection directly from local clients to your ISP via the Vigor router. When PPPoA protocol is selected, the PPPoE package transmitted by PC will be transformed into PPPoA package and sent to WAN server. Thus, the PC can access Internet through such direction. For Wired LAN – If you check this box, PCs on the same network can use another set of PPPoE session (different with the Host PC) to access into Internet. For Wireless LAN – If you check this box, PCs on the same wireless network can use another set of PPPoE session (different with the Host PC) to access into Internet. |
| ISP Access Setup | Enter your allocated username, password and authentication parameters according to the information provided by your ISP. If |

you want to connect to Internet all the time, you can check **Always On**.

Username – Type in the username provided by ISP in this field. **Password** – Type in the password provided by ISP in this field. **PPP Authentication** – Select **PAP only** or **PAP or CHAP** for PPP.

Idle Timeout – Set the timeout for breaking down the Internet after passing through the time without any action. This setting is active only when the **Active on demand** option for Active Mode is selected in **WAN>> General Setup** page.

IP Address From ISP Usually ISP dynamically assigns IP address to you each time you connect to it and request. In some case, your ISP provides service to always assign you the same IP address whenever you request. In this case, you can fill in this IP address in the Fixed IP field. Please contact your ISP before you want to use this function. 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. Type the additional WAN IP address and check the Enable box. Then click OK to exit the dialog.



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

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

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

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

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

MPoA

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

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

| MPoA (RFC1483/268 | 34) 🔘 Enable 💿 Disable | WAN IP Network Settin | gs |
|---------------------|------------------------|--|-----------------|
| | | — Obtain an IP addres | s automatically |
| DSL Modem Settings | ; | Router Name | |
| Multi-PVC channel | Channel 1 💌 | Domain Name | , |
| Encapsulation | | *: Required for some IS | iPs |
| 14 | 183 Bridged IP LLC | Specify an IP addres | SAZANI ID AL |
| VPI | 0 | | 3 |
| VCI | 33 | IP Address | 0.0.0.0 |
| Modulation | Multimode 🗸 | Subnet Mask | 0.0.0.0 |
| Modulation | | Gateway IP Address | 0.0.0.0 |
| RIP Protocol | | | |
| Enable RIP | | Oefault MAC Address | |
| | | — 🔘 Specify a MAC Addre | ss |
| Bridge Mode | | MAC Address: 00 .50 | ·7F 92 ·F5 .01 |
| 🔲 Enable Bridge Mod | e | | |
| | | DNS Server IP Address | |
| | | Primary IP Address | |
| | | Secondary IP Address | |

Internet Access >> MPoA (RFC1483/2684)

| MPoA (RFC1483/2684) | Click Enable for activating this function. If you click Disable , this function will be closed and all the settings that you adjusted in this page will be invalid. |
|----------------------------|--|
| DSL Modem Settings | Set up the DSL parameters required by your ISP. These are vital for building DSL connection to your ISP. Multi-PVC channel - The selections displayed here are determined by the page of Internet Access – Multi PVCs. Select M-PVCs Channel means no selection will be chosen. Encapsulating Type - Drop down the list to choose the type provided by ISP. VPI - Type in the value provided by ISP. VCI - Type in the value provided by ISP. |
| RIP Protocol | Routing Information Protocol is abbreviated as RIP (RFC1058) specifying how routers exchange routing tables information. Click Enable RIP for activating this function. |
| Bridge Mode | If you choose Bridged IP as the protocol, you can check this box to invoke the function. The router will work as a bridge modem. |
| WAN IP Network Settings | This group allows you to obtain an IP address automatically and allows you type in IP address manually. |

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

Router Name – Type in the router name provided by ISP. **Domain Name** – Type in the domain name that you have assigned. Specify an IP address – Click this radio button to specify some data.

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. Type the additional WAN IP address and check the Enable box. Then click OK to exit the dialog.



IP Address – Type in the private IP address. **Subnet Mask** – Type in the subnet mask. Gateway IP Address – Type in gateway IP address. Default MAC Address Type in MAC address for the router. You can use **Default MAC Address** or specify another MAC address for your necessity. MAC Address – Type in the MAC address for the router manually. **DNS Server IP** Type in the primary IP address for the router. If necessary, type in secondary IP address for necessity in the future.

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

Address
4.1.3 Multi-PVCs

This router allows you to create multi-PVCs for different data transferring for using. Simply go to **Internet Access** and select **Multi-PVC Setup** page.

General

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

| WAN >> Multi-PVCs | |
|-------------------|--|
|-------------------|--|

| Multi-PVC | Cs | | | | | | | |
|-----------------|-----|--------|---------|------|--------|--------------|----------|-------------------------|
| General ATM QoS | | Port- | based B | Brid | | | | |
| Channel | | Enable | VPI | VCI | QoS Ty | /pe | Protocol | Encapsulation |
| 1. | | | 0 | 33 | UBR | * | PPPoE 💌 | LLC/SNAP 🔽 |
| 2. | | | 0 | 88 | UBR | * | MPoA 💌 | 1483 Bridged IP LLC 🛛 👻 |
| з. | WAN | | 1 | 43 | UBR | ~ | PPPoA 🗸 | VC MUX |
| 4. | WAN | | 1 | 44 | UBR | ~ | PPPoA 🔽 | VC MUX |
| 5. | WAN | | 1 | 45 | UBR | \mathbf{v} | PPPoA 🗸 | VC MUX |
| 6. | | | 1 | 46 | UBR | ~ | PPPoA 🗸 | VC MUX |
| 7. | | | 1 | 47 | UBR | \mathbf{v} | PPPoA 🔽 | VC MUX |
| 8. | | | 1 | 48 | UBR | ~ | PPPoA 🔽 | VC MUX |

Note: VPI/VCI must be unique for each channel!

| | OK | Clear | Cancel | |
|----|--------------|---------------|-------------|---|
| | | | | |
| Ch | alt this has | v to onoble t | hat ahannal | т |

| Enable | Check this box to enable that channel. The channels that you enabled here will be shown in the Multi-PVC channel drop down list on the web page of Internet Access . Though you can enable eight channels in this page, yet only one channel can be chosen on the web page of Internet Access . |
|----------|--|
| VPI | Type in the value provided by your ISP. |
| VCI | Type in the value provided by your ISP. |
| QoS Type | Select a proper QoS type for the channel. QoS Type UBR V UBR CBR ABR nrtVBR rtVBR |
| Protocol | Select a proper protocol for this channel. Protocol PPPoE PPPoA PPPoE MPoA |

Encapsulation

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

| | Encapsulation | | | |
|---------------|-----------------------------|---|--|--|
| | 1483 Route IP LLC | * | | |
| Encapsulation | 1483 Bridged IP LLC | | | |
| _ | 1483 Route IP LLC | | | |
| VC MUX 🕑 | 1483 Bridged IP VC-Mux | | | |
| VC MUX | 1483 Routed IP VC-Mux(IPoA) | | | |
| | 1483 Bridged IP(IPoE) | | | |

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

| WAN >> Multi-PV | s >> PVC | Channel 3 |
|-----------------|----------|-----------|
|-----------------|----------|-----------|

| WAN for Router-borne Application: Management | ~ |
|--|------------------------------------|
| 🛇 Enable 💿 Disable | |
| DSL Modem Settings | |
| VPI 1 QoS Type | UBR 💌 |
| VCI 43 Protocol | PPPoA 💌 |
| Encapsulati | on VC MUX 💌 |
| PPPoE/PPPoA Client | MPoA (RFC1483/2684) |
| ISP Access Setup | Obtain an IP address automatically |
| ISP Name | Router Name * |
| Username | Domain Name * |
| Password | *: Required for some ISPs |
| PPP Authentication PAP or CHAP | Specify an IP address |
| 🗹 Always On | IP Address |
| Idle Timeout | Subnet Mask |
| IP Address From ISP | Gateway IP Address |
| Fixed IP 🛛 Yes 💿 No (Dynamic IP) | DNS Server IP Address |
| Fixed IP Address | Primary IP Address |
| | Secondary IP Address |
| OK | Cancel |

ATM QoS

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

| lulti-PVCs | | | | |
|--------------------|---------------------|-------------------|-----|-----|
| General Channel | ATM QoS QoS Type | Port-based PCR | SCR | MBS |
| 1. | UBR 🔽 | 0 | 0 | 0 |
| 2. | UBR 🔽 | 0 | 0 | 0 |
| з. | UBR 🔽 | 0 | 0 | 0 |
| 4. | UBR 🔽 | 0 | 0 | 0 |
| 5. | UBR 🔽 | 0 | 0 | 0 |
| 6. | UBR 🔽 | 0 | 0 | 0 |
| 7. | UBR 🔽 | 0 | 0 | 0 |
| 8. | UBR 🔽 | 0 | 0 | 0 |

Note: 1.Set 0 means default value.

2.PCR(max) = ADSL Up Speed / 53 / 8.

| OK | Clear | Cancel |
|----|-------|--------|
| | | |

QoS Type

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



| PCR | It represents Peak Cell Rate. The default setting is "0". | |
|-----|---|--|
|-----|---|--|

- SCR It represents Sustainable Cell Rate. The value of SCR must be smaller than PCR.
- MBS It represents Maximum Burst Size. The range of the value is 10 to 50.

Port-based Bridge

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

WAN >> Multi-PVCs

| Multi-PVCs | | | | | | | |
|------------|--------|----|----|-----------|--------|--------------|---------|
| General | ATM Qo | S | | Port | -based | Bridge | |
| Channel | Enable | P1 | P2 | P3 | P4 | Service Type | Add Tag |
| 1. | | | | | | Normal 😽 | |
| 2. | | | | | | Normal 😒 | |
| з. | | | | | | Normal 🐱 | |
| 4. | | | | | | IGMP | |
| 5. | | | | | | Normal 👻 | |
| 6. | | | | | | Normal 😒 | |
| 7. | | | | | | Normal 👻 | |
| 8. | | | | | | Normal 💌 | |

Note: 1.Channel 1 to 2 are reserved for Nat/Route use.

ΟK

2.P1 is reserved for Nat/Route use.

| Enable | Check this box to enable that channel. Only channel 3 to 8 can be set in this page, for channel 1 to 2 are reserved for NAT using. |
|--------------|--|
| P1 to P4 | It means the LAN port 1 to 4. Check the box to designate the LAN port for channel 3 to 8. |
| Service Type | Normally, service type is used for the service of video stream (e.g., IPTV). It can divide the packets from remote control and from video stream into different PVC. In general, the protocol used by remote control is IGMP. Normal Normal IGMP Normal – It means that the PVC can accept all packets except IGMP. IGMP – It means that the PVC can accept packets of IGMP only. |
| Add Tag | To identify the usage of PVC, check this box to invoke this setting. And type the number for VLAN ID (number). |
| ~~~~~ | |

Clear

Cancel

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

4.2 LAN

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



4.2.1 Basics of LAN

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



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



What is Routing Information Protocol (RIP)

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

What is Static Route

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

What are Virtual LANs

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



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 D | HCP Setup | | | |
|------------------------------|-----------------------|----------------------------------|-------------------------|------------------|
| LAN IP Network Configuration | | DHCP Server Configuration | | |
| For NAT Usage | | 📀 Enable Server 🔘 Disable Server | | |
| 1st IP Address | 192.168.1.1 | | Relay Agent: 🔘 1st Subr | net 🔾 2nd Subnet |
| 1st Subnet Mask | 255.255.255.0 | | Start IP Address | 192.168.1.10 |
| For IP Routing Usage 🔘 | Enable 💿 Disable | | IP Pool Counts | 50 |
| 2nd IP Address | 192.168.2.1 | | Gateway IP Address | 192.168.1.1 |
| 2nd Subnet Mask | 255.255.255.0 | | DHCP Server IP Address | |
| 21 | nd Subnet DHCP Server | | for Relay Agent | |
| | | | DNS Server IP Address | |
| RIP Protocol Control | Disable 💙 | | 📃 Force DNS manual se | tting |
| | | | Primary IP Address | |
| | | | Secondary IP Address | |

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 . |
| 2 nd IP Address | Type in secondary IP address for connecting to a subnet. (Default: 192.168.2.1/24) |
| 2 nd Subnet Mask | An address code that determines the size of the network. (Default: 255.255.255.0/24) |
| 2 nd DHCP Server | You can configure the router to serve as a DHCP server for the 2nd subnet. |

| 🔄 http://192.168.1.1 - Router Web Configurator - Microsoft Internet Explorer | × |
|--|---|
| 2nd DHCP Server | |
| | |
| Start IP Address | |
| IP Pool Counts 0 (max. 10) | |
| Index Matched MAC Address given IP Address | |
| | |
| | |
| | |
| MAC Address : | |
| Add Delete Edit Cancel | |
| OK Clear All 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 2^{nd} DHCP server will help router to assign the correct IP address of the correct subnet to the correct host. So those hosts in 2^{nd} subnet won't get an IP address belonging to 1^{st} subnet.

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

RIP Protocol Control

| Disable | * |
|------------|---|
| Disable | |
| 1st Subnet | |
| 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.

er 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.

DHCP Server Configuration 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 – $(1^{st}$ **subnet**/ 2^{nd} **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 DN Configuration ha

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: 0:54:34 |
|---------------|-----------|-----------------------|---------------------------|
| Primary | | Secondary | |
| LAN Status | Prim | ary DNS: 194.109.6.66 | Secondary DNS: 168.95.1.1 |
| IP Address | TX Packet | s RX Packets | |
| 192.168.1.1 | 1311 | 1221 | |

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 Rou | ite Configuration | | Set | to Factory Default View R | outing Table |
|------------|---------------------|--------|------------|-----------------------------|--------------|
| Index | Destination Address | Status | Index | Destination Address | Status |
| <u>1.</u> | ??? | ? | <u>6.</u> | ??? | ? |
| <u>2.</u> | ??? | ? | <u>7.</u> | ??? | ? |
| <u>3.</u> | ??? | ? | <u>8.</u> | ??? | ? |
| <u>4.</u> | ??? | ? | <u>9.</u> | ??? | ? |
| <u>5.</u> | ??? | ? | <u>10.</u> | ??? | ? |

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. |
| Set to Factory Default | Clear all profiles. |
| Viewing Routing Table | Displays the routing table for your reference. |

Diagnostics >> View Routing Table



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.

| 🗹 Enable | | |
|----------|------------------------|---------------|
| | Destination IP Address | 192.168.10.0 |
| | Subnet Mask | 255.255.255.0 |
| | Gateway IP Address | 192.168.1.2 |
| | Network Interface | LAN 🔽 |

LAN >> Static Route Setup

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

| 🗹 Enable | | |
|----------|------------------------|---------------|
| | Destination IP Address | 211.100.88.0 |
| | Subnet Mask | 255.255.255.0 |
| | Gateway IP Address | 192.168.1.3 |
| | Network Interface | LAN 🔽 |

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

Diagnostics >> View Routing Table

Current Running Routing Table Refresh Key: C - connected, S - static, R - RIP, * - default, ~ - private A S~ 192.168.10.0/ 255.255.255.0 via 192.168.1.2, LAN C 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. Go to **LAN** page and select **VLAN**. The following page will appear. Click **Enable** to invoke VLAN function.

| .AN >> VLAN Confi | guration | | | |
|--------------------|----------|----|----|----|
| /LAN Configuration | | | | |
| Enable | | | | |
| | P1 | P2 | P3 | P4 |
| VLANO | | | | |
| VLAN1 | | | | |
| VLAN2 | | | | |
| VLAN3 | | | | |

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

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



LAN >> VLAN Configuration

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

| LAN Configuration | | | | |
|-------------------|---------------------|----|----|----------|
| | P1 | P2 | P3 | P4 |
| VLANO | ✓ | | | |
| VLAN1 | | | | v |
| VLAN2 | | | | |
| VLAN3 | | | | |

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.

| AN >> Bind IP to MAC | | |
|--|--------------------------|-----------------|
| Bind IP to MAC | | |
| Note: IP-MAC binding presets DHCP Allocati | | |
| If you select Strict Bind, unspecified | LAN clients cannot acces | s the Internet. |
| Enable O Disable O Strict Bind | | |
| ARP Table <u>Select All</u> <u>Sort</u> <u>Refresh</u> | IP Bind List | Select All Sort |
| IP Address Mac Address 192.168.1.10 00-0E-A6-2A-D5-A1 | Index IP Address | Mac Address |
| Add and Edit IP Address | | |
| Add | Edit Delete | |
| | ок | |

| 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.

| Index | Service Name | Public Port | Private IP | Status |
|------------|--------------|-------------|------------|--------|
| <u>1.</u> | | | | × |
| <u>2.</u> | | | | × |
| <u>3.</u> | | | | × |
| <u>4.</u> | | | | X |
| <u>5.</u> | | | | x |
| <u>6.</u> | | | | x |
| <u>7.</u> | | | | × |
| <u>8.</u> | | | | x |
| <u>9.</u> | | | | X |
| <u>10.</u> | | | | × |

NAT >> Port Redirection

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

NAT >> Port Redirection

| Index No. 1 | |
|--------------|--------------|
| 🔲 Enable | |
| Mode | Single 💌 |
| Service Name | Single Range |
| Protocol | V |
| 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 C | ontrol | Management Port Setu | р |
| 🔲 Allow management fro | om the Internet | 💿 User Define Ports (|) Default Ports |
| FTP Server | | Telnet Port | 23 (Default: 23) |
| 🗹 HTTP Server | | HTTP Port | 80 (Default: 80) |
| HTTPS Server | | HTTPS Port | 443 (Default: 443) |
| 🗹 Telnet Server | | FTP Port | 21 (Default: 21) |
| SSH Server | | SSH Port | |
| Disable PING from the | e Internet | | 22 (Default: 22) |
| Access List | | SNMP Setup | |
| List IP | Subnet Mask | 📃 Enable SNMP Agent | |
| 1 | * | Get Community | public |
| 2 | * | Set Community | private |
| 3 | ~ | Manager Host IP | |
| | | Trap Community | public |
| | | Notification Host IP | |
| | | Trap Timeout | 10 seconds |
| - | | K | |

4.3.2 DMZ Host

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



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

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

NAT >> DMZ Host Setup

| N 1 | |
|---|--|
| None 💌 | |
| Private IP | Choose PC |
| MAC Address of the True IP DMZ Host | |
| Note: When a True-IP DMZ host is turne be always on. | d on, it will force the router's WAN connection to |

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

NAT >> DMZ Host Setup

| DMZ Host Setup | | | | |
|----------------|-----------------------------|--|-------------------------------------|---|
| Index Enable | Aux. WAN IP | Private | IP | |
| 1. | 192.168.1.55 | | | Choose PC |
| | | OK Cle | ar | |
| Enable | Check to en | nable the DMZ | Z Host function. | |
| Private IP | Enter the part to select on | | ess of the DMZ h | ost, or click Choose PC |
| Choose PC | depicted be addresses c | elow. The wind f all hosts in y he list to be th 8.1.10 | low consists of a our LAN networ | utomatically pop up, as list of private IP k. Select one private IP |

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.

| MZ Host | Setup | | | |
|----------------|--------|--------------|--------------|-----------|
| WAN 1 Index | Enable | Aux. WAN IP | Private IP | |
| 1. | | 192.168.1.55 | 192.168.1.10 | Choose PC |

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

| Index | Comment | Local IP Address | Status |
|-----------|---------|------------------|--------|
| <u>1.</u> | | | х |
| <u>2.</u> | | | × |
| <u>3.</u> | | | × |
| <u>4.</u> | | | × |
| <u>5.</u> | | | × |
| <u>6.</u> | | | × |
| <u>7.</u> | | | × |
| <u>8.</u> | | | × |
| <u>9.</u> | | | × |
| 10. | | | × |

| 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

| 🗹 E | nable Open P | orts | | | | | |
|-----|--------------|--------------|----------|---------|----------|------------|----------|
| | Co | mment | P2P | | | | |
| | Lo | cal Computer | 192.1 | 68.1.10 | Cho | ose 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 |
| з. | 🗸 | 0 | 0 | 8. | 💙 | 0 | 0 |
| 4. | 💙 | 0 | 0 | 9. | 💙 | 0 | 0 |
| 5. | 💙 | 0 | 0 | 10. | 💙 | 0 | 0 |
| | | | | | | | |

Clear

Cancel

ΟK

| 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
- 2. UDP flood attack
- 3. ICMP flood attack
- 4. Port Scan attack
- 5. IP options
- 6. Land attack
- 7. Smurf attack
- 8. Trace route

- 9. SYN fragment
- 10. Fraggle attack
- 11. TCP flag scan
- 12. Tear drop attack
- 13. Ping of Death attack
- 14. ICMP fragment
- 15. Unknown protocol

Below shows the menu items for Firewall.

Firewall

General Setup

Filter Setup

DoS Defense

4.4.2 General Setup

Firewall >> General Setup

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

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

| Call Filter | 💿 Enable | Start Filter 9 | Get Set#1 💙 |
|----------------------------|-----------|----------------|-------------|
| | 🔘 Disable | | |
| Data Filter | 💿 Enable | Start Filter 9 | Get Set#2 💌 |
| | 🔘 Disable | | |
| Actions for default | : rule: | | |
| Application | | Action/Profile | Syslog |
| Filter | | Pass 💌 | |
| M/P2P Filter | | None 💌 | |
| <u> URL Content Filter</u> | | None 💌 | |
| <u>Web Content Filter</u> | | None 💙 | |
| Advance Setting | | Edit | |

OK Cancel

| | OR |
|--------------------|---|
| 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 3.14.4 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 3.14.4 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 3.14.4 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.

| http://192.168.1.5/doc/ipfgenady.html | m - Microsoft Internet Explor | ter | |
|---------------------------------------|-------------------------------|--------|---|
| Firewall >> General Set | up | | |
| Advance Setting | | | |
| Codepage | ANSI(1252)-Latin I | | * |
| Window size: | 65535 | | |
| Session timeout: | 1440 | Minute | |
| | OK Close | | |

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

 $(0\sim65535)$. 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

Firewall >> Filter Setup

Firewall >> Filter Setup >> Edit Filter Set

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

| ilter Se | etup | | Set to Factory Default |
|-----------|---------------------|------------|------------------------|
| Set | Comments | Set | Comments |
| <u>1.</u> | Default Call Filter | <u>7.</u> | |
| <u>2.</u> | Default Data Filter | <u>8.</u> | |
| <u>3.</u> | | <u>9.</u> | |
| <u>4.</u> | | <u>10.</u> | |
| <u>5.</u> | | <u>11.</u> | |
| <u>6.</u> | | <u>12.</u> | |

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

| Filter Set 1 | | | | |
|--------------|---------------------|---|--------------|-------------|
| Comments : | Default Call Filter | | | |
| Filter Rule | Active | Comments | Move Up | Move Down |
| 1 | ~ | Block NetBios | | <u>Down</u> |
| 2 | | | <u>UP</u> | <u>Down</u> |
| 3 | | | <u>UP</u> | <u>Down</u> |
| 4 | | | <u>UP</u> | <u>Down</u> |
| 5 | | | <u>UP</u> | <u>Down</u> |
| 6 | | | <u>UP</u> | <u>Down</u> |
| 7 | | | <u>UP</u> | |
| | | | Next Filter | Set None |
| | | OK Clear Cancel | | |
| 'ilter Rule | | Click a button numbered $(1 \sim 7)$ to button will open Edit Filter Rule w information, refer to the following | veb page. Fo | |

Active Enable or disable the filter rule.

the

| 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

| Comments: | Block NetBios | |
|---------------------------------------|--|--------|
| Index(1-15) in <u>Schedule</u> Setup: | ,,,, | |
| Direction: | LAN -> WAN 🔽 | |
| Source IP: | Any | Edit |
| Destination IP: | Any | Edit |
| Service Type: | TCP/UDP, Port: from 137~139 to undefined | Edit |
| Fragments: | Don't Care 💌 | |
| Application | Action/Profile | Syslog |
| Filter: | Block Immediately 🛛 👻 | |
| Branch to Other Filter Set: | None 😒 | |
| IM/P2P Filter: | None 😪 | |
| URL Content Filter | None 💌 | |
| Web Content Filter | None 🛩 | |
| Advance Setting | Edit | |

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

| Address Type | Group and Objects 🔽 |
|---------------------|--------------------------------------|
| Start IP Address | 0.0.0.0 |
| End IP Address | 0.0.0.0 |
| Subnet Mask | 0.0.0.0 |
| Invert Selection | |
| IP Group | None 💌 |
| or <u>IP Object</u> | None 💌 |
| or IP Object | None 1-RD Department |
| or IP Object | 2-Finanical Dept. 3-HR Department |

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.

| 92.168.1.5 - Service Typ | 9e Edit - Microsoft Internet Explorer |
|--------------------------|---------------------------------------|
| ervice Type Edit | |
| Service Type | User defined 💌 |
| Protocol | |
| Source Port | = 🖌 137 ~ 139 |
| Destination Port | = 💌 1 ~65535 |
| Service Group | None 🗸 |
| or <u>Service Object</u> | None 🔽 |
| or Service Object | None 😽 |
| or Service Object | None 🔽 |

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



4.4.4 DoS Defense

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

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

| F | irewal | >> | DoS | def | ense | Setur | 2 |
|---|--------|----|-----|-----|-------|-------|---|
| | Creat | | | au | 01100 | outup | |

| DoS defense Setup | | | |
|---|--------------------|------------|---------------|
| 🗹 Enable DoS Defense | | | |
| 🗌 Enable SYN flood defense | Threshold | 50 | packets / sec |
| | Timeout | 10 | sec |
| Enable UDP flood defense | Threshold | 150 | packets / sec |
| | Timeout | 10 | sec |
| Enable ICMP flood defense | Threshold | 50 | packets / sec |
| | Timeout | 10 | sec |
| Enable Port Scan detection | Threshold | 150 | packets / sec |
| Block IP options | 📃 Block TCP flag | scan | |
| 🔲 Block Land | 📃 Block Tear Dro | р | |
| Block Smurf | 🔲 Block Ping of D | eath | |
| Block trace route | 📃 Block ICMP frag | gment | |
| 🗌 Block SYN fragment | 📃 Block Unknown | Protocol | |
| 🔲 Block Fraggle Attack | | | |
| | | | |
| Enable DoS defense function to preve crackers. | ent the attacks fr | com hacker | or |
| OK Clea | ar 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 | Port Scan attacks the Vigor router by sending lots of packets to |

| detection | many ports in an attempt to find ignorant services would respond. Check the box to activate the Port Scan detection. Whenever detecting this malicious exploration behavior by monitoring the port-scanning Threshold rate, the Vigor router will send out a warning. By default, the Vigor router sets the threshold as 150 packets per second. |
|----------------------|---|
| Block IP options | Check the box to activate the Block IP options function. The Vigor router will ignore any IP packets with IP option field in the datagram header. The reason for limitation is IP option appears to be a vulnerability of the security for the LAN because it will carry significant information, such as security, TCC (closed user group) parameters, a series of Internet addresses, routing messagesetc. 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

System Maintenance >> SysLog / Mail Alert Setup

kind of attacks is detected.

| SysLog Access Setup | Mail Alert Setup Enable SMTP Server Mail To Return-Path Authentication User Name Password Enable E-Mail Alert: DoS Attack Im-P2P | Send a test e-mail |
|---------------------|--|--------------------|
| OK OK | Clear Cancel | |

| | Yigi | or Series | 172.16.3.4 | 343 | 3 |
|----------------------|-------|------------------|------------------------------------|---------------------------------|-----------------|
| Status TX Packets | RX | Packets | WAN IP (Fixed) | RX Packets | RX Rate |
| 4175 | | 3668 | 172.16.3.229 | 2558 | 126 |
| vall Log VPN Log U | | C-UL-P WANL- | Odam Natural Information | Net State Traffic Graph | |
| me | Host | Message | Others Network Information | Net State Trainc Graph | |
| me un 1.00:00:42 | Vigor | | ock(10s) 192.168.1.115,10605 -> 19 | 2.168.1.1.23 PR 6(tcp) len 20 |) 40 -\$ 394375 |
| un 1.00:00:34 | Vigor | DoS icmp_flood B | lock(10s) 192.168.1.115 -> 192.168 | 1.1.1 PR 1 (icmp) len 20 60 ici | np 0/8 |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |

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).

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

Objects Setting >> IP Object

4.5.1 IP Object

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

| P Object Profiles: | | | Set to Factory Defau |
|--------------------|------|------------|----------------------|
| Index | Name | Index | Name |
| <u>1.</u> | | <u>17.</u> | |
| <u>2.</u> | | <u>18.</u> | |
| <u>3.</u> | | <u>19.</u> | |
| <u>4.</u> | | <u>20.</u> | |
| <u>5.</u> | | <u>21.</u> | |
| <u>6.</u> | | <u>22.</u> | |
| <u>7.</u> | | <u>23.</u> | |
| <u>8.</u> | | <u>24.</u> | |
| <u>9.</u> | | <u>25.</u> | |
| <u>10.</u> | | <u>26.</u> | |
| <u>11.</u> | | <u>27.</u> | |
| <u>12.</u> | | <u>28.</u> | |
| <u>13.</u> | | <u>29.</u> | |
| <u>14.</u> | | <u>30.</u> | |
| <u>15.</u> | | <u>31.</u> | |
| <u>16.</u> | | <u>32.</u> | |

Set to Factory Default Clear all profiles.

Click the number under Index column for settings in detail.

Objects Setting >> IP Object

| 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: | | |
| | OK Clear Cancel | |
| Name | Type a name for this profile. Maximum 15 characters are allowed. | |
| nterface | 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 choo 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. | |
| | 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 Obje | ct Profiles: |
|---------|--------------|
|---------|--------------|

Objects Setting >> IP Group

| Index | Name |
|-----------|-----------------|
| <u>1.</u> | RD Department |
| <u>2.</u> | Financial Dept. |
| <u>3.</u> | HR Department |
| <u>4.</u> | |
| 5. | |

4.5.2 IP Group

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

| IP Group Table: | | | Set to Factory Default |
|-----------------|------|------------|------------------------|
| Index | Name | Index | Name |
| <u>1.</u> | | <u>17.</u> | |
| <u>2.</u> | | <u>18.</u> | |
| <u>3.</u> | | <u>19.</u> | |
| <u>4.</u> | | <u>20.</u> | |
| <u>5.</u> | | <u>21.</u> | |
| <u>6.</u> | | <u>22.</u> | |
| <u>7.</u> | | <u>23.</u> | |
| <u>8.</u> | | <u>24.</u> | |
| <u>9.</u> | | <u>25.</u> | |
| <u>10.</u> | | <u>26.</u> | |
| <u>11.</u> | | <u>27.</u> | |
| <u>12.</u> | | <u>28.</u> | |
| <u>13.</u> | | <u>29.</u> | |
| <u>14.</u> | | <u>30.</u> | |
| <u>15.</u> | | <u>31.</u> | |
| <u>16.</u> | | <u>32.</u> | |

Set to Factory Default Clear all profiles.

Click the number under Index column for settings in detail.
Objects Setting >> IP Group

| Profile Index : 1 | | | |
|---|---|--|--|
| Name: | Admin | | |
| Interface: | Any 🗸 | | |
| Available IP Objects | Selected IP Objects | | |
| 1-RD Department 2-Financial Dept. 3-HR Department | » « | | |
| l | 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 Obj | ject Profiles: | | Set to Factory Default |
|----------------------------|----------------|------------|------------------------|
| Index | Name | Index | Name |
| <u>1.</u> | | <u>17.</u> | |
| <u>2.</u> | | <u>18.</u> | |
| <u>3.</u> | | <u>19.</u> | |
| <u>4.</u> | | <u>20.</u> | |
| <u>5.</u> | | <u>21.</u> | |
| <u>6.</u> | | <u>22.</u> | |
| <u>7.</u> | | <u>23.</u> | |
| <u>8.</u> | | <u>24.</u> | |
| <u>9.</u> | | <u>25.</u> | |
| <u>10.</u> | | <u>26.</u> | |
| <u>11.</u> | | <u>27.</u> | |
| <u>12.</u> | | <u>28.</u> | |
| <u>13.</u> | | <u>29.</u> | |
| <u>14.</u> | | <u>30.</u> | |
| <u>15.</u> | | <u>31.</u> | |
| <u>16.</u> | | <u>32.</u> | |
| :< <u>1-32 33-64 6</u> | <u>5-96</u> >> | | <u>Next</u> > |

Set to Factory Default Clear all profiles.

Click the number under Index column for settings in detail.

```
Objects Setting >> Service Type Object Setup
```

| Name | wwww |
|------------------|---------------|
| Protocol | TCP 6 |
| Source Port | = 🖌 1 ~ 65535 |
| Destination Port | = 🖌 70 ~ 80 |

Name

Type a name for this profile.

Protocol



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 |
|-----------|------|
| <u>1.</u> | SIP |
| <u>2.</u> | RTP |
| <u>3.</u> | |

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 Gro | up Table: | | Set to Factory Default |
|------------------|-----------|------------|------------------------|
| Group | Name | Group | Name |
| <u>1.</u> | | <u>17.</u> | |
| <u>2.</u> | | <u>18.</u> | |
| <u>3.</u> | | <u>19.</u> | |
| <u>4.</u> | | <u>20.</u> | |
| <u>5.</u> | | <u>21.</u> | |
| <u>6.</u> | | <u>22.</u> | |
| <u>7.</u> | | <u>23.</u> | |
| <u>8.</u> | | <u>24.</u> | |
| <u>9.</u> | | <u>25.</u> | |
| <u>10.</u> | | <u>26.</u> | |
| <u>11.</u> | | <u>27.</u> | |
| <u>12.</u> | | <u>28.</u> | |
| <u>13.</u> | | <u>29.</u> | |
| <u>14.</u> | | <u>30.</u> | |
| <u>15.</u> | | <u>31.</u> | |
| <u>16.</u> | | <u>32.</u> | |

Set to Factory Default

Clear all profiles.

Click the number under Index column for settings in detail.

Objects Setting >> Service Type Group Setup

| Name: | VolP | | |
|-----------------------------------|-------------|-----------|---|
| Available Service T | ype Objects | Sele | lected Service Type Objects |
| 1-SIP 2-RTP | | | |
| | | » « | |
| | ОК | Clear | Cancel |
| Name | Type a nar | me for th | his profile. |
| Available Service Type Objects | | | service objects that you have added on >Service Type Object will be shown ir |
| Selected Service Type Objects | Click >> b | outton 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.

| Keyword Object | Profiles: | | Set to Factory Default |
|---------------------------|--------------------------------------|-------------------|------------------------|
| Index | Name | Index | Name |
| <u>1.</u> | | <u>17.</u> | |
| <u>2.</u> | | <u>18.</u> | |
| <u>3.</u> | | <u>19.</u> | |
| <u>4.</u> | | <u>20.</u> | |
| <u>5.</u> | | <u>21.</u> | |
| <u>6.</u> | | <u>22.</u> | |
| <u>7.</u> | | <u>23.</u> | |
| <u>8.</u> | | <u>24.</u> | |
| <u>9.</u> | | <u>25.</u> | |
| <u>10.</u> | | <u>26.</u> | |
| <u>11.</u> | | <u>27.</u> | |
| <u>12.</u> | | <u>28.</u> | |
| <u>13.</u> | | <u>29.</u> | |
| <u>14.</u> | | <u>30.</u> | |
| <u>15.</u> | | <u>31.</u> | |
| <u>16.</u> | | <u>32.</u> | |
| < <u>1-32 33-64 6</u> | <u>5-96 97-128 129-160 161</u> | -192 193-200 >> | <u>Next</u> >> |

Objects Setting >> Keyword Object

Set to Factory Default Clear all profiles.

Click the number under Index column for setting in detail.

Objects Setting >> Keyword Object Setup

| Profile Index : 1 Name | |
|------------------------|--|
| Contents | (Max 63 characters) |
| | OK Clear Cancel |
| Name | Type a name for this profile, e.g., game. |
| Contents | Type the content for such profile. For example, type <i>gambling</i> 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**.

| eyword Group T | able: | | Set to Factory Defaul |
|----------------|-------|------------|-----------------------|
| Index | Name | Index | Name |
| <u>1.</u> | | <u>17.</u> | |
| <u>2.</u> | | <u>18.</u> | |
| <u>3.</u> | | <u>19.</u> | |
| <u>4.</u> | | <u>20.</u> | |
| <u>5.</u> | | <u>21.</u> | |
| <u>6.</u> | | <u>22.</u> | |
| <u>7.</u> | | <u>23.</u> | |
| <u>8.</u> | | <u>24.</u> | |
| <u>9.</u> | | <u>25.</u> | |
| <u>10.</u> | | <u>26.</u> | |
| <u>11.</u> | | <u>27.</u> | |
| <u>12.</u> | | <u>28.</u> | |
| <u>13.</u> | | <u>29.</u> | |
| <u>14.</u> | | <u>30.</u> | |
| <u>15.</u> | | <u>31.</u> | |
| <u>16.</u> | | <u>32.</u> | |

Objects Setting >> Keyword Group

Set to Factory Default Clear all profiles.

Click the number under Index column for setting in detail.

Objects Setting >> Keyword Group Setup

| Name: | |
|----------------------------|--|
| Available Keyword Objects | Selected Keyword Objects(Max 16 Objects) |
| 1-Keyword-1 2-keyword-2 | » « |
| | OK Clear Cancel |
| ame | Type a name for this group. |
| vailable Keyword bjects | 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. |
| elected 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.

| ile Extension Ob | ject Profiles: | | Set to Factory De | <u>efault</u> |
|------------------|----------------|-----------|-------------------|---------------|
| Profile | Name | Profile | Name | |
| <u>1.</u> | | <u>5.</u> | | |
| <u>2.</u> | | <u>6.</u> | | |
| <u>3.</u> | | <u>7.</u> | | |
| <u>4.</u> | | <u>8.</u> | | |

Set to Factory Default Clear all profiles.

Objects Setting >> File Extension Object

Click the number under Profile column for configuration in details.

Objects Setting >> File Extension Object Setup

| Profile Index: 1 | | Profile | Name: de | fault | | | |
|--|------------------|------------------|------------------|------------------|--------------|-----------------|---------|
| Categories | | | F | ile Extensio | ons | | |
| Image Select All Clear All | .bmp | □.dib □.pcx | .gif | .jpeg . .pict | .jpg .png | □.jpg2 □.tif | .jp2 |
| Video Select All Clear All | □.asf □.qt | 🗌 .avi 🗌 .rm | .mov. | .mpe | .mpeg | .mpg .3gpp2 | .mp4 |
| Audio Select All Clear All | □.aac □.ra | □.aiff □.ram | □.au □.vox | .mp3 .wav | .m4a .wma | 🗌 .m4p | ogg . |
| Java Select All Clear All | □.class □.jse | 🗌 .jad 🗌 .jsp | □.jar □.jtk | 🗆 .jav | 🗌 .java | 🗌 .jcm | 🗌 .js |
| ActiveX Select All Clear All | □.alx □.viv | .apb .vrm | .axs | cx | .olb | .ole | 🗌 .tlb |
| Compression Select All Clear All | □.ace □.rar | 🗌 .arj 🗌 .sit | □.bzip2 □.zip | .bz2 | 🗌.cab | .gz | 🗌 .gzip |
| Executation Select All Clear All | 🗌 .bas 🗌 .scr | 🗌 .bat | .com | .exe | .inf | 🗌 .pif | .reg |
| | | ОК | Clear | Cano | el | | |

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.

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

Objects Setting >> IM Object Profile

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 Pro | ofile | | | |
|---|---|---|--|--|--|
| Profile Index: 1 Profile Name: Check for Disalloy | N: | | | | |
| | I | M Application | | | VoIP |
| MSN | 🗌 YahooIM | AIM | □ ICQ | | Skype |
| QQ | liChat | Jabber/G | oogleTalk 🔲 Goog | eChat | SIP |
| | W | eb IM (* = mo | re than one addres | is) | |
| URLs 🗌 WebIM URLs | <u>eMessenger</u> <u>ICQ Java*</u> <u>IMUnitive*</u> <u>MessengerFX*</u> | <u>WebMSN</u> <u>ICQ Flash*</u> <u>Wablet*</u> <u>MessengerAdi</u> | <u>meebo*</u> goowy* <u>mabber*</u> ctos WebYahoolM | <u>eBuddy</u> <u>IMhaha*</u> MSN2GO* | <u>IL ovelM*</u> get <u>Messenger</u> KoollM |
| | | OK OK | Clear Cancel | | |

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.

| P2P Profile Table: | | | Set to Factory Default |
|--------------------|------|------------|------------------------|
| Profile | Name | Profile | Name |
| <u>1.</u> | | <u>17.</u> | |
| <u>2.</u> | | <u>18.</u> | |
| <u>3.</u> | | <u>19.</u> | |
| <u>4.</u> | | <u>20.</u> | |
| <u>5.</u> | | <u>21.</u> | |
| <u>6.</u> | | <u>22.</u> | |
| <u>7.</u> | | <u>23.</u> | |
| <u>8.</u> | | <u>24.</u> | |
| <u>9.</u> | | <u>25.</u> | |
| <u>10.</u> | | <u>26.</u> | |
| <u>11.</u> | | <u>27.</u> | |
| <u>12.</u> | | <u>28.</u> | |
| <u>13.</u> | | <u>29.</u> | |
| <u>14.</u> | | <u>30.</u> | |
| <u>15.</u> | | <u>31.</u> | |
| <u>16.</u> | | <u>32.</u> | |



Set to Factory Default Clear all profiles.

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

| Profile Name: | | |
|---------------------|-------------------------------------|--|
| Check for Disallow: | | |
| Protocol | Applications | |
| 🔲 SoulSeek | SoulSeek | |
| 🔲 eDonkey | eDonkey, eMule, Shareaza | |
| FastTrack | KazaA, BearShare, iMesh | |
| 🗌 OpenFT | KCeasy, FilePipe | |
| 🗌 Gnutella | BearShare, Limewire, Shareaza, Foxy | |
| 🗌 OpenNap | Lopster, XNap, WinLop | |
| 🗌 BitTorrent | BitTorrent, BitSpirit, BitComet | |
| Winny | Winny, WinMX, Share | |

Objects Setting >> P2P Object Profile

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.

| Misc Profile Table | | | Set to Factory Default |
|--------------------|------|------------|------------------------|
| Profile | Name | Profile | Name |
| <u>1.</u> | | <u>17.</u> | |
| <u>2.</u> | | <u>18.</u> | |
| <u>3.</u> | | <u>19.</u> | |
| <u>4.</u> | | <u>20.</u> | |
| <u>5.</u> | | <u>21.</u> | |
| <u>6.</u> | | <u>22.</u> | |
| <u>7.</u> | | <u>23.</u> | |
| <u>8.</u> | | <u>24.</u> | |
| <u>9.</u> | | <u>25.</u> | |
| <u>10.</u> | | <u>26.</u> | |
| <u>11.</u> | | <u>27.</u> | |
| <u>12.</u> | | <u>28.</u> | |
| <u>13.</u> | | <u>29.</u> | |
| <u>14.</u> | | <u>30.</u> | |
| <u>15.</u> | | <u>31.</u> | |
| <u>16.</u> | | <u>32.</u> | |

Objects Setting >> Misc Object Profile

Set to Factory Default Clear all profiles.

Objects Setting >> Misc Object Profile

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

| Profile Index: 1 | | | |
|------------------|-----------|--------------|--------------|
| Profile Name: | | | |
| Check for Disall | ow: | | |
| | | Streaming | |
| MMS | RTSP | 🗌 TVAnts | PPStream |
| PPlive | 📃 FeiDian | UUSee | NSPlayer 🗌 |
| PCAST | TVKoo | SopCast | UDLiveX |
| TVUPlayer | MySee | 🗌 Joost | 🗌 FlashVideo |
| | OK | Clear Cancel | |

Profile Name

Type a name for this profile.

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

4.6 CSM Profile

Content Security Management (CSM)

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

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

IM/P2P Filter

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

URL Content Filter

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

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

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

Web Content Filter

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

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

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

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



4.6.1 IM/P2P Filter Profile

CSM >> 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.

| 1/P2P Filter Pro | file Table: | | Set to Factory Defaul |
|------------------|-------------|------------|-----------------------|
| Profile | Name | Profile | Name |
| <u>1.</u> | | <u>17.</u> | |
| <u>2.</u> | | <u>18.</u> | |
| <u>3.</u> | | <u>19.</u> | |
| <u>4.</u> | | <u>20.</u> | |
| <u>5.</u> | | <u>21.</u> | |
| <u>6.</u> | | <u>22.</u> | |
| <u>7.</u> | | <u>23.</u> | |
| <u>8.</u> | | <u>24.</u> | |
| <u>9.</u> | | <u>25.</u> | |
| <u>10.</u> | | <u>26.</u> | |
| <u>11.</u> | | <u>27.</u> | |
| <u>12.</u> | | <u>28.</u> | |
| <u>13.</u> | | <u>29.</u> | |
| <u>14.</u> | | <u>30.</u> | |
| <u>15.</u> | | <u>31.</u> | |
| <u>16.</u> | | <u>32.</u> | |

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 🛩 |
| <u>Misc Object</u> | 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.

| RL Content Filte | r Profile Table: | | Set to Factory Defau |
|------------------|------------------|-----------|----------------------|
| Profile | Name | Profile | Name |
| <u>1.</u> | | <u>5.</u> | |
| <u>2.</u> | | <u>6.</u> | |
| <u>3.</u> | | <u>7.</u> | |
| 4. | | 8. | |

CSM >> URL Content Filter Profile

| <pre><body><center> The requested Web page has been blocked by URL Content</center></body></pre> | ~ |
|--|---|
| | |
| Filter.Please contact your system administrator for further | |
| information. | |
| | |
| | |

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

0K

CSM >> URL Content Filter Profile

| Profile Index: 1 | | |
|--------------------------------------|--|--|
| Profile Name: Priority: | Both : Pass | Log: None V |
| Actio | le URL Access Control n: | Prevent web access from IP address Group/Object Selections |
| Pass | ~ | Edit |
| 2.Web Featu Enab Actio Pass | le Restrict Web Feature n: | File Extension Profile: None 🛩 |
| 1 | OK | Clear Cancel |
| Profile Name | Type the nam | ne for such profile. |
| | the condition below passin configuration Feature will b Both:Block - with the cond Feature below set in this pag inactive. Either: URL matching wit Web Feature the actions ex packages wit feature secon Either: Web the condition below, such f executed. For | -The router will block all the packages that match litions specified in URL Access Control and Web w. When you choose this setting, both configuration ge for URL Access Control and Web Feature will be Access Control First – When all the packages h the conditions specified in URL Access Control and below, such function can determine the priority for kecuted. For this one, the router will process the h the conditions set below for URL first, then Web |
| | Priority: | Both : Pass Both : Pass Both : Block Either : URL Access Control First Either : Web Feature First |
| Log | None – There | e 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.

116

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



Log:

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

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

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

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

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





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

| 🚰 http://192.168.1.5 - Group/Object Edit - Microsoft Internet | Explorer |
|---|----------|
| | |
| Object/Group Edit | |
| | |
| Keyword Object | None 💌 |
| or Keyword Object | None 🛩 |
| or Keyword Object | None 🛩 |
| or Keyword Object | None 💌 |
| or Keyword Object | None 🛩 |
| or <u>Keyword Group</u> | None 🛩 |
| or Keyword Group | None 🔽 |
| or Keyword Group | None 🛩 |
| or Keyword Group | None 🔽 |
| or Keyword Group | None 🛩 |
| or Keyword Group | None 💙 |
| or Keyword Group | None 🛩 |
| or Keyword Group | None 💙 |
| | |
| OK Clos | e |
| | |
| | |
| | |
| | |
| | |

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



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.

| Profile | Name | Profile | Name |
|---|-------------------------|------------------------|------|
| <u>1.</u> | | <u>5.</u> | |
| <u>2.</u> | | <u>6.</u> | |
| <u>3.</u> | | <u>7.</u> | |
| <u>4.</u> | | <u>8.</u> | |
| dministration M | essage (Max 255 charact | ters) | |
| dministration M body> <center><</center> | br>The requested We | eb page has been block | - |
| ilter.Pleas nformation. <th></th> <th>administrator for fur</th> <th>ther</th> | | administrator for fur | ther |
| | | | |

CSM >> Web Content Filter Profile

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

CSM >> Web Content Filter Profile

| Profile Index : 1 Profile Name: | | | |
|---|--|--|--|
| Action : Block 💙 Groups | Categories | log : Block 💌 | |
| Child Protection Select All Clear All | Chat Gambling Sex | Criminal Hacking Violence | Drugs/Alcohol Hate speech Weapons |
| Leisure Select All Clear All | Advertisements Games Hobbies Personals Sports | Entertainment Glamour Lifestyle Photo Searches Streaming Media | Food Health Motor Vehicles Shopping Travel |
| Business Select All Clear All | Computing/Internet | ☐ Finance ☐ Real Estate ☐ Search Engine | ☐ Job Search/Career ☐ Reference ☐ Web Mail |
| Others Select All Clear All | Education News Usenet news | Hosting sites Religion uncategorised sites | ☐ Kid Sites ☐ Sex Education |
| action | Pass - allow access categories listed or Block - restrict acc categories listed or If the web pages do | the box below. essing into the correst the box below. | onding webpage with the sponding webpage with specified feature set here |
| .og | Pass – Only the log Block – Only the l | | |

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

4.7 Bandwidth Management

Below shows the menu items for Bandwidth Management.

- Bandwidth Management

 Sessions Limit
 Bandwidth Limit
- Quality of Service

4.7.1 Sessions Limit

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

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

| Sessions Limit | |
|---|--|
| Enable O Disable | |
| Default Max Sessions: 100 | |
| Limitation List | |
| Index Start IP End IP Max Sessions | |
| | |
| | |
| | |
| | |
| | |
| | |
| Specific Limitation | |
| Start IP: End IP: | |
| Maximum Sessions: | |
| | |
| Add Edit Delete | |
| | |
| Time Schedule | |
| Index(1-15) in <u>Schedule</u> Setup:,,, | |
| Note: Action and Idle Timeout settings will be ignored. | |

Bandwidth Management >> Sessions Limit

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

0K

| 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.

| O LINGE | ole 💿 | Disable | | | | | |
|------------------------------|----------|------------|-----------------|-------------------|----------|----------|--|
| Default T | X Limit: | 200 | Kbps | Default RX Limit: | 800 | Kbps | |
| Limitatio | on List | | | | | | |
| Index | Start | IP | End | IP | TX limit | RX limit | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| Specific | Limitati | on | | | | | |
| Specific Start IP: | | on | | End IP: | | | |
| | | on Kbps | RX Limit | | ; | | |
| Start IP: | | | RX Limit Add | | ; | | |
| Start IP: | | | | t: Kbps | ; | | |

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

ОK

| 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. |

Bandwidth Management >> Bandwidth Limit

| 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.

| status | Bandwidth | Directon | Class 1 | Class 2 | Class 3 | Others | UDP Bai Con | | |
|---------------------|-----------|----------|------------|------------|------------|--------|----------------|---------|--------------|
| Enable | Kbps/Kbps | Outbound | 25% | 25% | 25% | 25% | Inac | tive | <u>Setup</u> |
| | | | | | | | | | |
| Class Rule Index | • | Name | e | | | F | Rule | Service | Туре |
| | 3 | Nam | e | | | | Rule Edit | Service | Туре |
| | 3 | Nami | e | | | | | Service | |

Bandwidth Management >> Quality of Service

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.

Bandwidth Management >> Quality of Service

| General Setup | | |
|---------------|-------------------|------------------------------|
| Enable the | QoS Control OUT 💌 | |
| Index | Class Name | Reserved_bandwidth Ratio |
| Class 1 | | 25 % |
| Class 2 | | 25 % |
| Class 3 | | 25 % |
| | Others | 25 % |
| | | |
| Enable UDP 8 | Bandwidth Control | Limited_bandwidth Ratio 25 % |
| 🔲 Outbound To | CP 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. |
|---------------------------------|--|
| 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. This link will be seen only if you click OK in WAN1 General Setup web page and click Setup again (for WAN1) on the Bandwidth Management>>Quality of |

Service.

Bandwidth Management >> Quality of Service

| line St | atistics | | Refresh Int | erval: 5 🔽 seconds | Refresh |
|---------|-----------|------------|--------------------------|-------------------------|----------|
| Index | Direction | Class Name | Reserved-bandwidth Ratio | Outbound Throughput (By | tes/sec) |
| 1 | OUT | | 25% | 0 | |
| 2 | OUT | | 25% | 0 | |
| З | OUT | | 25% | 0 | |
| 4 | OUT | Others | 25% | 0 | |
| | | | | | |
| | | Ot | hers | | |

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
```

| tatus | Bandwidth | Directon | Class 1 | Class 2 | Class 3 | Others | UDP Bar Con | | |
|--------------------|-----------|----------|------------|------------|------------|--------|----------------|---------|-------|
| Enable | Kbps/Kbps | Outbound | 25% | 25% | 25% | 25% | Inac | tive | Setup |
| lass Rub | P | | | | | | | | |
| Class Rub Index | e | Name | e | | | F | Rule | Service | Туре |
| | e | Nam | e | | | | Rule Edit | Service | Туре |
| Index | - | Nam | e | | | | | Service | |

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.

| class I | ndex #1 | | | | |
|---------|---------|---------------|-----------------|-----------------------|--------------|
| lame | Test | | | | |
| NO | Status | Local Address | Remote Address | DiffServ CodePoint | Service Type |
| 1 | Empty | - | - | - | - |
| | | - | Add Edit Delete | | |

For adding a new rule, click **Add** to open the following page. Bandwidth Management >> Quality of Service

| Rule Edit |
|-----------|
|-----------|

| 🗹 ACT | | | |
|------------------------|---------------------------|-----------|------|
| Local Address | Any | | Edit |
| Remote Address | Any | | Edit |
| DiffServ CodePoint | ANY | ~ | |
| Service Type | ANY | * | |
| Note: Please choose/se | tup the <u>Service Ty</u> | oe first. | |



ACTCheck this box to invoke these settings.Local AddressClick the Edit button to set the local IP address (on LAN) for

Remote AddressClick the Edit button to set the remote IP address (on

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

Edit

| Address Type | Subnet Address 😪 |
|------------------|------------------|
| Start IP Address | 0.0.0.0 |
| End IP Address | 0.0.0.0 |
| Subnet Mask | 0.0.0.0 |

Address Type – Determine the address type for the source address.

For **Single Address**, you have to fill in Start IP address. For **Range Address**, you have to fill in Start IP address and End IP address.

For **Subnet Address**, you have to fill in Start IP address and Subnet Mask.

| DiffServ CodePoint | All the packets of data will be divided with different levels and will be processed according to the level type by the system. Please assign one of the levels of the data for processing with QoS control. |
|--------------------|--|
| Service Type | It determines the service type of the data for processing with QoS control. It can also be edited. You can choose the predefined service type from the Service Type drop down list. Those types are predefined in factory. Simply choose the one that you want for using by current QoS. |

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

Bandwidth Management >> Quality of Service

| Class Ir | | | | | |
|----------|--------|---------------|----------------|-----------------------|----------------|
| Name | Test | | | | |
| NO | Status | Local Address | Remote Address | DiffServ CodePoint | Service Type |
| 1 🔿 | Active | Any | Any | IP precedence 1 | TELNET(TCP:23) |
| | | 4 | Add Edit Dele | te | |
| | | | 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

| status | Bandwidth | Directon | Class 1 | Class 2 | Class 3 | Others | | andwidth ntrol | |
|-------------------|-----------|----------|------------|------------|------------|--------|---------------------|------------------------|-------|
| Enable | Kbps/Kbps | Outbound | 25% | 25% | 25% | 25% | Ina | active | Setup |
| lace Dul | 0 | | | | | | | | |
| lass Rul Index | e | Name | B | | | | Rule | Service | Туре |
| | - | Name | B | | | | Rule <u>Edit</u> | Service | Туре |
| | - | Nami | e | | | | | Service <u>Edit</u> | |

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

```
Bandwidth Management >> Quality of Service
```

| User Defined | l Service Type | | |
|--------------|----------------|-----------------|------|
| NO | Name | Protocol | Port |
| 1 | Empty | - | - |
| | | Add Edit Delete | |
| | | Cancel | |

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

Bandwidth Management >> Quality of Service

| Service Type Edit | | |
|--------------------|---|---|
| Service Name | | |
| Service Type | | TCP 🖌 6 |
| Port Configurat | tion | |
| Туре | | 💿 Single 🔘 Range |
| Port Num | ber | 0 - 0 |
| Service Name | ок Type in a new | Cancel w service for your request. |
| Service Type | Choose the ty service. | ype (TCP, UDP or TCP/UDP) for the new |
| Port Configuration | have to type number on th Port Numbe | or Range as the Type . If you select Range, you in the starting port number and the end porting he boxes below. $\mathbf{r} - Type$ in the starting port number and the end her 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.

| Applications |
|--------------|
| Dynamic DNS |
| ▶ Schedule |
| ▶ RADIUS |
| ▶ UPnP |
| ▶ IGMP |
| Wake on LAN |

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

| Dynamic DNS Setup | | Set to Factory Default |
|----------------------|-------------|------------------------|
| 🗹 Enable Dynamic DNS | S Setup (| View Log Force Update |
| Accounts: | | |
| Index | Domain Name | Active |
| <u>1.</u> | | × |
| <u>2.</u> | | × |
| <u>3.</u> | | × |
| | | |
| | | |



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. | |

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

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

| ndex : 1 | |
|----------------------|----------------------------------|
| 🗹 Enable Dynamic DNS | |
| Service Provider | dyndns.org (www.dyndns.org) 💙 |
| Service Type | Dynamic 💌 |
| Domain Name | chronic6853 dyndns.info 🖌 |
| Login Name | chronic6853 (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. |

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

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

Disable the Function and Clear all Dynamic DNS Accounts

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

Delete a Dynamic DNS Account

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

4.8.2 Schedule

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

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

| Schedule: | | | Set to Factory Default |
|-----------|--------|------------|------------------------|
| Index | Status | Index | Status |
| <u>1.</u> | х | <u>9.</u> | х |
| <u>2.</u> | х | <u>10.</u> | х |
| <u>3.</u> | × | <u>11.</u> | × |
| <u>4.</u> | Х | <u>12.</u> | × |
| <u>5.</u> | х | <u>13.</u> | × |
| <u>6.</u> | х | <u>14.</u> | × |
| <u>7.</u> | х | <u>15.</u> | × |
| <u>8.</u> | × | | |

Applications >> Schedule

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 Sc | hedule 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 | minute(s).(max. 255, 0 for default) |
| | How Often | |
| | 🔘 Once | |
| | 💿 Weekdays | |
| | 🗌 Sun 🗹 Mon 🗹 | Tue 🗹 Wed 🗹 Thu 🗹 Fri 🔲 Sat |

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

Example

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



- 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.
- 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.

| RADIUS Setup | | |
|------------------------------|---|--|
| 🗹 Enable | | |
| Server IP Add | Iress | |
| Destination Po | ort 1812 | |
| Shared Secre | t | |
| Confirm Share | ed Secret | |
| C | OK Clear Cancel | |
| 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. | |

Applications >> RADIUS

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

| UPnP | |
|----------------------------------|-----|
| 🗹 Enable UPnP Service | |
| Enable Connection control Serv | ice |
| 📃 Enable Connection Status Servi | ce |

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.

| eneral | Services |
|--|--|
| Connect to the Internet using: | Select the services running on your network that Internet users can access. |
| IP Broadband Connection on Router | Services |
| This connection allows you to connect to the Internet through a shared connection on another computer. | □ Ftp Example ☑ msnmsgr (192.168.29.11:13135) 60654 UDP ☑ msnmsgr (192.168.29.11:7824) 13251 UDP ☑ msnmsgr (192.168.29.11:8789) 63231 TCP |
| Settings | Add Edit Delete |

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 | | | | | | |
| will access any Enable IGMP : Enable IGMP S | to act as a mult / multicast grou | p. But this fu ast traffic is | unction take no only forwarded | to ports that h | Bridge Mode i | s enabled. of that group. |
| | | C |)K Can | cel | | L Defeet |
| Working Multicas | t Groups | | | | | <u>Refresh</u> |
| Index | Group ID | | P1 | P2 | P3 | P4 |
| Enable IGMP | Proxy | | | able this func cuted through | - | • |
| 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 treate 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 | | | | |

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

239.255.255.254.

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

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

4.8.6 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

| can wake up thr | LAN integrates with <u>Bind IP to MAC</u> function, only binded PCs rough IP. |
|-----------------|--|
| Wake by: | MAC Address 💌 |
| IP Address: | 😒 |
| MAC Address: | Wake Up! |
| Result | |
| | |

| Wake by | ke byTwo types provide for you to wake up the binded IP. If y choose Wake by MAC Address, you have to type the co MAC address of the host in MAC Address boxes. If you choose Wake by IP Address, you have to choose the cor address. | |
|-------------|---|---|
| | Wake by: | MAC Address MAC Address IP Address |
| IP Address | Firewall>>Bind IP to | have been configured in MAC will be shown in this drop down ress from the drop down list that you |
| MAC Address | Type any one of the M | AC address of the binded PCs. |
| Wake Up | Click this button to wake up the selected IP. See the following figure. The result will be shown on the box. | |

| Wake by: MAC Address 💌 | |
|------------------------|--|
| | |
| IP Address: 💙 | |
| MAC Address: | |
| Result | |

Application >> Wake on LAN

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.

| VPN and Remote Access |
|-----------------------|
| Remote Access Control |
| PPP General Setup |
| ▶ IPSec General Setup |
| IPSec Peer Identity |
| Remote Dial-in User |
| EAN to LAN |
| Connection Management |
| |

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 | | | | |
|-------------|-----------------------------|--|--|--|--|
| ∠ E | nable PPTP VPN Service | | | | |
| ∠ E | nable IPSec VPN Service | | | | |
| ✓ E | nable 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.



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 >> F | PPP General | Setup |
|----------------|-------------|-------------|-------|
|----------------|-------------|-------------|-------|

| PPP General Setup | |
|--|--|
| PPP/MP Protocol | IP Address Assignment for Dial-In Users |
| Dial-In PPP Authentication | (When DHCP Disable set) Start IP Address 192.168.1.200 |
| Dial-In PPP Encryption (MPPE) Optional MPPE | |
| Mutual Authentication (PAP) 🛛 🔘 Yes 💿 No | |
| Username | |
| Password | |
| | К |

| Dial-In PPP Authentication PAP Only | Select this option to force the router to authenticate dial-in users with the PAP protocol. |
|---|---|
| PAP or CHAP | Selecting this option means the router will attempt to authenticate dial-in users with the CHAP protocol first. If the dial-in user does not support this protocol, it will fall back to use the PAP protocol for authentication. |
| Dial-In PPP Encryption (MPPE Optional MPPE | This option represents that the MPPE encryption method will be optionally employed in the router for the remote dial-in user. If the remote dial-in user does not support the MPPE encryption algorithm, the router will transmit "no MPPE encrypted packets". Otherwise, the MPPE encryption scheme will be used to encrypt the data. Optional MPPE Require MPPE(40/128 bit) Maximum MPPE(128 bit) Require MPPE (40/128bits) - Selecting this option will force the router to encrypt packets by using the MPPE encryption algorithm. In addition, the remote dial-in user will use 40-bit to perform encryption prior to using 128-bit for encryption. In other words, if 128-bit MPPE encryption method is not available, then 40-bit encryption scheme will be applied to encrypt the data. Maximum MPPE - This option indicates that the router will use the MPPE encryption scheme with maximum bits (128-bit) to encrypt the data. |
| Mutual Authentication (PAP) | The Mutual Authentication function is mainly used to communicate with other routers or clients who need bi-directional authentication in order to provide stronger security, for example, Cisco routers. So you should enable this function when your peer router requires mutual authentication. You should further specify the User Name and Password of the mutual authentication peer. |
| Start IP Address | Enter a start IP address for the dial-in PPP connection. You should choose an IP address from the local private network. For example, if the local private network is 192.168.1.0/255.255.255.0, you could choose 192.168.1.200 as the Start IP Address. |

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 v | will not be encrypted. |
| High (ESP) 🗹 DES 🗹 30 | DES 🔽 AES |
| Data will be encrypted and a | authentic. |

Cancel

ΟK

| 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.

VPN and Remote Access >> IPSec Peer Identity

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

Set to Factory Default

Click it to clear all indexes.

Index

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

Name

Display the profile name of that index.

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

VPN and Remote Access >> IPSec Peer Identity

| Profile Name | ??? | |
|-----------------|---------------------|------------|
| Enable this a | ccount | |
| Accept Any | Peer ID | |
| O Accept Subj | ect Alternative Nam | e |
| Туре | | IP Address |
| IP | | |
| O Accept Subj | ect Name | |
| Country (C) | | |
| State (ST) | | |
| Location (L) | | |
| Orginization (C |) | |
| Orginization Ur | iit (OU) | |
| Common Name | (CN) | |
| | | |

| 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.

| emote Acce | ss User Accounts: | | | Set to Fac | tory Delau |
|------------|-------------------|--------|------------|------------|------------|
| Index | User | Status | Index | User | Status |
| <u>1.</u> | ??? | × | <u>17.</u> | ??? | × |
| <u>2.</u> | ??? | × | <u>18.</u> | ??? | × |
| <u>3.</u> | ??? | × | <u>19.</u> | ??? | × |
| <u>4.</u> | ??? | × | <u>20.</u> | ??? | × |
| <u>5.</u> | ??? | × | <u>21.</u> | ??? | × |
| <u>6.</u> | ??? | × | <u>22.</u> | ??? | × |
| <u>7.</u> | ??? | × | <u>23.</u> | ??? | × |
| <u>8.</u> | ??? | × | <u>24.</u> | ??? | × |
| <u>9.</u> | ??? | × | <u>25.</u> | ??? | × |
| <u>10.</u> | ??? | × | <u>26.</u> | ??? | × |
| <u>11.</u> | ??? | × | <u>27.</u> | ??? | × |
| <u>12.</u> | ??? | × | <u>28.</u> | ??? | × |
| <u>13.</u> | ??? | × | <u>29.</u> | ??? | × |
| <u>14.</u> | ??? | × | <u>30.</u> | ??? | × |
| <u>15.</u> | ??? | × | <u>31.</u> | ??? | × |
| <u>16.</u> | ??? | × | <u>32.</u> | ??? | × |

VPN and Remote Access >> Remote Dial-in User

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

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

VPN and Remote Access >> Remote Dial-in User

| User account and Authentication | Username ??? | |
|---------------------------------|--|--|
| Enable this account | Password | |
| Idle Timeout 300 second(s) | | |
| | IKE Authentication Method | |
| Allowed Dial-In Type | 🔄 🗹 Pre-Shared Key | |
| 🗹 РРТР | IKE Pre-Shared Key Digital Signature(X.509) None | |
| 🗹 IPSec Tunnel | | |
| ☑ L2TP with IPSec Policy None | | |
| | IPSec Security Method | |
| | Medium(AH) | |
| | High(ESP) 🗹 DES 🗹 3DES 🗹 AES | |
| | Local ID (optional) | |

| Enable this account | Check the box to enable this function. Idle Timeout- If the dial-in user is idle over the limitation of the timer, the router will drop this connection. By default, the Idle Timeout is set to 300 seconds. |
|---------------------------|--|
| РРТР | 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 and provides up to **32** profiles simultaneously. The following figure shows the summary table.

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

VPN and Remote Access >> LAN to LAN

Set to Factory Default

Name

Click to clear all indexes.

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

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

Status

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

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

| Profile Index : 1 1. Common Settings | | |
|--|--------------------|---|
| Profile Name Enable this profile Netbios Naming Packet | ??? ● Pass ● Block | Call Direction Both Dial-Out Dial-In Always on Idle Timeout 300 second(s) Enable PING to keep alive PING to the IP |
| 2. Dial-Out Settings | | |
| Type of Server I am ca PPTP IPSec Tunnel L2TP with IPSec Poli Server IP/Host Name for (such as draytek.com or | cy None | Username ??? Password PPP Authentication PAP/CHAP V VJ Compression On Off IKE Authentication Method Ore-Shared Key IKE Pre-Shared Key Digital Signature(X.509) None V IPSec Security Method Omedium(AH) High(ESP) DES without Authentication V Advanced Index(1-15) in Schedule Setup: , , , , , , , |

VPN and Remote Access >> LAN to LAN

| 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 by no where to know this situation. To resolve this dilemma, by continuously sending PING packets to the remote host, the Vigor router can know the true existence of this VPN connection and react accordingly. This is independent of DPD (dead peer detection). | | |
| РРТР | Build a PPTP VPN connection to the server through the Internet. You should set the identity like User Name and Password below for the authentication of remote server. | | |
| IPSec Tunnel | Build an IPSec VPN connection to the server through Internet. | | |
| L2TP with | Build a L2TP VPN connection through the Internet. You can select to use L2TP alone or with IPSec. Select from below: None: Do not apply the IPSec policy. Accordingly, the VPN connection employed the L2TP without IPSec policy can be viewed as one pure L2TP connection. Nice to Have: Apply the IPSec policy first, if it is applicable during negotiation. Otherwise, the dial-out VPN connection becomes one pure L2TP connection. Must: Specify the IPSec policy to be definitely applied on the L2TP connection. | | |
| User Name | This field is applicable when you select PPTP or L2TP with or without IPSec policy above. | | |
| Password | This field is applicable when you select PPTP or L2TP with or without IPSec policy above. | | |
| PPP Authentication | This field is applicable when you select PPTP or L2TP with or without IPSec policy above. PAP/CHAP is the most common selection due to wild compatibility. | | |
| VJ compression | This field is applicable when you select PPTP or L2TP with or without IPSec policy above. VJ Compression is used for TCP/IP protocol header compression. Normally set to Yes to improve bandwidth utilization. | | |
| IKE Authentication Method | Improve bandwidth utilization. This group of fields is applicable for IPSec Tunnels and L2TP with IPSec Policy. Pre-Shared Key - Input 1-63 characters as pre-shared key. Digital Signature (X.509) - Select one predefined Profiles set | | |

| | in the VPN and Remote Access >>IPSec Peer Identity. |
|-----------------------|--|
| IPSec Security Method | This group of fields is a must for IPSec Tunnels and L2TP with IPSec Policy. |
| Medium | Authentication Header (AH) means data will be authenticated, but not be encrypted. By default, this option is active. |
| | High (ESP-Encapsulating Security Payload)- means payload (data) will be encrypted and authenticated. Select from below: DES without Authentication -Use DES encryption algorithm and not apply any authentication scheme. DES with Authentication-Use DES encryption algorithm and apply MD5 or SHA-1 authentication algorithm. 3DES without Authentication-Use triple DES encryption algorithm and not apply any authentication scheme. 3DES with Authentication-Use triple DES encryption algorithm and paply MD5 or SHA-1 authentication algorithm. AES without 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 not apply any authentication scheme. |
| Advanced | Specify mode, proposal and key life of each IKE phase, Gateway, etc. The window of advance setup is shown as below: |
| | http://192.168.1.5 - IKE advanced settings - Microsoft Internet Explorer IKE advanced settings IKE phase 1 mode IKE phase 1 proposal DES_MD5_G1/DES_MD5_G1/3DES_MD5_G2 |

IKE phase 2 proposal

IKE phase 1 key lifetime

IKE phase 2 key lifetime

Perfect Forward Secret

Local ID

Main mode.

schemes.

HMAC_SHA1/HMAC_MD5 💌

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

IKE phase 1 proposal-To propose the local available

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

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

(900 ~ 86400)

(600 ~ 86400)

🔘 Enable

28800

3600

💿 Disable

algorithms.

IKE phase 1 key lifetime-For security reason, the lifetime of key should be defined. The default value is 28800 seconds. You may specify a value in between 900 and 86400 seconds. **IKE phase 2 key lifetime**-For security reason, the lifetime of key should be defined. The default value is 3600 seconds. You may specify a value in between 600 and 86400 seconds. **Perfect Forward Secret (PFS)**-The IKE Phase 1 key will be reused to avoid the computation complexity in phase 2. The default value is inactive this function.

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

| 3. Dial-In Settings | | | | | |
|---|---|--|--|--|--|
| Allowed Dial-In Type | | | | | |
| ✓ PPTP ✓ IPSec Tunnel ✓ L2TP with IPSec Policy None ✓ Specify Remote VPN Gateway Peer VPN Server IP | | Username | ??? | | |
| | | Password | | | |
| | | VJ Compression | 💿 On 🔘 Off | | |
| | | IKE Authentication ✓ Pre-Shared Key IKE Pre-Shared Key | | | |
| or Peer ID | | Digital Signature(X. | | | |
| | | IPSec Security Met Medium (AH) High (ESP) DES M 30 | | | |
| 4. TCP/IP Network Sett | ings | | | | |
| 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 | 0.0.0.0 | 40 | | | |
| Remote Network Mask | 255.255.255.0 | | | | |
| More | | | Change default route to this VPN tunnel (Only _ single WAN supports this) | | |
| 2 | ОК | Clear Cancel | | | |
| Allowed Dial-In Typ | e Determine | e the dial-in connection | n with different types. | | |
| РРТР | 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 | | remote dial-in user to n through Internet. | mote dial-in user to trigger an IPSec VPN hrough Internet. | | |
| L2TP Allow the remote dial-in user to make a L2TP VPN connection through the Internet. You can select to us alone or with IPSec. Select from below: None - Do not apply the IPSec policy. Accordingly, connection employed the L2TP without IPSec policy viewed as one pure L2TP connection. | | | You can select to use L2TF below: policy. Accordingly, the VP without IPSec policy can be | | |

| | Nice to Have - Apply the IPSec policy first, if it is applicable during negotiation. Otherwise, the dial-in VPN connection becomes one pure L2TP connection. Must - Specify the IPSec policy to be definitely applied on the L2TP connection. |
|-------------------------------|---|
| Specify Remote VPN Gateway | You can specify the IP address of the remote dial-in user or peer ID (should be the same with the ID setting in dial-in type) by checking the box. Enter Also, you should further specify the corresponding security methods on the right side. |
| | If you uncheck the checkbox, the connection type you select above will apply the authentication methods and security methods in the general settings. |
| User Name | This field is applicable when you select PPTP or L2TP with or without IPSec policy above. |
| Password | This field is applicable when you select PPTP or L2TP with or without IPSec policy above. |
| VJ Compression | VJ Compression is used for TCP/IP protocol header compression. This field is applicable when you select PPTP or L2TP with or without IPSec policy above. |
| IKE Authentication Method | This group of fields is applicable for IPSec Tunnels and L2TP with IPSec Policy when you specify the IP address of the remote node. The only exception is Digital Signature (X.509) can be set when you select IPSec tunnel either with or without specify the IP address of the remote node. Pre-Shared Key - Check the box of Pre-Shared Key to invoke this function and type in the required characters (1-63) as the pre-shared key. Digital Signature (X.509) –Check the box of Digital Signature to invoke this function and select one predefined Profiles set in the VPN and Remote Access >> IPSec Peer Identity . |
| IPSec Security Method | This group of fields is a must for IPSec Tunnels and L2TP with IPSec Policy when you specify the remote node. Medium- Authentication Header (AH) means data will be authenticated, but not be encrypted. By default, this option is active. High- Encapsulating Security Payload (ESP) means payload (data) will be encrypted and authenticated. You may select encryption algorithm from Data Encryption Standard (DES), Triple DES (3DES), and AES. |
| My WAN IP | This field is only applicable when you select 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

VPN and Remote Access >> Connection Management

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

| | | | | | | | | | - |
|----------------------|-------------------------|-----------|---|------------|----------------------------|------------|------------------|---------|---|
| Dial-out | Tool | | | | Refre | sh Sec | onds : 10 | Refresh |) |
| VPN Con Current P | nection Statu age: 1 | 15 | | | | Pa | ge No. | Go >> | |
| VPN | Туре | Remote IP | Virtual Network | Tx Pkts | Tx Rate (Bps) | Rx Pkts | Rx Rate (Bps) | UpTime | |
| | | | | | ××××××× : C ××××××× : C | | | | - |
| Dial | | Click | k this button | to exec | ute dial o | out fur | nction. | | |
| Refresh | Seconds | | Choose the time for refresh the dial information among 5, 10, and 30. | | | | | | |
| Refresh | | Clicl | 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 X509 Lo | IMPORT REFRESH | | |
| | | | |

Generate

Click this button to open Generate Certificate Request window.

Certificate Management >> Local Certificate

| Subject Alternative Name | |
|--------------------------|------------|
| Туре | IP Address |
| IP | |
| Subject Name | |
| Country (C) | |
| State (ST) | |
| Location (L) | |
| Orginization (O) | |
| Orginization Unit (OU) | |
| Common Name (CN) | |
| Email (E) | |
| Кеу Туре | RSA 🗸 |
| Key Size | 1024 Bit 🔽 |

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

| Import | Click this button to import a saved file as the certification information. |
|---------|--|
| Refresh | Click this button to refresh the information listed below. |
| View | Click this button to view the detailed settings for certificate request. |

After clicking **Generate**, the generated information will be displayed on the window below: Certificate Management >> Local Certificate

| Name Subject | | Status | Modify |
|--|--|---|---|
| Local /C=TW/ST=HC/L=HC/O=Draytek/O | | Requesting | View Delete |
| GENERATE | IMPORT REFRESH | | |
| MIIBqj EwJIQz CQEWE3 AoGBAL a1X//f m6+Of4 hkiG9w 9yojHp eorpDa | EGIN CERTIFICATE REQUEST CCARMCAQAwajELMAkGA1UEBhMCVFcxCzAJJ EQMA4GA1UEChMHRHJheXRlazELMAkGA1UEC N1cHBvcnRAZHJheXRlay5jb2OwgZ8wDQYJJ MJdTsqfF97FEpYy+IqeJVJGuSRtqG6Etw8 gnEccQA2LPSQIQ85Qychwq07Bm0EDf10wH xZ4QQnjXXgciCOBj1iAa6MLScelsynZhkg OBAQUFAAOBgQCq3sdwVc21t9qn4U6X2BJsV stNsmWsMRuAwGeKCWc8S/gLtHnr6iccMoTo 1/rC9ZwCraOt8XUmPqNoiytq8BxStTE8vUJ ND CERTIFICATE REQUEST | CxMCURQxIjAgB KoZIhvcNAQEBB yTU5HQvXpAzcr yCalAZQoGvIiO hQ1QN5uFAgMBA Jzu7JHafSSeUn pQFx/LWdaEPU5 | gkqhkiG9w0B QADgYOAMIGJ gJBGrikTUBX DMC7f5w9xA8 AGgADANBgkq aYDZefCmGfX LqryBKKgC9t |

X509 Local Certificate Configuration

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.

| 🕘 http | ://192.168.1.5 - Certificate Informati | ion - Microsoft Internet Explorer | |
|--------|--|-----------------------------------|----------|
| | | | <u>~</u> |
| | Certific | ate Detail Information | |
| | Certificate Name: | Trusted CA-1 | |
| | Issuer: | | |
| | Subject: | | |
| | Subject Alternative Name: | | |
| | Valid From: | | |
| | Valid To: | | |
| | | Close | |
| | | | ~ |

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 Ma | Certificate Management >> Certificate Backup | | | |
|----------------|---|--|--|--|
| | | | | |
| Certificate Ba | ckup / Restoration | | | |
| Backup | | | | |
| | Encrypt password: | | | |
| | Confirm password: | | | |
| | Click Backup to download certificates to your local PC as a file. | | | |
| Restoration | | | | |
| | Select a backup file to restore. | | | |
| | Browse. | | | |
| | Decrypt password: | | | |
| | Click Restore to upload the file. | | | |

4.11 Wireless LAN

This function is used for "n" models only.

Outlinets Managements, Cartificate Dealeur

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 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.

| Wireless LAN | |
|----------------|--|
| General Setup | |
| Security | |
| Access Control | |
| ▶ WPS | |
| ▶ WDS | |
| AP Discovery | |
| Station List | |

Wireless LAN >> General Setup

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.

| ble Wireless | LAN | | |
|--|--|---|---|
| Mode : | | Mixed(11b+11g+1 | 1n) 🔽 |
| Only schedul | n <u>Schedule</u> 9 e profiles that are ignored. | t have the action "Force Down" an | ,, e applied to the WLAN, all |
| Enable H | Hide SSID | SSID | Isolate LAN Member |
| 1 | | DrayTek | |
| 2 | | | |
| 3 🔲 | | | |
| 4 | | | |
| Isolate LAN Wireless clier Channel: Ch | nts (stations) : nts (stations) annel 6, 2437M | | ss wired PCs on LAN. |
| Wireless clier Isolate LAN Wireless clier Channel: Ch | nts (stations) : nts (stations) annel 6, 2437M e: necessary |) with the same SSID cannot acce | ss wired PCs on LAN. |
| Wireless clien Isolate LAN Wireless clien Channel: Ch: Long Preambl Packet-OVER T x Burst | nts (stations) : nts (stations) annel 6, 2437M e: necessary |) with the same SSID cannot acce Hz 💌 Long Preamble: | ss wired PCs on LAN. |
| Wireless clier Isolate LAN Wireless clier Channel: Ch: Long Preambl Packet-OVER T x Burst Note: | nts (stations) : nts (stations) annel 6, 2437M e: necessary DRIVE TM |) with the same SSID cannot acce Hz 💌 Long Preamble: | ss wired PCs on LAN. |
| Wireless clier Isolate LAN Wireless clier Channel: Ch: .ong Preambl Packet-OVER Tx Burst Note: The same tec | nts (stations) : nts (stations) annel 6, 2437M e: necessary DRIVE TM |) with the same SSID cannot acce Hz Long Preamble: for some old 802.11 b devices on | ss wired PCs on LAN. |
| Wireless clier Isolate LAN Wireless clier Channel: Ch: .ong Preambl Packet-OVER T x Burst Note: | nts (stations) : nts (stations) annel 6, 2437M e: necessary DRIVE TM |) with the same SSID cannot acce Hz Long Preamble: for some old 802.11 b devices on | ss wired PCs on LAN. |
| Wireless clier Isolate LAN Wireless clier Channel: Ch: .ong Preambl Packet-OVER Tx Burst Note: The same tec | nts (stations) : annel 6, 2437M e: necessary DRIVE TM |) with the same SSID cannot acce Hz Long Preamble: for some old 802.11 b devices on t also be supported in clients to bu | ss wired PCs on LAN. |
| Wireless clier Isolate LAN Wireless clier Channel: Channel: Channel: Channel: Channel: Channel: Channel Channel: Channel: Channel Channel Dacket-OVER Tx Burst Note: The same tech Rate Control | nts (stations) : annel 6, 2437M e: necessary DRIVE TM |) with the same SSID cannot acce Hz Long Preamble: for some old 802.11 b devices onl t also be supported in clients to be Upload | ss wired PCs on LAN. Uy(lower performance) oost WLAN performance. Download |
| Wireless clier Isolate LAN Wireless clier Channel: Ch: .ong Preambl Packet-OVER Tx Burst Note: The same teo Rate Control SSID 1 | nts (stations) : annel 6, 2437M e: necessary DRIVE TM |) with the same SSID cannot acce Hz Long Preamble: for some old 802.11 b devices onl it also be supported in clients to be Upload 30000 kbps | ss wired PCs on LAN. |
| Wireless clien Isolate LAN Wireless clien Channel: Chi- ong Preamble Packet-OVER Tx Burst Note: The same teo Rate Control SSID 1 SSID 2 | nts (stations) : annel 6, 2437M e: necessary DRIVE TM |) with the same SSID cannot acce Hz Long Preamble: for some old 802.11 b devices onl t also be supported in clients to be Upload 30000 kbps 30000 kbps | ss wired PCs on LAN. y(lower performance) oost WLAN performance. Download 30000 kbps 30000 kbps |

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(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 filed is blank and the function will always work. |
| Hide SSID | Check it to prevent from wireless sniffing and make it harder for unauthorized clients or STAs to join your wireless LAN. Depending on the wireless utility, the user may only see the information except SSID or just cannot see any thing about Vigor wireless router while site surveying. The system allows you to set four sets of SSID for different usage. In default, the first set of SSID will be enabled. You can hide it for your necessity. |
| SSID | Means the identification of the wireless LAN. SSID can be any text numbers or various special characters. The default SSID is "Draytek. We suggest you to change it. |
| Isolate | LAN – Check this box to make the wireless clients (stations) with the same SSID cannot access wired PCs on LAN. Member –Check this box to make the wireless clients (stations) with the same SSID not accessing for each other. |
| Channel | Means the channel of frequency of the wireless LAN. The default channel is 6. You may switch channel if the selected channel is under serious interference. If you have no idea of choosing the frequency, please select Auto to let system determine for you. |

| 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 PreambleThis 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 OVERDBUVEThis feature can exhause the performance in data

Packet-OVERDRIVEThis 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**).

| rigor and boz. The wheless osli Adapter officy | | | |
|---|--|---------------------|------|
| Configuration Status Option About | | | _ |
| General Setting | Advance Setting | | |
| 🗹 Auto launch when Windows <u>s</u> tart up | 🔲 Disable <u>R</u> adio | | |
| Remember mini status position | \underline{F} ragmentation Threshold : | 23 | 346 |
| Auto hide mini status | RTS Threshold : | 23 | 347 |
| Set <u>m</u> ini status always on top | Frequency : | 802.11b/g/n - 2.4GH | * |
| Enable IP Setting and Proxy Setting in Profile | Ad-hoc <u>C</u> hannel: | 1 | ~ |
| Group Roaming Ad-hoc | Po <u>w</u> er Save Mode: | Disable | ~ |
| | Tx <u>B</u> urst : | Disable | * |
| WLAN type to connect | | | |
| Infrastructure and Ad-hoc <u>n</u> etwork | | | |
| O Infrastructurg network only | | | |
| Ad-hoc network only | | | |
| Automatically connect to non-preferred networks | | | |
| | | | |
| | OK | Cancel | pply |

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 | A: | | | |
| Encr | yption Mode: | | TKIP | |
| | Pre-Shared Key(F | PSK): | ****** | |
| | Type 8~63 ASCI "cfgs01a2" or " | | | digits leading by "Ox", for example |
| WEP | 9 | | | |
| | Encryption Mode | | 64-Bit 💌 | |
| | | | ***** | |
| | ○Кеу 2 : | | ***** | |
| | ○Кеу 3 : | | ***** | |
| | ⊖Key 4 : | | ***** | |
| Туре | 64 bit WEP key 9 5 ASCII character 142333132". | or 10 Hexade | ecimal digits leadir | ng by "Ox", for example "AB312" or |
| Туре | 128 bit WEP key a 13 ASCII characte 3456789abc" or "0x | | | ing by "Ox", for example 3". |

Mode

There are several modes provided for you to choose.

Mode:



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.

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

WPA

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...").

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 |
| Ľ | M IT |

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

WEP

| | 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. |
| ОК | 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 2710 series which served as an AP, press **WPS** button once on the front panel of the router or click **Start PBC** on web configuration interface. On the side

of a station with network card installed, press Start PBC button of network card.



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



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



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

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

Wireless LAN >> WPS (Wi-Fi Protected Setup)

🗹 Enable WPS 🗘

Wi-Fi Protected Setup Information

| WPS Status | Configured |
|---------------------|------------|
| SSID | default |
| Authentication Mode | Disable |

Device Configure

| _ | |
|------------------------------|-----------|
| Configure via Push Button | Start PBC |
| Configure via Client PinCode | 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.

arepsilon : 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 WPS LED on the router will blink fast when WPS is in progress. It will return to normal condition after two minutes. (You need to setup WPS within two minutes) |
| Configure via Client PinCode | Please input the PIN code specified in wireless client you wish to connect, and click Start PIN button. The WLAN LED on the router will blink fast when WPS is in progress. It will return to normal condition after two minutes. (You need to setup WPS within two minutes) |

4.11.6 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.

| Mode: | Disable 🗸 | Bridge | | |
|--|---|--|--|--|
| | | Enable Peer MAC Address | | |
| Security: Disable |) WEP 🔘 Pre-shared Key | | | |
| | VEP key set in <u>Security Settings</u> . | Note: Disable unused links to get better performance. | | |
| Pre-shared Key | | Repeater | | |
| Type : TKIP Key : *********************************** | | Enable Peer MAC Addess | | |
| | | Access Point Function: Inable Disable | | |
| | | Status: | | |
| | | Link Status Note: The status is valid only when the peer all supports this function. | | |

Wireless LAN >> WDS Settings



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. Disable Disable Bridge Repeater |
|-----------------------|---|
| 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.

Wireless LAN >> Access Point Discovery

| | BSSID | Channel SSID |
|--------------------|---|--|
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | Scan |
| | See Statistics. | |
| | Note: During the sc connect with the rou | anning process (~5 seconds), no station is allowed to uter. |
| | Add to WDS Setting | <u>s</u> : |
| | AP's MAC address | |
| | Add to | 💿 Bridge 💦 Repeater |
| | | |
| | | |
| Scan | | It is used to discover all the connected AP. The results will |
| Scan | | It is used to discover all the connected AP. The results will shown on the box above this button. |
| | | shown on the box above this button. It displays the statistics for the channels used by APs. |
| | | shown on the box above this button. |
| | | shown on the box above this button. It displays the statistics for the channels used by APs. Wireless LAN>> Site Survey Statistics |
| Scan Statistics | | shown on the box above this button. It displays the statistics for the channels used by APs. Wireless LAN>> Site Survey Statistics |
| | | shown on the box above this button. It displays the statistics for the channels used by APs. Wireless LAN>> Site Survey Statistics |
| | | shown on the box above this button. It displays the statistics for the channels used by APs. Wireless LAN>> Site Survey Statistics Recommended channels for usage: 12345678910111213 |

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.

Wireless LAN >> Station List

| | Status | MAC Address | Associated with | |
|---------|--|-----------------------------|-------------------------------------|------------------|
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | Refresh | | |
| | Status Codes : | | | |
| | C: Connected, M E: Connected, V | | | |
| | P: Connected, V | VPA. | | |
| | A: Connected, \ B: Blocked by A | | | |
| | N: Connecting. | | | |
| | F: Fail to pass V | VPA/PSK authentication. | | |
| | Note: After a st | tation connects to the rout | er successfully, it may be | |
| | turned off witho connection expi | | will still be on the list until the | |
| | | | | |
| | Add to <u>Access (</u> | Control : | | |
| | Client's MAC add | dress :::: | : | |
| | | Add | | |
| Refresh | | Click t | his button to refresh the stat | us of station li |
| Add | | Click t | his button to add current typ | ed MAC addre |

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.

| System Maintenance |
|------------------------|
| System Status |
| ▶ TR-069 |
| Administrator Password |
| Configuration Backup |
| SysLog / Mail Alert |
| Time and Date |
| Management |
| Reboot System |
| Firmware Upgrade |
| |

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 | : Vigor2710 series |
|-----------------------|-----------------------|
| Firmware Version | : 3.2.1_RC11 |
| Build Date/Time | : Aug 6 2008 18:07:02 |
| ADSL Firmware Version | : 211801_A Annex A |

| LAN | | WAN | |
|-----------------|---------------------|-----------------|---------------------|
| MAC Address | : 00-50-7F-92-F5-00 | Link Status | : Disconnected |
| 1st IP Address | : 192.168.1.5 | MAC Address | : 00-50-7F-92-F5-01 |
| 1st Subnet Mask | : 255.255.255.0 | Connection | : PPPoE |
| DHCP Server | : Yes | IP Address | : |
| DNS | : 194.109.6.66 | Default Gateway | : |

| Wireless LAN | | |
|---------------------------------|-----------|--|
| MAC Address : 00-50-7f-92-f5-00 | | |
| 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. | |
| 1 st IP Address | Display the IP address of the LAN interface. | |
| 1 st 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.

| S\ | /stem | Maintenance | >> | TR-069 | Setting |
|----|-------|-------------|----|---------|---------|
| 3 | stem | Maintenance | // | 114-009 | Setting |

| ACS and CPE Settings | | | | |
|--------------------------|---------------|--|--|--|
| ACS Server On | Internet 💌 | | | |
| ACS Server | | | | |
| URL | | | | |
| Username | | | | |
| Password | | | | |
| CPE Client © Enable | | | | |
| URL | | | | |
| Port | 8069 | | | |
| Username | vigor | | | |
| Password | | | | |
| Periodic Inform Settings | | | | |
| 🔘 Disable | | | | |
| 📀 Enable | | | | |
| Interval Time | 900 second(s) | | | |
| | ОК | | | |
| ACS Server On | Choose the interface for the router connecting to ACS server. ACS Server On Internet PVC |
|--------------------------|---|
| 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 | |
| New Password | |
| Confirm Password | 1 |
| Old Password | OK Type in the old password. The factory default setting for password is " admin ". |
| New Password | Type in new password in this filed. |
| Confirm Password | Type in the new password again. |

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

4.12.4 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

| Restoration | |
|-------------|--|
| | Select a configuration file. |
| | Browse |
| | Click Restore to upload the file. |
| | Restore |
| Backup | |
| | Click Backup to download current running configurations as a file. |
| | Backup Cancel |

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

| File Dov | vnload 🛛 🗙 |
|----------|---|
| ? | You are downloading the file: config.cfg from 192.168.1.1 |
| | Would you like to open the file or save it to your computer? Open Save Cancel More Info Image: Always ask before opening this type of file Save Save <t< th=""></t<> |

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

| Save As | | | | | | ? 🗙 |
|---|--|--------------------|---|-----|------|--------|
| Save in: | 🞯 Desktop | | ~ | 0 Ø | 📂 🛄• | |
| My Recent Documents Desktop My Documents | My Documents My Computer My Network Pk RVS-COM Lite Annex A MWSnap300 TeleDanmark Tools Config V2k2_232_con W2k6_250_con | aces fig_1 | | | | |
| My Computer | | | | | | |
| | File name: | config | | | ~ | Save |
| My Network | Save as type: | Configuration file | | | * | Cancel |

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

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

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

Restore Configuration

System Maintenance >> Configuration Backup

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

| Configuration Restoration | Backup / Restoration |
|------------------------------|--|
| | Select a configuration file. Browse Click Restore to upload the file. Restore |
| Backup | Click Backup to download current running configurations as a file. |
| | Backup Cancel |

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

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.

| S١ | /stem | Maintenance >> | S | vsL og | / Mail | Alert | Setup |
|--------|-------|----------------|-----|----------|----------|-------|-------|
| \sim | Storn | manneenaneer | · • | y SLOG I | / ITTGUT | Alert | occup |

| SysLog / Mail Alert Setup | | | | |
|--|--|--|--|--|
| SysLog Access Setup Server IP Address Destination Port Firewall Log VPN Log Call Log WAN Log Router/DSL information OK | Mail Alert Setup ✓ Enable Send a test e-mail SMTP Server | | | |
| Enable (Syslog Access) Check ' | 'Enable " to activate function of syslog. | | | |
| | ldress of the Syslog server. | | | |
| Destination Port Assign | a port for the Syslog protocol. | | | |
| corresp | he box listed on this web page to send the onding message of firewall, VPN, User Access, AN, 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.

| m Router Tools V3.5.1 | 🕨 🕥 About Router Tools | |
|-----------------------|---------------------------------|--|
| | 🐴 Firmware Upgrade Utility | |
| | 🔟 Syslog | |
| | 🔂 Uninstall Router Tools V3.5.1 | |
| | 🕘 Visit DrayTek Web Site | |

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.

| Status TX Pac | | Vigor series RX Packets 1470 | | WAN IP (Fixed) | TX Packets 0 RX Packets 0 | TX Rate 0 RX Rate 0 |
|---|-----------|------------------------------------|--|---|---|---|
| vall Log VPN on Line Router: IP Address | | ess Log Call Log | Host Name: | Network Information Network Information Network | | |
| 192.168.1.1 | 255.255.2 | 00-50-7F-54-6 | NIC Description: NIC Information — MAC Address: IP Address: | Si5 900-Based | PCI Fast Ethernet Adapt Default Geteway: DHCP Server: | er - Packet St 192.168.1.1 192.168.1.1 |
| < | | > | Subnet Mask: | 255.255.255.0 | Lease Obtained: | Mon Jan 22 01:28:23 2007 |
| | Refresh | | DNS Servers: | | Lease Expires: | Thu Jan 25 01:28:23 2007 |

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 | | |
|---|---|--|
| Time Information | | |
| Current System Time 20 | 00 Jan 1 Sat 1 : 54 : 44 Inquire Time | |
| Time Setup | | |
| 🔘 Use Browser Time | | |
| 💿 Use Internet Time Client | | |
| Time Protocol | NTP (RFC-1305) 🔽 | |
| Server IP Address | pool. ntp. org | |
| Time Zone | (GMT) Greenwich Mean Time : Dublin | |
| Enable Daylight Saving | | |
| Automatically Update Inter | rval 30 min 💌 | |
| Current System Time Jse Browser Time | Click Inquire Time to get the current time. Select this option to use the browser time from the | |
| | remote administrator PC host as router's system time. | |
| Jse Internet Time | Select to inquire time information from Time Server of the Internet using assigned protocol. | |
| Fime Protocol | Select a time protocol. | |
| Server IP Address Type the IP address of the time server. | | |
| lime Zone | Select the time zone where the router is located. | |
| Automatically Update Inter | rval Select a time interval for updating from the NTP serve | |
| Click OK to save these setting | 198. | |

4.12.7 Management

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

| S | /stem | Main | tenan | ce >> | Μ | anad | emer | ht |
|------------|--------|--------------|-----------|-------|---|------|------|----|
| - U | 0.0111 | THE OWNER OF | COLLOCH 1 | 00 | | anag | | |

| Management Setup | | | |
|-------------------------|----------------|-------------------------|--------------------|
| Management Access Co | introl | Management Port Setu | р |
| 🔲 Allow management fro | m the Internet | 💿 User Define Ports 🛛 🤇 |) Default Ports |
| FTP Server | | Telnet Port | 23 (Default: 23) |
| MTTP Server | | HTTP Port | 80 (Default: 80) |
| HTTPS Server | | HTTPS Port | 443 (Default: 443) |
| 🗹 Telnet Server | | FTP Port | |
| SSH Server | | | |
| ☑ Disable PING from the | Internet | SSH Port | 22 (Default: 22) |
| Access List | | SNMP Setup | |
| List IP | Subnet Mask | Enable SNMP Agent | |
| 1 | ~ | Get Community | public |
| 2 | ~ | Set Community | private |
| 3 | ~ | Manager Host IP | |
| | | Trap Community | public |
| | | Notification Host IP | |
| | | Trap Timeout | 10 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 Mainten | nce >> Reboot System |
|----------------|---------------------------------------|
| Reboot System | |
| | Do you want to reboot your router ? |
| | Osing current configuration |
| | O Using factory default configuration |
| | |

ΟK

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

Firmware Upgrade Procedures:

| Web Firmware Upgrade | |
|---|---------|
| Select a firmware file. | |
| | Browse. |
| Click Upgrade to upload the file. Upgrade | |
| | |
| TFTP Firmware Upgrade from LAN | |
| Current Firmware Version: 3.2.1 RC5 | |

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

Do you want to upgrade firmware ?

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

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 4.

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.

| Diagnostics |
|--------------------|
| Dial-out Trigger |
| Routing Table |
| ARP Cache Table |
| DHCP Table |
| NAT Sessions Table |
| Data Flow Monitor |
| Traffic Graph |
| Ping Diagnosis |
| Trace Route |
| |

4.13.1 Dial-out Trigger

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

Diagnostics >> Dial-out Trigger

| | - |
|--|---|
| 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 0 | |
| 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 0 | |
| 00 00 00 00 00 00 00-00 00 00 00 00 00 0 | |
| | |
| 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.



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

| IP Address 192.168.1.1 | MAC Address 00-50-7F-C2-80-20 | Netbios Name | |
|---------------------------|----------------------------------|-----------------|--|
| 192.168.1.10 | 00-0E-A6-2A-D5-A1 | OK-LCCGJYIY075U | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |

Clear

Click it to reload the page.

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.

| Diagnos | agnostics >> View DHCP Assigned IP Addresses | | | | |
|------------------|--|-------------|-------------|---------|---|
| DHCP IP | CP IP Assignment Table | | | | |
| DHCP se Index | rver: Stop 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

| Private | IP :Port | #Pseudo Port | Peer IP :Port | Interface | |
|---------|----------|--------------|---------------|-----------|--|
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |

| Peer IP:Port | It indicates the destination IP address and port of remote host. |
|--------------|--|
| Interface | It displays the representing number for different interface. |
| Refresh | Click it to reload the page. |

4.13.6 Data Flow Monitor

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

_

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

Diagnostics >> Data Flow Monitor

| ~ | Enable | Data | Flow | Monitor | |
|---|--------|------|------|---------|--|
| | | | | | |

| | | Refresh Se | conds: 10 🚩 Page: 1 | * | <u>Refresh</u> |
|-------|------------|---------------|------------------------|----------|----------------|
| Index | IP Address | TX rate(Kbps) | <u>RX_rate(Kbps)</u> 😪 | Sessions | Action |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |

Note: 1. Click "Block" to prevent specified PC from surfing Internet for 5 minutes.

web page.

The IP blocked by the router will be shown in red, and the session column will display the remaining time that the specified IP will be blocked.

| - | | | |
|-----------------------------|---|--|--|
| Enable Data Flow Monitor | Check this box to enable this function. | | |
| Refresh Seconds | Use the drop down list to choose the time interval of refreshing data flow that will be done by the system automatically. | | |
| | Refresh Seconds: 5 V 5 10 15 30 | | |
| Refresh | Click this link to refresh this page manually. | | |
| Index | Display the number of the data flow. | | |
| IP Address | Display the IP address of the monitored device. | | |
| TX rate (kbps) | Display the transmission speed of the monitored device. | | |
| RX rate (kbps) | Display the receiving speed of the monitored device. | | |
| Sessions | Display the session number that you specified in Limit Session | | |

Action

Block - can prevent specified PC accessing into Internet within 5 minutes.



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

| age: | 1 💌 | <u>Refresh</u> |
|------|---------------|----------------|
| 1 | Sessions | Action |
| | blocked / 298 | <u>Unblock</u> |
| | | |
| | | |
| | | |

4.13.7 Traffic Graph

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



Diagnostics >> Traffic Graph

4.13.8 Ping Diagnosis

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

```
Diagnostics >> Ping Diagnosis
```

| | g a LAN PC or you don't want to s gh, please select "Unspecified". | pecify |
|----------------------|---|--------------|
| Ping to: Host / IP 🚩 | IP Address: | |
| Host / IP Gateway | Run | |
| Result DNS | | <u>Clear</u> |
| | | ~ |
| | | |
| | | |
| | | |
| | | |
| | | ~ |

| 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. |

4.13.9 Trace Route

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

| Protocol: | |
|--------------------|----------|
| Host / IP Address: | Run |
| Result | Clear |
| | <u>~</u> |
| | |
| | |
| | |
| | |
| | |
| | |

| 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. |

Diagnostics >> Trace Route



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:

VPN and Remote Access >> PPP General Setup

- 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**.

| PPP General Setup PPP/MP Protocol Dial-In PPP Authentication Dial-In PPP Encryption (MPPE) Optional MPPE Mutual Authentication (PAP) Vsername Password | IP Address Assignment for D (When DHCP Disable set) Start IP Address | ial-In Users 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 | >> IPS | Sec Gei | neral Setup |
|---------|--------|--------|--------|---------|-------------|
|---------|--------|--------|--------|---------|-------------|

| /DNI 1KF | :/IDSec | : Genera | l Setur |
|----------|-----------|----------|---------|
| FIN LINE | .7 18 060 | , deneru | i occup |

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

| 101 111 | oot up for Romoto Biar in users and | Bynamio II Glione (Enn to Enny. | |
|---------|-------------------------------------|---------------------------------|--|
| | IKE Authentication Method | | |
| | Pre-Shared Key | ••••• | |
| | Confirm Pre-Shared Key | •••• | |
| | IPSec Security Method | | |
| | 🗹 Medium (AH) | | |
| | Data will be authentic, but will r | not be encrypted. | |
| | High (ESP) 🔽 DES 🔽 3DES | V AES | |
| | Data will be encrypted and auth | entic. | |
| | | 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.

| Profile Index : 1 1. Common Settings | | | | |
|---|------------------|-----------------------|------------------------|--|
| Profile Name | Branch 1 | Call Direction 💿 Both | ၊ 🔘 Dial-Out 🔘 Dial-In | |
| 🗹 Enable this profile | | Always on | | |
| Netbios Naming Packet | 💿 Pass i 🔘 Block | Idle Timeout | 300 second(s) | |
| | | 📃 Enable PING to keep | alive | |
| | | PING to the IP | | |

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

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

| 2. Dial-Out Settings | |
|--|--|
| Type of Server I am calling | Username |
| О РРТР | Password |
| IPSec Tunnel | PPP Authentication PAP/CHAP |
| O L2TP with IPSec Policy None | VJ Compression On Off |
| Server IP/Host Name for VPN. | IKE Authentication Method |
| (such as draytek.com or 123.45.67.89) 220.135.240.210 | Pre-Shared Key |
| 220.135.240.210 | IKE Pre-Shared Key |
| | Digital Signature(X.509) |
| | None 🗸 |
| | |
| | IPSec Security Method Medium(AH) |
| | High(ESP) DES without Authentication |
| | Advanced |
| | |
| | Index(1-15) in <u>Schedule</u> 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.

| Type of Server I am calling | Username | draytek |
|---------------------------------------|--|--------------------|
| 💿 РРТР | Password | ••••• |
| O IPSec Tunnel | PPP Authentication | |
| O L2TP with IPSec Policy None | VJ Compression | 💿 On 🔘 Off |
| Server IP/Host Name for VPN. | IKE Authentication M | ethod |
| (such as draytek.com or 123.45.67.89) | Pre-Shared Key | |
| 220.135.240.210 | IKE Pre-Shared Key | |
| | Digital Signature(X.5) | 09) |
| | None 🛩 | |
| | | |
| | IPSec Security Metho | d |
| | Medium(AH) High(ESP) DES with | out Authentication |
| | | |
| | Advanced | |
| | Index(1-15) in Schedule | Setup: |
| | | |

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

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

| Username | |
|--|---|
| Password | |
| VJ Compression | 💿 On 🔘 Off |
| Pre-Shared Key IKE Pre-Shared Key Digital Signature(X.509 None IPSec Security Method Medium (AH) High (ESP) |) |
| | Password VJ Compression IKE Authentication Med Pre-Shared Key IKE Pre-Shared Key Digital Signature(X.509 None IPSec Security Method Medium (AH) |

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

| 3. Dial-In Settings | | | |
|---|---|------------|--|
| Allowed Dial-In Type | | | |
| PPTP | Username | draytek | |
| IPSec Tunnel | Password | ••••• | |
| L2TP with IPSec Policy None | VJ Compression | 💿 On 🔘 Off | |
| Specify Remote VPN Gateway Peer VPN Server IP 220.135.240.210 or Peer ID | IKE Authentication Method ✓ Pre-Shared Key IKE Pre-Shared Key Digital Signature(X.509) None | | |
| | IPSec Security Met | hod | |
| | Medium (AH) | | |
| | High (ESP) | DES 🗹 AES | |

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

| 4. TCP/IP Network Settings | | | | |
|----------------------------|---------------|---|-----------------------------|--|
| My WAN IP | 0.0.0.0 | RIP Direction | Disable 🖌 | |
| Remote Gateway IP | 0.0.0.0 | From first subnet to ren do | note network, you have to | |
| Remote Network IP | 192.168.2.0 | | Route 💌 | |
| Remote Network Mask | 255.255.255.0 | | | |
| | More | Change default route single WAN supports this | to this VPN tunnel (Only) | |
| | ОК СІ | ear Cancel | | |

Settings in Router B in the remote office:

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

| PPP General Setup | | | | |
|--------------------------------------|--------------|----------------|--------------|---------------|
| PPP/MP Protocol | | IP Address As | signment for | Dial-In Users |
| Dial-In PPP | P or CHAP 🔽 | (When DHCP | Disable set) | |
| Authentication | | Start IP Addre | SS | 192.168.2.200 |
| Dial-In PPP Encryption Opt (MPPE) | ional MPPE | * | | |
| Mutual Authentication (PAP |) 🔵 Yes 💽 No | | | |
| Username | | | | |
| Password | | | | |

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

| VPN 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).

| 141 11 | l oot ap for Remote Blar in asers ana | by name in chore (chirt to chirt). | |
|--------|---------------------------------------|------------------------------------|--|
| | IKE Authentication Method | | |
| | Pre-Shared Key | •••• | |
| | Confirm Pre-Shared Key | •••• | |
| | IPSec Security Method | | |
| | 🗹 Medium (AH) | | |
| | Data will be authentic, but will r | not be encrypted. | |
| | High (ESP) 🛛 🗹 DES 🔽 3DES | ✓ AES | |
| | Data will be encrypted and auth | entic. | |
| | | 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 Branch 1 | Call Direction Both Dial-Out Dial-In Always on Idle Timeout 300 second(s) Enable PING to keep alive PING to the IP | | | |

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

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

2. Dial-Out Settings

| Type of Server I am calling PPTP IPSec Tunnel L2TP with IPSec Policy | Username ??? Password |
|--|--|
| Server IP/Host Name for VPN. (such as draytek.com or 123.45.67.89) 220.135.240.208 | IKE Authentication Method Pre-Shared Key IKE Pre-Shared Key Digital Signature(X.509) None Digital Signature(X.509) None Psec Security Method Medium(AH) High(ESP) 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 Username draytek ⊙ РРТР Password O IPSec Tunnel PPP Authentication PAP/CHAP 🔽 ○ L2TP with IPSec Policy None VJ Compression 📀 On 🔘 Off Server IP/Host Name for VPN. **IKE Authentication Method** (such as draytek.com or 123.45.67.89) Pre-Shared Key 220.135.240.208 IKE Pre-Shared Key Digital Signature(X.509) None 🔽 **IPSec Security Method** Medium(AH) ○ High(ESP) DES without Authentication Advanced Index(1-15) in Schedule Setup:

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

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

3. Dial-In Settings

| or bidi in oottings | | |
|---|--|------------|
| Allowed Dial-In Type | | |
| PPTP | Username | ??? |
| 🗹 IPSec Tunnel | Password | |
| L2TP with IPSec Policy None | VJ Compression | 💿 On 🔘 Off |
| ✓ Specify Remote VPN Gateway Peer VPN Server IP 220.135.240.208 or Peer ID | IKE Authentication Me ✓ Pre-Shared Key Digital Signature(X.509 None ✓ IPSec Security Method ✓ Medium (AH) High (ESP) ✓ DES ✓ 3DES |) |

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 | | |
| 🗹 РРТР | Username | draytek |
| 🔲 IPSec Tunnel | Password | ••••• |
| L2TP with IPSec Policy None | VJ Compression | 💿 On 🔘 Off |
| Specify Remote VPN Gateway Peer VPN Server IP 220.135.240.208 or Peer ID | IKE Authentication M Pre-Shared Key IKE Pre-Shared Key Digital Signature(X.5) None IPSec Security Methe Medium (AH) High (ESP) | 09) Dd |
| | 🗹 DES 🗹 3DE | S 🗹 AES |

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

| | 4. TCP/IP Network Setti | ings | | |
|-----------------|-------------------------|---------------|---|--------------------------------|
| | My WAN IP | 0.0.0.0 | RIP Direction | Disable 💌 |
| | Remote Gateway IP | 0.0.0.0 | From first subnet to rem do | note network, you have to |
| | Remote Network IP | 192.168.1.0 | | Route 🛩 |
| | Remote Network Mask | 255.255.255.0 | | |
| | | More | Change default route single WAN supports this | to this VPN tunnel (Only) |
| 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:

VPN and Remote Assass >> PPP Canaral Satur

- 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**.

| PP General Setup | | |
|--|--------------------------|-----------------|
| PPP/MP Protocol | IP Address Assignment fo | r Dial-In Users |
| Dial-In PPP PAP or CHAP | (When DHCP Disable set) | |
| Authentication | Start IP Address | 192.168.1.200 |
| Dial-In PPP Encryption Optional MPPE | | |
| Autual Authentication (PAP) 🛛 🔘 Yes 💿 No | | |
| Jsername | | |
| Password | | |

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

VPN and Remote Access >> Remote Dial-in User

| | 4100 | o | |
|----------|--------|---------|-------|
| 7PN 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 r | not be encrypted. |
| High (ESP) 🛛 🗹 DES 🔽 3DES | ✓ AES |
| Data will be encrypted and auth | entic. |
| | 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.

| User account and Authentication | Username ??? | |
|---|--|--|
| Enable this account Idle Timeout Second(s) | Password | |
| Allowed Dial-In Type PPTP IPSec Tunnel L2TP with IPSec Policy None | IKE Authentication Method Pre-Shared Key KE Pre-Shared Key Digital Signature(X.509) None | |
| | IPSec Security Method Medium(AH) High(ESP) Ø DES Ø 3DES Ø AES Local ID (optional) | |

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

VPN and Remote Access >> Remote Dial-in User

| Index No. 1 | | |
|---------------------------------|-------------------------|------------|
| User account and Authentication | Username | ??? |
| Enable this account | Password | |
| Idle Timeout 300 second(s) | | |
| | IKE Authentication Meth | od |
| Allowed Dial-In Type | 🗹 Pre-Shared Key | |
| PPTP | IKE Pre-Shared Key | |
| 🔲 IPSec Tunnel | Digital Signature(X.509 | a) |
| L2TP with IPSec Policy None | None | · / |
| | | |
| | IPSec Security Method | |
| | Medium(AH) | |
| | High(ESP) 🛛 🗹 DES 🗹 | 3DES 🗹 AES |
| | Local ID (optional) | |
| ОК С | ear Cancel | |

Settings in the remote host:

- 1. For Win98/ME, you may use "Dial-up Networking" to create the PPTP tunnel to Vigor router. For Win2000/XP, please use "Network and Dial-up connections" or "Smart VPN Client", complimentary software to help you create PPTP, L2TP, and L2TP over IPSec tunnel. You can find it in CD-ROM in the package or go to www.draytek.com download center. Install as instructed.
- 2. After successful installation, for the first time user, you should click on the **Step 0**. **Configure** button. Reboot the host.

| 🝾 Smart VPN Client 3.2.2 (WinXP) | | |
|--|--|--|
| Step 0. This step will add the ProhibitIpSec registry value to computer in order to configure a L2TP/IPSec connection using a pre-shared key or a L2TP connection. For more infomation, please read the article Q240262 in the Microsoft Knowledgement Base. | | |
| Configure | | |
| Step 1. Dial to ISP If you have already gotten a public IP, you can skip this step. | | |
| Dial | | |
| Step 2. Connect to VPN Server | | |
| Connect | | |
| Insert Remove Setup | | |
| Status: No connection PPTP ISP @ VPN @ | | |

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

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

| Dial To VPN | × | |
|-------------------------------|---|--|
| Session Name: | Office | |
| VPN Server IP/HOST | Name(such as 123.45.67.89 or draytek.com) | |
| 192,168,1,1 | | |
| 192,100,1,1 | | |
| User Name : | draytek_user1 | |
| Password : | **** | |
| Type of VPN | | |
| ○ PPTP | ◯L2TP | |
| ⊙ IPSec Tunnel | OL2TP over IPSec | |
| PPTP Encryption - | | |
| No encryption | n | |
| | | |
| | | |
| O Maximum strength encryption | | |
| Use default ga | Use default gateway on remote network | |
| ОК | 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 Setti | ng | X |
|--|---------------------------------|--------------------------------|
| My IP : | 172.16.3.100 |) 🖌 |
| Type of IPSec | | |
| Remote Su | | 0.0.0.0 |
| Remote Su | bnet Mask : | 255 . 255 . 255 . 0 |
| 📀 Virture IP | DrayT | ek Virture Interface 🛛 👻 |
| | n IP address a an IP address | utomatically (DHCP over IPSec) |
| IP Addr | ess: | 192 . 168 . 1 . 201 |
| Subnet | Mask: | 255 . 255 . 255 . 0 |
| Security Method O Medium(AH) MDS | • |)High(ESP) DES |
| Authority Method | | |
| Certification | Authority: | Browse |
| 0 | к | 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.

| 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 | |
| O PPTP | OL2TP |
| O IPSec Tunnel | OL2TP over IPSec |
| -PPTP Encryption - | |
| 🔘 No encryptio | n |
| Require encr | yption |
| 🔵 Maximum str | ength encryption |
| Use default ga | ateway on remote network |
| ОК | Cancel |

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

5.3 QoS Setting Example

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

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

Bandwidth Management >> Quality of Service

| tatus | Bandwidth | Directon | Class 1 | Class 2 | Class 3 | Others | UDP Bai Con | | |
|------------------|-----------|----------|------------|------------|------------|--------|----------------|---------|------|
| Enable | Kbps/Kbps | Outbound | 25% | 25% | 25% | 25% | Inac | tive | Setu |
| | | | | | | | | | |
| lass Rule | 0 | | | | | | | | _ |
| Index Class 1 | | Nam | e | | | | Rule Edit | Service | Туре |

2. 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 Ser |
|--------------------------|----------------|
| General Setup | |
| 🗵 Enable the QoS Control | OUT 🖌 |
| Index | IN ame |
| Class 1 | BOTH |
| Class 2 | |
| | |

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

| Class Ind | ex #1 | | | | |
|-----------|--------|---------------|----------------|-----------------------|----------------|
| Name E | -mail | | | | |
| NO | Status | Local Address | Remote Address | DiffServ CodePoint | Service Type |
| 1 🔿 | Active | Any | Any | IP precedence 1 | TELNET(TCP:23) |
| | | | Add Edit Delet | e | |
| | | | OK Cancel | | |

Bandwidth Management >> Quality of Service

Bandwidth Management >> Quality of Service

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

| General Setup | | |
|----------------|-------------------|------------------------------|
| | QoS Control OUT 💌 | |
| Index | Class Name | Reserved_bandwidth Ratio |
| Class 1 | E-mail | 25 % |
| Class 2 | | 25 % |
| Class 3 | | 25 % |
| | Others | 25 % |
| | | |
| 🔲 Enable UDP B | Bandwidth Control | Limited_bandwidth Ratio 25 % |
| 🔲 Outbound TO | CP ACK Prioritize | Online Statistics |
| | OK Clear | Cancel |

 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 Ir | ndex #2 | | | | |
|----------|---------|---------------|----------------|-----------------------|--------------|
| Name | HTTPS | | | | |
| NO | Status | Local Address | Remote Address | DiffServ CodePoint | Service Type |
| 1 | Empty | - | - | - | - |
| | | 4 | Add Edit Delet | te | |
| | | | OK Cancel | | |

6. Click **Setup** link for setting reserved bandwidth ratio.

Bandwidth Management >> Quality of Service

Bandwidth Management >> Quality of Service

| atus | Bandwidth | Directon | Class 1 | Class 2 | Class 3 | Others | UDP Bar Con | | |
|-------------------|-----------|----------|------------|------------|------------|--------|----------------|----------------------|--------------|
| Enable | Kbps/Kbps | Outbound | 25% | 25% | 25% | 25% | Inac | tive | <u>Setup</u> |
| lace Dub | | | | | | | | | |
| lass Rul Index | B | Name | e | | | F | tule | Service | е Туре |
| | | Namo | e | | | | tule Edit | Service | е Туре |
| Index | | Nami | e | | | | | Service <u>Ed</u> | |

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

| Enable the QoS (| Control BOTH | |
|-------------------------------------|--------------|--|
| Index | Class Name | Reserved_bandwidth Ratio |
| Class 1 | E-mail | 25 % |
| Class 2 | HTTPS | 25 % |
| Class 3 | | 25 % |
| | Others | 25 % |
| Enable UDP Bandw Outbound TCP AC | | Limited_bandwidth Ratio 25 Online Statistic |

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

| ne | VPN | | | | |
|----|--------|---------------|----------------|-----------------------|--------------|
| NO | Status | Local Address | Remote Address | DiffServ CodePoint | Service Type |
| 1 | Empty | - | - | - | - |
| | | - | Add Edit Delet | в | |

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

Bandwidth Management >> Quality of Service

Bandwidth Management >> Quality of Service

| 🗹 ACT | | | |
|------------------------|----------------------------|----------|--|
| Local Address | Any | Edit | |
| Remote Address | Any | Edit | |
| DiffServ CodePoint | ANY | * | |
| Service Type | ANY | * | |
| Note: Please choose/se | tup the <u>Service Typ</u> | e first. | |

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

| 🗹 ACT | | |
|------------------------|-----------------------------|--------|
| Local Address | Any | Edit |
| Remote Address | 192.168.1.66 | Edit |
|)iffServ CodePoint | ANY | ~ |
| Service Type | ANY | ~ |
| Note: Please choose/se | tup the <u>Service Type</u> | first. |

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 D | HCP Setup | | | |
|-------------------------|-----------------------|---|---|-----------------|
| LAN IP Network Config | uration | | DHCP Server Configura | tion |
| For NAT Usage | | | 💿 Enable Server 🔘 Disat | ble Server |
| 1st IP Address | 192.168.1.5 | | Relay Agent: 🔘 1st Subr | et 🔾 2nd Subnet |
| 1st Subnet Mask | 255.255.255.0 | | Start IP Address | 192.168.1.10 |
| For IP Routing Usage 🔘 | Enable 💿 Disable | | IP Pool Counts | 50 |
| 2nd IP Address | 192.168.2.1 | | Gateway IP Address | 192.168.1.5 |
| 2nd Subnet Mask | 255.255.255.0 | | DHCP Server IP Address | |
| RIP Protocol Control | nd Subnet DHCP Server | r | for Relay Agent DNS Server IP Address Force DNS manual se Primary IP Address Secondary IP Address | tting |
| | | | ОК | |

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 D | HCP Setup | | |
|------------------------------|-----------------------|---|------------------|
| LAN IP Network Configuration | | DHCP Server Configuration | |
| For NAT Usage | | ◯Enable Server ⓒDisat | ole Server |
| 1st IP Address | 192.168.1.5 | Relay Agent: 🔘 1st Subr | net O 2nd Subnet |
| 1st Subnet Mask | 255.255.255.0 | Start IP Address | 192.168.1.10 |
| For IP Routing Usage 🔘 | Enable 💿 Disable | IP Pool Counts | 50 |
| 2nd IP Address | 192.168.2.1 | Gateway IP Address | 192.168.1.5 |
| 2nd Subnet Mask | 255.255.255.0 | DHCP Server IP Address for Relay Agent | 192.168.3.11 |
| 2 | nd Subnet DHCP Server | | |
| | | DNS Server IP Address | |
| RIP Protocol Control | Disable 🎽 | 📃 Force DNS manual se | tting |
| | | Primary IP Address | |
| | | Secondary IP Address | |
| | | ж | |

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

Install Now!

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

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

- 7. Choose the one that matches with your operating system and click the corresponding link to download correct firmware (zip file).
- 8. Next, decompress the zip file.
- 9. Double click on the icon of router tool. The setup wizard will appear.



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

| 🛍 Firmware Upgrade | Utility 3.5.1 | |
|---------------------|----------------|------|
| Time Out(Sec.) 5 | Router IP: | |
| Port | Firmware file: | |
| 69 | | |
| Password: | Abort | Send |
| | | |

- 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.

| ៉ Firmware Upgrade | Utility 3.5.1 |
|--------------------|----------------------------------|
| Time Out(Sec.) | Router IP: |
| 5 | 192.168.1.1 |
| Port | Firmware file: |
| 69 | C:\Documents and Settings\Carrie |
| Password: | |
| | Abort Send |
| | |
| | |

14. Click Send.

| ៉ Firmware Upgrade | Utility 3.5.1 | |
|---------------------|----------------------------------|--|
| Time Out(Sec.) 5 | Router IP: | |
| Port | Firmware file: | |
| 69 Password: | C:\Documents and Settings\Carrie | |
| | Abort Send | |
| Sending | | |

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

| Name | Subject | Status | Modify |
|----------|----------------|--------|-------------|
| Local | | | View Delete |
| GENERATE | IMPORT REFRESH | | |
| | bortinodeo | | ~ |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | ~ |

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 | |
| Туре | IP Address 🛛 💌 |
| IP | |
| Subject Name | |
| Country (C) | |
| State (ST) | |
| Location (L) | |
| Orginization (O) | |
| Orginization Unit (OU) | |
| Common Name (CN) | |
| Email (E) | |
| Кеу Туре | RSA 🛩 |
| Key Size | 1024 Bit 🗸 |
| | Generate |

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

| Name | Subject | Status | Modify |
|--|--|---|--|
| Local | /C=TW/ST=HC/L=HC/O=Draytek/O | Requesting | View Delete |
| ENERATE | IMPORT REFRESH | | |
| MIIBqj EwJIQz CQEWE3 AoGBAL a1X//f m6+0f4 hkiG9w 9yojHp eorpDa | EGIN CERTIFICATE REQUEST CCARMCAQAwajELMAkGAIUEBhMCVFcxCzAJ CCMA4GAIUEChMHRHJheXRlazELMAkGAIUE N1cHBvcnRA2HJheXRlay5jb20wgZ8wDQYJ MJdTaqfF97FEpYy+IqeJVJGuSRtqG6Etw8 gnEccQA2LPSQIQ85Qychwq07Bm0EDf10wH x24QQnjXXgciC0Bj1iAa6MLScelsynZhkg OBAQUFAA0BgQCq3sdwVc21t9qn4U6X2BJs stNsmWsMRuAw6eKCWc8S/gLtHnf6iccMoT 1/rC92wCra0t8XUmPqNoiytq8BxStTE8vU ND CERTIFICATE REQUEST | CxMCURQxIjAgB KoZIhvcNAQEBB yTU5HQvXpAzcr wCalAZQoGvIiO nQ1QN5uFAgMBA Vzu7JHafSSeUn oQFx/LWdaEPU5 | gkqhkiG9w0B QADgY0AMIGJ gJBGrikTUBX DMC7f5w9xA8 AGgADANBgkq adYD2efCmGfX LqryBKKgC9t |

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 | <u>Home</u> |
|---|-------------|
| 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, will be able to securely identify yourself to other people over the web, sign your e-mail messages, encrypt your e-mail messages, and mo depending upon the type of certificate you request. | |
| Select a task: | |
| Retrieve the CA certificate or certificate revocation list | |
| Request a certificate Ocheck on a pending certificate | |
| ○ Check on a pending certificate | |
| Next | > |

Select Advanced request.

| Microsoft Certificate Services vigor | <u>Home</u> |
|---|-------------|
| Choose Request Type | |
| Please select the type of request you would like to make: | |
| User certificate request: User Certificate | |
| | |
| Next | > |

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

| Microsoft Certificate Services vigor Home |
|---|
| Advanced Certificate Requests |
| You can request a certificate for yourself, another user, or a computer using one of the following methods. Note that the policy of the certification authority (CA) will determine the certificates that you can obtain. |
| Submit a certificate request to this CA using a form. |
| ● Submit a certificate request using a base64 encoded PKCS #10 file or a renewal request using a base64 encoded PKCS #7 file. |
| Request a certificate for a smart card on behalf of another user using the Smart Card Enrollment Station. You must have an enrollment agent certificate to submit a request for another user. |
| Next > |

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

| Microsoft Certifica | te Services vigor | Home |
|---------------------|--|--|
| Submit A Save | d Request | |
| Dests a baseful | appared and DIZCE #10 partificators | aguast as DI/CS #7 renewal request generated by an external application (such as a use |
| | | request or PKCS #7 renewal request generated by an external application (such as a web t to the certification authority (CA). |
| Caused Damaged | | |
| Saved Request: | | |
| | BEGIN CERTIFICATE REQU | |
| | MIIBqjCCARMCAQAwQTELMAkGA1UH | |
| | BgkqhkiG9w0BCQEWEXByZXNzQGRy | |
| | A4GNADCBiQKBgQDQYB7wmZFfFhN9 hX4bp89cUF9dloACGGiM/tcBOckd | |
| (1100 110 01 111). | x/GOA7CTvO/fQzpxroCwlJTjLSjS | |
| | < | |
| | Browse for a file to insert. | |
| | | |
| Certificate Templa | nte: | |
| | Administrator 👻 | |
| | Administrator | |
| Additional Attribut | Authenticated Session | |
| | Basic EFS | |
| Attributes: | EFS Recovery Agent User | |
| | IPSEC (Offline request) | Σ |
| | Router (Offline request) | |
| | Subordinate Certification Authority | |
| | Web Server | Submit > |

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

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

and you will find the below window showing "-----BEGINE CERTIFICATE-----...." Certificate Management >> Local Certificate

| Local /C=TW/ST=HC/L=HC/0=Draytek/O Requesting View Delete EENERATE IMPORT REFRESH X509 Local Certificate Request BEGIN CERTIFICATE REQUEST MIIBqjCCARMCAQAwajELMAKGA1UEBhMCVFcxCzAJBgNVBAgTAkhDMQswCQYDVQH EwJIQzEQMA4GA1UEChMHRHJneXR1azELMAkGA1UECxMCUkQxIjAgBgkqhkiG9w0B CQEWESN1cHBvcnRAZHJneXR1ay5jb20wgZ@bQYJKoZIhvcNAQEBBQADgYOAMIGJ AoGBALMJdTsqfF97FEpY+IqqJVJGuSRtqG6Etw8yTUSHQvXpAzcrgJBGrikTUBX a1X//fgnEccQA2LFSQIQ85Qychwq07bm0EDf10wHwca1AZQoGvIi0DNC7f5w9xA8 m6+0f4xZ4QQnjXXgciC0Bj1iAa6MLSce1synZhkgnQ1QNSuFAgMBAAGgADANBgkq hkiG9w0BAQUFAA0BgQCq3sdwVc21t9qn4U6X2BJsVzu7JHafSSeUnaYD2efCmGfX 9yojHpstNamWsMRuAwGeKCWc8S/gLtHnr6iccMOTOQFx/LWdaEPUSLqryBKKgC9t eorpDa1/rC92wCra0t8XUmPqNoiytq8BxStTESvULiIxmwaBvc1hWFSXKVLU7g=- END | Name | Subject | Status | Modify |
|--|----------|------------------------------|------------|-------------|
| X509 Local Certificate Request BEGIN CERTIFICATE REQUEST MIIBqjCCARMCAQAwajELMAKGA1UEBhMCVFcxCzAJBgNVBAgTAkhDMQswCQYDVQQH EwJIQZEQMA4GA1UEChMHRIJheXRlazELMAKGA1UECxMCUkQxIjAgBgkqhkiG9w0B CQEWESMicHBvcnRa2HJheXRlay5jb20wg28vDQYJKoZIhvcNAQEBBQADgYOAMIGJ AoGBALMJdTsqfF97FEpYy+IqeJVJGuSRtqG6Etw8yTUSHQvXpAzcrgJBGrikTUBX a1X//fgnEccQA2LPSQIQ85Qychwq07Bm0EDf10wHwCalA2QoGvIi0DMC7f5w9xA8 m6+0f4xZ4QQnjXXgciC0Bj1iAa6MLScelsyn2hkgnQ1QNSuFAgMBAAGgADANBgkq hkiG9w0BAQUFAA0BgQCq3sdwVc21t9qn4U6X2BJsVzu7JHafSSeUnaYD2efCmGfX 9yojHpstNsmWsMRukwGeKCWc8S/gLtHnficcMoToQFx/LWdaEPUSLqryBKKgC9t eorpDa1/rC9ZwCra0t8XUmPqNoiytq8BxStTE8vULiIxmwaBvc1hWFSXKVLU7g== | Local | /C=TW/ST=HC/L=HC/O=Draytek/O | Requesting | View Delete |
| BEGIN CERTIFICATE REQUEST MIIBqjCCARMCAQAwajELMAKGA1UEBhMCVFcxCzAJBgNVBAgTAkhDMQswCQYDVQQH EwJIQZEQMA4GA1UEChMHRHJheXRlazELMAkGA1UECxMCUkQxIjAgBgkqhkiG9wOB CQEWE3N1cHBvcnRAZHJheXRlay5jb20wgZ8wDQYJKoZIhvcNAQEBBQADgYOAMIGJ AoGBALMJdTsqfF97FEpYy+IqeJVJGuSRtqG6Etw8yTUSHQvXpAzcrgJBGrikTUBX a1X//fgnEccQA2LPSQIQ85QychwqO7BmOEDf10wHwCalAZQoGVi0DMC7f5w9xA8 m6+0f4xZ4QQnjXXgciCOBj1iAa6MLScelsynZhkgnQ1QNSuFAgMBAAGgADANBgkq hkiG9w0BAQUFAA0BgQCq3sdwVc21t9qn4U6X2BJsVzu7JHafSseUnaYD2efCmGfX 9yojHpstNsmWsMRukwGeKCWc8S/gLtHnf6iccMoToQFx/LWdaEPUSJqryBKKgC9t eorpDa1/rC9ZwCra0t8XUmPqNoiytq8BxStTE8vULiIxmwaBvc1hWFSXKVLU7g== | GENERATE | IMPORT REFRESH | | |
| MIIBqjCCARMCAQAwajELMAKGAIUEBhMCVFcxCzAJBgNVBAgTAkhDMQswCQYDVQQH EwJIQzEQMA4GA1UEChMHRHJheXRlazELMAkGA1UECxMCUkQxIjAgBgkqhkiG9w0B CQEWE3N1cHBvcnRAZHJheXRlay5jb20wgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJ AcGBALMJdTsqfF97FEpYy+IqaJVJGuSRtqGEtw8yTUSHqvXpAzcrgJBGrikTUBX a1X//fgnEccQA2LPSQIQ85Qychwq07Bm0EDf10WHwCalAZQoGVi0DMC7f5w9xA8 m6+0f4xZ4QQnjXXgciC0Bj1iAa6MLScelsynZhkgnQ1QNSuFAgMBAAGgADANBgkq hkiG9w0BAQUFAA0BgQCq3sdwVc21t9qn4U6X2BJsVzu7JHafSSeUna7D2efCmGfX 9yojHpstNsmWsMRukwGeKCWc8S/gLtHhf6iccMoToQFx/LWdaEPUSLqryBKKgC9t eorpDa1/rC9ZwCra0t8XUmPqNoiytq8BxStTE8vULiIxmwaBvc1hWFSXKVLU7g== | X509 L | ocal Certificate Request | | |
| | | EGIN CERTIFICATE REQUEST | | ^ |

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

| Name : | Local |
|-------------------------------|---|
| Issuer : | /C=US/CN=vigor |
| Subject : | /emailAddress=press@draytek.com/C=TV//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.
 - Microsoft Certificate Services Microsoft Internet Explorer ③ 上-頁 · ◎ · 図 ② ☆ ♪ 搜尋 ☆ 我的最爱 ④ 媒體 Ø ◎ · ◎ · ◎ · ◎ · ◎ 網址 (D) 🍓 http://172.16.2.179/certsrv/certcarc.asp ✓ → 移至 連結 msn 🔨 -🗸 🔎 搜尋 🝷 🛹 醒目提示 🛛 🕺 選項 🛛 🔀 封鎖快顯視窗 (319) 🔹 🔤 Hotmail 🚜 Messenger [2 我的 MSN Retrieve The CA Certificate Or Certificate Revocation List Install this CA certification path to allow your computer to trust certificates issued from this certification authority It is not necessary to manually install the CA certification path if you request and install a certificate from this certification authority, because the CA certification path will be installed for you automatically. Choose file to download: CA Certificate: Current [vigor(1)] Previous [vigor] ○DER encoded or ●Base 64 encoded Download CA certificate Download CA certification path Download latest certificate revocation list
- 3. Back to Vigor router, go to **Trusted CA Certificate**. Click **IMPORT** button and browse the file to import the certificate (.cer file) into Vigor router. When finished, click refresh and you will find the below illustration.

Certificate Management >> Trusted CA Certificate

| 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 Trouble Shooting

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

- Checking if the hardware status is OK or not.
- Checking if the network connection settings on your computer are OK or not.
- Pinging the router from your computer.
- Checking if the ISP settings are OK or not.
- Backing to factory default setting if necessary.

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

6.1 Checking If the Hardware Status Is OK or Not

Follow the steps below to verify the hardware status.

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



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

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

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

For Windows



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

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



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



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

| 🛨 eth0 Properties 🛛 🔹 💽 🔀 |
|---|
| General Authentication Advanced |
| Connect using: |
| B ASUSTeK/Broadcom 440x 10/100 lr |
| This connection uses the following items: |
| Client for Microsoft Networks |
| Eile and Printer Sharing for Microsoft Networks QoS Packet Scheduler |
| Internet Protocol (TCP/IP) |
| Install Uninstall Properties |
| |
| Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks. |
| Show icon in notification area when connected Notify me when this connection has limited or no connectivity |
| |
| OK Cancel |

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

| Internet Protocol (TCP/IP) Prop | erties 🛛 🛛 🔀 |
|--|-------------------|
| General Alternate Configuration | |
| You can get IP settings assigned autr this capability. Otherwise, you need to the appropriate IP settings. | |
| Obtain an IP address automatica | ally |
| OUse the following IP address: — | |
| IP address: | |
| S <u>u</u> bnet mask: | |
| Default gateway: | |
| ⊙ Obtain DNS server address auto | omatically |
| OUse the following DNS server a | ddresses: |
| Preferred DNS server: | |
| Alternate DNS server: | |
| | Ad <u>v</u> anced |
| | OK Cancel |

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.

| | | | Netw | /ork | | |
|-----------|--------------|-------------|-------------|----------------|-------------|------------|
| É | | | 2 | | | |
| iow All D | isplays Sour | nd Network | Startup Dis | k | | |
| | Lc | cation: Au | itomatic | | • | |
| | | Show: Bu | ilt-in Ethe | rnet | • | |
| | TCP/ | P PPPoE | AppleT | alk Proxies | Ethernet | |
| | | IF FFFOE | Apple1 | aik Proxies | Ethernet | |
| Confi | gure IPv4: | Using DHC | P | | • | |
| IF | P Address: | 192.168.1. | 10 | | (Renew D | HCP Lease |
| Sub | net Mask: | 255.255.25 | 5.0 | DHCP Client | ID: | |
| | Router: | 192.168.1. | 1 | | (If require | :d) |
| DN | IS Servers: | | | | | (Optional) |
| Search | Domains: | | | | | (Optional) |
| IPv6 | Address: | fe80:0000:0 | 0000:0000 | :020a:95ff:fe8 | d:72e4 | |
| | | Configure | IPv6) | | | (?) |

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.



- 3. Type ping 192.168.1.1 and press [Enter]. It the link is OK, the line of **"Reply from 192.168.1.1:bytes=32 time<1ms TTL=255"** will appear.
- 4. If the line does not appear, please check the IP address setting of your computer.

For MacOs (Terminal)

- 1. Double click on the current used MacOs on the desktop.
- 2. Open the Application folder and get into Utilities.
- 3. Double click **Terminal**. The Terminal window will appear.
- 4. Type **ping 192.168.1.1** and press [Enter]. It the link is OK, the line of **"64 bytes from 192.168.1.1: icmp_seq=0 ttl=255 time=xxxx ms**" will appear.

| e forminal — bash — 80) Last login: Sat Jan 3 02:24:18 on ttyp1 | |
|--|---------|
| Welcome to Darwin! | 21 |
| Vigor10:~ draytek\$ ping 192.168.1.1 | |
| PING 192.168.1.1 (192.168.1.1): 56 data bytes | |
| 있는 것 같은 것 같 | Acc |
| 64 bytes from 192.168.1.1: icmp_seq=0 ttl=255 time=0 | |
| 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=8 | .72 ms |
| νC | |
| 192.168.1.1 ping statistics | |
| 5 packets transmitted, 5 packets received, 0% packet | loss |
| round-trip min/ava/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/PPPoA Users

- 1. Check if the **Enable** option is selected.
- 2. Check if **Username** and **Password** are entered with correct values that you **got from** your **ISP**.

Internet Access >> PPPoE / PPPoA

| PPPoE / PPPoA Clie | nt Mode | | |
|--|--|--|--|
| PPPoE/PPPoA Clier | nt 💿 Enable 🔘 Disable | ISP Access Setup | |
| PPPoE/PPPoA Clien DSL Modem Setting Multi-PVC channel VPI VCI Encapsulating Type Protocol Modulation PPPoE Pass-throug For Wired LAN | Channel 1 V Channel 1 V 33 LLC/SNAP V PPPoE V Multimode V | ISP Access Setup ISP Name Username Password Password PPP Authentication PAP or CHAP ▼ ✓ Always On Idle Timeout -1 second(s) IP Address From ISP WAN IP Alias Fixed IP Yes ● No (Dynamic IP) Fixed IP Address ● Default MAC Address ● Specify a MAC Address MAC Address: 00 .50 .7F Index(1-15) in Schedule Setup: => | |
| | | | |

OK

For MPoA Users

- 1. Check if the **Enable** option is selected.
- 2. Check if all parameters of **DSL Modem Settings** are entered with correct value that provided by your ISP. Especially, check if the encapsulation is selected properly or not (it should be the same with the setting on **Quick Start Wizard**).
- 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**.

| MPoA (RFC1483/268 | 34) 🔘 Enable 💿 Disable | WAN IP Network Settin | gs |
|----------------------|------------------------|-------------------------|------------------|
| | | – Obtain an IP addres | s automatically |
| DSL Modem Settings | | Router Name | |
| Multi-PVC channel | Channel 1 🛩 | Domain Name | |
| Encapsulation | | *: Required for some IS | 3Ps |
| | 83 Bridged IP LLC | Specify an IP addres | ss WAN IP Alias |
| VPI | 0 | IP Address | 0.0.0.0 |
| VCI | 33 | Subnet Mask | 0.0.0.0 |
| Modulation | Multimode 💌 | Gateway IP Address | 0.0.0.0 |
| RIP Protocol | | | |
| 📃 Enable RIP | | Oefault MAC Address | |
| | | – 🔘 Specify a MAC Addre | SS. |
| Bridge Mode | | MAC Address: 00 .50 |) .7F 92 .F5 .01 |
| 📃 Enable Bridge Mode | e | | |
| | | DNS Server IP Address | |
| | | Primary IP Address | |
| | | Secondary IP Address | |

Internet Access >> MPoA (RFC1483/2684)

6.5 Backing to Factory Default Setting If Necessary

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

Warning: After pressing **factory default setting**, you will loose all settings you did before. Make sure you have recorded all useful settings before you pressing. The password of factory default is null.

Software Reset

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

Go to **System Maintenance** and choose **Reboot System** on the web page. The following screen will appear. Choose **Using factory default configuration** and click **OK**. After few seconds, the router will return all the settings to the factory settings.

System Maintenance >> Reboot System

| Do you want to reboot your router ? | |
|---------------------------------------|--|
| Osing current configuration | |
| O Using factory default configuration | |

Hardware Reset

While the router is running (ACT LED blinking), press the **Factory Reset** button and hold for more than 5 seconds. When you see the **ACT** LED blinks rapidly, please release the button. Then, the router will restart with the default configuration.



After restore the factory default setting, you can configure the settings for the router again to fit your personal request.

6.6 Contacting Your Dealer

If the router still cannot work correctly after trying many efforts, please contact your dealer for further help right away. For any questions, please feel free to send e-mail to support@draytek.com.