



Vigor2910

Dual-WAN Security Router

User's Guide

Version: 3.5

Date: 2008/08/08

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. The scope of delivery and other details are subject to change without prior notice.

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.

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 by 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.
- Do not stack the routers.
- The router should be used in a sheltered area, within a temperature range of +5 to +40 Celsius.
- Do not expose the router to direct sunlight or other heat sources. The housing and electronic components may be damaged by direct sunlight or heat sources.
- Do not deploy the cable for LAN connection outdoor to prevent electronic shock hazards.
- Keep the package out of reach of children.
- When you want to dispose of the router, please follow local regulations on conservation of the environment.

Warranty

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

Be a Registered Owner

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

Firmware & Tools Updates

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

<http://www.draytek.com>

European Community Declarations

Manufacturer: DrayTek Corp.

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

Product: Vigor2910 Series Routers

DrayTek Corp. declares that Vigor2910 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 89/336/EEC 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 73/23/EEC by complying with the requirements set forth in EN60950.

The **Vigor2910 Series** are designed for the WLAN 2.4GHz network throughout EC region, Switzerland, and the restrictions of France.

Regulatory Information

Federal Communication Commission Interference Statement

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

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

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

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

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



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

Table of Contents

1

Preface	1
1.1 Web Configuration Buttons Explanation	1
1.2 LED Indicators and Connectors	1
1.2.1 For Vigor2910	2
1.2.2 For Vigor2910G	3
1.2.3 For Vigor2910i	4
1.2.4 For Vigor2910V	5
1.2.5 For Vigor2910VG	6
1.2.6 For Vigor2910VGi	7
1.3 Hardware Installation	8
1.4 Printer Installation	9

2

Configuring Basic Settings	15
2.1 Changing Password	15
2.2 Quick Start Wizard	17
2.2.1 PPPoE	18
2.2.2 PPTP	20
2.2.3 Static IP	21
2.2.4 L2TP	22
2.2.5 DHCP	23
2.3 Online Status	24
2.4 Saving Configuration	26

3

Advanced Web Configuration	27
3.1 WAN	27
3.1.1 Basics of Internet Protocol (IP) Network	27
3.1.2 Network Connection by 3G USB Modem	28
3.1.3 General Setup	28
3.1.4 Internet Access	31
3.1.5 Load-Balance Policy	39
3.2 LAN	42
3.2.1 Basics of LAN	42
3.2.2 General Setup	44
3.2.3 Static Route	46
3.2.4 Bind IP to MAC	49
3.3 NAT	50
3.3.1 Port Redirection	50
3.3.2 DMZ Host	53
3.3.3 Open Ports	56

3.4 Objects and Groups	58
3.4.1 IP Object	58
3.4.2 IP Group	60
3.4.3 Service Type Object	61
3.4.4 Service Type Group	62
3.4.5 IM Object	63
3.4.6 P2P Object	64
3.4.7 Misc Object	66
3.5 CSM	66
3.5.1 IM/P2P Filter Profile	68
3.5.2 URL Content Filter Profile	68
3.5.3 Web Content Filter Profile	71
3.6 Firewall	72
3.6.1 Basics for Firewall	72
3.6.2 General Setup	74
3.6.3 Filter Setup	75
3.6.4 DoS Defense	81
3.7 Bandwidth Management	84
3.7.1 Sessions Limit	84
3.7.2 Bandwidth Limit	85
3.7.3 Quality of Service	86
3.8 Applications	93
3.8.1 Dynamic DNS	93
3.8.2 Schedule	95
3.8.3 RADIUS	97
3.8.4 UPnP	98
3.8.5 Wake On LAN	99
3.9 VPN and Remote Access	101
3.9.1 VPN Client Wizard	101
3.9.2 VPN Server Wizard	107
3.9.3 Remote Access Control	111
3.9.4 PPP General Setup	112
3.9.5 IPSec General Setup	113
3.9.6 IPSec Peer Identity	114
3.9.7 Remote Dial-in User	116
3.9.8 LAN to LAN	119
3.9.9 VPN Backup Management	128
3.9.10 Connection Management	131
3.10 Certificate Management	133
3.10.1 Local Certificate	133
3.10.2 Trusted CA Certificate	135
3.10.3 Certificate Backup	136
3.11 VoIP	137
3.11.1 DialPlan	138
3.11.2 SIP Accounts	142
3.10.3 Phone Settings	145
3.11.4 Status	155
3.12 ISDN	156
3.12.1 General Setup	156
3.12.2 Dialing to a Single ISP	158
3.12.3 Dialing to Dual ISPs	159

3.12.4 Virtual TA	159
3.12.5 Call Control	163
3.13 Wireless LAN	165
3.13.1 Basic Concepts.....	165
3.13.2 General Settings.....	168
3.13.3 Security	170
3.13.4 Access Control.....	172
3.13.5 WDS.....	173
3.13.6 AP Discovery	175
3.13.7 Station List	176
3.13.8 Station Rate Control	178
3.14 VLAN	178
3.14.1 Wired VLAN	178
3.14.2 Wireless VLAN.....	179
3.14.3 VLAN Cross Setup.....	183
3.14.4 Wireless Rate Control.....	184
3.15 USB Application	185
3.15.1 FTP General Settings	185
3.15.2 FTP User Management	185
3.15.3 USB Disk Status	187
3.16 System Maintenance.....	188
3.16.1 System Status.....	188
3.16.2 TR-069 Setting.....	189
3.16.3 Administrator Password.....	191
3.16.4 Configuration Backup	191
3.16.5 Syslog/Mail Alert	193
3.16.6 Time and Date	195
3.16.7 Management.....	196
3.16.8 Reboot System	197
3.16.9 Firmware Upgrade	198
3.17 Diagnostics.....	199
3.17.1 Dial-out Trigger	199
3.17.2 Routing Table	200
3.17.3 ARP Cache Table	200
3.17.4 DHCP Table.....	201
3.17.5 NAT Sessions Table	201
3.17.6 Wireless VLAN Online Station Table	202
3.17.7 Data Flow Monitor.....	202
3.17.8 Traffic Graph.....	204
3.17.9 Ping Diagnosis.....	206
3.17.10 Trace Route	206

4

Application and Examples	209
4.1 Create a LAN to LAN Connection Between Remote Office and Headquarter.....	209
4.2 Create a Remote Dial-in User Connection Between the Teleworker and Headquarter.....	216
4.3 QoS Setting Example.....	220
4.4 LAN – Created by Using NAT	224
4.5 Calling Scenario for VoIP function	226
4.5.1 Calling via SIP Sever	226

4.5.2 Peer-to-Peer Calling	228
4.6 Upgrade Firmware for Your Router	229
4.7 Request a certificate from a CA server on Windows CA Server	231
4.8 Request a CA Certificate and Set as Trusted on Windows CA Server	236
4.9 VPN Backup Application	238
4.10 ERD Mechanism for VPN Backup	242

5

Trouble Shooting245

5.1 Checking If the Hardware Status Is OK or Not.....	245
5.2 Checking If the Network Connection Settings on Your Computer Is OK or Not	245
5.3 Pinging the Router from Your Computer	248
5.4 Checking If the ISP Settings are OK or Not.....	250
5.5 Problems for 3G Network Connection	251
5.6 Backing to Factory Default Setting If Necessary	252
5.7 Contacting Your Dealer	253


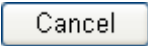
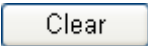
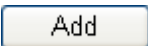
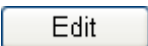
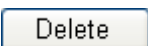
1

Preface

The Vigor2910 series router provides Dual-WAN interface (which is a configuration second WAN) for Internet access to make the Internet connection more reliable. The wireless LAN supports more secure features and the transmission speed is up to 108Mbps (SuperG™). Object-oriented firewall is flexible and allows your network be safe. In addition, through VoIP function, the communication fee for you and remote people can be reduced.

1.1 Web Configuration Buttons Explanation

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

	Save and apply current settings.
	Cancel current settings and recover to the previous saved settings.
	Discard current settings and allow users to input settings again.
	Add new settings for specified item.
	Edit the settings for the selected item.
	Delete the selected item with the corresponding settings.

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

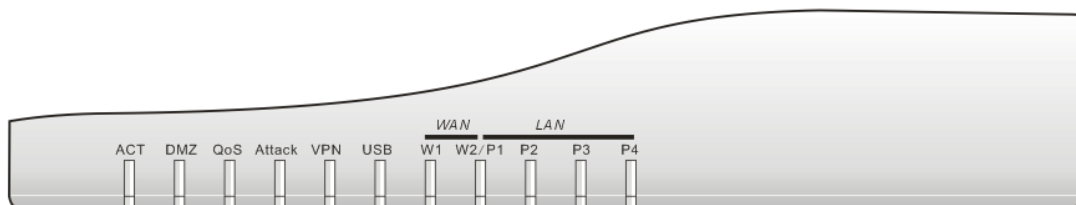
1.2 LED Indicators and Connectors

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

The displays of LED indicators and connectors for the routers are different slightly. The following sections will introduce them respectively.

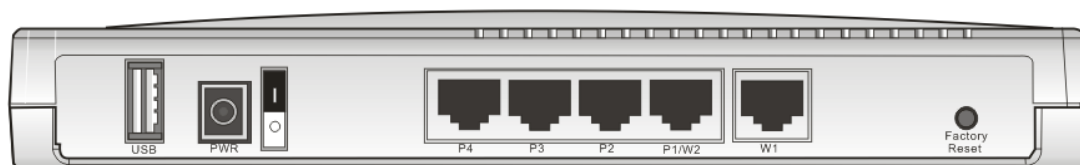
1.2.1 For Vigor2910

LED Explanation



LED	Status	Explanation
ACT (Activity)	Blinking	The router is powered on and running properly.
	Off	The router is powered off.
DMZ	On	DMZ Host is specified in certain site.
QoS	On	The QoS function is active.
	Off	The QoS function is inactive.
Attack	On	DoS Defense function is active.
	Blinking	An attack is detected.
VPN	On	The VPN tunnel is launched.
USB *	On	The USB interface printer or 3G USB modem is ready.
WAN(W1-W2)	Orange	A normal 10Mbps WAN link is ready.
	Green	A normal 100Mbps WAN link is ready.
	Blinking	Ethernet packets are transmitting.
LAN (P1, P2, P3, P4)	Orange	A normal 10Mbps connection is through its corresponding port.
	Green	A normal 100Mbps connection is through its corresponding port.
	Blinking	Ethernet packets are transmitting.

Connector Explanation

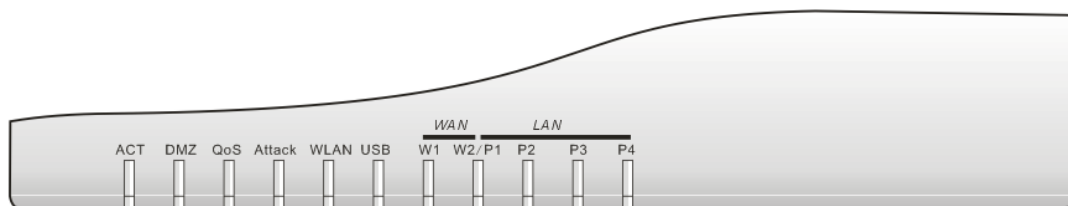


Interface	Description
USB*	Connector for a USB printer or 3G USB modem.
PWR	Connector for a power adapter with 12-15VDC.
ON/OFF	Power Switch.
LAN P4 – P1	Connectors for local networked devices.
W2/W1	Connector for accessing Internet with the ADSL,ADSL2/2+ line
Factory Reset	Restore the default settings. 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.

Note: For the USB port can be used to connect 3G USB modem or USB printer, therefore the original name (printer) is changed into USB in the future.

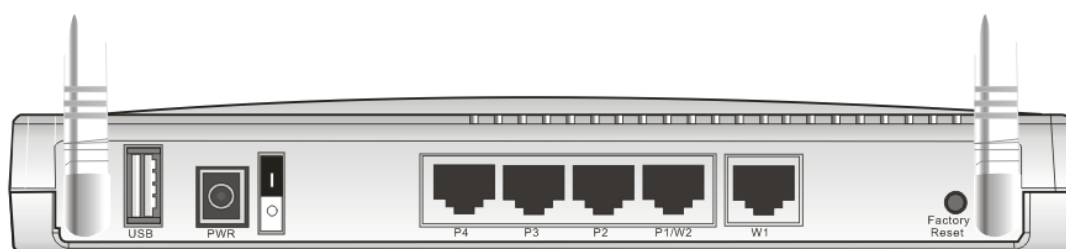
1.2.2 For Vigor2910G

LED Explanation



LED	Status	Explanation
ACT (Activity)	Blinking	The router is powered on and running properly.
	Off	The router is powered off.
DMZ	On	DMZ Host is specified in certain site.
QoS	On	The QoS function is active.
	Off	The QoS function is inactive.
Attack	On	DoS Defense function is active.
	Blinking	An attack is detected.
WLAN	On	Wireless access point is ready.
	Blinking	Wireless traffic goes through.
	Off	Wireless access point is turned off.
USB *	On	The USB interface printer or 3G USB modem is ready.
WAN(W1-W2)	Orange	A normal 10Mbps WAN link is ready.
	Green	A normal 100Mbps WAN link is ready.
	Blinking	Ethernet packets are transmitting.
LAN (P1, P2, P3, P4)	Orange	A normal 10Mbps connection is through its corresponding port.
	Green	A normal 100Mbps connection is through its corresponding port.
	Blinking	Ethernet packets are transmitting.

Connector Explanation

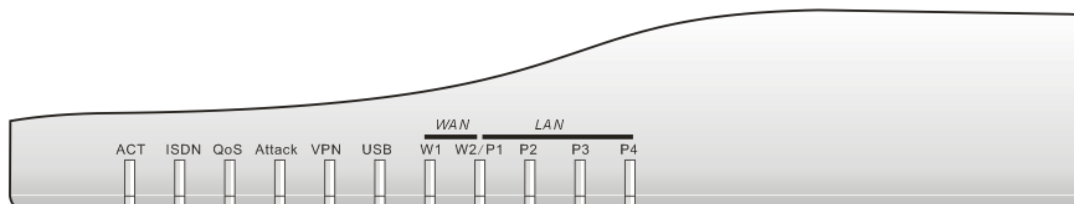


Interface	Description
USB*	Connector for a USB printer or 3G USB modem.
PWR	Connector for a power adapter with 12-15VDC.
ON/OFF	Power Switch.
LAN P4 – P1	Connectors for local networked devices.
W2/W1	Connector for accessing Internet with the ADSL,ADSL2/2+ line
Factory Reset	Restore the default settings. 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.

Note: For the USB port can be used to connect 3G USB modem or USB printer, therefore the original name (printer) is changed into USB in the future.

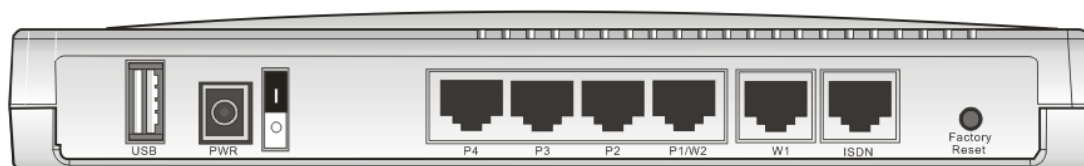
1.2.3 For Vigor2910i

LED Explanation



LED	Status	Explanation
ACT (Activity)	Blinking	The router is powered on and running properly.
	Off	The router is powered off.
ISDN	On	The ISDN network is correctly setup.
	Blinking	A successful connection on the ISDN BRI B1/B2 channel.
QoS	On	The QoS function is active.
	Off	The QoS function is inactive.
Attack	On	DoS Defense function is active.
	Blinking	An attack is detected.
VPN	On	The VPN tunnel is launched.
USB *	On	The USB interface printer or 3G USB modem is ready.
WAN(W1-W2)	Orange	A normal 10Mbps WAN link is ready.
	Green	A normal 100Mbps WAN link is ready.
	Blinking	Ethernet packets are transmitting.
LAN (P1, P2, P3, P4)	Orange	A normal 10Mbps connection is through its corresponding port.
	Green	A normal 100Mbps connection is through its corresponding port.
	Blinking	Ethernet packets are transmitting.

Connector Explanation

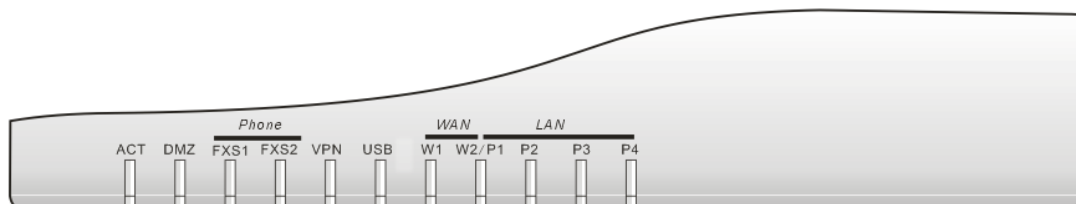


Interface	Description
USB*	Connector for a USB printer or 3G USB modem.
PWR	Connector for a power adapter with 12-15VDC.
ON/OFF	Power Switch.
LAN P4 – P1	Connectors for local networked devices.
W2/W1	Connector for accessing Internet with the ADSL,ADSL2/2+ line
ISDN	Connector for NT1 (or NT1+) box provided by ISDN service provider.
Factory Reset	Restore the default settings. Usage: Turn on the router (ACT LED is blinking). Press the hole and keep for more than 5 seconds. When you see the ACT LED begins to blink rapidly than usual, release the button. Then the router will restart with the factory default configuration.

Note: For the USB port can be used to connect 3G USB modem or USB printer, therefore the original name (printer) is changed into USB in the future.

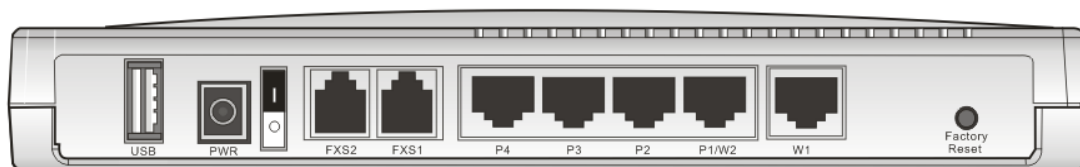
1.2.4 For Vigor2910V

LED Explanation



LED	Status	Explanation
ACT (Activity)	Blinking	The router is powered on and running properly.
	Off	The router is powered off.
DMZ	On	DMZ Host is specified in certain site.
FXS1/FXS2	On	The phone is off hook (the handset of phone is hanging).
	Blinking	A phone call is incoming or on-line.
VPN	On	The VPN tunnel is launched.
USB *	On	The USB interface printer or 3G USB modem is ready.
WAN(W1-W2)	Orange	A normal 10Mbps WAN link is ready.
	Green	A normal 100Mbps WAN link is ready.
	Blinking	Ethernet packets are transmitting.
LAN (P1, P2, P3, P4)	Orange	A normal 10Mbps connection is through its corresponding port.
	Green	A normal 100Mbps connection is through its corresponding port.
	Blinking	Ethernet packets are transmitting.

Connector Explanation

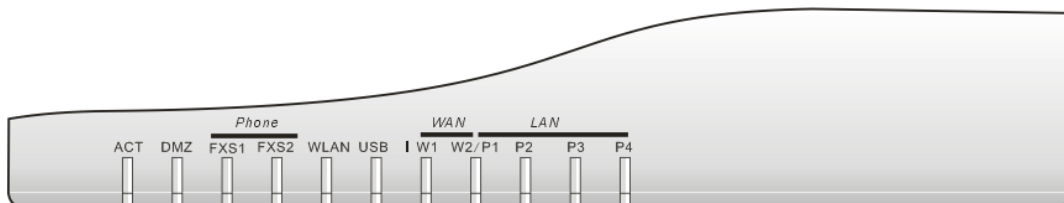


Interface	Description
USB*	Connector for a USB printer or 3G USB modem.
PWR	Connector for a power adapter with 12-15VDC.
ON/OFF	Power Switch.
FXS2 & FXS1	Connectors for telephone set and analog phone with VoIP communication.
LAN P4 – P1	Connectors for local networked devices.
W2/W1	Connector for accessing Internet with the ADSL,ADSL2/2+ line
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.

Note: For the USB port can be used to connect 3G USB modem or USB printer, therefore the original name (printer) is changed into USB in the future.

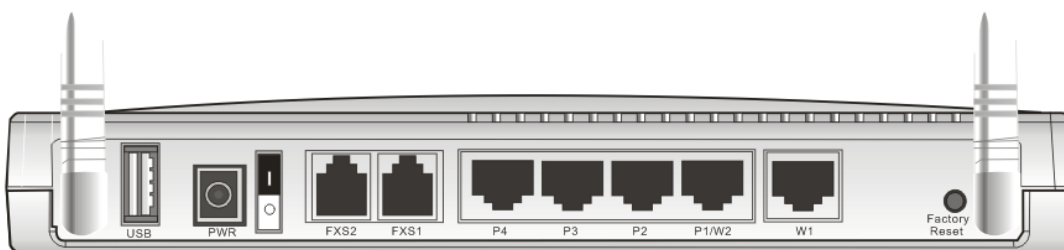
1.2.5 For Vigor2910VG

LED Explanation



LED	Status	Explanation
ACT (Activity)	Blinking	The router is powered on and running properly.
	Off	The router is powered off.
DMZ	On	DMZ Host is specified in certain site.
FXS1/FXS2	On	The phone is off hook (the handset of phone is hanging).
	Blinking	A phone call is incoming or on-line.
WLAN	On	Wireless access point is ready.
	Blinking	Wireless traffic goes through.
	Off	Wireless access point is turned off.
USB *	On	The USB interface printer or 3G USB modem is ready.
WAN(W1-W2)	Orange	A normal 10Mbps WAN link is ready.
	Green	A normal 100Mbps WAN link is ready.
	Blinking	Ethernet packets are transmitting.
LAN (P1, P2, P3, P4)	Orange	A normal 10Mbps connection is through its corresponding port.
	Green	A normal 100Mbps connection is through its corresponding port.
	Blinking	Ethernet packets are transmitting.

Connector Explanation

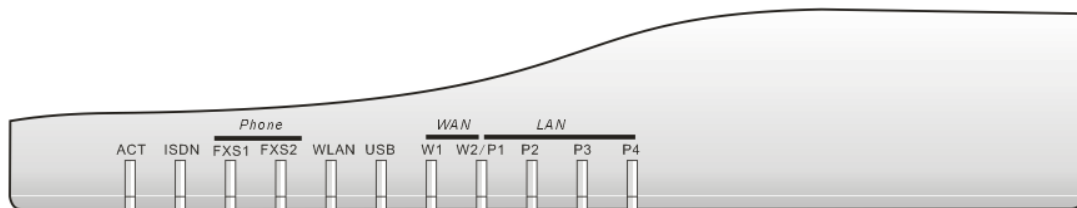


Interface	Description
USB*	Connector for a USB printer or 3G USB modem.
PWR	Connector for a power adapter with 12-15VDC.
ON/OFF	Power Switch.
FXS2 & FXS1	Connectors for telephone set and the analog phone with VoIP communication.
LAN P4 – P1	Connectors for local networked devices.
W2/W1	Connector for accessing Internet with the ADSL,ADSL2/2+ line
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.

Note: For the USB port can be used to connect 3G USB modem or USB printer, therefore the original name (printer) is changed into USB in the future.

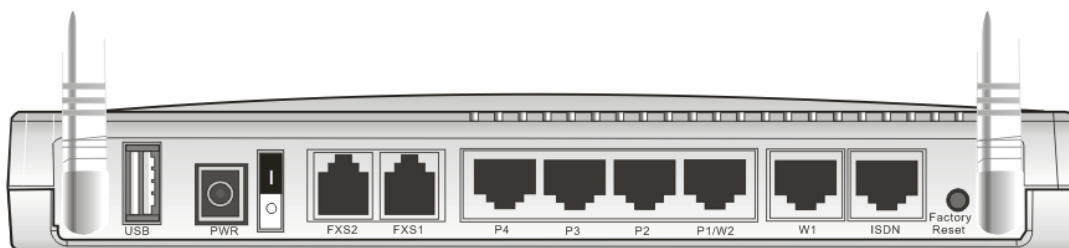
1.2.6 For Vigor2910VGi

LED Explanation



LED	Status	Explanation
ACT (Activity)	Blinking	The router is powered on and running properly.
	Off	The router is powered off.
ISDN	On	The ISDN network is correctly setup.
	Blinking	A successful connection on the ISDN BRI B1/B2 channel.
FXS1/FXS2	On	The phone is off hook (the handset of phone is hanging).
	Blinking	A phone call is incoming or on-line.
WLAN	On	Wireless access point is ready.
	Blinking	Wireless traffic goes through.
	Off	Wireless access point is turned off.
USB *	On	The USB interface printer or 3G USB modem is ready.
WAN(W1-W2)	Orange	A normal 10Mbps WAN link is ready.
	Green	A normal 100Mbps WAN link is ready.
	Blinking	Ethernet packets are transmitting.
LAN (P1, P2, P3, P4)	Orange	A normal 10Mbps connection is through its corresponding port.
	Green	A normal 100Mbps connection is through its corresponding port.
	Blinking	Ethernet packets are transmitting.

Connector Explanation



Interface	Description
USB*	Connector for a USB printer or 3G USB modem.
PWR	Connector for a power adapter with 12-15VDC.
ON/OFF	Power Switch.
FXS2 & FXS1	Connectors for telephone set and analog phone with VoIP communication.
LAN P4 – P1	Connectors for local networked devices.
W2/W1	Connector for accessing Internet with the ADSL,ADSL2/2+ line
ISDN	Connector for NT1 (or NT1+) box provided by ISDN service provider.
Factory Reset	Restore the default settings. Usage: Turn on the router (ACT LED is blinking). Press the hole and keep for more than 5 seconds. When you see the ACT LED begins to blink rapidly than usual, release the button. Then the router will restart with the factory default configuration.

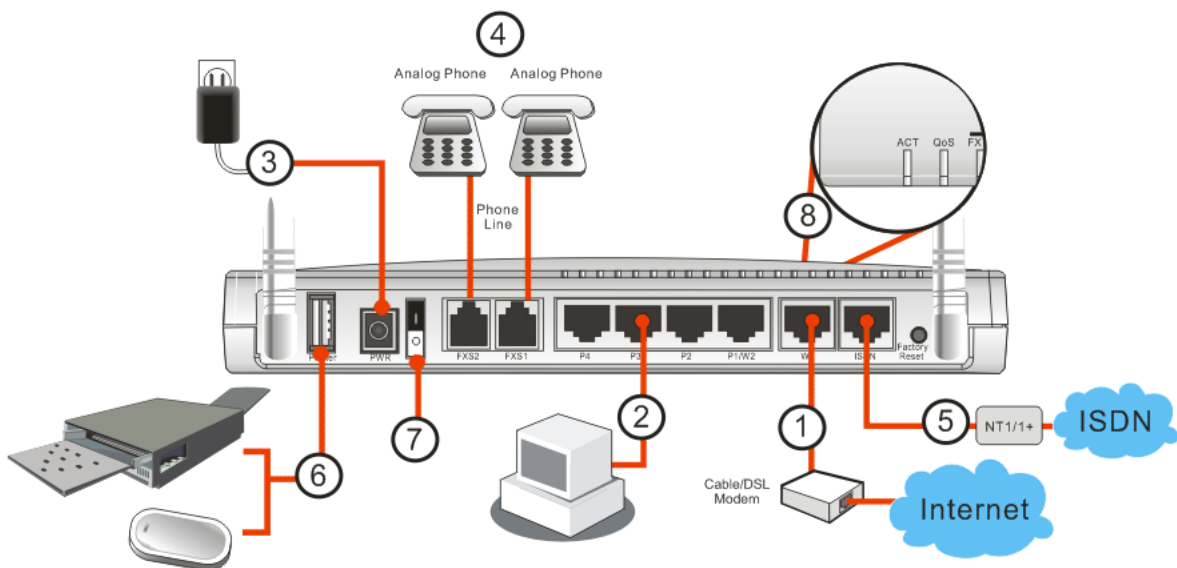
Note: For the USB port can be used to connect 3G USB modem or USB printer, therefore the original name (printer) is changed into USB in the future.

1.3 Hardware Installation

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

1. Connect this device to a router/modem with an Ethernet cable.
2. Connect one port of 4-port switch to your computer with a RJ-45 cable. This device allows you to connect 4 PCs directly.
3. Connect one end of the power cord to the power port of this device. Connect the other end to the wall outlet of electricity.
4. Connect the telephone sets with phone lines (for using VoIP function). For the user of the model without VoIP ports, skip this step.
5. Connect the ISDN NT1/1+ box with ISDN cable. This connection is available for Europe only.
6. Connect the printer/3.5G modem (e.g., Huawei E220 HSDPA USB Modem) to the router with the USB cable and connect the power cord if required. If you do not have a printer/3.5G modem for using, skip this step. For detailed configuration of printer, refer to section 1.4; detailed configuration of 3.5G modem, please refer to section 3.1.
7. Power on the router.
8. Check the **ACT** LED to assure network connections.

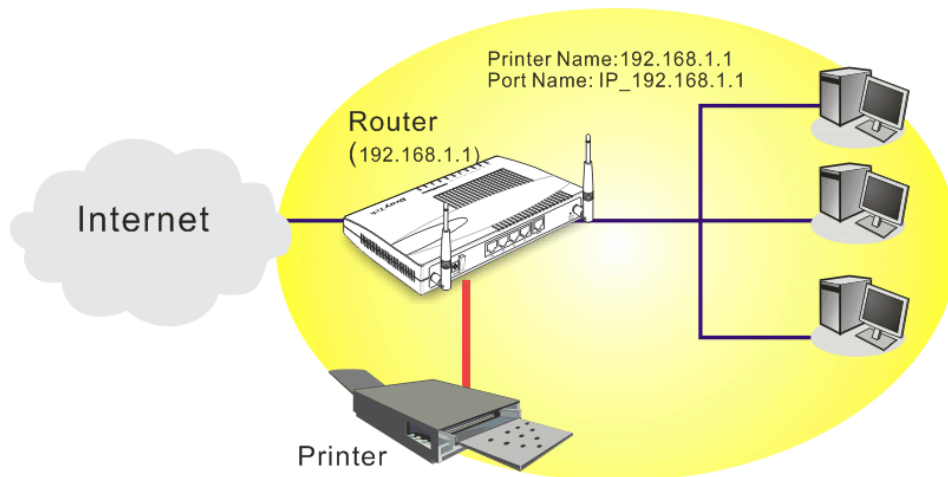
(For the detailed information of LED status, please refer to section 1.1.)



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

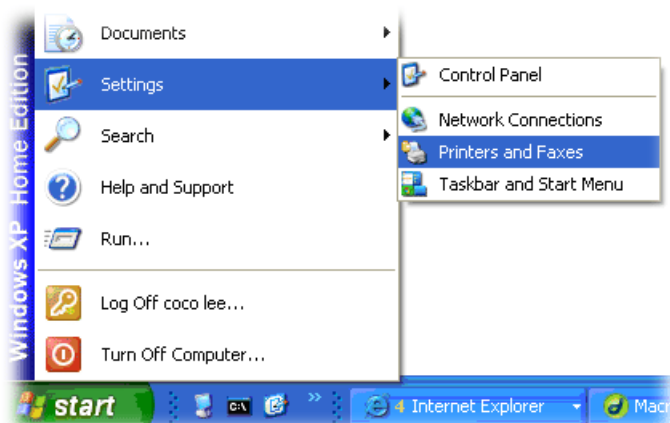
1.4 Printer Installation

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

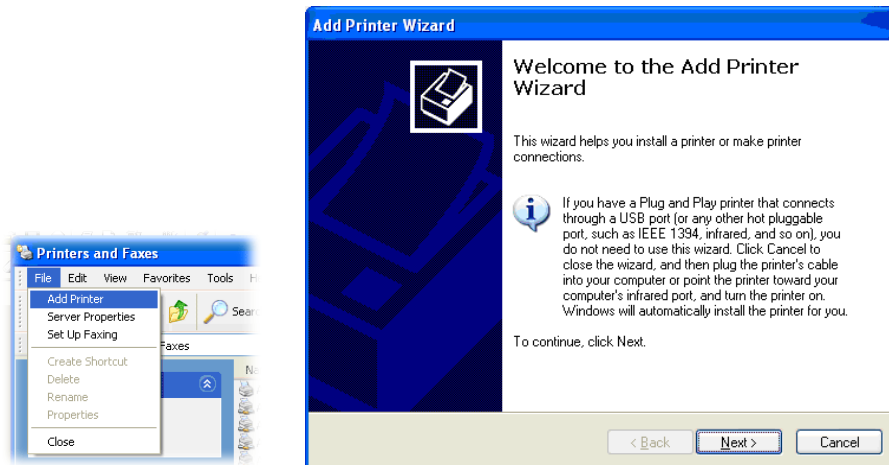


Before using it, please follow the steps below to configure settings for connected computers (or wireless clients).

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



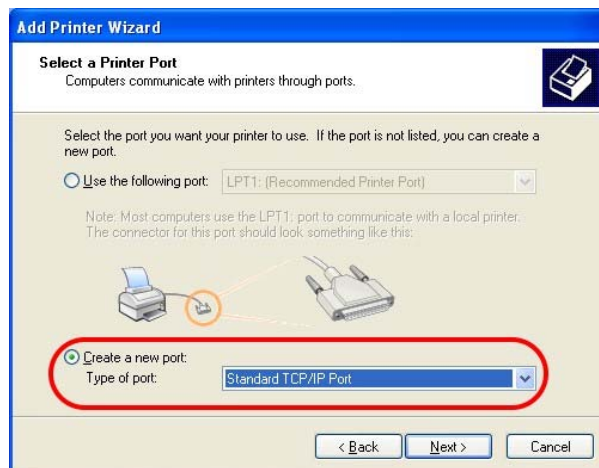
3. Open **File->Add a New Computer**. A welcome dialog will appear. Please click **Next**.



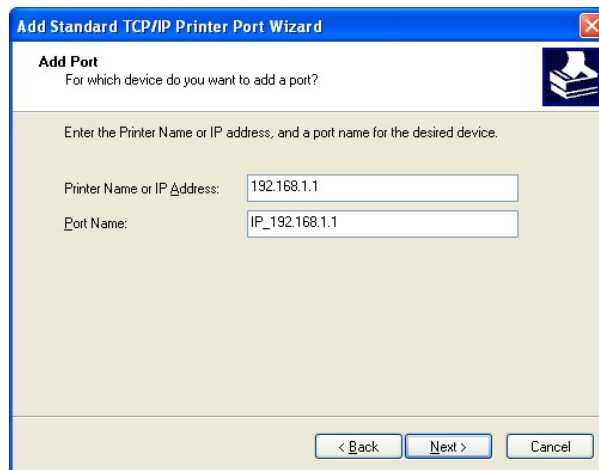
4. Click **Local printer attached to this computer** and click **Next**.



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

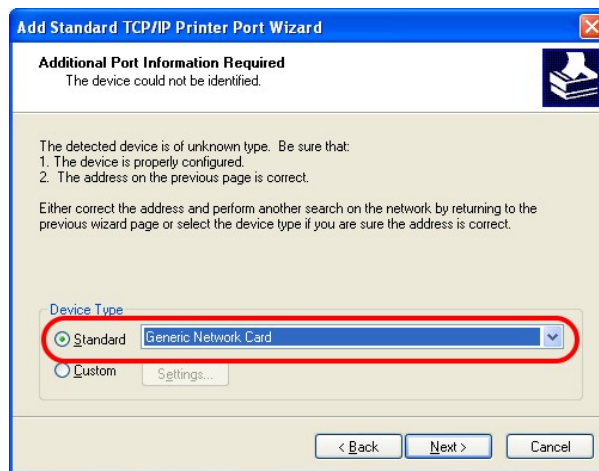


6. In the following dialog, type **192.168.1.1** (router's LAN IP) in the field of **Printer Name or IP Address** and type **IP_192.168.1.1** as the port name. Then, click **Next**.



The screenshot shows the 'Add Standard TCP/IP Printer Port Wizard' window, specifically the 'Add Port' step. The title bar reads 'Add Standard TCP/IP Printer Port Wizard'. Below the title bar, there is a printer icon and the text 'Add Port' and 'For which device do you want to add a port?'. The main area contains the instruction 'Enter the Printer Name or IP address, and a port name for the desired device.' There are two text input fields: 'Printer Name or IP Address:' with the value '192.168.1.1' and 'Port Name:' with the value 'IP_192.168.1.1'. At the bottom, there are three buttons: '< Back', 'Next >', and 'Cancel'.

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



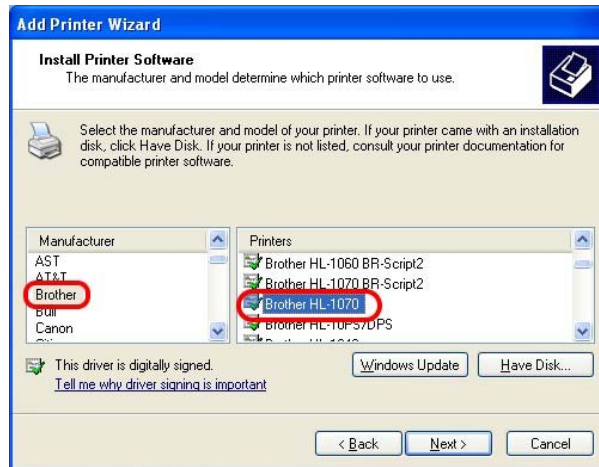
The screenshot shows the 'Add Standard TCP/IP Printer Port Wizard' window, specifically the 'Additional Port Information Required' step. The title bar reads 'Add Standard TCP/IP Printer Port Wizard'. Below the title bar, there is a printer icon and the text 'Additional Port Information Required' and 'The device could not be identified.' The main area contains the text 'The detected device is of unknown type. Be sure that:' followed by a list: '1. The device is properly configured.' and '2. The address on the previous page is correct.' Below this, it says '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.' There is a 'Device Type' section with two radio buttons: 'Standard' (selected) and 'Custom'. Next to 'Standard' is a dropdown menu showing 'Generic Network Card'. There is also a 'Settings...' button next to the 'Custom' radio button. At the bottom, there are three buttons: '< Back', 'Next >', and 'Cancel'.

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

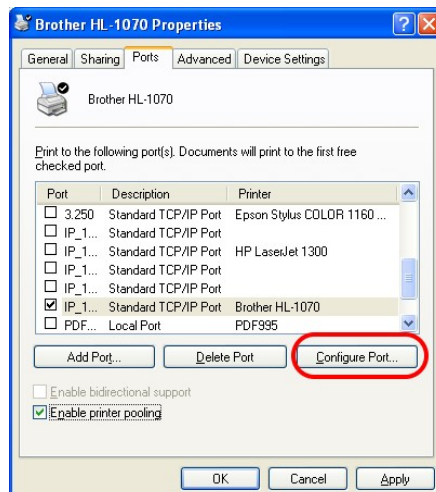


The screenshot shows the 'Add Standard TCP/IP Printer Port Wizard' window, specifically the 'Completing the Add Standard TCP/IP Printer Port Wizard' step. The title bar reads 'Add Standard TCP/IP Printer Port Wizard'. Below the title bar, there is a printer icon and the text 'Completing the Add Standard TCP/IP Printer Port Wizard'. The main area contains the text 'You have selected a port with the following characteristics:' followed by a list of characteristics: 'SNMP: No', 'Protocol: RAW, Port 9100', 'Device: 192.168.1.1', 'Port Name: IP_192.168.1.1', and 'Adapter Type: Generic Network Card'. At the bottom, it says 'To complete this wizard, click Finish.' There are three buttons: '< Back', 'Finish', and 'Cancel'.

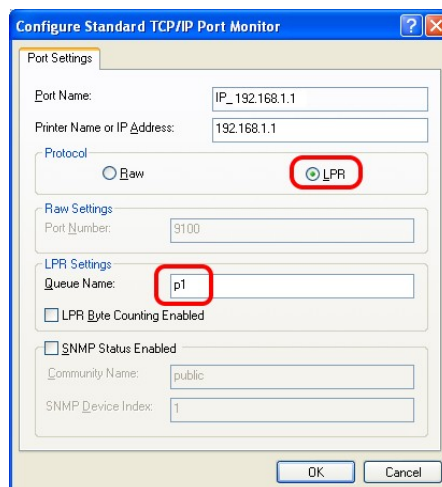
9. Now, your system will ask you to choose right name of the printer that you installed onto the router. Such step can make correct driver loaded onto your PC. When you finish the selection, click **Next**.



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



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



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

Note 1: Some printers with the fax/scanning or other additional functions are not supported. If you do not know whether your printer is supported or not, please visit www.draytek.com to find out the printer list. Open **Support Center->FAQ->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 use the router properly, it is necessary for you to change the password of web configuration for security and adjust primary basic settings.

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

2.1 Changing Password

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

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



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

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



- Now, the **Main Screen** will pop up. Notice that the main screen differs according to the model of the router that you have. Below is an example.

Vigor2910 Series
Dual-WAN Security Router

DrayTek
www.draytek.com

Quick Start Wizard
Online Status

WAN
LAN
NAT
Firewall
Objects Setting
CSM
Bandwidth Management
Applications
VPN and Remote Access
Certificate Management
VoIP
ISDN
Wireless LAN
VLAN
USB Application
System Maintenance
Diagnostics

All Rights Reserved.

System Status

Model Name : DrayTek Vigor2910
Firmware Version : 3.2.1 RC2
Build Date/Time : Tue Jul 29 18:35:51.48 2008

System	
CPU Usage	: 2 %
Total Memory	: 16M
Memory usage	: 61 %

LAN	
MAC Address	: 00-50-7F-DD-15-18
1st IP Address	: 192.168.1.1
1st Subnet Mask	: 255.255.255.0
DHCP Server	: Yes
Primary DNS	:
Secondary DNS	:

VoIP	
Port	: 1 2
SIP registrar	:
Account ID	change_me change_me
Register	:
Codec	:
In Calls	: 0 0
Out Calls	: 0 0

WAN 1	
Link Status	: Connected
MAC Address	: 00-50-7F-DD-15-19
Connection	: Static IP
IP Address	: 172.16.3.229
Default Gateway	: 172.16.3.4
Primary DNS	:
Secondary DNS	:

WAN 2	
Link Status	: Disconnected
MAC Address	: 00-50-7F-DD-15-1A
Connection	: ---
IP Address	: ---
Default Gateway	: ---
Primary DNS	:
Secondary DNS	:

Wireless LAN	
MAC Address	: 00-14-85-08-69-19
Frequency Domain	: Europe
Firmware Version	: v2.01.10.10.5.4

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

System Maintenance >> Administrator Password Setup

Administrator Password

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

OK

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

Connect to 192.168.1.1

Login to the Router Web Configurator

User name:

Password:

☐ Remember my password

OK Cancel

2.2 Quick Start Wizard

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

Quick Start Wizard

Enter login password

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

New Password

••••

Confirm Password

••••

< Back

Next >

Finish

Cancel

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

Quick Start Wizard

Select WAN Interface

Select WAN Interface:

WAN1

Display Name:

Physical Mode:

Ethernet

Physical Type:

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

< Back

Next >

Finish

Cancel

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

Quick Start Wizard

Connect to Internet

WAN 1

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

- ☒ PPPoE
- ☐ PPTP
- ☐ L2TP
- ☐ Static IP
- ☐ DHCP

< Back

Next >

Finish

Cancel

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

2.2.1 PPPoE

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

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

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

Quick Start Wizard

PPPoE Client Mode

WAN 1

Enter the user name and password provided by your ISP.

User Name

84005755@hinet.net

Password

••••••

Confirm Password

••••••

< Back

Next >

Finish

Cancel

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

Password Assign a valid password provided by the ISP.

Confirm Password Retype the password for confirmation.

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

Quick Start Wizard

Please confirm your settings:

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

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

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

Quick Start Wizard Setup OK !!!

2.2.2 PPTP

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

Quick Start Wizard

PPTP Client Mode

WAN 1
Enter the user name, password, WAN IP configuration and PPTP server IP provided by your ISP.

User Name	<input type="text"/>
Password	<input type="password"/>
Confirm Password	<input type="password"/>
WAN IP Configuration	
<input type="radio"/> Obtain an IP address automatically	
<input checked="" type="radio"/> Specify an IP address	
IP Address	<input type="text" value="172.16.3.229"/>
Subnet Mask	<input type="text" value="255.255.0.0"/>
Gateway	<input type="text" value="172.16.3.4"/>
Primary DNS	<input type="text"/>
Second DNS	<input type="text"/>
PPTP Server	<input type="text"/>

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

Quick Start Wizard

Please confirm your settings:

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

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

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

Quick Start Wizard Setup OK !!!

2.2.3 Static IP

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

Quick Start Wizard

Static IP Client Mode

WAN 1	
Enter the Static IP configuration provided by your ISP.	
WAN IP	<input type="text" value="172.16.3.229"/>
Subnet Mask	<input type="text" value="255.255.255.0"/>
Gateway	<input type="text" value="172.16.3.1"/>
Primary DNS	<input type="text" value="168.95.1.1"/>
Secondary DNS	<input type="text"/> (optional)

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

Quick Start Wizard

Please confirm your settings:

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

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

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

Quick Start Wizard Setup OK !!!

2.2.4 L2TP

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

Quick Start Wizard

L2TP Client Mode

WAN 1
Enter the user name, password, WAN IP configuration and L2TP server IP provided by your ISP.

User Name	<input type="text"/>
Password	<input type="password"/>
Confirm Password	<input type="password"/>
WAN IP Configuration	
<input type="radio"/> Obtain an IP address automatically	
<input checked="" type="radio"/> Specify an IP address	
IP Address	<input type="text" value="172.16.3.229"/>
Subnet Mask	<input type="text" value="255.255.0.0"/>
Gateway	<input type="text" value="172.16.3.4"/>
Primary DNS	<input type="text"/>
Second DNS	<input type="text"/>
L2TP Server	<input type="text"/>

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

Quick Start Wizard

Please confirm your settings:

WAN Interface:	WAN1
Physical Mode:	Ethernet
Physical Type:	Auto negotiation
Internet Access:	L2TP

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

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

Quick Start Wizard Setup OK !!!

2.2.5 DHCP

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

Quick Start Wizard

DHCP Client Mode

WAN 1

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

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

< Back

Next >

Finish

Cancel

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

Quick Start Wizard

Please confirm your settings:

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

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

< Back

Next >

Finish

Cancel

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

Quick Start Wizard Setup OK !!!

2.3 Online Status

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

Online status for PPPoE

Online Status

System Status				System Uptime: 0:0:41	
LAN Status		Primary DNS: 61.31.233.1		Secondary DNS: 139.175.55.244	
IP Address	TX Packets	RX Packets			
192.168.50.111	240	210			
WAN 1 Status				>> Drop PPPoE	
Enable	Line	Name	Mode	Up Time	
Yes	Ethernet		PPPoE	0:00:00	
IP	GW IP	TX Packets	TX Rate	RX Packets	RX Rate
219.81.160.205	211.78.218.40	6	29	6	12
WAN 2 Status					
Enable	Line	Name	Mode	Up Time	
Yes	Ethernet		Static IP	0:00:32	
IP	GW IP	TX Packets	TX Rate	RX Packets	RX Rate
192.168.4.103	192.168.4.1	1	3	1	9

Online status for PPTP (for WAN2)

Online Status

System Status				System Uptime: 0:12:8	
LAN Status		Primary DNS: 194.109.6.66		Secondary DNS: 194.98.0.1	
IP Address	TX Packets	RX Packets			
192.168.50.111	4910	3663			
WAN 1 Status					
Enable	Line	Name	Mode	Up Time	
Yes	Ethernet	WAN1	Static IP	0:10:08	
IP	GW IP	TX Packets	TX Rate	RX Packets	RX Rate
192.168.22.111	192.168.22.105	91	21	99	3
WAN 2 Status					>> Drop PPTP
Enable	Line	Name	Mode	Up Time	
Yes	Ethernet	WAN2	PPTP	0:00:15	
IP	GW IP	TX Packets	TX Rate	RX Packets	RX Rate
192.168.29.202	192.168.29.1	103	119	14	6

Online status for Static IP(for WAN1)

Online Status

System Status				System Uptime: 0:12:8	
LAN Status		Primary DNS: 194.109.6.66		Secondary DNS: 194.98.0.1	
IP Address	TX Packets	RX Packets			
192.168.50.111	4910	3663			
WAN 1 Status					
Enable	Line	Name	Mode	Up Time	
Yes	Ethernet	WAN1	Static IP	0:10:08	
IP	GW IP	TX Packets	TX Rate	RX Packets	RX Rate
192.168.22.111	192.168.22.105	91	21	99	3
WAN 2 Status					>> Drop PPTP
Enable	Line	Name	Mode	Up Time	
Yes	Ethernet	WAN2	PPTP	0:00:15	
IP	GW IP	TX Packets	TX Rate	RX Packets	RX Rate
192.168.29.202	192.168.29.1	103	119	14	6

Online status for DHCP

Online Status

System Status				System Uptime: 0:1:57	
LAN Status		Primary DNS: 168.95.1.1		Secondary DNS: 168.95.1.1	
IP Address	TX Packets	RX Packets			
192.168.50.111	856	783			
WAN 1 Status				>> Release	
Enable	Line	Name	Mode	Up Time	
Yes	Ethernet		DHCP Client	0:01:49	
IP	GW IP	TX Packets	TX Rate	RX Packets	RX Rate
192.168.22.10	192.168.22.105	3	3	7	9
WAN 2 Status				>> Drop PPPoE	
Enable	Line	Name	Mode	Up Time	
Yes	Ethernet		PPPoE	0:01:39	
IP	GW IP	TX Packets	TX Rate	RX Packets	RX Rate
202.211.100.176	202.211.100.170	35	8	46	4

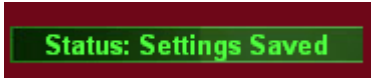
Detailed explanation is shown below:

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.
WAN1/2 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/WAN2) is ready for accessing Internet; the words in red mean that the WAN connection of that interface (WAN1/WAN2) is not ready for accessing Internet.

2.4 Saving Configuration

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



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 Advanced Web Configuration

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

3.1 WAN

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

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.

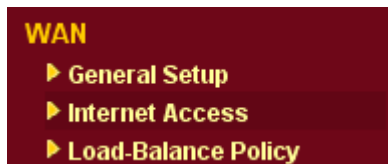
3.1.2 Network Connection by 3G USB Modem

For 3G mobile communication through Access Point is popular more and more, Vigor 2910 adds the function of 3G network connection for such purpose. By connecting 3G USB Modem to the USB port of Vigor2910, it can support HSDPA/UMTS/EDGE/GPRS/GSM and the future 3G standard (HSUPA, etc). Vigor2910 with 3G USB Modem allows you to receive 3G signals at any place such as your car or certain location holding outdoor activity and share the bandwidth for using by more people. Users can use four LAN ports on the router to access Internet. Also, they can access Internet via SuperG wireless function of Vigor2910G, and enjoy the powerful firewall, bandwidth management, VPN, VoIP features of Vigor2910 series.



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

Below shows the menu items for Internet Access.



3.1.3 General Setup

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

This router supports dual WAN function. It allows users to access Internet and combine the bandwidth of the dual WAN to speed up the transmission through the network. Each WAN port (WAN1- through WAN port/WAN2- through LAN1 port) can connect to different ISPs, Even if the ISPs use different technology to provide telecommunication service (such as DSL, Cable modem, etc.). If any connection problem occurred on one of the ISP connections, all the traffic will be guided and switched to the normal communication port for proper operation. Please configure WAN1 and WAN2 settings.

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

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

General Setup

WAN1	WAN2
Enable: <input type="checkbox"/> Yes <input type="checkbox"/> No	Enable: <input type="checkbox"/> Yes <input type="checkbox"/> No
Display Name: <input type="text"/>	Display Name: <input type="text"/>
Physical Mode: Ethernet	Physical Mode: <input type="text"/> Ethernet
Physical Type: Auto negotiation	Physical Type: <input type="text"/> Ethernet
Load Balance Mode: Auto Weight	Load Balance Mode: <input type="text"/> Auto Weight
Line Speed(Kbps): DownLink <input type="text"/>	Line Speed(Kbps): DownLink <input type="text"/>
UpLink <input type="text"/>	UpLink <input type="text"/>
Active Mode: Always On	Active Mode: Always On
Active on demand:	Active on demand:
<input type="radio"/> WAN2 Fail	<input type="radio"/> WAN1 Fail
<input checked="" type="radio"/> WAN2 Upload speed exceed <input type="text"/> Kbps	<input checked="" type="radio"/> WAN1 Upload speed exceed <input type="text"/> Kbps
WAN2 Download speed exceed <input type="text"/> Kbps	WAN1 Download speed exceed <input type="text"/> Kbps

Note: WAN2 and LAN P1 share the P1 port. When WAN2 is enabled, P1 is used as WAN2.

OK

Enable

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

Display Name

Type the description for the WAN1/WAN2 interface.

Physical Mode

For WAN1, the physical connection is done and fixed through Ethernet port; yet the physical connection for WAN2 is done through an Ethernet port (P1) or USB port. You cannot change it.

Physical Mode:

Ethernet

Ethernet

3G USB Modem

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

WAN >> Internet Access

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

Physical Type

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

Physical Type:

Auto negotiation

Auto negotiation

10M half duplex

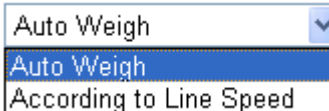
10M full duplex

100M half duplex

100M full duplex

Load Balance Mode

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

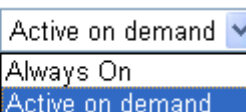
Load Balance Mode: 

Line Speed

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

Active Mode

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

Active Mode: 

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

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

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

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

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

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

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

3.1.4 Internet Access

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

WAN >> Internet Access

Internet Access

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

WAN >> Internet Access

Internet Access

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

Index

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

Display Name

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

Physical Mode

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

Physical Mode Physical Mode

Ethernet	Ethernet
3G USB Modem	Ethernet

Access Mode

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

Static or Dynamic IP	▼
None	
PPPoE	
Static or Dynamic IP	
PPTP/L2TP	

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

Details Page

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

Details Page for PPPoE

To use **PPPoE** as the accessing protocol of the internet, please choose **Internet Access** from **WAN** menu. Then, select **PPPoE** mode for WAN2. The following web page will be shown.

WAN >> Internet Access

WAN 1

<p>PPPoE Client Mode</p> <p><input type="radio"/> Enable <input checked="" type="radio"/> Disable</p> <p>ISP Access Setup</p> <p>Username <input type="text"/></p> <p>Password <input type="text"/></p> <p>Index(1-15) in Schedule Setup: => <input type="text"/>, <input type="text"/>, <input type="text"/>, <input type="text"/></p> <p>ISDN Dial Backup Setup</p> <p>Dial Backup Mode <input type="text" value="None"/></p> <p>WAN Connection Detection</p> <p>Mode <input type="text" value="ARP Detect"/></p> <p>Ping IP <input type="text"/></p> <p>TTL: <input type="text"/></p> <p>MTU <input type="text" value="1442"/> (Max: 1492)</p>	<p>PPP/MP Setup</p> <p>PPP Authentication <input type="text" value="PAP or CHAP"/></p> <p>Idle Timeout <input type="text" value="-1"/> second(s)</p> <p>IP Address Assignment Method (IPCP)</p> <p><input type="text" value="WAN IP Alias"/></p> <p>Fixed IP: <input type="radio"/> Yes <input checked="" type="radio"/> No (Dynamic IP)</p> <p>Fixed IP Address <input type="text"/></p> <p><input checked="" type="radio"/> Default MAC Address <input type="radio"/> Specify a MAC Address</p> <p>MAC Address: <input type="text" value="00"/> <input type="text" value="50"/> <input type="text" value="7F"/> <input type="text" value="DD"/> <input type="text" value="15"/> <input type="text" value="19"/></p>
--	---

OK Cancel

PPPoE Client Mode

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

ISP Access Setup

Enter your allocated username, password and authentication parameters according to the information provided by your ISP. 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.

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

ISDN Dial Backup Setup

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

Dial Backup Mode

None
Packet Trigger

This setting is available for *i* model only.

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

None - Disable the backup function.

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

WAN Connection Detection

Such function allows you to verify whether network connection is alive or not through ARP Detect or Ping Detect.

Mode – Choose **ARP Detect** or **Ping Detect** for the system to execute for WAN detection.

Ping IP – If you choose Ping Detect as detection mode, you have to type IP address in this field for pinging.

TTL (Time to Live) – Displays value for your reference. TTL value is set by telnet command.

MTU

It means Max Transmit Unit for packet. The default setting is 1442.

PPP/MP Setup

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

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

IP Address Assignment Method (IPCP)

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

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

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

OK Clear All Close

Fixed IP – Click **Yes** to use this function and type in a fixed IP

address in the box of **Fixed IP Address**.

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

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

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

Details Page for Static or Dynamic IP

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

To use **Static or Dynamic IP** as the accessing protocol of the internet, please choose **Internet Access** from **WAN** menu. Then, select **Static or Dynamic IP** mode for WAN2. The following web page will be shown.

WAN >> Internet Access

WAN 1

Static or Dynamic IP (DHCP Client) <input checked="" type="radio"/> Enable <input type="radio"/> Disable	WAN IP Network Settings WAN IP Alias <input type="radio"/> Obtain an IP address automatically Router Name <input type="text"/> * Domain Name <input type="text"/> * * : Required for some ISPs <input checked="" type="radio"/> Specify an IP address IP Address <input type="text"/> 172.16.3.229 Subnet Mask <input type="text"/> 255.255.0.0 Gateway IP Address <input type="text"/> 172.16.3.4
ISDN Dial Backup Setup Dial Backup Mode <input type="text"/> None	
Keep WAN Connection <input type="checkbox"/> Enable PING to keep alive PING to the IP <input type="text"/> PING Interval <input type="text"/> 0 minute(s)	
WAN Connection Detection Mode <input type="text"/> ARP Detect Ping IP <input type="text"/> TTL:	DNS Server IP Address Primary IP Address <input type="text"/> Secondary IP Address <input type="text"/>
MTU <input type="text"/> 1442 (Max: 1500)	<input checked="" type="radio"/> Default MAC Address <input type="radio"/> Specify a MAC Address MAC Address: <input type="text"/> 00 <input type="text"/> 50 <input type="text"/> 7F <input type="text"/> DD <input type="text"/> 15 <input type="text"/> 19
RIP Protocol <input type="checkbox"/> Enable RIP	

OK Cancel

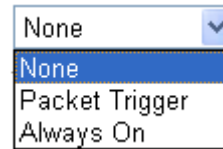
Static or Dynamic IP (DHCP Client)

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

ISDN Dial Backup Setup

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

Dial Backup Mode



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

None - Disable the backup function.

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

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

Keep WAN Connection

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

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

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

WAN Connection Detection

Such function allows you to verify whether network connection is alive or not through ARP Detect or Ping Detect.

Mode – Choose ARP Detect or Ping Detect for the system to execute for WAN detection.

Ping IP – If you choose Ping Detect as detection mode, you have to type IP address in this field for ping.

TTL (Time to Live) – Displays value for your reference. TTL value is set by telnet command.

MTU

It means Max Transmit Unit for packet. The default setting is 1442.

RIP Protocol

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

WAN IP Network Settings

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

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

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

OK Clear All Close

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

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

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

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

IP Address: Type the IP address.

Subnet Mask: Type the subnet mask.

Gateway IP Address: Type the gateway IP address.

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

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

DNS Server IP Address

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

Details Page for PPTP/L2TP

To use **PPTP** as the accessing protocol of the internet, please choose **Internet Access** from **WAN** menu. Then, select **PPTP** mode for WAN2. The following web page will be shown.

WAN >> Internet Access

WAN 1

PPTP/L2TP Client Mode <input type="radio"/> Enable PPTP <input type="radio"/> Enable L2TP <input checked="" type="radio"/> Disable Server Address <input type="text"/> Specify Gateway IP Address <input type="text" value="172.16.3.4"/>	PPP Setup PPP Authentication <input type="text" value="PAP or CHAP"/> Idle Timeout <input type="text" value="-1"/> second(s) IP Address Assignment Method (IPCP) <input type="button" value="WAN IP Alias"/> Fixed IP: <input type="radio"/> Yes <input checked="" type="radio"/> No (Dynamic IP) Fixed IP Address <input type="text"/> WAN IP Network Settings <input type="radio"/> Obtain an IP address automatically <input checked="" type="radio"/> Specify an IP address IP Address <input type="text" value="172.16.3.229"/> Subnet Mask <input type="text" value="255.255.0.0"/>
ISP Access Setup Username <input type="text"/> Password <input type="text"/> Index(1-15) in Schedule Setup: => <input type="text"/> , <input type="text"/> , <input type="text"/> , <input type="text"/> ISDN Dial Backup Setup Dial Backup Mode <input type="text" value="None"/>	MTU <input type="text" value="1442"/> (Max: 1460)

PPTP/L2TP Client Mode

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

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

Disable - Click this radio button to close the connection through PPTP or L2TP.

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

Specify Gateway IP Address - Specify the gateway IP address for DHCP server.

ISP Access Setup

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

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

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

ISDN Dial Backup Setup

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

Dial Backup Mode

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

information.

None - Disable the backup function.

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

MTU

It means Max Transmit Unit for packet. The default setting is 1442.

PPP Setup

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

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

IP Address Assignment Method(IPCP)

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

Fixed IP Address -Type a fixed IP address.

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

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

OK Clear All Close

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

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

WAN IP Network Settings

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

Specify an IP address – Click this radio button to specify some data.

IP Address – Type the IP address.

Subnet Mask – Type the subnet mask.

Details Page for PPP

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

WAN >> Internet Access

WAN 2

PPP Client Mode ☐ Enable ☒ Disable

SIM PIN code

Modem Initial String (Default: AT&FE0V1X1&D2&C1S0=0)

APN Name

Modem Dial String (Default: ATDT*99#)

PPP Username (Optional)

PPP Password (Optional)

Index(1-15) in **Schedule** Setup:
=> , , ,

PPP Client Mode

Click Enable to activate this mode for WAN2.

SIM PIN code

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

Modem Initial String

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

APN Name

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

Modem Dial String

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

PPP Username

Type the PPP username (optional).

PPP Password

Type the PPP password (optional).

Index (1-15)

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

3.1.5 Load-Balance Policy

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

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

WAN >> Load-Balance Policy

Load-Balance Policy

Index	Enable	Protocol	WAN	Src IP Start	Src IP End	Dest IP Start	Dest IP End	Dest Port Start	Dest Port End
1	<input type="checkbox"/>	any	WAN1						
2	<input type="checkbox"/>	any	WAN1						
3	<input type="checkbox"/>	any	WAN1						
4	<input type="checkbox"/>	any	WAN1						
5	<input type="checkbox"/>	any	WAN1						
6	<input type="checkbox"/>	any	WAN1						
7	<input type="checkbox"/>	any	WAN1						
8	<input type="checkbox"/>	any	WAN1						
9	<input type="checkbox"/>	any	WAN1						
10	<input type="checkbox"/>	any	WAN1						

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

[Next](#) >>

OK

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

Enable Check this box to enable this policy.

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

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

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

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

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

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

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

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

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

WAN >> Load-Balance Policy

Index: 1

<input checked="" type="checkbox"/> Enable	
Protocol	TCP
Binding WAN interface	WAN1
Src IP Start	192.168.1.3
Src IP End	192.168.1.5
Dest IP Start	168.95.0.0
Dest IP End	168.95.0.100
Dest Port Start	80
Dest Port End	100

OK

Cancel

Enable

Check this box to enable this policy.

Protocol

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

Protocol

any	▼
any	
TCP	
UDP	
TCP/UDP	
ICMP	
IGMP	

Binding WAN interface

Choose the WAN interface (WAN1 or WAN2) for binding.

Src IP Start

Type the source IP start for the specified WAN interface.

Src IP End

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

Dest IP Start

Type the destination IP start for the specified WAN interface.

Dest IP End

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

Dest Port Start

Type the destination port start for the destination IP.

Dest Port End

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

3.2 LAN

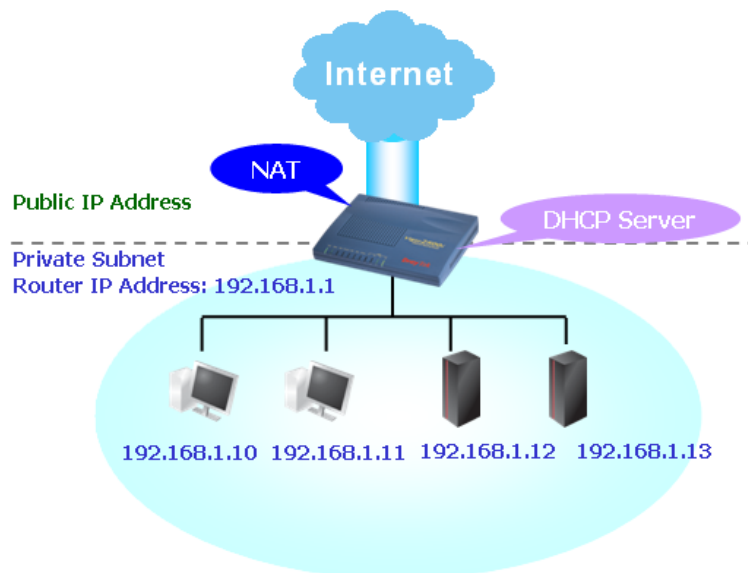
Local Area Network (LAN) is a group of subnets regulated and ruled by router. The design of network structure is related to what type of public IP addresses coming from your ISP.

LAN

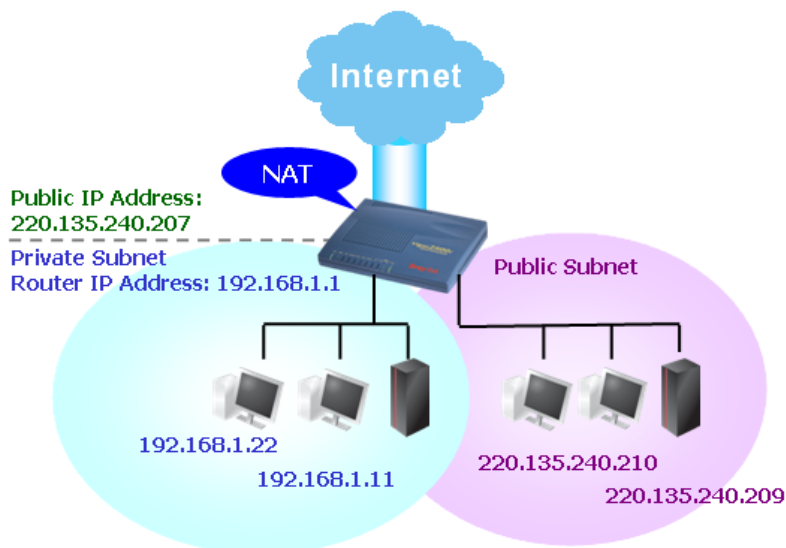
- ▶ General Setup
- ▶ Static Route
- ▶ Bind IP to MAC

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)

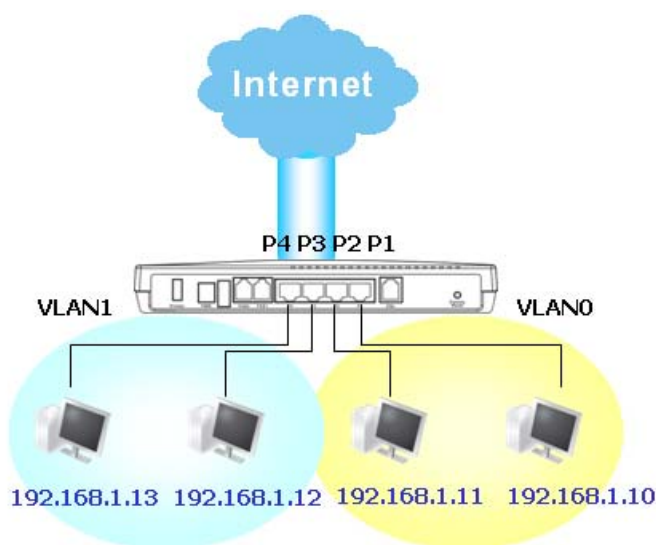
Vigor router will exchange routing information with neighboring routers using the RIP to accomplish IP routing. This allows users to change the information of the router such as IP address and the routers will automatically inform for each other.

What is Static Route

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

What are Virtual LANs and Rate Control

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



3.2.2 General Setup

This page provides you the general settings for LAN.

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

LAN >> General Setup

Ethernet TCP / IP and DHCP Setup

LAN IP Network Configuration		DHCP Server Configuration	
For NAT Usage		<input checked="" type="radio"/> Enable Server <input type="radio"/> Disable Server	
1st IP Address	<input type="text" value="192.168.1.1"/>	Relay Agent:	<input type="radio"/> 1st Subnet <input type="radio"/> 2nd Subnet
1st Subnet Mask	<input type="text" value="255.255.255.0"/>	Start IP Address	<input type="text" value="192.168.1.10"/>
For IP Routing Usage	<input type="radio"/> Enable <input checked="" type="radio"/> Disable	IP Pool Counts	<input type="text" value="50"/>
2nd IP Address	<input type="text" value="192.168.2.1"/>	Gateway IP Address	<input type="text" value="192.168.1.1"/>
2nd Subnet Mask	<input type="text" value="255.255.255.0"/>	DHCP Server IP Address for Relay Agent	<input type="text"/>
<input checked="" type="button" value="2nd Subnet DHCP Server"/>		DNS Server IP Address	
RIP Protocol Control <input type="text" value="Disable"/>		<input type="checkbox"/> Force DNS manual setting	
		Primary IP Address <input type="text"/>	
		Secondary IP Address <input type="text"/>	

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

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

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

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

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

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

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

2nd DHCP Server

Start IP Address	<input type="text"/>						
IP Pool Counts	<input type="text" value="0"/> (max. 10)						
<table border="1"><thead><tr><th>Index</th><th>Matched MAC Address</th><th>given IP Address</th></tr></thead><tbody><tr><td colspan="3" style="height: 100px;"></td></tr></tbody></table>		Index	Matched MAC Address	given IP Address			
Index	Matched MAC Address	given IP Address					
MAC Address : <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/>							
<input type="button" value="Add"/> <input type="button" value="Delete"/> <input type="button" value="Edit"/> <input type="button" value="Cancel"/>							

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.

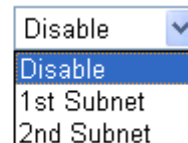
IP Pool Counts: Enter the number of IP addresses in the pool. The maximum is 10. For example, if you type 3 and the 2nd IP address of your router is 220.135.240.1, the range of IP address by the DHCP server will be from 220.135.240.2 to 220.135.240.11.

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



A screenshot of a web interface dropdown menu for 'RIP Protocol Control'. The menu is open, showing three options: 'Disable' (which is highlighted in blue), '1st Subnet', and '2nd Subnet'. The dropdown is located to the right of the text 'RIP Protocol Control'.

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

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

DHCP Server Configuration

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

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

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

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

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

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

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

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

of the router, which means the router is the default gateway.

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

DNS Server Configuration

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

Force DNS manual setting - Force Vigor2910 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: 0:7:39	
LAN Status		Primary DNS: 194.109.6.66		Secondary DNS: 168.95.1.1
IP Address	TX Packets	RX Packets		
192.168.1.1	490	408		

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.

3.2.3 Static Route

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

LAN >> Static Route Setup

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

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

Index	The number (1 to 10) under Index allows you to open next page to set up static route.
Destination Address	Displays the destination address of the static route.
Status	Displays the status of the static route.
Viewing Routing Table	Displays the routing table for your reference.

[Diagnostics >> View Routing Table](#)

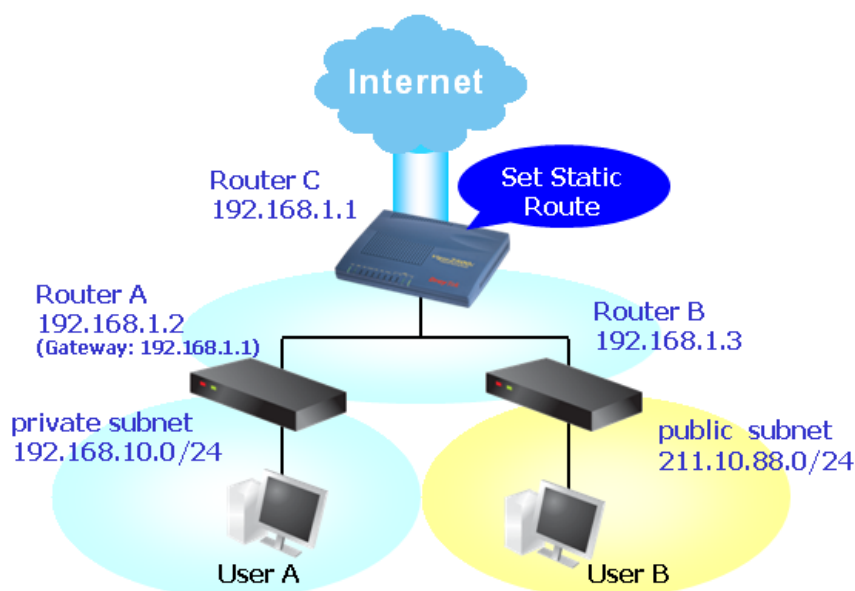
Current Running Routing Table				Refresh
Key: C - connected, S - static, R - RIP, * - default, ~ - private				
*	0.0.0.0/	0.0.0.0 via 172.16.3.1,	WAN1	
C~	192.168.1.0/	255.255.255.0 is directly connected,	LAN	
C	172.16.3.0/	255.255.255.0 is directly connected,	WAN1	

Add Static Routes to Private and Public Networks

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

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

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



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

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

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

LAN >> Static Route Setup

Index No. 1

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

OK Cancel

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

LAN >> Static Route Setup

Index No. 2

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

OK Cancel

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

Diagnostics >> View Routing Table

Current Running Routing Table

| Refresh |

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


3.2.4 Bind IP to MAC

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

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

LAN >> Bind IP to MAC

Bind IP to MAC

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

☒ **Enable** ☐ **Disable** ☐ **Strict Bind**

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

IP Address	Mac Address
192.168.1.13	00-0E-A6-2A-D5-A1
192.168.1.10	00-0D-0B-A7-86-F3
192.168.1.100	00-08-A1-36-97-5D

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

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

Add and Edit
IP Address
Mac Address

Enable

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

Disable

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

Strict Bind

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

ARP Table

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

Add and Edit

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

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

Refresh

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

IP Bind List

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

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

3.3 NAT

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

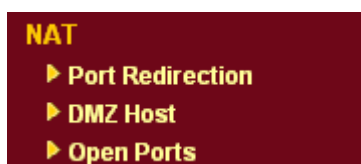
When the outgoing packets destined to some public server on the Internet reach the NAT router, the router will change its source address into the public IP address of the router, select the available public port, and then forward it. At the same time, the router shall list an entry in a table to memorize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

The benefit of the NAT includes:

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

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

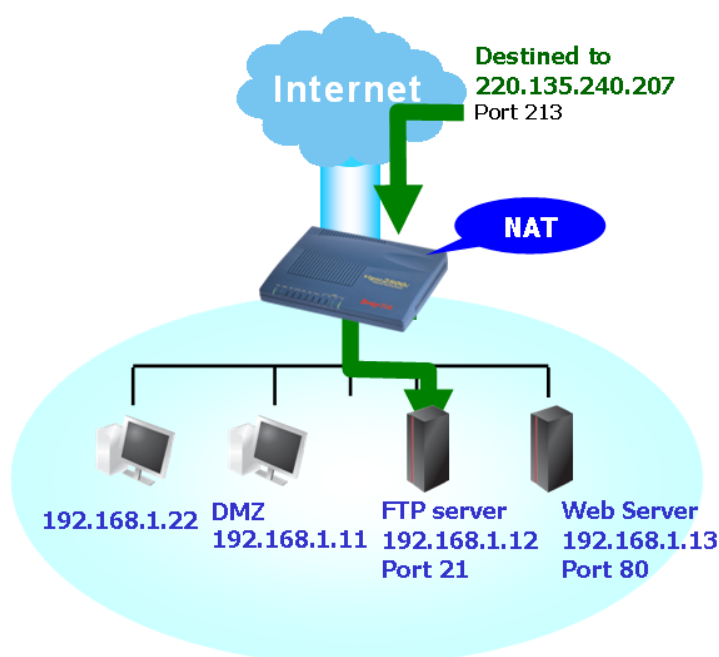
Below shows the menu items for NAT.



3.3.1 Port Redirection

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

Since the server is actually located inside the LAN, the network well protected by NAT of the router, and identified by its private IP address/port, the goal of Port Redirection function is to forward all access request with public IP address from external users to the mapping private IP address/port of the server.



The port redirection can only apply to incoming traffic.

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

NAT >> Port Redirection

Port Redirection				Set to Factory Default
Index	Service Name	Public Port	Private IP	Status
1.				×
2.				×
3.				×
4.				×
5.				×
6.				×
7.				×
8.				×
9.				×
10.				×

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

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

NAT >> Port Redirection

Index No. 1

<input checked="" type="checkbox"/> Enable	
Mode	Range ▼
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.

OK Clear Cancel

Mode

Two options are provided here for you to choose. To set a range for the specific service, select Range.

Service Name

Enter the description of the specific network service.

Protocol

Select the transport layer protocol (TCP or UDP).

Public Port

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

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.

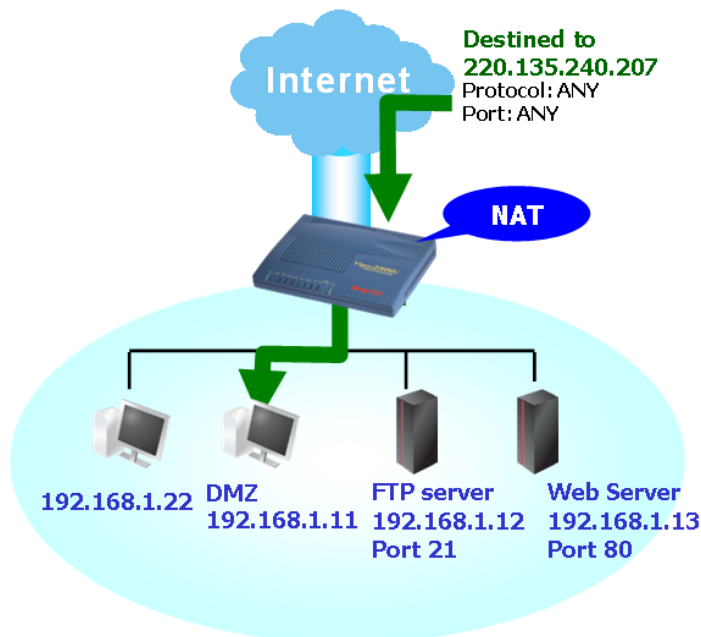
Management Setup

Management Access Control <input checked="" type="checkbox"/> Allow management from the Internet <input type="checkbox"/> FTP Server <input checked="" type="checkbox"/> HTTP Server <input checked="" type="checkbox"/> HTTPS Server <input checked="" type="checkbox"/> Telnet Server <input type="checkbox"/> SSH Server <input checked="" type="checkbox"/> Disable PING from the Internet	Management Port Setup <input checked="" type="radio"/> User Define Ports <input type="radio"/> Default Ports Telnet Port: <input type="text" value="23"/> (Default: 23) HTTP Port: <input type="text" value="80"/> (Default: 80) HTTPS Port: <input type="text" value="443"/> (Default: 443) FTP Port: <input type="text" value="21"/> (Default: 21) SSH Port: <input type="text" value="22"/> (Default: 22)												
Access List <table border="1"> <thead> <tr> <th>List</th> <th>IP</th> <th>Subnet Mask</th> </tr> </thead> <tbody> <tr> <td>1</td> <td><input type="text"/></td> <td><input type="text"/></td> </tr> <tr> <td>2</td> <td><input type="text"/></td> <td><input type="text"/></td> </tr> <tr> <td>3</td> <td><input type="text"/></td> <td><input type="text"/></td> </tr> </tbody> </table>	List	IP	Subnet Mask	1	<input type="text"/>	<input type="text"/>	2	<input type="text"/>	<input type="text"/>	3	<input type="text"/>	<input type="text"/>	SNMP Setup <input type="checkbox"/> Enable SNMP Agent Get Community: <input type="text" value="public"/> Set Community: <input type="text" value="private"/> Manager Host IP: <input type="text"/> Trap Community: <input type="text" value="public"/> Notification Host IP: <input type="text"/> Trap Timeout: <input type="text" value="10"/> seconds
List	IP	Subnet Mask											
1	<input type="text"/>	<input type="text"/>											
2	<input type="text"/>	<input type="text"/>											
3	<input type="text"/>	<input type="text"/>											

OK

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

DMZ Host Setup

WAN 1

Active True IP

Private IP

MAC Address of the True IP DMZ Host

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

WAN 2

Enable ☒

Private IP

WAN1

This page allows you to set Private IP or Active True IP as the DMZ host.

WAN 1

Active True IP

None

Private IP

Active True IP

Private IP

If you choose Private IP as the selection for DMZ host, please type in private IP or select any one by clicking the Choose PC button.

MAC Address of the True IP DMZ Host

If you choose Active True IP as the selection for DMZ host, please type in MAC address in these fields.

If you previously have set up **WAN IP Alias** on **WAN1** interface while configuring **PPPoE**, **Static or Dynamic IP** or **PPTP** (by accessing into **WAN>>Internet Access**), you will find them in **Aux. WAN IP list** for your selection.

NAT >> DMZ Host Setup

DMZ Host Setup

WAN 1

Index	Enable	Aux. WAN IP	Private IP	
1.	<input type="checkbox"/>	172.16.3.229	<input type="text"/>	<input type="button" value="Choose PC"/>
2.	<input type="checkbox"/>	172.16.3.89	<input type="text"/>	<input type="button" value="Choose PC"/>

WAN 2

Enable ☐

Private IP

Enable

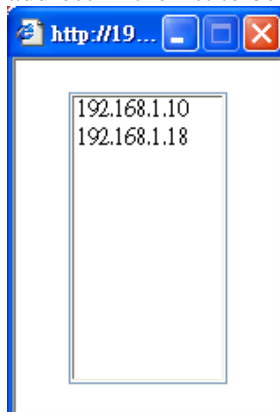
Check to enable the DMZ Host function.

Private IP

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

Choose PC

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



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

NAT >> DMZ Host Setup

DMZ Host Setup

WAN 1				
Index	Enable	Aux. WAN IP	Private IP	
1.	<input checked="" type="checkbox"/>	172.16.3.229	192.168.1.10	<input type="button" value="Choose PC"/>
2.	<input type="checkbox"/>	172.16.3.89		<input type="button" value="Choose PC"/>

WAN 2		
Enable	Private IP	
<input type="checkbox"/>		<input type="button" value="Choose PC"/>

3.3.3 Open Ports

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

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

[NAT >> Open Ports](#)

Open Ports Setup				Set to Factory Default
Index	Comment	WAN Interface	Local IP Address	Status
1.				X
2.				X
3.				X
4.				X
5.				X
6.				X
7.				X
8.				X
9.				X
10.				X

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

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

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

NAT >> Open Ports >> Edit Open Ports

Index No. 1

☒ Enable Open Ports

Comment

WAN Interface

WAN IP

Local Computer

	Protocol	Start Port	End Port		Protocol	Start Port	End Port
1.	<input type="text" value="TCP"/>	<input type="text" value="4500"/>	<input type="text" value="4700"/>	6.	<input type="text" value="-----"/>	<input type="text" value="0"/>	<input type="text" value="0"/>
2.	<input type="text" value="UDP"/>	<input type="text" value="4500"/>	<input type="text" value="4700"/>	7.	<input type="text" value="-----"/>	<input type="text" value="0"/>	<input type="text" value="0"/>
3.	<input type="text" value="-----"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	8.	<input type="text" value="-----"/>	<input type="text" value="0"/>	<input type="text" value="0"/>
4.	<input type="text" value="-----"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	9.	<input type="text" value="-----"/>	<input type="text" value="0"/>	<input type="text" value="0"/>
5.	<input type="text" value="-----"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	10.	<input type="text" value="-----"/>	<input type="text" value="0"/>	<input type="text" value="0"/>

Enable Open Ports

Check to enable this entry.

Comment

Make a name for the defined network application/service.

WAN Interface

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

WAN IP

Choose one of the WAN IPs from this drop-down list. This selection is available and can be seen only if you have set WAN IP Alias previously.

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

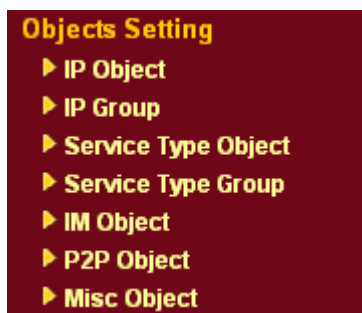
Specify the starting port number of the service offered by the local host.

End Port

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

3.4 Objects and Groups

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).



Besides, you can define object profiles for different policy of IM (Instant Messenger)/P2P (Peer to Peer)/Misc application.

3.4.1 IP Object

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

Objects Setting >> IP Object

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

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

Set to Factory Default Clear all profiles.

Click the number under Index column for settings in detail.

Objects Setting >> IP Object

Profile Index : 1

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

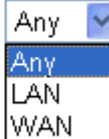
OK Cancel

Name

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

Interface

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

Interface: 

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

Address Type

Determine the address type for the IP address.

Select **Single Address** if this object contains one IP address only.

Select **Range Address** if this object contains several IPs within a range.

Select **Subnet Address** if this object contains one subnet for IP address.

Select **Any Address** if this object contains any IP address.

Start IP Address

Type the start IP address for Single Address type.

End IP Address

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

Subnet Mask

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

Invert Select

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

Below is an example of IP objects settings.

Objects Setting >> IP Object

IP Object Profiles:

Index	Name	Index
1.	RD Department	17.
2.	Financial Dept.	18.
3.	HR Department	19.
4.		20.
5.		21.

3.4.2 IP Group

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

[Objects Setting >> IP Group](#)

IP Group Table: [Set to Factory Default](#)

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

Set to Factory Default Clear all profiles.

Click the number under Index column for settings in detail.

[Objects Setting >> IP Group](#)

Profile Index : 1

Name:

Interface:

Available IP Objects
1-RD Department
2-Financial Dept.
3-HR Department

<<"/>

Selected IP Objects

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

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

Available IP Objects All the available IP objects with the specified interface chosen above will be shown in this box.

Selected IP Objects Click >> button to add the selected IP objects in this box.

3.4.3 Service Type Object

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

Objects Setting >> Service Type Object

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

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

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

[Next](#) >>

Set to Factory Default Clear all profiles.

Click the number under Index column for settings in detail.

Objects Setting >> Service Type Object Setup

Profile Index : 1

Name

Protocol

Source Port

Destination Port

www

TCP6

=1~65535

=80~80

OK

Cancel

Name Type a name for this profile.
Protocol Specify the protocol(s) which this profile will apply to.

TCP6

Any

ICMP

IGMP

TCP

UDP

TCP/UDP

Other

Source/Destination Port **Source Port** and the **Destination Port** column are available for TCP/UDP protocol. It can be ignored for other protocols. The filter rule will filter out any port number.
(=) – when the first and last value are the same, it indicates one port; when the first and last values are different, it indicates a range for the port and available for this profile.

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

Below is an example of service type objects settings.

Service Type Object Profiles:

Index	Name
<u>1.</u>	SIP
<u>2.</u>	RTP
<u>3.</u>	

3.4.4 Service Type Group

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

Objects Setting >> Service Type Group

Service Type Group Table:

| [Set to Factory Default](#) |

Group	Name	Group	Name
<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.

Profile Index : 1

Name:

Available Service Type Objects

1-SIP
2-RTP

Selected Service Type Objects

Name

Type a name for this profile.

Available Service Type Objects

You can add IP objects from IP Objects page. All the available IP objects will be shown in this box.

Selected Service Type Objects

Click >> button to add the selected IP objects in this box.

3.4.5 IM Object

You can define policy profiles for IM (Instant Messenger) application. The object profile(s) configured here will be seen and adopted in **CSM>>IM/P2P Filter Profile** page.

Objects Setting >> IM Object Profile

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

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

Set to Factory Default

Clear all profiles.

Click the number under Index column for settings in detail.

Objects Setting >> IM Object Profile

Profile Index: 1

Profile Name:

Check for Disallow:

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

* : Does NOT support Skype autologin blocking.

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

OK Clear Cancel

Profile Name

Type a name for the CSM profile.

Check for Disallow

Check the items that disallow to use. Any device that uses such profile might not be allowed to access into the forbidden items.

3.4.6 P2P Object

You can define policy profiles for P2P (Point-to-Point) application. The object profile(s) configured here will be seen and adopted in **CSM>>IM/P2P Filter Profile** page.

Objects Setting >> P2P Object Profile

P2P Profile Table:

[Set to Factory Default](#)

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

Set to Factory Default

Clear all profiles.

Click the number under Index column for settings in detail.

Objects Setting >> CSM-P2P Object Profile

Profile Index: 1

Profile Name:

Check for Disallow:

Protocol	Applications
<input type="checkbox"/> SoulSeek	SoulSeek
<input type="checkbox"/> eDonkey	eDonkey, eMule, Shareaza
<input type="checkbox"/> FastTrack	Kazaa, iMesh
<input type="checkbox"/> Gnutella	BearShare, Limewire, Shareaza, Foxy
<input checked="" type="checkbox"/> BitTorrent	BitTorrent, BitSpirit, BitComet
<input type="checkbox"/> Winny	Winny, WinMX, Share

Other P2P Applications			
<input type="checkbox"/> Xunlei	<input type="checkbox"/> Vagaa	<input type="checkbox"/> PP365	<input type="checkbox"/> POCO
<input type="checkbox"/> Clubbox	<input type="checkbox"/> Ares		

Profile Name

Type a name for the CSM profile.

Check for Disallow

Check the items that disallow to use. Any device that uses such profile might not be allowed to access into the forbidden items.

In the above figure, BitTorrent protocol is disallowed if you apply such object profile as filtering rule (setting in **Firewall**).

3.4.7 Misc Object

You can define policy profiles for Misc application. The object profile(s) configured here will be seen and adopted in **CSM>>IM/P2P Filter Profile** page.

Objects Setting >> Misc Object Profile

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

Set to Factory Default Clear all profiles.

Click the number under Index column for settings in detail.

Objects Setting >> Misc Object Profile

Profile Index: 1

Profile Name:

Check for Disallow:

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

Profile Name Type a name for the CSM profile.

Check for Disallow Check the items that disallow to use. Any device that uses such profile might not be allowed to access into the forbidden items.

3.5 CSM

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.

IM/P2P Filter

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

URL Content Filter

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

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

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

Web Content Filter

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

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

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

CSM

- ▶ IMP2P Filter Profile
- ▶ URL Content Filter Profile
- ▶ Web Content Filter Profile

3.5.1 IM/P2P Filter Profile

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

CSM >> IM/P2P Filter Profile

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

Set to Factory Default Clear all profiles.

Click the number under Index column for settings in detail.

CSM >> IM/P2P Filter Profile

Profile Index: [1](#)

Profile Name:

IM Object	None ▾
P2P Object	None ▾
Misc Object	None ▾

OK

Cancel

Profile Name Type a name for the CSM profile.

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

3.5.2 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.

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

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

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

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

CSM >> URL Content Filter Profile

Content Filter Setup

☒ Enable URL Access Control

- ☐ Enable URL Access Log
☒ Black List (block those matching keyword)
☐ White List (pass those matching keyword)

No	ACT	Keyword	No	ACT	Keyword
1	<input type="checkbox"/>	<input type="text"/>	5	<input type="checkbox"/>	<input type="text"/>
2	<input type="checkbox"/>	<input type="text"/>	6	<input type="checkbox"/>	<input type="text"/>
3	<input type="checkbox"/>	<input type="text"/>	7	<input type="checkbox"/>	<input type="text"/>
4	<input type="checkbox"/>	<input type="text"/>	8	<input type="checkbox"/>	<input type="text"/>

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

☐ Prevent web access from IP address

☐ Enable Restrict Web Feature

- ☐ Java ☐ ActiveX ☐ Compressed files ☐ Executable files ☐ Multimedia files
☐ Cookie ☐ Proxy

☐ Enable Excepting Subnets

No	Act	IP Address		Subnet Mask
1	<input type="checkbox"/>	<input type="text"/>	~	<input type="text"/>
2	<input type="checkbox"/>	<input type="text"/>	~	<input type="text"/>
3	<input type="checkbox"/>	<input type="text"/>	~	<input type="text"/>
4	<input type="checkbox"/>	<input type="text"/>	~	<input type="text"/>

Time Schedule

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

Note: Action and Idle Timeout settings will be ignored.

Enable URL Access Control

Check the box to activate URL Access Control.

Black List (block those matching keyword)	Click this button to restrict accessing into the corresponding webpage with the keywords listed on the box below.
White List (pass those matching keyword)	Click this button to allow accessing into the corresponding webpage with the keywords listed on the box below.
Keyword	The Vigor router provides 8 frames for users to define keywords and each frame supports multiple keywords. The keyword could be a noun, a partial noun, or a complete URL string. Multiple keywords within a frame are separated by space, comma, or semicolon. In addition, the maximal length of each frame is 32-character long. After specifying keywords, the Vigor router will decline the connection request to the website whose URL string matched to any user-defined keyword. It should be noticed that the more simplified the blocking keyword list, the more efficiently the Vigor router perform.
Prevent web access from IP address	<p>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.</p> <p>You must clear your browser cache first so that the URL content filtering facility operates properly on a web page that you visited before.</p>
Enable Restrict Web Feature	<p>Check the box to activate the function.</p> <p>Java - Check the checkbox to activate the Block Java object function. The Vigor router will discard the Java objects from the Internet.</p> <p>ActiveX - Check the box to activate the Block ActiveX object function. Any ActiveX object from the Internet will be refused.</p> <p>Compressed file - Check the box to activate the Block Compressed file function to prevent someone from downloading any compressed file. The following list shows the types of compressed files that can be blocked by the Vigor router. .</p> <p>zip, rar, .arj, .ace, .cab, .sit</p> <p>Executable file - Check the box to reject any downloading behavior of the executable file from the Internet.</p> <p>.exe, .com, .scr, .pif, .bas, .bat, .inf, .reg</p> <p>Cookie - Check the box to filter out the cookie transmission from inside to outside world to protect the local user's privacy.</p> <p>Proxy - Check the box to reject any proxy transmission. To control efficiently the limited-bandwidth usage, it will be of great value to provide the blocking mechanism that filters out the multimedia files downloading from web pages. Accordingly, files with the following extensions will be blocked by the Vigor router.</p> <p>.mov .mp3 .rm .ra .au .wmv .wav .asf .mpg .mpeg .avi .ram</p>
Enable Excepting Subnets	Four entries are available for users to specify some specific IP addresses or subnets so that they can be free from the <i>URL Access Control</i> . To enable an entry, click on the empty checkbox, named as ACT , in front of the appropriate entry.
Time Schedule	Specify what time should perform the URL content filtering facility.

3.5.3 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, powered by SurfControl. The database covering over 70 languages and 200 countries, over 1 billion Web pages divided into 40 easy-to-understand categories. This database is updated as frequent as daily by a global team of Internet researchers. The server will look up the URL and return a category to your router. Your Vigor router will then decide whether to allow access to this site according to the categories you have selected. Please note that this action will not introduce any delay in your Web surfing because each of multiple load balanced database servers can handle millions of requests for categorization.

Click **CSM** and click **Web Content Filter** to open the setup page.

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

CSM >> Web Content Filter Setup

Web Content Filter Profile

Select a server:

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

☐ Enable Web Content Filter

Groups

Child Protection

Leisure

Business

Others

Categories (Tick categories to block. Untick to unblock)

☐ Chat

☐ Gambling

☐ Sex

☐ Criminal

☐ Hacking

☐ Violence

☐ Drugs/Alcohol

☐ Hate speech

☐ Weapons

☐ Advertisements

☐ Games

☐ Hobbies

☐ Personals

☐ Sports

☐ Entertainment

☐ Glamour

☐ Lifestyle

☐ Photo Searches

☐ Streaming Media

☐ Food

☐ Health

☐ Motor Vehicles

☐ Shopping

☐ Travel

☐ Computing/Internet

☐ Politics

☐ Remote proxies

☐ Finance

☐ Real Estate

☐ Search Engine

☐ Job Search/Career

☐ Reference

☐ Web Mail

☐ Education

☐ News

☐ Usenet news

☐ Hosting sites

☐ Religion

☐ Block all uncategorised sites

☐ Kid Sites

☐ Sex Education

Time Schedule

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

Note: Action and Idle Timeout settings will be ignored.

3.6 Firewall

3.6.1 Basics for Firewall

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

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

Quick Start Wizard

Enter login password

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

New Password	<input type="password"/>
Confirm Password	<input type="password"/>

If you did not set password during installation; you can go to **System Maintenance** to set up your password.

System Maintenance >> Administrator Password Setup

Administrator Password

Old Password	<input type="password"/>
New Password	<input type="password"/>
Confirm Password	<input type="password"/>

Firewall Facilities

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

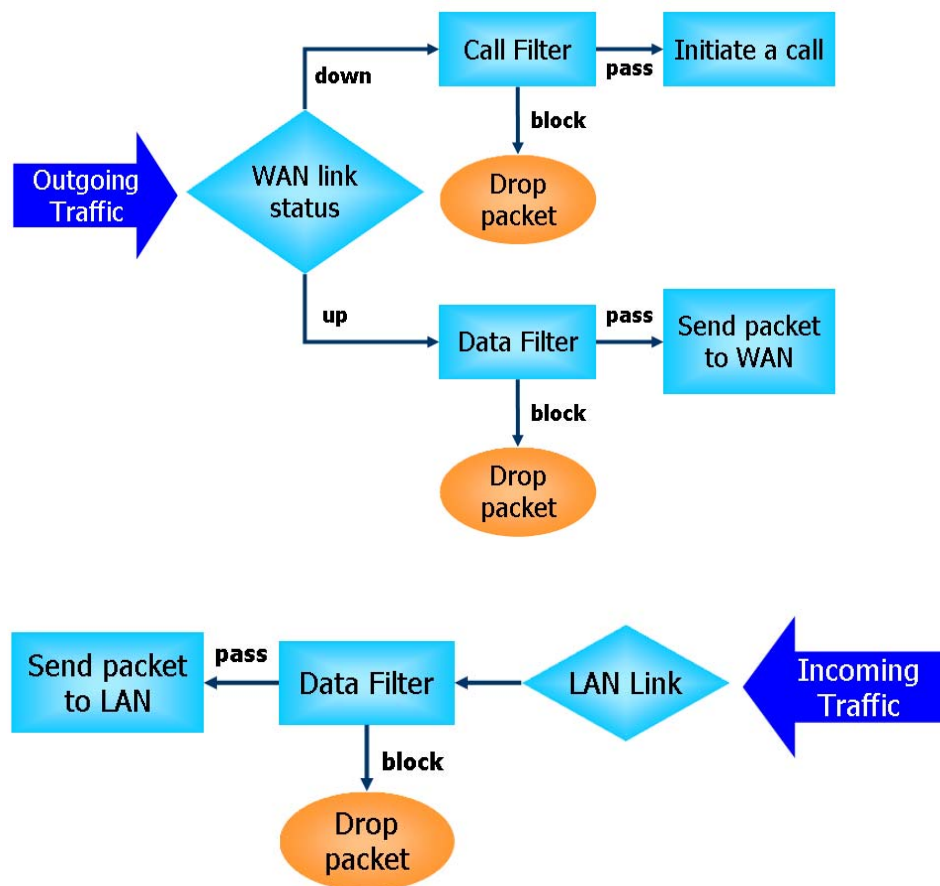
- User-configurable IP filter (Call Filter/ Data Filter).
- Stateful Packet Inspection (SPI): tracks packets and denies unsolicited incoming data
- Selectable Denial of Service (DoS) /Distributed DoS (DDoS) attacks protection

IP Filters

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

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

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



Stateful Packet Inspection (SPI)

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

Denial of Service (DoS) Defense

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

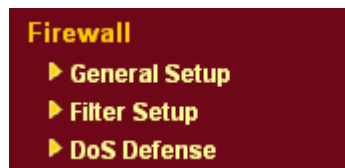
The **DoS Defense** function enables the Vigor router to inspect every incoming packet based on the attack signature database. Any malicious packet that might duplicate itself to paralyze the host in the secure LAN will be strictly blocked and a Syslog message will be sent as warning, if you set up Syslog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

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

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

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

Below shows the menu items for Firewall.



3.6.2 General Setup

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

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

General Setup

Call Filter	<input checked="" type="radio"/> Enable <input type="radio"/> Disable	Start Filter Set	Set#1 ▼
Data Filter	<input checked="" type="radio"/> Enable <input type="radio"/> Disable	Start Filter Set	Set#2 ▼

Actions for default rule:

Application	Action/Profile	Syslog
Filter	Pass ▼	<input type="checkbox"/>
IM/P2P Filter	None ▼	<input type="checkbox"/>

☐ Apply IP filter to VPN incoming packets
☒ Accept large incoming fragmented UDP or ICMP packets (for some games, ex. CS)

OK Cancel

Call Filter

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

Data Filter

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

Filter

Default rule is applied in this page.

Pass – All the packets are allowed to pass through the router without considering settings configured in **Firewall>>Filter Setup**.

Block - All the packets are not allowed to pass through the router without considering settings configured in **Firewall>>Filter Setup**.

Filter

Pass ▼

Pass

Block

For troubleshooting needs, you can specify to record Filter information 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.

IM/P2P Filter

Select an IM/P2P profile for global IM/P2P application blocking. All the hosts in LAN must follow the standard configured in the selected profile selected here. For detailed information, refer to the section of CSM profile setup.

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**”.

3.6.3 Filter Setup

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

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

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

Filter Set 1

Comments :

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

Next Filter Set **Filter Rule**

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

Active

Enable or disable the filter rule.

Comment

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

Move Up/Down

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

Next Filter Set

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

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

Filter Set 1 Rule 1

☒ Check to enable the Filter Rule

Comments:

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

Direction:

Source IP:

Destination IP:

Service Type:

Fragments:

Application

Filter:

Branch to Other Filter Set:

IM/P2P Filter:

Action/Profile

Syslog ☐

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

IP Address Edit - Microsoft Internet Explorer

IP Address Edit

Address Type

Start IP Address

End IP Address

Subnet Mask

Invert Selection ☐

IP Group

or **IP Object**

or IP Object

or IP Object

or IP Object

To set the IP address manually, please choose **Any Address/Single**

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

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

Service Type

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

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

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

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

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

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

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

	<p>Service Group/Object - Use the drop down list to choose the one that you want.</p>
Fragments	<p>Specify the action for fragmented packets. And it is used for Data Filter only.</p> <p>Don't care -No action will be taken towards fragmented packets.</p> <p>Unfragmented -Apply the rule to unfragmented packets.</p> <p>Fragmented - Apply the rule to fragmented packets.</p> <p>Too Short - Apply the rule only to packets that are too short to contain a complete header.</p>
Filter	<p>Specifies the action to be taken when packets match the rule.</p> <p>Block Immediately - Packets matching the rule will be dropped immediately.</p> <p>Pass Immediately - Packets matching the rule will be passed immediately.</p> <p>Block If No Further Match - A packet matching the rule, and that does not match further rules, will be dropped.</p> <p>Pass If No Further Match - A packet matching the rule, and that does not match further rules, will be passed through.</p> <p>For troubleshooting needs, you can specify to record Filter information by checking the Syslog box. It will be sent to Syslog server. Please refer to section 3.14.4 Syslog/Mail Alert for more detailed information.</p>
Branch to other Filter Set	<p>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.</p>
IP Address	<p>Specify a source and destination IP address for this filter rule to apply to. Place the symbol “!” before a specific IP Address will prevent this rule from being applied to that IP address. To apply the rule to all IP address, enter any or leave the field blank.</p>
Content Management	<p>All the hosts within the range configured with above conditions must follow the standard configured in the CSM profile (configured in Objects and Groups>>CSM Profiles) selected here. Please choose one of the CSM profiles applied by this filter rule.</p> <p>For troubleshooting needs, you can specify to record CSM information by checking the Syslog box. It will be sent to Syslog server. Please refer to section 3.14.4 Syslog/Mail Alert for more detailed information.</p>

Example

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

Firewall >> General Setup

General Setup

Call Filter: ☒ Enable ☐ Disable Start Filter Set: Set#1

Data Filter: ☒ Enable ☐ Disable Start Filter Set: Set#2

Actions for default rule:

Application: Filter Action/Profile: Pass Log: ☐

IM/P2P Filter: None ☐

☐ Apply IP filter to VPN incoming packets

☒ Accept large incoming fragmented UDP or ICMP packets

Firewall >> Filter Setup

Filter Setup

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

Firewall >> Filter Setup >> Edit Filter Set

Filter Set 1

Comments: Default Call Filter

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

Firewall >> Edit Filter Set >> Edit Filter Rule

Filter Set 1 Rule 1

☒ Check to enable the Filter Rule

Comments: Block NetBios

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

Direction: LAN -> WAN

Source IP: Any Edit

Destination IP: Any Edit

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

Fragments: Don't Care

Application: Filter: Block Immediately Syslog: ☐

Branch to Other Filter Set: None

Content Security Management: None

OK Clear Cancel

3.6.4 DoS Defense

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

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

Firewall >> DoS defense Setup

DoS defense Setup

☒ Enable DoS Defense

<input type="checkbox"/> Enable SYN flood defense	Threshold	<input type="text" value="50"/>	packets / sec
	Timeout	<input type="text" value="10"/>	sec
<input type="checkbox"/> Enable UDP flood defense	Threshold	<input type="text" value="150"/>	packets / sec
	Timeout	<input type="text" value="10"/>	sec
<input type="checkbox"/> Enable ICMP flood defense	Threshold	<input type="text" value="50"/>	packets / sec
	Timeout	<input type="text" value="10"/>	sec
<input type="checkbox"/> Enable Port Scan detection	Threshold	<input type="text" value="150"/>	packets / sec
<input type="checkbox"/> Block IP options	<input type="checkbox"/> Block TCP flag scan		
<input type="checkbox"/> Block Land	<input type="checkbox"/> Block Tear Drop		
<input type="checkbox"/> Block Smurf	<input type="checkbox"/> Block Ping of Death		
<input type="checkbox"/> Block trace route	<input type="checkbox"/> Block ICMP fragment		
<input type="checkbox"/> Block SYN fragment	<input type="checkbox"/> Block UnknownProtocol		
<input type="checkbox"/> Block Fraggle Attack			

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

OK Clear All Cancel

Enable Dos Defense

Check the box to activate the DoS Defense Functionality.

Enable SYN flood defense

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

Enable UDP flood defense

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

Enable ICMP flood defense

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

Enable PortScan detection

Port Scan attacks the Vigor router by sending lots of packets to many ports in an attempt to find ignorant services would respond. Check the box to activate the Port Scan detection. Whenever detecting this malicious exploration behavior by monitoring the

port-scanning Threshold rate, the Vigor router will send out a warning. By default, the Vigor router sets the threshold as 150 packets per second.

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

SYN packets with the identical source and destination addresses, as well as the port number to victims.

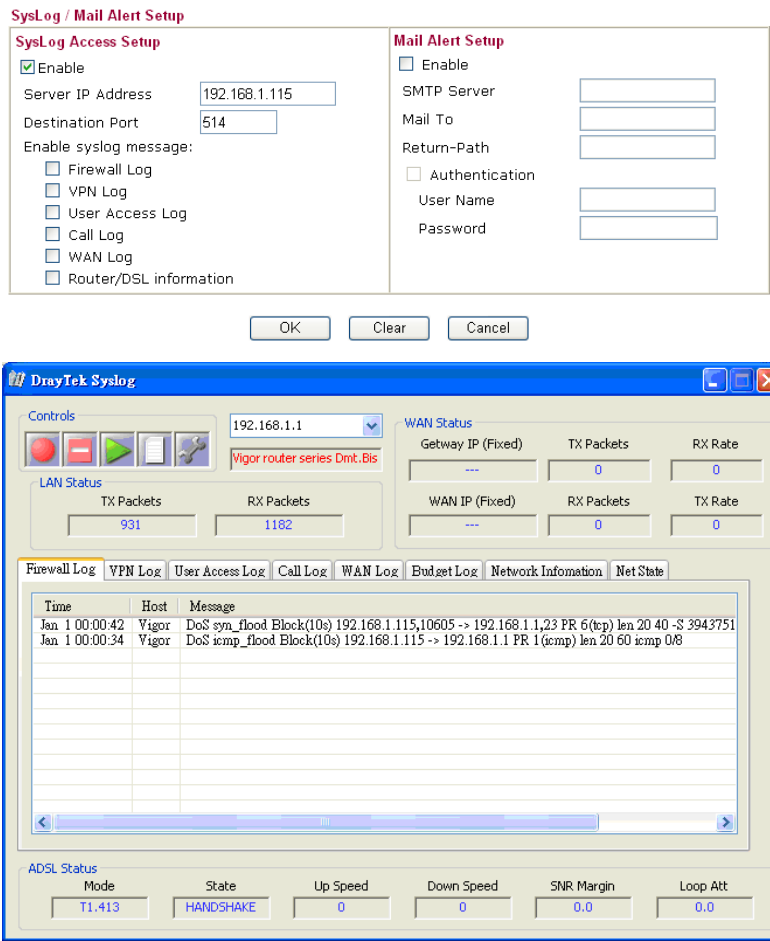
Block Unknown Protocol

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

Warning Messages

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

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



3.7 Bandwidth Management

Below shows the menu items for Bandwidth Management.



3.7.1 Sessions Limit

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

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

Bandwidth Management >> Sessions Limit

Sessions Limit

☐ Enable ☒ Disable

Default Max Sessions:

Limitation List

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

Specific Limitation

Start IP: End IP:

Maximum Sessions:

Time Schedule

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

Note: Action and Idle Timeout settings will be ignored.

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

Enable

Click this button to activate the function of limit session.

Disable

Click this button to close the function of limit session.

Default session limit

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

Limitation List

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

Start IP

Defines the start IP address for limit session.

End IP

Defines the end IP address for limit session.

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

3.7.2 Bandwidth Limit

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

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

Bandwidth Management >> Bandwidth Limit

Bandwidth Limit

☐ Enable
 ☒ Disable

Default TX Limit: Kbps
 Default RX Limit: Kbps

Limitation List

Index	Start IP	End IP	TX limit	RX limit	Shared

Specific Limitation

Start IP:
 End IP:

☒ Each
 ☐ Shared
 TX Limit: Kbps
 RX Limit: Kbps

Time Schedule

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

Note: Action and Idle Timeout settings will be ignored.

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

Enable	Click this button to activate the function of limit bandwidth.
Disable	Click this button to close the function of limit bandwidth.
Default TX limit	Define the default speed of the upstream for each computer in LAN.

Default RX limit	Define the default speed of the downstream for each computer in LAN.
Limitation List	Display a list of specific limitations that you set on this web page.
Start IP	Define the start IP address for limit bandwidth.
End IP	Define the end IP address for limit bandwidth.
Each/Shared	Select Each to make each IP within the range of Start IP and End IP having the same speed defined in TX limit and RX limit fields; select Shared to make all the IPs within the range of Start IP and End IP share the total bandwidth of TX limit and RX limit.
TX limit	Define the limitation for the speed of the upstream. If you do not set the limit in this field, the system will use the default speed for the specific limitation you set for each index.
RX limit	Define the limitation for the speed of the downstream. If you do not set the limit in this field, the system will use the default speed for the specific limitation you set for each index.
Add	Add the specific speed limitation onto the list above.
Edit	Allows you to edit the settings for the selected limitation.
Delete	Remove the selected settings existing on the limitation list.
Index (1-15) in Schedule Setup	You can type in four sets of time schedule for your request. All the schedules can be set previously in Application – Schedule web page and you can use the number that you have set in that web page.

3.7.3 Quality of Service

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

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

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

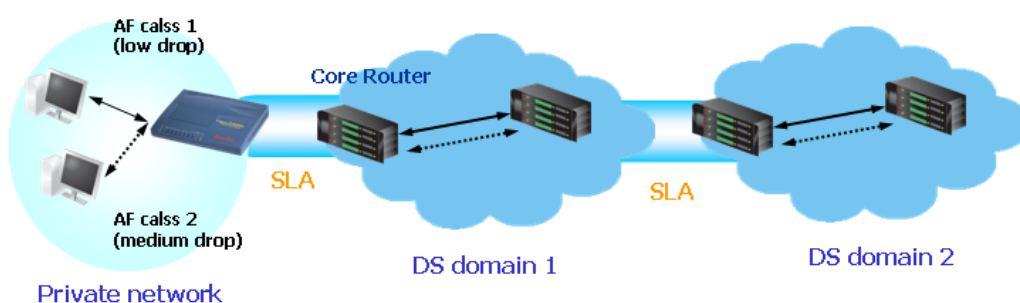
There are two components within Primary configuration of QoS deployment:

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

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

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

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



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

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

Bandwidth Management >> Quality of Service

General Setup

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

Class Rule

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

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

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

General Setup for WAN Interface

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

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

WAN1 General Setup

☒ **Enable the QoS Control** OUT

WAN Inbound Bandwidth Kbps

WAN Outbound Bandwidth Kbps

Note: Before enable QoS, you should test the real bandwidth first.
QoS may not work properly if the bandwidth is not accurate.

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

☐ Enable UDP Bandwidth Control Limited_bandwidth Ratio %

☐ Outbound TCP ACK Prioritize [Online Statistics](#)

OK

Clear

Cancel

Enable the QoS Control

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

WAN Inbound Bandwidth

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

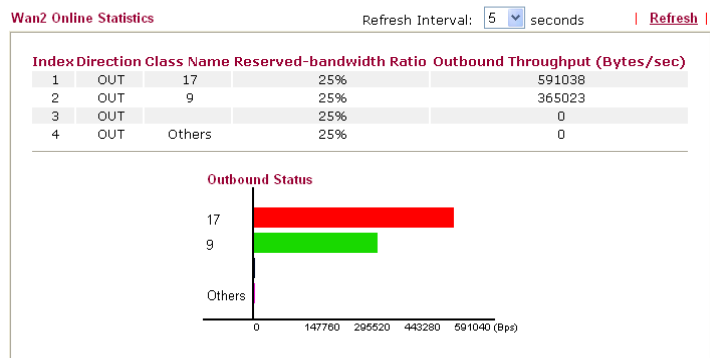
WAN Outbound Bandwidth

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

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

- Reserved Bandwidth Ratio** It is reserved for the group index in the form of ratio of **reserved bandwidth to upstream speed** and **reserved bandwidth to downstream speed**.
- Enable UDP Bandwidth Control** Check this and set the limited bandwidth ratio on the right field. This is a protection of TCP application traffic since UDP application traffic such as streaming video will exhaust lots of bandwidth.
- Outbound TCP ACK Prioritize** The difference in bandwidth between download and upload are great in ADSL2+ environment. For the download speed might be impacted by the uploading TCP ACK, you can check this box to push ACK of upload more faster to speed the network traffic.
- Limited_bandwidth Ratio** The ratio typed here is reserved for limited bandwidth of UDP application.
- On Line Statistics** Display an online statistics for quality of service for your reference.

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



Edit the Class Rule for QoS

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

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

General Setup

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

Class Rule

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

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

Class Index #1

Name

NO	Status	Local Address	Remote Address	DiffServ CodePoint	Service Type
1 <input type="radio"/>	Active	Any	Any	ANY	ANY

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

Bandwidth Management >> Quality of Service

Rule Edit

☒ ACT

Local Address

Remote Address

DiffServ CodePoint

Service Type

Note: Please choose/setup the Service Type first.

ACT

Check this box to invoke these settings.

Source Address

Click the **SrcEdit** button to set the source address for the rule.

Destination Address

Click the **DestEdit** button to set the destination address for the rule.

SrcEdit/DestEdit

It allows you to edit source address information.

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

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

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

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

DiffServ CodePoint

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

Service Type

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

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

Bandwidth Management >> Quality of Service

Class Index #1

Name

NO	Status	Local Address	Remote Address	DiffServ CodePoint	Service Type
1 <input type="radio"/>	Active	Any	Any	IP precedence 2	SYSLOG(UDP:514)
2 <input type="radio"/>	Active	192.168.1.15	192.168.1.65	AF Class1 (Low Drop)	FTP(TCP:20)
<div>Add Edit Delete</div>					

OK Cancel

Edit the Service Type for Class Rule

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

Bandwidth Management >> Quality of Service

General Setup

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

Class Rule

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

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

User Defined Service Type

NO	Name	Protocol	Port
1	Empty	-	-

For adding a new rule, click **Add** to open the following page. If you want to edit an existed service type, please select the radio button of that one and click **Edit** to open the following page for modification.

Service Type Edit

Service Name	<input type="text"/>		
Service Type	TCP	<input type="button" value="v"/>	<input type="text" value="6"/>
Port Configuration			
Type	<input checked="" type="radio"/> Single <input type="radio"/> Range		
Port Number	<input type="text" value="0"/>	-	<input type="text" value="0"/>

Service Name

Type in a new service for your request.

Service Type

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

Port Configuration

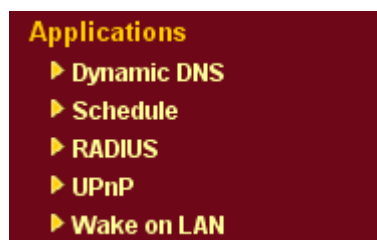
Click **Single** or **Range**. If you select Range, you have to type in the starting port number and the end porting number on the boxes below.

Port Number – Type in the starting port number and the end porting number here if you choose Range as the type.

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

3.8 Applications

Below shows the menu items for Applications.



3.8.1 Dynamic DNS

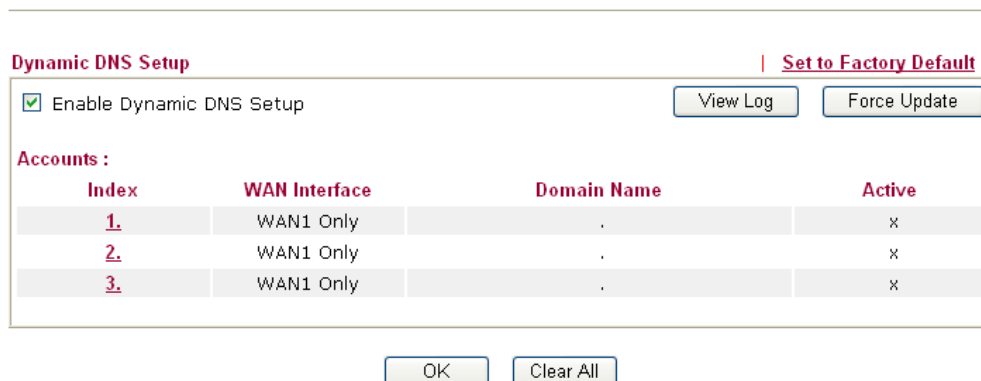
The ISP often provides you with a dynamic IP address when you connect to the Internet via your ISP. It means that the public IP address assigned to your router changes each time you access the Internet. The Dynamic DNS feature lets you assign a domain name to a dynamic WAN IP address. It allows the router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

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

Enable the Function and Add a Dynamic DNS Account

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

Applications >> Dynamic DNS Setup

A screenshot of the "Dynamic DNS Setup" configuration page in a web interface. At the top left is the title "Dynamic DNS Setup" and at the top right is a link "Set to Factory Default". Below the title is a checkbox labeled "Enable Dynamic DNS Setup" which is checked. To the right of the checkbox are two buttons: "View Log" and "Force Update". Below this is a section titled "Accounts :" followed by a table. The table has four columns: "Index", "WAN Interface", "Domain Name", and "Active". There are three rows in the table, each with a red underlined index number (1, 2, 3) in the first column, "WAN1 Only" in the second column, a period "." in the third column, and an "x" in the fourth column. At the bottom of the page are two buttons: "OK" and "Clear All".

Index	WAN Interface	Domain Name	Active
<u>1.</u>	WAN1 Only	.	x
<u>2.</u>	WAN1 Only	.	x
<u>3.</u>	WAN1 Only	.	x

Set to Factory Default

Clear all profiles and recover to factory settings.

Enable Dynamic DNS Setup

Check this box to enable DDNS function.

Index

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

WAN Interface

Display current WAN interface used for accessing Internet.

Domain Name	Display the domain name that you set on the setting page of DDNS setup.
Active	Display if this account is active or inactive.
View Log	Display DDNS log status.
Force Update	Force the router updates its information to DDNS server.

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

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

Index : 1

☒ Enable Dynamic DNS Account

WAN Interface WAN1 First

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

Service Type Dynamic

Domain Name chronic6853 dyndns.info dyndns.info

Login Name chronic6853 (max. 23 characters)

Password •••••••• (max. 23 characters)

☐ Wildcards

☐ Backup MX

Mail Extender

Enable Dynamic DNS Account	Check this box to enable the current account. If you did check the box, you will see a check mark appeared on the Active column of the previous web page in step 2).
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, Static). If you choose Custom, you can modify the domain that is chosen in the Domain Name field.
Domain Name	Type in a 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.

3.8.2 Schedule

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

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

Applications >> Schedule

Schedule:		Set to Factory Default	
Index	Status	Index	Status
1.	x	9.	x
2.	x	10.	x
3.	x	11.	x
4.	x	12.	x
5.	x	13.	x
6.	x	14.	x
7.	x	15.	x
8.	x		

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

Set to Factory Default

Clear all profiles and recover to factory settings.

Index

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

Status

Display if this schedule setting is active or inactive.

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

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

Index No. 1

☒ Enable Schedule Setup

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

Start Time (hh:mm) 0 : 0

Duration Time (hh:mm) 0 : 0

Action Force On

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

How Often

☐ Once

☒ Weekdays

☐ Sun ☒ Mon ☒ Tue ☒ Wed ☒ Thu ☒ Fri ☐ Sat

OK Clear Cancel

Enable Schedule Setup

Check to enable the schedule.

Start Date (yyyy-mm-dd)

Specify the starting date of the schedule.

Start Time (hh:mm)

Specify the starting time of the schedule.

Duration Time (hh:mm)

Specify the duration (or period) for the schedule.

Action

Specify which action Call Schedule should apply during the period of the schedule.

Force On -Force the connection to be always on.

Force Down -Force the connection to be always down.

Enable Dial-On-Demand -Specify the connection to be dial-on-demand and the value of idle timeout should be specified in **Idle Timeout** field.

Disable Dial-On-Demand -Specify the connection to be up when it has traffic on the line. Once there is no traffic over idle timeout, the connection will be down and never up again during the schedule.

Idle Timeout

Specify the duration (or period) for the schedule.

How often -Specify how often the schedule will be applied

Once -The schedule will be applied just once

Weekdays -Specify which days in one week should perform the schedule.

Example

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

Office**Hour:****(Force On)**

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

1. Make sure the PPPoE connection and **Time Setup** is working properly.
2. Configure the PPPoE always on from 9:00 to 18:00 for whole week.

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

3.8.3 RADIUS

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

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

Applications >> RADIUS

RADIUS Setup

<input checked="" type="checkbox"/> Enable	
Server IP Address	<input type="text"/>
Destination Port	<input type="text" value="1812"/>
Shared Secret	<input type="text"/>
Confirm Shared Secret	<input type="text"/>

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.

3.8.4 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 provides the associated support for MSN Messenger to allow full use of the voice, video and messaging features.

Applications >> UPnP

UPnP

☒ Enable UPnP Service

☐ Enable Connection control Service

☐ Enable Connection Status Service

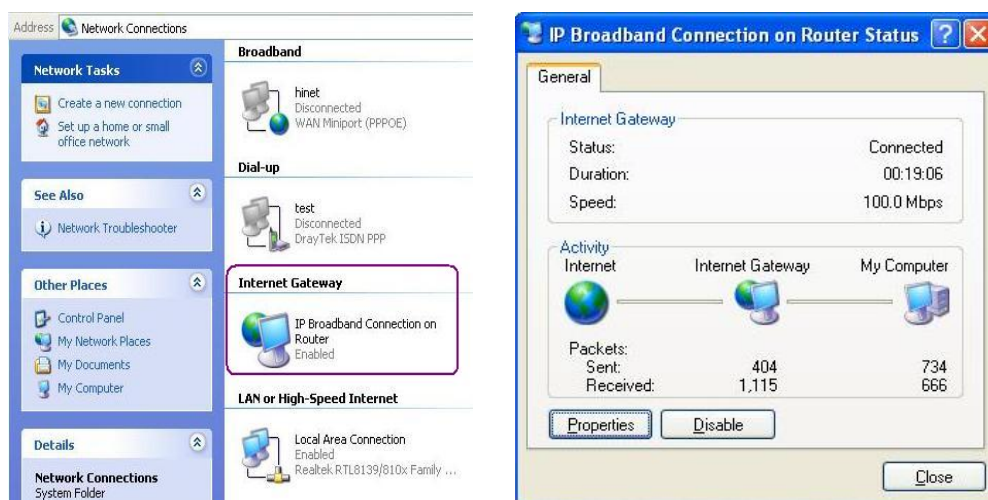
Note: If you intend running UPnP service inside your LAN, you should check the appropriate service above to allow control, as well as the appropriate UPnP settings.

OK Clear Cancel

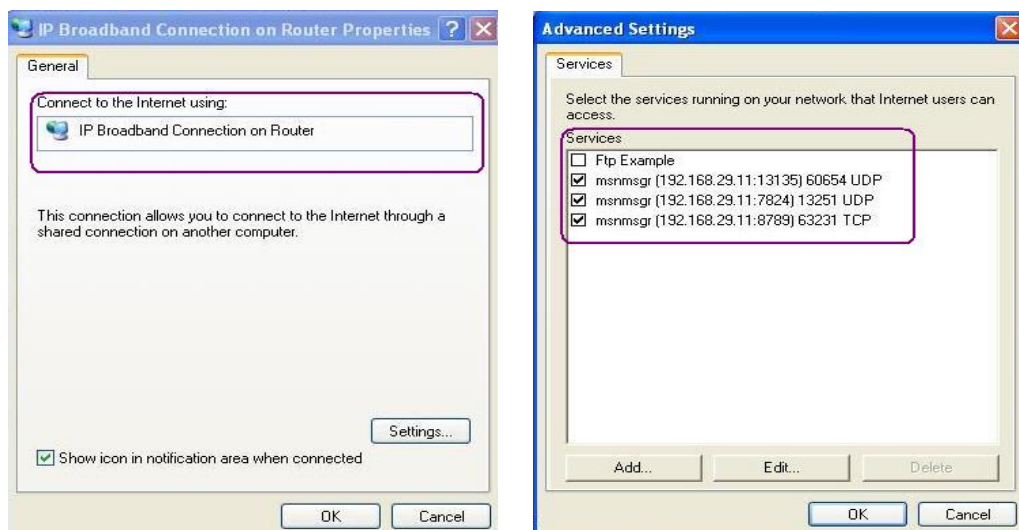
Enable UPNP Service

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

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



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



The reminder as regards concern about Firewall and UPnP

Can't work with Firewall Software

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

Security Considerations

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

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

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

3.8.5 Wake On LAN

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

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

Application >> Wake on LAN

Wake on LAN

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

Wake by: MAC Address ▾
IP Address: ---
MAC Address: □:□:□:□:□:□ Wake Up!

Result

Wake by

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

Wake by: MAC Address ▾
MAC Address
IP Address

IP Address

The IP addresses that have been configured in **LAN>>Bind IP to MAC** will be shown in this drop down list. Choose the IP address from the drop down list that you want to wake up.

MAC Address

Type any one of the MAC address of the binded PCs.

Wake Up

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

Application >> Wake on LAN

Wake on LAN

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

Wake by: MAC Address ▾
IP Address: ---
MAC Address: □:□:□:□:□:□ Wake Up!

Result

Send command to client done.

3.9 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.

Besides, here provides ISDN LAN to LAN and remote dial-in functions (for *i* model only).

Below shows the menu items for VPN and Remote Access.



3.9.1 VPN Client Wizard

Such wizard is used to configure VPN settings for VPN client. Such wizard will guide to set the LAN-to-LAN profile for VPN dial out connection (from server to client) step by step.

VPN and Remote Access >> VPN Client Wizard

Choose VPN Establishment Environment

A screenshot of a web-based configuration wizard. The title is "Choose VPN Establishment Environment". It contains two main sections. The first section is "LAN-to-LAN VPN Client Mode Selection:" with a dropdown menu currently showing "Route Mode". The second section is "Please choose a LAN-to-LAN Profile:" with a dropdown menu showing "[Index] [Status] [Name]". Below these sections is a "Note" in red text: "Note: If the remote network only allows you to dial in with single IP, please choose NAT mode, otherwise choose Route Mode." At the bottom of the form are four buttons: "< Back", "Next >", "Finish", and "Cancel".

LAN-to-LAN Client Mode Selection

Choose the client mode.

Route Mode/NAT Mode – If the remote network only allows you to dial in with single IP, please choose this mode, otherwise please choose Route Mode.

Route Mode ▾

Route Mode

NAT Mode

Please choose a LAN-to-LAN Profile

There are 32 VPN tunnels for users to set.

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

When you finish the mode and profile selection, please click **Next** to open the following page.

VPN and Remote Access >> VPN Client Wizard

VPN Connection Setting

Security ranking (1 is the highest; 5 is the lowest)

1. L2TP over IPSec
2. IPSec
3. PPTP (Encryption)
4. L2TP
5. PPTP (None Encryption)

Throughput ranking (1 is the highest; 5 is the lowest)

1. PPTP (None Encryption)
2. L2TP
3. IPSec
4. L2TP over IPSec
5. PPTP (Encryption)

Select VPN Type:

PPTP (None Encryption) ▾

PPTP (None Encryption)

PPTP (Encryption)

IPSec

L2TP

L2TP over IPSec (Nice to Have)

L2TP over IPSec (Must)

< Back

Next >

Finish

Cancel

In this page, you have to select suitable VPN type for the VPN client profile. There are six types provided here. Different type will lead to different configuration page. After making

the choices for the client profile, please click **Next**. You will see different configurations based on the selection(s) you made.

- When you choose **PPTP (None Encryption)** or **PPTP (Encryption)**, you will see the following graphic:

VPN and Remote Access >> VPN Client Wizard

VPN Client PPTP None Encryption Settings

Profile Name	VPN-1
VPN Connection Through	WAN1 First
<input type="checkbox"/> Always on	
Server IP/Host Name for VPN (e.g. 5551234, draytek.com or 123.45.67.89)	draytek.com
Username	marketing
Password	••••••••
Remote Network IP	192.168.1.6
Remote Network Mask	255.255.255.0

< Back Next > Finish Cancel

- When you choose **IPSec**, you will see the following graphic:

VPN and Remote Access >> VPN Client Wizard

VPN Client IPSec Settings

Profile Name	VPN-1
VPN Connection Through	WAN1 First
<input type="checkbox"/> Always on	
Server IP/Host Name for VPN (e.g. 5551234, draytek.com or 123.45.67.89)	draytek.com
IKE Authentication Method	
<input type="radio"/> Pre-Shared Key	
Confirm Pre-Shared Key	
<input checked="" type="radio"/> Digital Signature (X.509)	None
IPSec Security Method	
<input checked="" type="radio"/> Medium (AH)	
<input type="radio"/> High (ESP)	
Remote Network IP	192.168.1.6
Remote Network Mask	255.255.255.0

< Back Next > Finish Cancel

- When you choose **L2TP**, you will see the following graphic:

VPN and Remote Access >> VPN Client Wizard

VPN Client L2TP Settings

Profile Name	VPN-1
VPN Connection Through	WAN1 First
<input type="checkbox"/> Always on	
Server IP/Host Name for VPN (e.g. 5551234, draytek.com or 123.45.67.89)	draytek.com
Username	marketing
Password	••••••••
Remote Network IP	192.168.1.6
Remote Network Mask	255.255.255.0

< Back Next > Finish Cancel

- When you choose **L2TP over IPSec (Nice to Have)**, you will see the following graphic:

VPN and Remote Access >> VPN Client Wizard

VPN Client L2TP over IPSec (Nice to Have) Settings

Profile Name	VPN-1
VPN Connection Through	WAN1 First
<input type="checkbox"/> Always on	
Server IP/Host Name for VPN (e.g. 5551234, draytek.com or 123.45.67.89)	draytek.com
IKE Authentication Method	
<input type="radio"/> Pre-Shared Key	
Confirm Pre-Shared Key	
<input checked="" type="radio"/> Digital Signature (X.509)	None
IPSec Security Method	
<input checked="" type="radio"/> Medium (AH)	
<input type="radio"/> High (ESP)	DES without Authentication
Username	marketing
Password	••••••••
Remote Network IP	192.168.1.6
Remote Network Mask	255.255.255.0

< Back Next > Finish Cancel

- When you choose **L2TP over IPSec (Must)**, you will see the following graphic:

VPN Client L2TP over IPSec (Must) Settings

Profile Name	VPN-1
VPN Connection Through	WAN1 First
<input type="checkbox"/> Always on	
Server IP/Host Name for VPN (e.g. 5551234, draytek.com or 123.45.67.89)	draytek.com
IKE Authentication Method	
<input type="radio"/> Pre-Shared Key	
Confirm Pre-Shared Key	
<input checked="" type="radio"/> Digital Signature (X.509)	None
IPSec Security Method	
<input checked="" type="radio"/> Medium (AH)	
<input type="radio"/> High (ESP)	DES without Authentication
Username	marketing
Password	••••••••
Remote Network IP	192.168.1.6
Remote Network Mask	255.255.255.0

Profile Name

Type a name for such profile. The length of the file is limited to 10 characters.

VPN Connection Through

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

WAN1 First	▼
WAN1 First	
WAN1 Only	
WAN2 First	
WAN2 Only	

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

WAN1 Only - While connecting, the router will use WAN1 as the only channel for VPN connection.

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

WAN2 Only - While connecting, the router will use WAN2 as the only channel for VPN connection.

Always On

Check to enable router always keep VPN connection.

Pre-Shared Key

IKE Authentication Method 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- Specify a key for IKE authentication
Confirm Pre-Shared Key-Confirm the pre-shared key.

Digital Signature (X.509)

Check the box of Digital Signature to invoke this function and select one predefined in the X.509 Peer ID

	Profiles (set from VPN and Remote Access>>IPSec Peer Identity).
IPSec Security Method	<p>Medium - Authentication Header (AH) means data will be authenticated, but not be encrypted. By default, this option is active.</p> <p>High - Encapsulating Security Payload (ESP) means payload (data) will be encrypted and authenticated. You may select encryption algorithm from Data Encryption Standard (DES), Triple DES (3DES), and AES.</p>
User Name	This field is used to authenticate for connection when you select PPTP or L2TP with or without IPSec policy above.
Password	This field is used to authenticate for connection when you select PPTP or L2TP with or without IPSec policy above.
Remote Network IP	Please type one LAN IP address (according to the real location of the remote host) for building VPN connection.
Remote Network Mask	Please type the network mask (according to the real location of the remote host) for building VPN connection.

After finishing the configuration, please click **Next**. The confirmation page will be shown as follows. If there is no problem, you can click one of the radio buttons listed on the page and click **Finish** to execute the next action.

VPN and Remote Access >> VPN Client Wizard

Please confirm your settings

LAN-to-LAN Index:	3
Profile Name:	VPN-1
VPN Connection Type:	L2TP over IPSec (Must)
VPN Connection Through:	WAN1 First
Always on:	No
Server IP/Host Name:	draytek.com
IKE Authentication Method:	Digital Signature (X.509)
IPSec Security Method:	AH-SHA1
Remote Network IP:	192.168.1.6
Remote Network Mask:	255.255.255.0

Click **Back** to modify changes if necessary. Otherwise, click **Finish** to save the current settings and proceed to the following action:

- ☒ Go to the VPN Connection Management.
- ☐ Do another VPN Client Wizard setup.
- ☐ View more detailed configurations.

< Back

Next >

Finish

Cancel

Go to the VPN Connection Management	Click this radio button to access VPN and Remote Access>>Connection Management for viewing VPN Connection status.
Do another VPN Server Wizard Setup	Click this radio button to set another profile of VPN Server through VPN Server Wizard.
View more detailed configuration	Click this radio button to access VPN and Remote Access>>LAN to LAN for viewing detailed configuration.

3.9.2 VPN Server Wizard

Such wizard is used to configure VPN settings for VPN server. Such wizard will guide to set the LAN-to-LAN profile for VPN dial in connection (from client to server) step by step.

VPN and Remote Access >> VPN Server Wizard

Choose VPN Establishment Environment

VPN Server Mode Selection: Site to Site VPN (LAN-to-LAN)

Please choose a LAN-to-LAN Profile: [Index] [Status] [Name]

Please choose a Dial-in User Accounts: [Index] [Status] [Name]

Allowed Dial-in Type:

☐ PPTP

☐ IPSec

☒ L2TP with IPSec Policy None

< Back Next > Finish Cancel

VPN Server Mode Selection

Choose the direction for the VPN server.

Site to Site VPN/Remote Dial-in User – To set a LAN-to-LAN profile automatically, please choose Site to Site VPN.

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.

Site to Site VPN (LAN-to-LAN)

Site to Site VPN (LAN-to-LAN)

Remote Dial-in User (Teleworker)

Please choose a LAN-to-LAN Profile

This item is available when you choose **Site to Site VPN** (LAN-to-LAN) as VPN server mode. There are 32 VPN tunnels for users to set.

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

Please choose a Dial-in User Accounts

This item is available when you choose Remote Dial-in User (Teleworker) as VPN server mode. There are 32 VPN tunnels for users to set.

Allowed Dial-in Type

This item is available after you choose any one of dial-in user account profiles. Next, you have to select suitable dial-in type for the VPN server profile. There are six types provided here (similar to VPN Client Wizard).

☒ PPTP
☒ IPSec
☒ L2TP with IPSec Policy

None

None

Nice to Have

Must

Different Dial-in Type will lead to different configuration page.

After making the choices for the server profile, please click **Next**. You will see different configurations based on the selection you made.

- When you check **PPTP/IPSec/L2TP** (three types) or **PPTP/IPSec** (two types) or **L2TP with Policy (Nice to Have/Must)**, you will see the following graphic:

VPN Authentication Setting

Profile Name	VPN-Ser1
PPTP / L2TP / L2TP over IPSec Authentication	
Username	server1
Password	••••••••
IPSec / L2TP over IPSec Authentication	
<input checked="" type="checkbox"/> Pre-Shared Key	
Confirm Pre-Shared Key	
<input checked="" type="checkbox"/> Digital Signature (X.509)	None
Peer IP/VPN Client IP	192.168.1.99
Peer ID	
Site to Site Information	
Remote Network IP	0.0.0.0
Remote Network Mask	255.255.255.0

< Back

Next >

Finish

Cancel

Profile Name

Type a name for such profile. The length of the file is limited to 10 characters.

User Name

This field is used to authenticate for connection when you select PPTP or L2TP with or without IPSec policy above.

Password

This field is used to authenticate for connection when you select PPTP or L2TP with or without IPSec policy above.

Pre-Shared Key

For IPSec/L2TP IPSec authentication, you have to type a pre-shared key.

Confirm Pre-Shared Key

Type the pre-shared key again for confirmation.

Digital Signature (X.509)

In addition to pre-shared key, you can select one predefined setting in the X.509 Peer ID Profiles (set from **VPN and Remote Access>>IPSec Peer Identity**) for IPSec/L2TP over IPSec authentication.

Peer IP/VPN Client IP

Type the WAN IP address or VPN client IP address for the remote client.

Peer ID

Type the ID name for the remote client.

Remote Network IP

Please type one LAN IP address (according to the real location of the remote host) for building VPN connection.

Remote Network Mask

Please type the network mask (according to the real location of the remote host) for building VPN connection.

- When you check **PPTP/L2TP** (two types) or **PPTP** or **L2TP with Policy (None)**, you will see the following graphic:

VPN Authentication Setting

Profile Name	VPN-Ser1
PPTP / L2TP / L2TP over IPSec Authentication	
Username	server1
Password	••••••••
Peer IP/VPN Client IP	
Site to Site Information	
Remote Network IP	0.0.0.0
Remote Network Mask	255.255.255.0

< Back

Next >

Finish

Cancel

- When you check **IPSec**, you will see the following graphic:

VPN Authentication Setting

Profile Name	VPN-Ser1
IPSec / L2TP over IPSec Authentication	
<input type="checkbox"/> Pre-Shared Key	
Confirm Pre-Shared Key	
<input checked="" type="checkbox"/> Digital Signature (X.509)	None
Peer IP/VPN Client IP	
Peer ID	
Site to Site Information	
Remote Network IP	0.0.0.0
Remote Network Mask	255.255.255.0

< Back

Next >

Finish

Cancel

After finishing the configuration, please click **Next**. The confirmation page will be shown as follows. If there is no problem, you can click one of the radio buttons listed on the page and click **Finish** to execute the next action.

Please Confirm Your Settings

VPN Environment:	Site to Site VPN (LAN-to-LAN)
Index:	3
Profile Name:	VPN-Ser1
Username:	server1
Allowed Service:	PPTP+IPSec
Peer IP/VPN Client IP:	
Peer ID:	
Remote Network IP:	0.0.0.0
Remote Network Mask:	255.255.255.0

Click **Back** to modify changes if necessary. Otherwise, click **Finish** to save the current settings and proceed to the following action:

- ☒ Go to the VPN Connection Management.
☐ Do another VPN Server Wizard setup.
☐ View more detailed configurations.

< Back

Next >

Finish

Cancel

Go to the VPN Connection Management

Click this radio button to access **VPN and Remote Access>>Connection Management** for viewing VPN Connection status.

Do another VPN Server Wizard Setup

Click this radio button to set another profile of VPN Server through VPN Server Wizard.

View more detailed configuration

Click this radio button to access **VPN and Remote Access>>LAN to LAN** for viewing detailed configuration.

3.9.3 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. And, if you want to enable ISDN dial-in function, please check "Enable ISDN Dial-In" in this page.

VPN and Remote Access >> Remote Access Control Setup

Remote Access Control Setup

- | | |
|-------------------------------------|--------------------------|
| <input checked="" type="checkbox"/> | Enable PPTP VPN Service |
| <input checked="" type="checkbox"/> | Enable IPSec VPN Service |
| <input checked="" type="checkbox"/> | Enable L2TP VPN Service |
| <input checked="" type="checkbox"/> | Enable ISDN Dial-In |

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

OK

Clear

Cancel

Enable PPTP VPN Service

Check this box to activate the VPN service through PPTP protocol.

Enable IPSec VPN Service

Check this box to activate the VPN service through IPSec protocol.

- Enable L2TP VPN Service** Check this box to activate the VPN service through L2TP protocol.
- Enable ISDN Dial-IN** This feature is available for *i* model. Check this box to activate the ISDN dial-in.

3.9.4 PPP General Setup

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

VPN and Remote Access >> PPP General Setup

PPP General Setup

PPP/MP Protocol		IP Address Assignment for Dial-In Users
Dial-In PPP Authentication	PAP or CHAP	Start IP Address 192.168.1.200
Dial-In PPP Encryption (MPPE)	Optional MPPE	
Mutual Authentication (PAP)	<input type="radio"/> Yes <input checked="" type="radio"/> No	
Username		
Password		

OK

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

- 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. But, you have to notice that the first two IP addresses of 192.168.1.200 and 192.168.1.201 are reserved for ISDN remote dial-in user.

3.9.5 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	
<input checked="" type="checkbox"/> Medium (AH)	
Data will be authentic, but will not be encrypted.	
High (ESP)	<input checked="" type="checkbox"/> DES <input checked="" type="checkbox"/> 3DES <input checked="" type="checkbox"/> AES
Data will be encrypted and authentic.	

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

3.9.6 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 users**.

VPN and Remote Access >> IPSec Peer Identity

X509 Peer ID Accounts: [Set to Factory Default](#)

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

Set to Factory Default Click it to clear all indexes.

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

Name Display the profile name of that index.

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

Profile Index : 1

Profile Name	<input type="text" value="one"/>
<input checked="" type="checkbox"/> Enable this account	
<input type="radio"/> Accept Any Peer ID	
<input checked="" type="radio"/> Accept Subject Alternative Name	
Type	<input type="text" value="IP Address"/>
IP	<input type="text"/>
<input type="radio"/> Accept Subject Name	
Country (C)	<input type="text"/>
State (ST)	<input type="text"/>
Location (L)	<input type="text"/>
Organization (O)	<input type="text"/>
Organization Unit (OU)	<input type="text"/>
Common Name (CN)	<input type="text"/>
Email (E)	<input type="text"/>

Profile Name

Type in a name in this file.

Enable this account-Check this box to enable such profile.**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)**.

3.9.7 Remote Dial-in User

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

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

VPN and Remote Access >> Remote Dial-in User

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

Set to Factory Default

Click to clear all indexes.

Index

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

User

Display the username for the specific dial-in user of the LAN to LAN profile. The symbol ??? represents that the profile is empty.

Status

Display the access state of the specific dial-in user. The symbol V and X represent the specific dial-in user to be active and inactive, respectively.

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

Index No. 1

<p>User account and Authentication</p> <p><input type="checkbox"/> Enable this account</p> <p>Idle Timeout <input type="text" value="300"/> second(s)</p> <hr/> <p>Allowed Dial-In Type</p> <p><input checked="" type="checkbox"/> ISDN</p> <p><input checked="" type="checkbox"/> PPTP</p> <p><input checked="" type="checkbox"/> IPsec Tunnel</p> <p><input checked="" type="checkbox"/> L2TP with IPsec Policy <input type="text" value="None"/></p> <p><input type="checkbox"/> Specify Remote Node</p> <p>Remote Client IP or Peer ISDN Number <input type="text"/></p> <p>or Peer ID <input type="text"/></p> <p>Netbios Naming Packet <input checked="" type="radio"/> Pass <input type="radio"/> Block</p> <p>Multicast via VPN <input type="radio"/> Pass <input checked="" type="radio"/> Block (for some IGMP, IP-Camera, DHCP Relay...etc.)</p>	<p>Username <input data-bbox="1050 320 1241 347" type="text" value="???"/></p> <p>Password <input type="password"/></p> <hr/> <p>IKE Authentication Method</p> <p><input checked="" type="checkbox"/> Pre-Shared Key</p> <p>IKE Pre-Shared Key <input type="text"/></p> <p><input type="checkbox"/> Digital Signature (X.509)</p> <p><input type="text" value="None"/></p> <hr/> <p>IPsec Security Method</p> <p><input checked="" type="checkbox"/> Medium (AH)</p> <p>High (ESP)</p> <p><input checked="" type="checkbox"/> DES <input checked="" type="checkbox"/> 3DES <input checked="" type="checkbox"/> AES</p> <p>Local ID <input type="text"/> (optional)</p> <hr/> <p>Callback Function</p> <p><input type="checkbox"/> Check to enable Callback function</p> <p><input type="checkbox"/> Specify the callback number</p> <p>Callback Number <input type="text"/></p> <p><input checked="" type="checkbox"/> Check to enable Callback Budget Control</p> <p>Callback Budget <input type="text" value="30"/> minute(s)</p>
---	--

OK Clear Cancel

Enable this account

Check the box to enable this function.

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

ISDN

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

PPTP

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

IPsec Tunnel

Allow the remote dial-in user to 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.

Specify Remote Node

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

aggressive mode).

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

Netbios Naming Packet

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

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

Multicast via VPN

Some programs might send multicast packets via VPN connection.

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

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

User Name

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

Password

This field is applicable when you select ISDN, 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 in the X.509 Peer ID Profiles (set from **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.

Callback Function

The callback function provides a callback service only for the ISDN dial-in user (for *i* model only). The remote user will be charged the connection fee by the telecom.

Check to enable Callback function-Enables the callback function.

Specify the callback number-The option is for extra security. Once enabled, the router will ONLY call back to the specified Callback Number.

Check to enable callback budget control-By default, the callback function has a time restriction. Once the callback budget has been exhausted, the callback mechanism will be disabled automatically.

Callback Budget (Unit: minutes)- Specify the time budget for the dial-in user. The budget will be decreased automatically per callback connection.

3.9.8 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 (ISDN connection, VPN connection - including PPTP, IPsec Tunnel, and L2TP by itself or over IPsec) and corresponding security methods, etc.

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

VPN and Remote Access >> LAN to LAN

LAN-to-LAN Profiles:			Set to Factory Default		
Index	Name	Status	Index	Name	Status
1.	2.29	X	17.	???	X
2.	2.229	X	18.	???	X
3.	24	X	19.	???	X
4.	25	X	20.	???	X
5.	26	X	21.	???	X
6.	27	X	22.	???	X
7.	28	X	23.	???	X
8.	29	X	24.	???	X
9.	30	X	25.	???	X
10.	???	X	26.	???	X
11.	???	X	27.	???	X
12.	???	X	28.	???	X
13.	???	X	29.	???	X
14.	???	X	30.	???	X
15.	???	X	31.	???	X
16.	???	X	32.	???	X

[XXXXXX: This Dial-Out Profile has already joined for VPN BACKUP Mechanism]

[XXXXXX: This Dial-Out Profile does not join for VPN TRUNK]

Set to Factory Default

Click to clear all indexes.

Name

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

Status

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

LAN to LAN profiles are suitable for dial-out usage. If the profile name displayed in red, it means that the profile has been grouped into VPN TRUNK. If the profile name displayed in black, it means that profile is not grouped into VPN TRUNK and can be invoked individually.

Index	Name	Status
1.	2.5	√
2.	2.5-1	√
3.	2.29	√
4.	2.229	√
5.	26	√
6.	27	√
7.	28	√
8.	29	√
9.	30	√
10.	31	√

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.

When VPN TRUNK is activated, several fields (e.g., Dial-in Settings, Dial-in selection in Call Direction and others) might be locked and dimmed. Please refer to **VPN and Remote Access>>VPN Backup Management** for more details.

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

VPN and Remote Access >> LAN to LAN

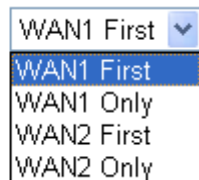
Profile Index : 1

1. Common Settings

Profile Name <input type="text" value="first"/> <input type="checkbox"/> Enable this profile VPN Connection Through: <input type="text" value="WAN1 First"/> Netbios Naming Packet <input checked="" type="radio"/> Pass <input type="radio"/> Block Multicast via VPN <input type="radio"/> Pass <input checked="" type="radio"/> Block (for some IGMP,IP-Camera,DHCP Relay..etc.)	Call Direction <input checked="" type="radio"/> Both <input type="radio"/> Dial-Out <input type="radio"/> Dial-In <input type="checkbox"/> Always on Idle Timeout <input type="text" value="300"/> second(s) <input type="checkbox"/> Enable PING to keep alive PING to the IP <input type="text"/>
--	---

2. Dial-Out Settings

Type of Server I am calling <input checked="" type="radio"/> ISDN <input type="radio"/> PPTP <input type="radio"/> IPSec Tunnel <input type="radio"/> L2TP with IPSec Policy <input type="text" value="None"/>	Link Type <input type="text" value="64k bps"/> Username <input type="text" value="???"/> Password <input type="text"/> PPP Authentication <input type="text" value="PAP/CHAP"/> VJ Compression <input checked="" type="radio"/> On <input type="radio"/> Off
Dial Number for ISDN or Server IP/Host Name for VPN. (such as 5551234, draytek.com or 123.45.67.89) <input type="text"/>	IKE Authentication Method <input checked="" type="radio"/> Pre-Shared Key IKE Pre-Shared Key <input type="text"/> <input type="radio"/> Digital Signature(X.509) <input type="text" value="None"/>
	IPSec Security Method <input checked="" type="radio"/> Medium(AH) <input type="radio"/> High(ESP) <input type="text" value="DES without Authentication"/> <input type="button" value="Advanced"/>
	Index(1-15) in Schedule Setup: <input type="text"/> , <input type="text"/> , <input type="text"/> , <input type="text"/>
	Callback Function (CBCP) <input type="checkbox"/> Require Remote to Callback <input type="checkbox"/> Provide ISDN Number to Remote

Profile Name	Specify a name for the profile of the LAN to LAN connection.
Enable this profile	Check here to activate this profile.
VPN Connection Through	Use the drop down menu to choose a proper WAN interface for this profile. This setting is useful for dial-out only.
	VPN Connection Through: 
	<p>WAN1 First - While connecting, the router will use WAN1 as the first channel for VPN connection. If WAN1 fails, the router will use another WAN interface instead.</p> <p>WAN1 Only - While connecting, the router will use WAN1 as the only channel for VPN connection.</p> <p>WAN2 First - While connecting, the router will use WAN2 as the first channel for VPN connection. If WAN2 fails, the router will use another WAN interface instead.</p> <p>WAN2 Only - While connecting, the router will use WAN2 as the only channel for VPN connection.</p>
Netbios Naming Packet	<p>Pass – click it to have an inquiry for data transmission between the hosts located on both sides of VPN Tunnel while connecting.</p> <p>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.</p>
Multicast via VPN	<p>Some programs might send multicast packets via VPN connection.</p> <p>Pass – Click this button to let multicast packets pass through the router.</p> <p>Block – This is default setting. Click this button to let multicast packets be blocked by the router.⁴</p>
Call Direction	<p>Specify the allowed call direction of this LAN to LAN profile.</p> <p>Both:-initiator/responder</p> <p>Dial-Out- initiator only</p> <p>Dial-In- responder only.</p>
Always On or Idle Timeout	<p>Always On-Check to enable router always keep VPN connection.</p> <p>Idle Timeout: The default value is 300 seconds. If the connection has been idled over the value, the router will drop the connection.</p>
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.

<p>Enable PING to Keep Alive is used to handle abnormal IPSec VPN connection disruption. It will help to provide</p>

the state of a VPN connection for router's judgment of redial.

Normally, if any one of VPN peers wants to disconnect the connection, it should follow a serial of packet exchange procedure to inform each other. However, if the remote peer disconnect without notice, Vigor router will by no where to know this situation. To resolve this dilemma, by continuously sending PING packets to the remote host, the Vigor router can know the true existence of this VPN connection and react accordingly. This is independent of DPD (dead peer detection).

ISDN

If you want to connect two networks with ISDN connection, please select ISDN radio button to build ISDN dial-out connection to the server. You should set up Link Type and identity like User Name and Password for the authentication of remote server. You can further set up Callback (CBCP) function below. This feature is useful for *i* model only.

PPTP

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

IPSec Tunnel

Build 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 ISDN, PPTP or L2TP with or without IPSec policy above.

Password

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

PPP Authentication

This field is applicable when you select ISDN, PPTP or L2TP with or without IPSec policy above. PAP/CHAP is the most common selection due to wild compatibility.

VJ compression

This field is applicable when you select ISDN, PPTP or L2TP with or without IPSec policy above. VJ Compression is used for TCP/IP protocol header compression. Normally set to **Yes** to improve bandwidth utilization.

IKE Authentication Method

This group of fields is applicable for IPSec Tunnels and L2TP with IPSec Policy.

Pre-Shared Key-Input 1-63 characters as pre-shared key.

Digital Signature (X.509) – Click this radio button to invoke this function and select one predefined in the X.509 Peer ID Profiles (set from **VPN and Remote Access>>IPSec Peer Identity**).

IPSec Security Method

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

Medium

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

High (ESP-Encapsulating Security Payload)- means payload (data) will be encrypted and authenticated. Select from below:

DES without Authentication -Use DES encryption algorithm and not apply any authentication scheme.

DES with Authentication-Use DES encryption algorithm and apply MD5 or SHA-1 authentication algorithm.

3DES without Authentication-Use triple DES encryption algorithm and not apply any authentication scheme.

3DES with Authentication-Use triple DES encryption algorithm and apply MD5 or SHA-1 authentication algorithm.

AES without Authentication-Use AES encryption algorithm and not apply any authentication scheme.

AES with Authentication-Use AES encryption algorithm and apply MD5 or SHA-1 authentication algorithm.

Advanced

Specify mode, proposal and key life of each IKE phase, Gateway etc.

The window of advance setup is shown as below:

IKE advanced settings

IKE phase 1 mode: ☒ Main mode ☐ Aggressive mode

IKE phase 1 proposal: DES_MD5_G1/DES_SHA1_G1/3DES_MD5_G1/3DES_MD5_G2/AES128_MD5_G2/AES256_SHA1_G2/AES256_SHA1_G14

IKE phase 2 proposal: HMAC_SHA1/HMAC_MD5

IKE phase 1 key lifetime: 28800 (900 ~ 86400)

IKE phase 2 key lifetime: 3600 (600 ~ 86400)

Perfect Forward Secret: ☒ Disable ☐ Enable

Local ID:

OK Close

IKE phase 1 mode -Select from **Main** mode and **Aggressive** mode. The ultimate outcome is to exchange security proposals to create a protected secure channel. **Main** mode is more secure than **Aggressive** mode since more exchanges are done in a secure channel to set up the IPSec session. However, the **Aggressive** mode is faster. The default value in Vigor router is Main mode.

IKE phase 1 proposal-To propose the local available authentication schemes and encryption algorithms to the VPN peers, and get its feedback to find a match. Two combinations are available for **Aggressive** mode and thirty for **Main** mode. We suggest you select the combination that covers the most schemes. Below shows the available proposals:

```

DES_MD5_G1
DES_SHA1_G1
3DES_MD5_G1
3DES_SHA1_G1
AES128_MD5_G1
AES128_SHA1_G1
AES192_MD5_G1
AES192_SHA1_G1
AES256_MD5_G1
AES256_SHA1_G1
DES_MD5_G2
DES_SHA1_G2
3DES_MD5_G2
3DES_SHA1_G2
AES128_MD5_G2
AES128_SHA1_G2
AES192_MD5_G2
AES192_SHA1_G2
AES256_MD5_G2
AES256_SHA1_G2
DES_MD5_G14
DES_SHA1_G14
3DES_MD5_G14
3DES_SHA1_G14
AES128_MD5_G14
AES128_SHA1_G14
AES192_MD5_G14
AES192_SHA1_G14
AES256_MD5_G14
AES256_SHA1_G14
AES256_SHA1_G14

```

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

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

IKE phase 2 key lifetime-For security reason, the lifetime of key should be defined. The default value is 3600 seconds. You may specify a value in between 600 and 86400 seconds.

Perfect Forward Secret (PFS)-The IKE Phase 1 key will be reused to avoid the computation complexity in phase 2. The default value is inactive this function.

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

Callback Function (for *i* models only)

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

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

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

3. Dial-In Settings

Allowed Dial-In Type <input checked="" type="checkbox"/> ISDN <input checked="" type="checkbox"/> PPTP <input checked="" type="checkbox"/> IPsec Tunnel <input checked="" type="checkbox"/> L2TP with IPsec Policy None		Username ??? Password VJ Compression <input checked="" type="radio"/> On <input type="radio"/> Off
<input type="checkbox"/> Specify ISDN CLID or Remote VPN Gateway Peer ISDN Number or Peer VPN Server IP or Peer ID 		IKE Authentication Method <input checked="" type="checkbox"/> Pre-Shared Key IKE Pre-Shared Key <input type="checkbox"/> Digital Signature(X.509) None
		IPsec Security Method <input checked="" type="checkbox"/> Medium (AH) High (ESP) <input checked="" type="checkbox"/> DES <input checked="" type="checkbox"/> 3DES <input checked="" type="checkbox"/> AES
		Callback Function (CBCP) <input type="checkbox"/> Enable Callback Function <input type="checkbox"/> Use the Following Number to Callback Callback Number Callback Budget 0 minute(s)

4. TCP/IP Network Settings

My WAN IP 0.0.0.0 Remote Gateway IP 0.0.0.0 Remote Network IP 0.0.0.0 Remote Network Mask 255.255.255.0 More	RIP Direction Disable From first subnet to remote network, you have to do Route <input type="checkbox"/> Change default route to this VPN tunnel (Only single WAN supports this)
---	--

OK Clear Cancel

Allowed Dial-In Type

Determine the dial-in connection with different types.

ISDN

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

PPTP

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

IPsec Tunnel

Allow the remote dial-in user to trigger an IPsec VPN connection through Internet.

L2TP

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

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

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

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

Specify CLID or Remote

You can specify the IP address of the remote dial-in user or

VPN Gateway	<p>peer ID (should be the same with the ID setting in dial-in type) by checking the box. Enter Peer ISDN number if you select ISDN above (This feature is useful for <i>i</i> model only.). Also, you should further specify the corresponding security methods on the right side.</p> <p>If you uncheck the checkbox, the connection type you select above will apply the authentication methods and security methods in the general settings.</p>
User Name	This field is applicable when you select ISDN, PPTP or L2TP with or without IPSec policy above.
Password	This field is applicable when you select ISDN, 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 ISDN, PPTP or L2TP with or without IPSec policy above.
IKE Authentication Method	<p>This group of fields is applicable for IPSec Tunnels and L2TP with IPSec Policy when you specify the IP address of the remote node. The only exception is Digital Signature (X.509) can be set when you select IPSec tunnel either with or without specify the IP address of the remote node.</p> <p>Pre-Shared Key - Check the box of Pre-Shared Key to invoke this function and type in the required characters (1-63) as the pre-shared key.</p> <p>Digital Signature (X.509) – Check the box of Digital Signature to invoke this function and select one predefined in the X.509 Peer ID Profiles (set from VPN and Remote Access>>IPSec Peer Identity).</p>
IPSec Security Method	<p>This group of fields is a must for IPSec Tunnels and L2TP with IPSec Policy when you specify the remote node.</p> <p>Medium- Authentication Header (AH) means data will be authenticated, but not be encrypted. By default, this option is active.</p> <p>High- Encapsulating Security Payload (ESP) means payload (data) will be encrypted and authenticated. You may select encryption algorithm from Data Encryption Standard (DES), Triple DES (3DES), and AES.</p>
Callback Function	<p>The callback function provides a callback service only for the ISDN LAN to LAN connection (this feature is useful for <i>i</i> model only). The remote user will be charged the connection fee by the telecom.</p> <p>Check to enable Callback function-Enables the callback function.</p> <p>Callback number-The option is for extra security. Once enabled, the router will ONLY call back to the specified Callback Number.</p> <p>Callback budget- By default, the callback function has limitation of callback period. Once the callback budget is exhausted, the function will be disabled automatically.</p> <p>Callback Budget (Unit: minutes)- Specify the time budget for the dial-in user. The budget will be decreased</p>

automatically per callback connection. The default value 0 means no limitation of callback period.

My WAN IP

This field is only applicable when you select ISDN, PPTP or L2TP with or without IPSec policy above. The default value is 0.0.0.0, which means the Vigor router will get a PPP IP address from the remote router during the IPCP negotiation phase. If the PPP IP address is fixed by remote side, specify the fixed IP address here. Do not change the default value if you do not select ISDN, PPTP or L2TP.

Remote Gateway IP

This field is only applicable when you select ISDN, PPTP or L2TP with or without IPSec policy above. The default value is 0.0.0.0, which means the Vigor router will get a remote Gateway PPP IP address from the remote router during the IPCP negotiation phase. If the PPP IP address is fixed by remote side, specify the fixed IP address here. Do not change the default value if you do not select ISDN, PPTP or L2TP.

**Remote Network IP/
Remote Network Mask**

Add a static route to direct all traffic destined to this Remote Network IP Address/Remote Network Mask through the VPN connection. For IPSec, this is the destination clients IDs of phase 2 quick mode.

More

Add a static route to direct all traffic destined to more Remote Network IP Addresses/ Remote Network Mask through the VPN connection. This is usually used when you find there are several subnets behind the remote VPN router.

RIP Direction

The option specifies the direction of RIP (Routing Information Protocol) packets. You can enable/disable one of direction here. Herein, we provide four options: TX/RX Both, TX Only, RX Only, and Disable.

RIP Version

Select the RIP protocol version. Specify Ver. 2 for greatest compatibility.

**From first subnet to
remote network, you
have to do**

If the remote network only allows you to dial in with single IP, please choose **NAT**, otherwise choose **Route**.

**Change default route to
this VPN tunnel**

Check this box to change the default route with this VPN tunnel. Be aware that this setting is available only for one WAN interface is enabled. It is not available when both WAN interfaces are enabled.

3.9.9 VPN Backup Management

VPN Backup Management is a backup mechanism to set multiple VPN tunnels for using as backup tunnel. It can assure the network connection would not be cut off due to network environment blocked by any reason.

Features of VPN Backup

- VPN Backup can judge abnormal situation for the environment of VPN server and correct it to complete the backup of VPN Tunnel in real-time.
- VPN Backup is complaint with all WAN modes (single/multi)
- Dial-out connection types contain IPSec, PPTP, L2TP, L2TP over IPSec and ISDN (depends on hardware specification)
- The web page is simple to understand and easy to configure
- Filly compliant with VPN Server LAN Sit Single/Multi Network
- Mail Alert support, please refer to **System Maintenance >> SysLog / Mail Alert** for detailed configuration
- Syslog support, please refer to **System Maintenance >> SysLog / Mail Alert** for detailed configuration
- Specific ERD (Environment Recovery Detection) mechanism which can be operated by using Telnet command

VPN Backup profile will be activated when initial connection of single VPN tunnel is off-line. Before setting VPN TRUNK backup profile, please configure at least two sets of LAN to LAN profiles (with fully configured dial-out settings) first, otherwise you will not have selections for grouping Member1 and Member2.

VPN and Remote Access >> VPN Backup Management

Backup Profile List | [Set to Factory Default](#)

Note: [Active:NO]The LAN-to-LAN Profile is disable or under Dial-In(Call Direction) at present.

No.	Status	Name	Member1(Active)Type	Member2(Active)Type

Status

☒ **Enable** ☐ **Disable**

Profile Name

Member1

Please choose the combination that you want.

Member2

Please choose the combination that you want.

Add

Edit

Delete

Set to Factory Default

Click to clear all VPN Backup profile.

No

The order of VPN Backup profile.

Status

“v” means such profile is enabled.

”x” means such profile is disabled.

Name (on Backup Profile field)	Display the name of VPN TRUNK profile.
Member1 (on Backup Profile field)	Display the dial-out profile selected from the Member1 drop down list below.
Active (on Backup Profile field)	<p>“Yes” means normal condition.</p> <p>”No” means the state might be disabled or that profile currently is set with Dial-in mode (for call direction) in LAN to LAN.</p>
Type (on Backup Profile field)	Display the connection type for that profile, such as IPSec, PPTP, L2TP, L2TP over IPSec (NICE), L2TP over IPSec(MUST) and so on.
Member2 (on Backup Profile field)	Display the dial-out profile selected from the Member2 drop down list below.
Status	After choosing one of the profile listed above, please click Enable to activate this profile. If you click Disable , the selected VPN Backup profile will not have any effect for VPN tunnel.
Profile Name	Type a name for VPN Backup profile. Each profile can group two VPN connections set in LAN to LAN. The saved VPN profiles in LAN to LAN will be shown on Member1 and Member2 fields.
Member 1/Member2	<p>Display the selection for LAN to LAN dial-out profiles (configured in VPN and Remote Access >> LAN to LAN) for you to choose for grouping under certain VPN backup profile.</p> <p>No - Index number of LAN to LAN dial-out profile.</p> <p>Name - Profile name of AN-to-LAN dial-out profile.</p> <p>Connection Type - Connection type of AN-to-LAN dial-out profile.</p> <p>VPN ServerIP (Private Network) - VPN Server IP of LAN to LAN dial-out profiles.</p>
Add	Add and save new profile to the backup profile list. The corresponding members (LAN to LAN profiles) grouped in such new VPN TRUNK profile will be locked. The profiles in LAN to LAN will be displayed in red.
Edit	Click this button to save the changes to the Status (Enable or Disable), profile name, member1 or member2.
Delete	Click this button to delete the selected VPN TRUNK profile. The corresponding members (LAN to LAN profiles) grouped in the deleted VPN TRUNK profile will be released and that profiles in LAN to LAN will be displayed in black.

Time for activating VPN Backup profile

VPN TRUNK backup will be activated automatically after the initial connection of single VPN Tunnel off-line. The content in Member1/2 within VPN TRUNK backup profile is similar to dial-out profile configured in LAN to LAN web page. VPN TRUNK backup profile will process and handle everything unless it is off-line once it is activated.

How can you set a VPN Backup profile?

1. Go to **VPN and Remote Access>>LAN to LAN**. Set two or more LAN to LAN profiles first.
2. Access into **VPN and Remote Access>>VPN Backup Management**.
3. Set one group of VPN backup profile by choosing **Enable** radio button, type a name for such profile, choose one of the LAN to LAN profiles from Member1 drop down list, choose one of the LAN to LAN profiles from Member2 drop down list, last click **Add**.

VPN and Remote Access >> VPN Backup Management

Backup Profile List
[Set to Factory Default](#)

Note: [Active:NO]The LAN-to-LAN Profile is disable or under Dial-In(Call Direction) at present.

No.	Status	Name	Member1(Active)Type	Member2(Active)Type
1	v	VpnBackup	3(YES)IPSec	4(YES)L2TP over IPSec(MUST)
2	v	PptpBackup	1(YES)PPTP	2(YES)PPTP

Status ☒ **Enable** ☐ **Disable**

Profile Name

Member1

Member2

No.	<Name>	<Connection-Type>	<VPN ServerIP(Private Network)>
5	2.2	L2TP	192.168.2.2(192.168.26.0)
6	27	IPSec	192.168.0.27(192.168.27.0)
7	28	PPTP	192.168.0.28(192.168.28.0)
8	29	L2TP over IPSec(NICE)	192.168.0.29(192.168.29.0)
9	30	L2TP over IPSec(NICE)	192.168.0.30(192.168.30.0)
10	31	L2TP over IPSec(NICE)	192.168.0.31(192.168.31.0)
11	32	L2TP over IPSec(NICE)	192.168.0.32(192.168.32.0)

4. Index No.1 is the first VPN backup profile. LAN to LAN profile of Index 3 is chosen as Member1; LAN to LAN profile of index 4 is chosen as Member2. At the same time, LAN to LAN profiles of 3 and 4 will be expressed in red to indicate that they are fixed.

Index	Name	Status
1.	2.5	v
2.	2.5-1	v
3.	2.29	v
4.	2.229	v
5.	26	v
6.	27	v
7.	28	v
8.	29	v
9.	30	v
10.	31	v

3.9.10 Connection Management

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

VPN and Remote Access >> Connection Management

Dial-out Tool

Refresh Seconds : 10 Refresh

General Mode: Dial

Backup Mode: Dial

VPN Connection Status

Current Page: 1 Page No. Go >>

VPN	Type	Remote IP	Virtual Network	Tx Pkts	Tx Rate	Rx Pkts	Rx Rate	UpTime
xxxxxxxx : Data is encrypted.								
xxxxxxxx : Data isn't encrypted.								

General Mode

This filed displays the profile configured in LAN to LAN (with Index number and VPN Server IP address). The VPN connection built by General Mode does not support VPN backup function.

General Mode: (28) 192.168.0.28

Backup Mode: (28) 192.168.0.28

atus

pe Remote

Tunnel 192.168

A1 Auth 192.168

PTP 192.168

A1 Auth 192.168

(28) 192.168.0.28

(29) 192.168.0.29

(30) 192.168.0.30

(31) 192.168.0.31

(32) 192.168.0.32

(33) 192.168.0.33

(34) 192.168.0.34

(35) 192.168.0.35

(36) 192.168.0.36

(37) 192.168.0.37

(38) 192.168.0.38

xxxxxxxx : Data is encrypted.

xxxxxxxx : Data isn't encrypted.

Backup Mode

This filed displays the profile name saved in VPN TRUNK Management (with Index number and VPN Server IP address). The VPN connection built by Backup Mode supports VPN backup function.

Backup Mode: (VpnLB) 192.168.2.103

atus

pe Remote

Tunnel 192.168.2.103

A1 Auth 192.168.2.103

(VpnLB) 192.168.2.203

(PptpLB) 192.168.2.5

(PptpLB) 192.168.2.5

(test) 192.168.0.26

(test) 192.168.0.27

Tunnel 192.168.2.103 192.168.1.0/24 51 3

A1 Auth

Dial

Click this button to execute dial out function.

Refresh Seconds

Choose the time for refresh the dial information among 5, 10, and 30.

Refresh

Click this button to refresh the whole connection status.

Note: The status of LAN to LAN for ISDN is shown on the page of **Online Status**.

Online Status

System Status				System Uptime: 1:19:30	
LAN Status		Primary DNS: 194.109.6.66		Secondary DNS: 168.95.1.1	
IP Address	TX Packets		RX Packets		
192.168.1.1	2945		2547		
WAN 1 Status					
Enable	Line	Name	Mode	Up Time	
Yes	Ethernet		Static IP	1:19:23	
IP	GW IP	TX Packets	TX Rate	RX Packets	RX Rate
172.16.3.229	172.16.3.1	388	3	701	6
WAN 2 Status					
Enable	Line	Name	Mode	Up Time	
No	Ethernet		---	00:00:00	
IP	GW IP	TX Packets	TX Rate	RX Packets	RX Rate
---	---	0	0	0	0
ISDN Status					
		>> Dial ISDN		>> Drop B1	>> Drop B2
Channel	Active Connection	TX Pkts	TX Rate	RX Pkts	RX Rate
B1	Idle [---]	0	0	0	0
B2	Idle [---]	0	0	0	0
D	DOWN				
				Up Time	AOC
				0:0:0	0
				0:0:0	0

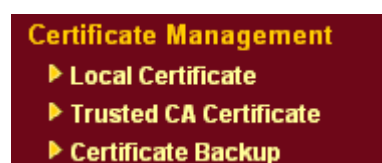
3.10 Certificate Management

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.



3.10.1 Local Certificate

Certificate Management >> Local Certificate

X509 Local Certificate Configuration

Name	Subject	Status	Modify
Local	---	---	<input type="button" value="View"/> <input type="button" value="Delete"/>

X509 Local Certificate

Generate

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

Generate Certificate Request

Subject Alternative Name	
Type	IP Address
IP	<input type="text"/>
Subject Name	
Country (C)	<input type="text"/>
State (ST)	<input type="text"/>
Location (L)	<input type="text"/>
Organization (O)	<input type="text"/>
Organization Unit (OU)	<input type="text"/>
Common Name (CN)	<input type="text"/>
Email (E)	<input type="text"/>
Key Type	RSA
Key Size	1024 Bit

Generate

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

Import

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

Refresh

Click this button to refresh the information listed below.

View

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

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

Certificate Management >> Local Certificate

X509 Local Certificate Configuration

Name	Subject	Status	Modify
Local	/C=TW/O=Draytek/OU=RD/emailA...	Requesting	<input type="button" value="View"/> <input type="button" value="Delete"/>
<input type="button" value="GENERATE"/> <input type="button" value="IMPORT"/> <input type="button" value="REFRESH"/>			
X509 Local Certificate Request			
<pre> -----BEGIN CERTIFICATE REQUEST----- MIIBsjCCARsCAQAwUDELMakGA1UEBhMCVFcxEDAOBgNVBAAoTBORyYX10ZWsx CzAJBgNVBAsTA1JEMSIwIAAYJKoZIhvcNAQkBFhNzZXJ2aWNlQGRyYX10ZWsu Y29tMIGfMAOGCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDPioahu/gFQaYB1ce5OERSDfWknIdH blo1kt9cTdLUDaFk6s8d3wDeQytoV1LBjz2IDFOxjX6ip7evl87twwTsg4lgZ6Qk /rGhuVTKd9j6P1crnkP7du84t23tWBdMD4W5c8VmSyDjShLhjdXVYPWpNKVrOT2 RZjkrMaHEWpVpWIDAQABoCIwIAAYJKoZIhvcNAQkOMRMwETAPBgNVHREECDA GhwTAqAEqMAOGCSqGSIb3DQEBAQUAA4GBAB43O4N9nod8rIudBAfTt9ltso/tY Nb2kfEZikisNdZUoUEnkcejeOndc+H83VDA23ACEJpzTPFxqklbeZo7a+wE57/ +OVhNagBaGqeJ9trvYqeZybCrSjRU1PN1Hccfo7ANJ/M/D1EPgKn+PWCho6LgVsJHrV kC2HdVj8kJEimO -----END CERTIFICATE REQUEST----- </pre>			

3.10.2 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.

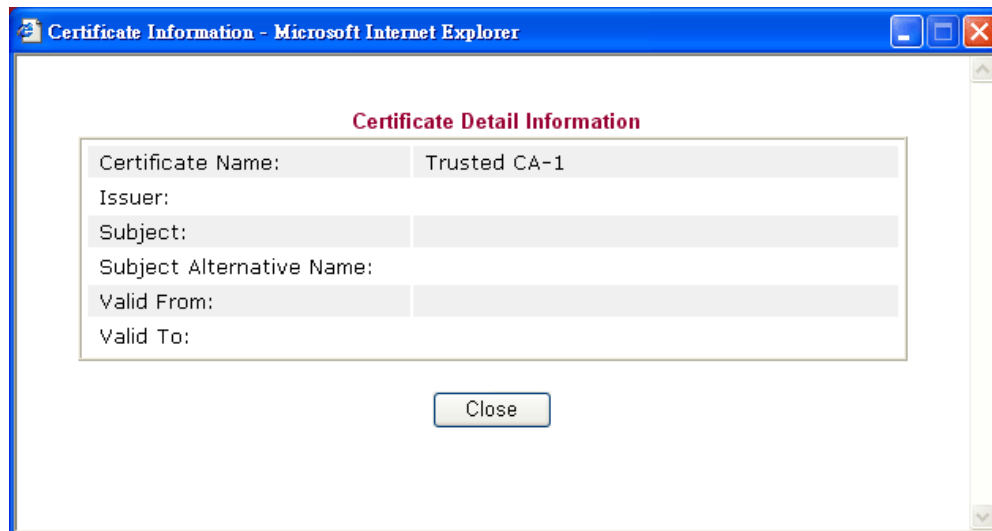
[Browse...](#)

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.



3.10.3 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**.

Certificate Management >> Certificate Backup

Certificate Backup / Restoration

Backup

Encrypt password:

Retype password:

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

Restoration

Select a backup file to restore.

Decrypt password:

Click to upload the file.

3.11 VoIP

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

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

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

sip: user:password @ host: port

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

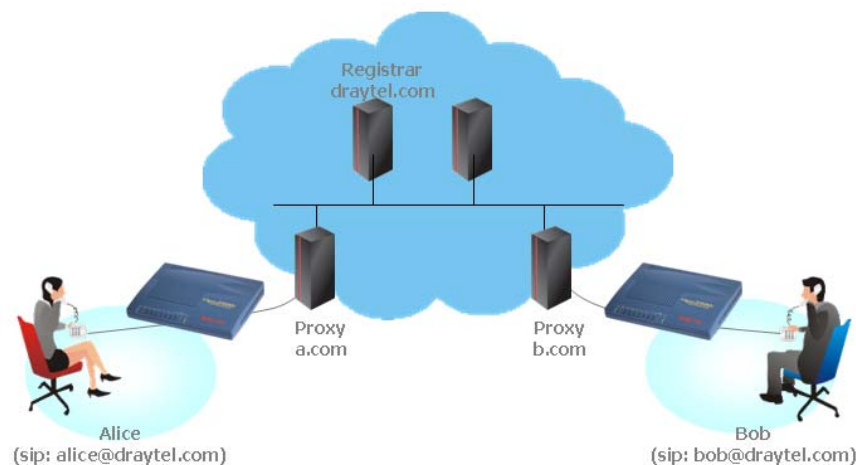
After a call is setup, the voice streams transmit via RTP (Real-Time Transport Protocol). Different codecs (methods to compress and encode the voice) can be embedded into RTP packets. Vigor V models provide various codecs, including G.711 A/μ-law, G.723, G.726 and G.729 A & B. Each codec uses a different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

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

- **Calling via SIP Servers**

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

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



The major benefit of this mode is that you don't have to memorize your friend's IP address, which might change very frequently if it's dynamic. Instead of that, you will

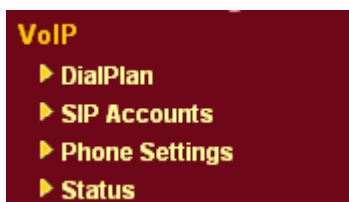
only have to using **dial plan** or directly dial your friend's **account name** if you are with the same SIP Registrar. Please refer to the **section 4.5.1**.

- **Peer-to-Peer**

Before calling, you have to know your friend's IP Address. The Vigor VoIP Routers will build connection between each other. Please refer to the **section 4.5.2**.



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



3.11.1 DialPlan

This page allows you to set phone book and digit map for the VoIP function. Click the **Phone Book** and **Digit Map** links on the page to access into next pages for dialplan settings.

VoIP >> DialPlan Setup

DialPlan Configuration

[Phone Book](#)

[Digit Map](#)

Phone Book

In this section, you can set your VoIP contacts in the “phonebook”. It can help you to make calls quickly and easily by using “speed-dial” **Phone Number**. There are total 60 index entries in the phonebook for you to store all your friends and family members’ SIP addresses. **Loop through** and **Backup Phone Number** will be displayed if you are using Vigor 2910VGi for setting the phone book.

VoIP >> DialPlan Setup

Phone Book

Index	Phone number	Display Name	SIP URL	Dial Out Account	Loop through	Backup Phone Number	Status
1.	688	david	01@iptel.org	Default	None		x
2.				Default	None		x
3.				Default	None		x
4.				Default	None		x
5.				Default	None		x
6.				Default	None		x
7.				Default	None		x
8.				Default	None		x
9.				Default	None		x
10.				Default	None		x
11.				Default	None		x
12.				Default	None		x
13.				Default	None		x
14.				Default	None		x
15.				Default	None		x
16.				Default	None		x
17.				Default	None		x
18.				Default	None		x
19.				Default	None		x
20.				Default	None		x

<< [1-20](#) | [20-40](#) | [40-60](#) >>

[Next](#) >>

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

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

VoIP >> DialPlan Setup

Phone Book Index No. 1

<input checked="" type="checkbox"/> Enable	
Phone Number	<input type="text" value="688"/>
Display Name	<input type="text" value="david"/>
SIP URL	<input type="text" value="01"/> @ <input type="text" value="iptel.org"/>

Enable

Click this to enable this entry.

Phone Number

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

Display Name

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

SIP URL

Enter your friend's SIP Address

This page will differ for different models. Below is a sample page obtained from Vigor 2910VGi. The selection of **Loop through** and **Backup Phone Number** is only available for 2910VGi model.

VoIP >> DialPlan Setup

Phone Book Index No. 1

<input checked="" type="checkbox"/> Enable		
Phone Number	<input type="text" value="688"/>	
Display Name	<input type="text" value="david"/>	
SIP URL	<input type="text" value="01"/>	<input type="text" value="@iptel.org"/>
Dial Out Account	<input type="button" value="Default"/>	
Loop through	<input type="button" value="None"/>	
Backup Phone Number	<input type="text"/>	

Enable

Click this to enable this entry.

Phone Number

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

Display Name

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

SIP URL

Enter your friend's SIP Address

Dial Out Account

Choose one of the SIP accounts for this profile to dial out. If caller and callee do not use the same SIP server, sometimes, the VoIP phone call connection may not succeed. By using the specified dial out account, the successful connection can be assured.

Dial Out Account

Default
1-1
2-???
3-???
4-???
5-???
6-???

Loop through

For the model of Vigor 2910VGi, the selection should be as the following:

Loop through

None
ISDN

Backup Phone Number

When the VoIP phone is obstructs or the Internet breaks down for some reasons, the backup phone will be dialed out to replace the VoIP phone number. At this time, the phone call will be changed from VoIP phone into PSTN call according to the loop through direction chosen. Note that, during the phone switch, the blare of phone will appear for a short time. And when the VoIP phone is switched into the PSTN phone, the telecom co. might charge you for the connection fee. Please

type in backup phone number (PSTN number) for this VoIP phone setting.

Digit Map

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

VoIP >> DialPlan Setup

Digit Map Setup

#	Enable	Prefix Number	Mode	OP Number	Min Len	Max Len	Interface
1	<input checked="" type="checkbox"/>	03	Replace	8863	7	9	VoIP1
2	<input checked="" type="checkbox"/>	886	Strip	886	7	9	VoIP1
3	<input type="checkbox"/>		None		0	0	VoIP1
4	<input type="checkbox"/>		None		0	0	VoIP1
5	<input type="checkbox"/>		None		0	0	VoIP1
6	<input type="checkbox"/>		None		0	0	VoIP1
7	<input type="checkbox"/>		None		0	0	VoIP1
8	<input type="checkbox"/>		None		0	0	VoIP1
9	<input type="checkbox"/>		None		0	0	VoIP1
10	<input type="checkbox"/>		None		0	0	VoIP1
11	<input type="checkbox"/>		None		0	0	VoIP1
12	<input type="checkbox"/>		None		0	0	VoIP1
13	<input type="checkbox"/>		None		0	0	VoIP1
14	<input type="checkbox"/>		None		0	0	VoIP1
15	<input type="checkbox"/>		None		0	0	VoIP1
16	<input type="checkbox"/>		None		0	0	VoIP1
17	<input type="checkbox"/>		None		0	0	VoIP1
18	<input type="checkbox"/>		None		0	0	VoIP1
19	<input type="checkbox"/>		None		0	0	VoIP1
20	<input type="checkbox"/>		None		0	0	VoIP1

OK

Cancel

Enable

Check this box to invoke this setting.

Prefix Number

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

Mode

None - No action.

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

Strip - When you choose this mode, the OP number will be deleted by the prefix number for calling out through the specific VoIP interface. Take the above picture (Prefix Table Setup web page) as an example, the OP number of 886 will be deleted completely for the prefix number is set with 886.

Replace - When you choose this mode, the OP number will be replaced by the prefix number for calling out through the specific VoIP interface. Take the above picture (Prefix Table Setup web page) as an example, the prefix number of 03 will be replaced by 8863. For example: dial number of

“03111111” will be changed to “8863111111” and sent to SIP server.

Mode

OP Number

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

Min Len

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

Max Len

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

Interface

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

3.11.2 SIP Accounts

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

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

VoIP >> SIP Accounts

SIP Accounts List

Refresh

Index	Profile	Domain/Realm	Proxy	Account Name	Ring Port			Status
1	david	iptel.org	iptel.org	8201	<input checked="" type="checkbox"/> VoIP1	<input type="checkbox"/> VoIP2	<input type="checkbox"/> ISDN	-
2				change_me	<input type="checkbox"/> VoIP1	<input type="checkbox"/> VoIP2	<input type="checkbox"/> ISDN	-
3				change_me	<input type="checkbox"/> VoIP1	<input type="checkbox"/> VoIP2	<input type="checkbox"/> ISDN	-
4				change_me	<input type="checkbox"/> VoIP1	<input type="checkbox"/> VoIP2	<input type="checkbox"/> ISDN	-
5				change_me	<input type="checkbox"/> VoIP1	<input type="checkbox"/> VoIP2	<input type="checkbox"/> ISDN	-
6				change_me	<input type="checkbox"/> VoIP1	<input type="checkbox"/> VoIP2	<input type="checkbox"/> ISDN	-

R: success registered on SIP server
-: fail to register on SIP server

NAT Traversal Setting

STUN server:	<input type="text" value="stun.fwdnet.net"/>
External IP:	<input type="text"/>
SIP PING interval:	<input type="text" value="150"/> sec

OK

Index

Click this link to access into next page for setting SIP account.

Profile	Display the profile name of the account.
Domain/Realm	Display the domain name or IP address of the SIP registrar server.
Proxy	Display the domain name or IP address of the SIP proxy server.
Account Name	Display the account name of SIP address before @.
Ring Port	Specify which port will ring when receiving a phone call.
STUN Server	Type in the IP address or domain of the STUN server.
External IP	Type in the gateway IP address.
SIP PING interval	The default value is 150 (sec). It is useful for a Nortel server NAT Traversal Support.
Status	Show the status for the corresponding SIP account. R means such account is registered on SIP server successfully. – means the account is failed to register on SIP server.

VoIP >> SIP Accounts

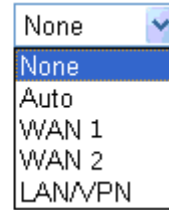
SIP Account Index No. 1

Profile Name	<input type="text" value="test"/> (11 char max.)
Register via	<input type="button" value="None"/> <input type="checkbox"/> make call without register
SIP Port	<input type="text" value="5060"/>
Domain/Realm	<input type="text" value="iptel.org"/> (63 char max.)
Proxy	<input type="text" value="iptel.org"/> (63 char max.)
<input type="checkbox"/> Act as outbound proxy	
Display Name	<input type="text"/> (23 char max.)
Account Number/Name	<input type="text" value="8201"/> (63 char max.)
<input type="checkbox"/> Authentication ID	<input type="text"/> (63 char max.)
Password	<input type="text"/> (63 char max.)
Expiry Time	<input type="button" value="1 hour"/> <input type="text" value="3600"/> sec
NAT Traversal Support	<input type="button" value="None"/>
Ring Port	<input checked="" type="checkbox"/> VoIP1 <input type="checkbox"/> VoIP2 <input type="checkbox"/> ISDN
Ring Pattern	<input type="button" value="1"/>

Profile Name	Assign a name for this profile for identifying. You can type similar name with the domain. For example, if the domain name is <i>draytel.org</i> , then you might set <i>draytel-1</i> in this field.
Register via	If you want to make VoIP call without register personal information, please choose None and check the box to achieve the goal. Some SIP server allows user to use VoIP function without registering. For such server, please check the box of make call without register . Choosing Auto is recommended.

The system will select a proper way for your VoIP call.

Register via



SIP Port

Set the port number for sending/receiving SIP message for building a session. The default value is **5060**. Your peer must set the same value in his/her Registrar.

Domain/Realm

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

Proxy

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

Act as Outbound Proxy

Check this box to make the proxy acting as outbound proxy.

Display Name

The caller-ID that you want to be displayed on your friend's screen.

Account Number/Name

Enter your account name of SIP Address, e.g. every text before @.

Authentication ID

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

Password

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

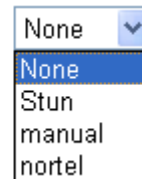
Expiry Time

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

NAT Traversal Support

If the router (e.g., broadband router) you use connects to internet by other device, you have to set this function for your necessity.

NAT Traversal Support



None – Disable this function.

Stun – Choose this option if there is Stun server provided for your router.

Manual – Choose this option if you want to specify an external IP address as the NAT transversal support.

Nortel – If the soft-switch that you use supports nortel solution, you can choose this option.

Ring Port

Set VoIP1, VoIP 2 or ISDN as the default ring port for this SIP account. If you choose either VoIP1 or VoIP2, the ISDN selection will be dimmed, vice versa.

Ring Pattern

Choose a ring tone type for the VoIP phone call.

Ring Pattern

1 ▾

1
2
3
4
5
6

Below shows successful SIP accounts for your reference.

VoIP >> SIP Accounts

SIP Accounts List

Refresh

Index	Profile	Domain/Realm	Proxy	Account Name	Ring Port			Status
1	draytek_1	draytel.org	draytel.org	813177	<input checked="" type="checkbox"/> VoIP1	<input type="checkbox"/> VoIP2	<input type="checkbox"/> ISDN	-
2	IPTTEL	iptel.org	iptel.org	kevin_yu	<input type="checkbox"/> VoIP1	<input type="checkbox"/> VoIP2	<input checked="" type="checkbox"/> ISDN	R
3	SeedNet	seednet.net.tw	139.175.232.13	070901002	<input type="checkbox"/> VoIP1	<input checked="" type="checkbox"/> VoIP2	<input type="checkbox"/> ISDN	-
4				change_me	<input type="checkbox"/> VoIP1	<input type="checkbox"/> VoIP2	<input type="checkbox"/> ISDN	-
5				change_me	<input type="checkbox"/> VoIP1	<input type="checkbox"/> VoIP2	<input type="checkbox"/> ISDN	-
6				change_me	<input type="checkbox"/> VoIP1	<input type="checkbox"/> VoIP2	<input type="checkbox"/> ISDN	-

R: success registered on SIP server
-: fail to register on SIP server

NAT Traversal Setting

STUN server:

External IP:

SIP PING interval: sec

OK

3.10.3 Phone Settings

This page allows user to set phone settings for VoIP 1 and VoIP 2 respectively.

VoIP >> Phone Settings

Phone List

Index	Port	Call feature	Codec	Tone	Gain (Mic/Speaker)	Default SIP Account	DTMF Relay
1	FXS 1		G.729A/B	User Defined	5/5		InBand
2	FXS 2		G.729A/B	User Defined	5/5		InBand
3	ISDN		G.729A/B	User Defined	5/5		InBand

RTP

☐ Symmetric RTP

Dynamic RTP port start

Dynamic RTP port end

RTP TOS

OK

Phone List

Port – There are three phone ports provided here for you to configure.

Call feature – A brief description for call feature will be shown in this field for your reference.

Codec – The default Codec setting for each port will be

shown in this field for your reference. You can click the number below the Index field to change it for each phone port.

Tone - Display the tone settings that configured in the advanced settings page of Phone Index.

Gain - Display the volume gain settings for Mic/Speaker that configured in the advanced settings page of Phone Index.

Default SIP Account – “draytel_1” is the default SIP account. You can click the number below the Index field to change SIP account for each phone port.

DTMF Relay – Display DTMF mode that configured in the advanced settings page of Phone Index.

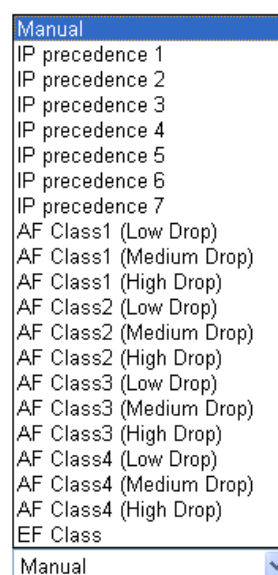
RTP

Symmetric RTP – Check this box to invoke the function. To make the data transmission going through on both ends of local router and remote router not misleading due to IP lost (for example, sending data from the public IP of remote router to the private IP of local router), you can check this box to solve this problem.

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

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

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



The image shows a dropdown menu for RTP TOS. The menu is open, displaying a list of options. The first option is 'Manual', which is highlighted in blue. Below it are seven 'IP precedence' options (1 through 7). Then there are twelve 'AF Class' options, each followed by a drop level in parentheses: 'AF Class1 (Low Drop)', 'AF Class1 (Medium Drop)', 'AF Class1 (High Drop)', 'AF Class2 (Low Drop)', 'AF Class2 (Medium Drop)', 'AF Class2 (High Drop)', 'AF Class3 (Low Drop)', 'AF Class3 (Medium Drop)', 'AF Class3 (High Drop)', 'AF Class4 (Low Drop)', 'AF Class4 (Medium Drop)', and 'AF Class4 (High Drop)'. The last option is 'EF Class'. At the bottom of the dropdown, there is a small blue arrow pointing downwards. Below the dropdown list, the text 'Manual' is visible, and a small blue arrow pointing downwards is also present.

RTP TOS

Detailed Settings for VoIP 1 and 2

Click the number **1** or **2** link under Index column, you can access into the following page for configuring Phone settings.

Phone Index No.1

Call feature <input type="checkbox"/> Hotline <input type="checkbox"/> Session Timer 3600 sec <input type="checkbox"/> T.38 Fax Function Call Forwarding disable SIP URL Time Out 30 sec <input type="checkbox"/> DND(Do Not Disturb) Mode Index(1-15) in Schedule Setup: <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> Note: Action and Idle Timeout settings will be ignored. Index(1-60) in Phone Book as Exception List: <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> CLIR (hide caller ID) <input type="checkbox"/> Call Waiting <input type="checkbox"/> Call Transfer		Codecs Prefer Codec G.729A/B (8Kbps) <input type="checkbox"/> Single Codec Packet Size 20ms Voice Active Detector Off Default SIP Account 1-??? <input type="checkbox"/> Play dial tone only when account registered Default Call Route <input type="radio"/> To ISDN: Dial *# for VoIP <input checked="" type="radio"/> To VoIP: Dial # for ISDN
--	--	---

OK Cancel Advanced

Hotline

Check the box to enable it. Type in the SIP URL in the field for dialing automatically when you pick up the phone set.

Session Timer

Check the box to enable the function. In the limited time that you set in this field, if there is no response, the connecting call will be closed automatically.

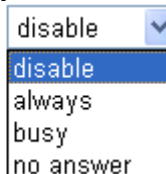
T.38 Fax Function

If the remote end also supports FAX function, you can check this box to enable this function.

Call Forwarding

There are four options for you to choose. **Disable** is to close call forwarding function. **Always** means all the incoming calls will be forwarded into SIP URL without any reason. **Busy** means the incoming calls will be forwarded into SIP URL only when the local system is busy. **No answer** means if the incoming calls do not receive any response, they will be forwarded to the SIP URL by the time out.

Call Forwarding



SIP URL – Type in the SIP URL (e.g., aaa@draytel.org or abc@iptel.org) as the site for call forwarded.

Time Out – Set the time out for the call forwarding. The default setting is 30 sec.

DND (Do Not Disturb) mode

Set a period of peace time without disturbing by VoIP phone call. During the period, the one who dial in will listen busy tone, yet the local user will not listen any ring tone.

Index (1-15) in Schedule - Enter the index of schedule profiles to control the DND mode according to the preconfigured schedules. Refer to section 3.5.2 **Schedule** for detailed configuration.

Index (1-60) in Phone Book - Enter the index of phone book

profiles. Refer to section **3.10.1 DialPlan – Phone Book** for detailed configuration.

Call Waiting

Check this box to invoke this function. A notice sound will appear to tell the user new phone call is waiting for your response. Click hook flash to pick up the waiting phone call.

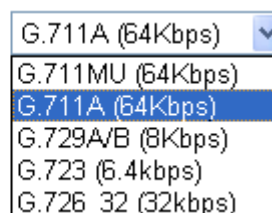
Call Transfer

Check this box to invoke this function. Click hook flash to initiate another phone call. When the phone call connection succeeds, hang up the phone. The other two sides can communicate, then.

Prefer Codec

Select one of five codecs as the default for your VoIP calls. The codec used for each call will be negotiated with the peer party before each session, and so may not be your default choice. The default codec is G.729A/B; it occupies little bandwidth while maintaining good voice quality. If your upstream speed is only 64Kbps, do not use G.711 codec. It is better for you to have at least 256Kbps upstream if you would like to use G.711.

Prefer Codec

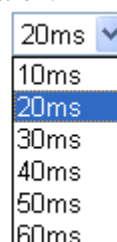


G.711A (64Kbps)	▼
G.711MU (64Kbps)	
G.711A (64Kbps)	
G.729A/B (8Kbps)	
G.723 (6.4kbps)	
G.726_32 (32kbps)	

Single Codec – If the box is checked, only the selected Codec will be applied.

Packet Size-The amount of data contained in a single packet. The default value is 20 ms, which means the data packet will contain 20 ms voice information.

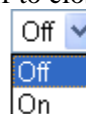
Packet Size



20ms	▼
10ms	
20ms	
30ms	
40ms	
50ms	
60ms	

Voice Active Detector - This function can detect if the voice on both sides is active or not. If not, the router will do something to save the bandwidth for other using. Click On to invoke this function; click off to close the function.

Voice Active Detector



Off	▼
Off	
On	

Default SIP Account

You can set SIP accounts (up to six groups) on SIP Account page. Use the drop down list to choose one of the profile names for the accounts as the default one for this phone setting.

Play dial tone only when account registered - Check this box to invoke the function.

Default Call Route

It determines the default direction for the call route of the router.

To ISDN (for VoIP) - The router is set by using ISDN call.

To change ISDN call into VoIP call, please dial the character in this field for transferring. The character that you can type can be *, #, and 0~9.

To VoIP (for ISDN) - The router is set by using VoIP call. To change VoIP call into ISDN call, please dial the character in this field for transferring. The character that you can type can be *, #, and 0~9.

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

VoIP >> Phone Settings

Advance Settings >> Phone Index No.1

Tone Settings		Caller ID Type: FSK_ETSI (UK)					
	Region	Low Freq (Hz)	High Freq (Hz)	T on 1 (msec)	T off 1 (msec)	T on 2 (msec)	T off 2 (msec)
Dial tone	UK	350	440	0	0	0	0
Ringing tone		400	450	400	200	400	2000
Busy tone		400	0	375	375	0	0
Congestion tone		480	620	400	350	225	525
Volume Gain		DTMF					
Mic Gain(1-10)		5	DTMF mode		InBand		
Speaker Gain(1-10)		5	Payload Type(rfc2833)		101		
MISC							
Dial Tone Power Level		27					
Ring Frequency		25					

OK Cancel

Region

Select the proper region which you are located. The common settings of **Caller ID Type**, **Dial tone**, **Ringing tone**, **Busy tone** and **Congestion tone** will be shown automatically on the page. If you cannot find out a suitable one, please choose **User Defined** and fill out the corresponding values for dial tone, ringing tone, busy tone, congestion tone by yourself for VoIP phone.

Advance Settings >> Phone Index

Tone Settings

Region	User Defined
	User Defined
	UK
	US
	Denmark
	Italy
	Germany
	Netherlands
	Portugal
	Sweden
	Australia
	Slovenia
	Czech
	Slovakia

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

Caller ID Type

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

Caller ID Type	FSK_ETSI
	FSK_ETSI
	FSK_ETSI (UK)
	FSK_BELLCORE (US/AU)
	DTMF
	DTMF (DK)
	DTMF (SE/NL/FIN)

Volume Gain

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

MISC

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

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

DTMF

InBand - Choose this one then the Vigor will send the DTMF tone as audio directly when you press the keypad on the phone

OutBand - Choose this one then the Vigor will capture the keypad number you pressed and transform it to digital form then send to the other side; the receiver will generate the tone according to the digital form it receive. This function is very

useful when the network traffic congestion occurs and it still can remain the accuracy of DTMF tone.

SIP INFO- Choose this one then the Vigor will capture the DTMF tone and transfer it into SIP form. Then it will be sent to the remote end with SIP message.

DTMF mode

Payload Type (rfc2833)

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

Detailed Settings for ISDN (available for VGi model only)

Click the number **3** link under Index column, you can access into the following page for configuring Phone settings.

VoIP >> Phone Settings

Hotline

Check the box to enable it. Type in the SIP URL in the field for dialing automatically when you pick up the phone set.

Session Timer

Check the box to enable the function. In the limited time that you set in this field, if there is no response, the connecting call will be closed automatically.

ISDN Loop Through Ring Port

Click the radio button to specify which port will ring if MSN mapping ring port (configured in **ISDN>>General Setup**) is not set properly.

Broadcast call – Both FXS1 and FXS2 will ring.

FXS 1- Such port will ring.

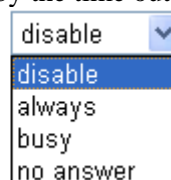
FXS 2- Such port will ring.

Call Forwarding

There are four options for you to choose. **Disable** is to close call forwarding function. **Always** means all the incoming calls will be forwarded into SIP URL without any reason. **Busy** means the incoming calls will be forwarded into SIP URL

only when the local system is busy. **No answer** means if the incoming calls do not receive any response, they will be forwarded to the SIP URL by the time out.

Call Forwarding

A dropdown menu for 'Call Forwarding' with the following options: 'disable' (selected), 'always', 'busy', and 'no answer'.

SIP URL – Type in the SIP URL (e.g., aaa@draytel.org or abc@iptel.org) as the site for call forwarded.

Time Out – Set the time out for the call forwarding. The default setting is 30 sec.

DND (Do Not Disturb) mode

Set a period of peace time without disturbing by VoIP phone call. During the period, the one who dial in will listen busy tone, yet the local user will not listen any ring tone.

Index (1-15) in Schedule - Enter the index of schedule profiles to control the DND mode according to the preconfigured schedules. Refer to section 3.5.2 **Schedule** for detailed configuration.

Index (1-60) in Phone Book - Enter the index of phone book profiles. Refer to section 3.10.1 **DialPlan – Phone Book** for detailed configuration.

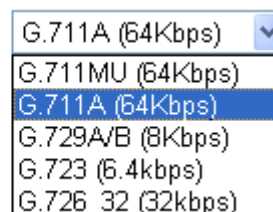
CLIR (hide caller ID)

Check this box to hide the caller ID on the display panel of the phone set.

Prefer Codec

Select one of five codecs as the default for your VoIP calls. The codec used for each call will be negotiated with the peer party before each session, and so may not be your default choice. The default codec is G.729A/B; it occupies little bandwidth while maintaining good voice quality. If your upstream speed is only 64Kbps, do not use G.711 codec. It is better for you to have at least 256Kbps upstream if you would like to use G.711.

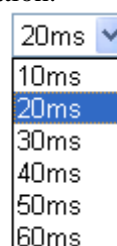
Prefer Codec

A dropdown menu for 'Prefer Codec' with the following options: 'G.711A (64Kbps)' (selected), 'G.711MU (64Kbps)', 'G.729A/B (8Kbps)', 'G.723 (6.4kbps)', and 'G.726_32 (32kbps)'.

Single Codec – If the box is checked, only the selected Codec will be applied.

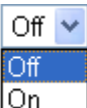
Packet Size-The amount of data contained in a single packet. The default value is 20 ms, which means the data packet will contain 20 ms voice information.

Packet Size

A dropdown menu for 'Packet Size' with the following options: '20ms' (selected), '10ms', '30ms', '40ms', '50ms', and '60ms'.

Voice Active Detector - This function can detect if the voice on both sides is active or not. If not, the router will do

something to save the bandwidth for other using. Click On to invoke this function; click off to close the function.

Voice Active Detector 

Default SIP Account

You can set SIP accounts (up to six groups) on SIP Account page. Use the drop down list to choose one of the profile names for the accounts as the default one for this phone setting.

Play dial tone only when account registered

Check this box to invoke the function.

FXO Feature

Enable ISDN to VoIP (On-Net) Calls – Check this box to make all the outgoing calls from ISDN line to be forwarded to receivers by Internet.

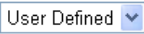
Enable VoIP to ISDN (Off-Net) Calls – Check this box to make all the incoming calls coming from Internet to be forwarded to receivers by ISDN line.

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

VoIP >> Phone Settings

Advance Settings >> ISDN

Tone Settings

Region 


	Low Freq (Hz)	High Freq (Hz)	T on 1 (msec)	T off 1 (msec)	T on 2 (msec)	T off 2 (msec)
Dial tone	350	440	0	0	0	0
Ringing tone	400	450	400	200	400	2000
Busy tone	400	0	375	375	0	0
Congestion tone	0	0	0	0	0	0

Volume Gain

Mic Gain(1-10)

Speaker Gain(1-10)

DTMF

DTMF mode 

Payload Type(rfc2833)

MISC

Dial Tone Power Level

Authentication PIN Code

☐ Check for ISDN to VoIP Calls

☐ Check for VoIP to ISDN Calls

Disallow VoIP to ISDN Calls with the Following Prefixes

☐

☐

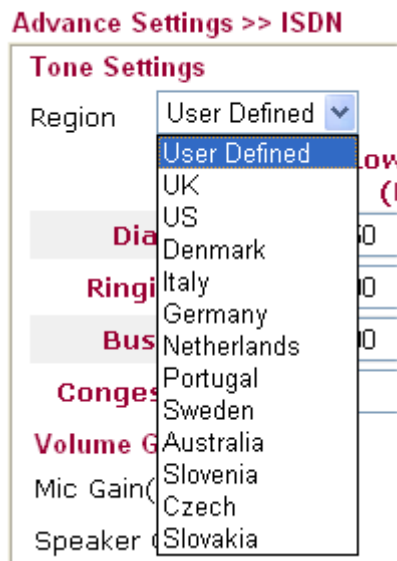
☐

☐

Region

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

page. If you cannot find out a suitable one, please choose **User Defined** and fill out the corresponding values for dial tone, ringing tone, busy tone, congestion tone by yourself for VoIP phone.



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

Volume Gain

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

MISC

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

Authentication PIN Code

Check for ISDN to VoIP Calls – Set a pin code for the router to authenticate which one is allowed to dial ISDN to VoIP call. The figure that you can type in this field is limited from three to eight with digits from zero to nine.

Check for VoIP to ISDN Calls - Set a pin code for the router to authenticate which one is allowed to dial VoIP to ISDN call. The figure that you can type in this field is limited from three to eight with digits from zero to nine.

DTMP

DTMF mode – There are four selections provided here:

InBand: Choose this one then the Vigor will send the DTMF tone as audio directly when you press the keypad on the phone

OutBand: Choose this one then the Vigor will capture the keypad number you pressed and transform it to digital form then send to the other side; the receiver will generate the tone according to the digital form it receive. This function is very useful when the network traffic congestion occurs and it still can remain the accuracy of DTMF tone.

SIP INFO: Choose this one then the Vigor will capture the DTMF tone and transfer it into SIP form. Then it will be sent to the remote end with SIP message.

DTMF mode

InBand

InBand

OutBand (RFC2833)

SIP INFO (cisco format)

SIP INFO (nortel format)

Payload Type (rfc2833) - Choose a number from 96 to 127, the default value was 101. This setting is available for the OutBand (RFC2833) mode.

Disallow VoIP to ISDN Calls with the Following Prefixes

Set the prefix of the phone number to forbid the user dialing through VoIP to ISDN. All the phone number with the prefix specified here will not be allowed to connect through the router. If a user dials the number by force, the router will disconnect it automatically. The figure that you can type in this field is limited one to eleven with digits from zero to nine.

3.11.4 Status

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

VoIP >> Status

Status

Refresh Seconds: 10

Port	Status	Codec	PeerID	Elapse (hh:mm:ss)	Tx Pkts	Rx Pkts	Rx Losses	Rx Jitter (ms)	In Calls	Out Calls	Speaker Gain
FXS 1	IDLE			00:00:00	0	0	0	0	0	0	5
FXS 2	IDLE			00:00:00	0	0	0	0	0	0	5
ISDN1	IDLE			00:00:00	0	0	0	0	0	0	5
ISDN2	IDLE			00:00:00	0	0	0	0	0	0	5

Log

Date (mm-dd-yyyy)	Time (hh:mm:ss)	Duration (hh:mm:ss)	In/Out	Peer ID
00-00-0	00:00:00	00:00:00	-	
00-00-0	00:00:00	00:00:00	-	
00-00-0	00:00:00	00:00:00	-	
00-00-0	00:00:00	00:00:00	-	
00-00-0	00:00:00	00:00:00	-	
00-00-0	00:00:00	00:00:00	-	
00-00-0	00:00:00	00:00:00	-	
00-00-0	00:00:00	00:00:00	-	
00-00-0	00:00:00	00:00:00	-	
00-00-0	00:00:00	00:00:00	-	
00-00-0	00:00:00	00:00:00	-	

Refresh Seconds

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

Refresh Seconds :

10

5

10

30

Port

It shows current connection status for the port of VoIP1, VoIP2, ISDN1 and ISDN2. The ISDN1/2 appears only when the router is equipped with ISDN interface. ISDN1 means B1 channel for the physical ISDN port; ISDN2 means B2 channel

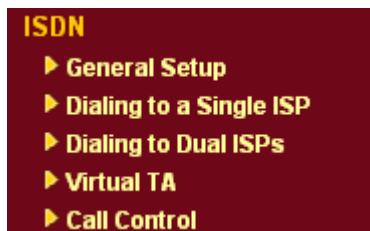
for the physical ISDN port. Be aware that ISDN1/2 port is available for the users living in Europe and using Vigor 2910VGi only. For other V models, only the status for VoIP1 and VoIP2 will be shown in this page.

Status	<p>It shows the VoIP connection status.</p> <p>IDLE - Indicates that the VoIP function is idle.</p> <p>HANG_UP - Indicates that the connection is not established (busy tone).</p> <p>CONNECTING - Indicates that the user is calling out.</p> <p>WAIT_ANS - Indicates that a connection is launched and waiting for remote user's answer.</p> <p>ALERTING - Indicates that a call is coming.</p> <p>ACTIVE-Indicates that the VoIP connection is launched.</p>
Codec	Indicates the voice codec employed by present channel.
PeerID	The present in-call or out-call peer ID (the format may be IP or Domain).
Connect Time	The format is represented as seconds.
Tx Pkts	Total number of transmitted voice packets during this connection session.
Rx Pkts	Total number of received voice packets during this connection session.
Rx Losses	Total number of lost packets during this connection session.
Rx Jitter	The jitter of received voice packets.
In Calls	The accumulating in-call times.
Out Calls	The accumulating out-call times.
Speaker Gain	The volume of present call.
Log	Display logs of VoIP calls.

3.12 ISDN

ISDN means integrated services digital network that is an international communications standard for sending voice, video, and data over digital telephone lines or normal telephone wires.

Below shows the menu items of ISDN for *i* models.



3.12.1 General Setup

This page provides some basic ISDN settings such as enabling the ISDN port or not, MSN numbers and blocked MSN numbers, etc.

ISDN Setup

ISDN Port <input checked="" type="radio"/> Enable <input type="radio"/> Disable Country Code <input type="text" value="International"/> Own Number <input type="text"/> "Own Number" means that the router will tell the remote end the ISDN number when it's placing an outgoing call.		Blocked MSN numbers for the router 1. <input type="text"/> 2. <input type="text"/> 3. <input type="text"/> 4. <input type="text"/> 5. <input type="text"/>
Index 1. 2. 3.	MSN numbers for the router <input type="text"/> <input type="text"/> <input type="text"/>	Mapping to VoIP Ports: <input type="checkbox"/> FXS1 <input type="checkbox"/> FXS2 <input type="checkbox"/> FXS1 <input type="checkbox"/> FXS2 <input type="checkbox"/> FXS1 <input type="checkbox"/> FXS2

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

OK

Cancel

ISDN Port

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

Country Code

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

Own Number

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

Blocked MSN Numbers for the router

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

MSN Numbers for the Router

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

Mapping to VoIP Ports

Check to specify ringing from **FXS1** and/or **FXS2** when the router accepts the incoming calls by identifying MSN number(s). If you do not specify any port in this field, the ISDN loop through ring port will be determined by the configuration in **ISDN port** in **VoIP>>Phone Settings**.

3.12.2 Dialing to a Single ISP

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

[ISDN >> Dialing to a Single ISP](#)

Single ISP

ISP Access Setup	PPP/MP Setup
ISP Name <input type="text" value="prima"/>	Link Type <input type="text" value="Dialup BOD"/>
Dial Number <input type="text" value="9834737"/>	PPP Authentication <input type="text" value="PAP or CHAP"/>
Username <input type="text" value="amor"/>	Idle Timeout <input type="text" value="180"/> second(s)
Password <input type="password" value="•••••"/>	IP Address Assignment Method (IPCP)
<input type="checkbox"/> Require ISP callback (CBCP)	Fixed IP <input type="radio"/> Yes <input checked="" type="radio"/> No (Dynamic IP)
Index(1-15) in Schedule Setup: => <input type="text"/> , <input type="text"/> , <input type="text"/> , <input type="text"/>	Fixed IP Address <input type="text"/>

OK

- ISP Name** Enter your ISP name.
- Dial Number** Enter the ISDN access number provided by your ISP.
- Username** Enter the username provided by your ISP.
- Password** Enter the password provided by your ISP.
- Require ISP Callback (CBCP)** If your ISP supports the callback function, check this box to activate the Callback Control Protocol during the PPP negotiation.
- Scheduler (1-15)** Enter the index of schedule profiles to control the Internet access according to the preconfigured schedules.
- Link Type** There are four link types: Link Disable, Dialup 64 Kbps, Dialup 128 Kbps, and Dialup BOD.
Link Disable - Disable the ISDN dial-out function.
Dialup 64Kbps - Use one ISDN B channel for Internet access.
Dialup 128Kbps - Use both ISDN B channels for Internet access.
Dialup BOD - BOD stands for bandwidth-on-demand. The router will use only one B channel in low traffic situations. Once the single B channel bandwidth is fully used, the other B channel will be activated automatically through the dialup. For more detailed BOD parameter settings, please refer to the **Advanced Setup** field > **Call Control and PPP/MP Setup**.
- PPP Authentication** **PAP Only** - Configure the PPP session to use the PAP protocol to negotiate the username and password with the ISP.
PAP or CHAP - Configure the PPP session to use the PAP or CHAP protocols to negotiate the username and password with the ISP.
- Idle Timeout** Idle timeout means the router will be disconnect after being idle for a preset amount of time. The default is 180 seconds. If you set the time to 0, the ISDN connection to the ISP will always remain on.
- Fixed IP** In most environments, you should not change these settings as most ISPs provide a dynamic IP address for the router when it connects to the ISP. If your ISP provides a fixed IP address, check

Yes to invoke this function and enter the IP address in the field of **Fixed IP Address**.

Fixed IP Address Type the IP address.

3.12.3 Dialing to Dual ISPs

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

[ISDN >> Dialing to Dual ISPs](#)

Dual ISP

Common Settings 1. <input checked="" type="checkbox"/> Enable Dual ISPs Function 2. <input type="checkbox"/> Require ISP callback (CBCP)	PPP/MP Setup Link Type <input type="text" value="Dialup BOD"/> PPP Authentication <input type="text" value="PAP or CHAP"/> Idle Timeout <input type="text" value="180"/> second(s)
Primary ISP Setup ISP Name <input type="text" value="prima"/> Dial Number <input type="text" value="9834737"/> Username <input type="text" value="amor"/> Password <input type="password" value="•••••"/> IP Address Assignment Method (IPCP) Fixed IP <input type="radio"/> Yes <input checked="" type="radio"/> No (Dynamic IP) Fixed IP Address <input type="text"/>	Secondary ISP Setup ISP Name <input type="text" value="dingo"/> Dial Number <input type="text" value="8849343"/> Username <input type="text" value="amor"/> Password <input type="password" value="•••••"/> IP Address Assignment Method (IPCP) Fixed IP <input type="radio"/> Yes <input checked="" type="radio"/> No (Dynamic IP) Fixed IP Address <input type="text"/>

OK

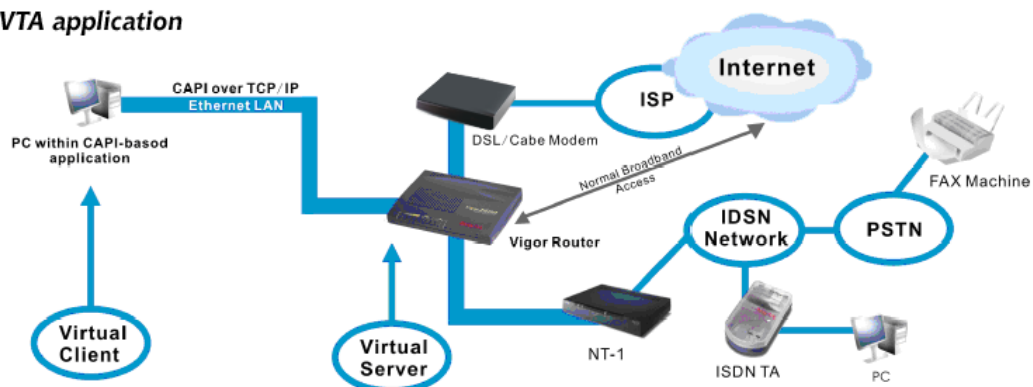
Most configuration parameters are the same as those of the previous part. This screen provides a checkbox to enable the Dual ISPs function and adds the secondary ISP Setup section field. Check the corresponding box and enter the second ISP information. About the details please refer to the descriptions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

3.12.4 Virtual TA

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

- The Virtual TA client only supports Microsoft™ Windows 98/SE/2000/XP platforms.
- The Virtual TA client only supports the CAPI 2.0 protocol and has no built-in FAX engine.
- One ISDN BRI interface has two B channels. The maximum number of active clients is also two.
- Before you configure the Virtual TA, you must set the correct country code.

VTA application



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

Before describing the configuration of Virtual TA in the Vigor routers, please heed the following limitations.

- The Virtual TA client only supports Microsoft™ Windows 98/SE/2000/XP platforms.
- The Virtual TA client only supports the CAPI 2.0 protocol and has no built-in FAX engine.
- One ISDN BRI interface has two B channels. The maximum number of active clients is also 2.
- Before you configure the Virtual TA, you must set the correct country code in **ISDN Setup**.

ISDN >> Virtual TA

Virtual TA Setup

Virtual TA Server : ☒ Enable ☐ Disable

Virtual TA Users Profiles						
	Username	Password	MSN1	MSN2	MSN3	Active
1.	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
2.	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
3.	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
4.	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
5.	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>

OK

Virtual TA Server

Enable: Select it to activate the server.

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

Virtual TA User Profiles

Username - Enter the username of a specific client.

Password - Enter the password of a specific client.

MSN 1/2/3 - MSN stands for Multiple Subscriber Number. It means you can apply to more than one ISDN lines number over a single subscribed line. Note that the service must be acquired from your telecom. Specify the MSN numbers for a specific client. If you have no MSN services, leave this field blank.

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

Install a Virtual TA Client

1. Insert the CD-ROM bundled with your Vigor router. Find **VTA Client** tool in the Utility menu and click on the Install button.
2. Follow the on-screen instructions of the installer. The last step will ask you to restart your computer. Click **OK** to restart your computer.
3. After the computer restarts, you will see a VT icon in the taskbar (usually in the bottom-right of the screen, near the clock) as shown below.

When the icon text is GREEN, the Virtual TA client is connected to the Virtual TA server and you can launch your CAPI-based software to use the client to access the router. If the icon text is RED, it means the client has lost the connection to the server. This time, please check the physical Ethernet connection.



Configure a Virtual TA Client/ Server

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

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

User Profile

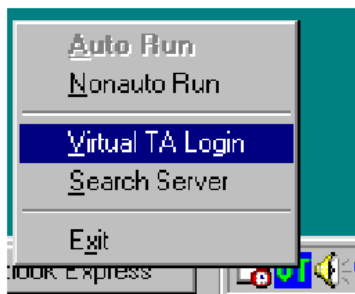
Note that creating a single user access account will limit the access to the Virtual TA server to only the specified account holders.

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

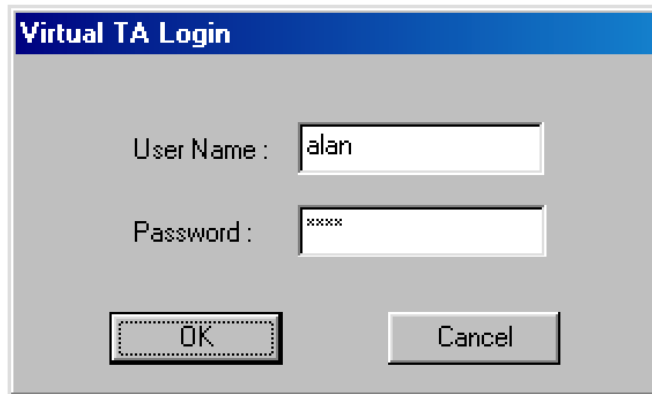
On the server - Click **Virtual TA (Remote CAPI) Setup** link, and fill in the Username and Password fields. Check the **Active** box to enable the account.



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



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



A dialog box titled "Virtual TA Login" with a blue header. It contains two input fields: "User Name :" with the text "alan" and "Password :" with the text "xxxx". Below the fields are two buttons: "OK" and "Cancel".

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

MSN Configuration

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

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



	Username	Password	MSN1	MSN2	MSN3	Active
1.	alan	123			<input checked="" type="checkbox"/>
2.						<input type="checkbox"/>

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

3.12.5 Call Control

Some applications require that the router (only for the ISDN models) be remotely activated, or be able to dial up to the ISP via the ISDN interface. Vigor routers provide this feature by allowing user to make a phone call to the router and then ask it to dial up to the ISP.

Accordingly, a teleworker can access the remote network to retrieve resources. Of course, a fixed IP address is required for WAN connection and some internal network resource has to be exposed for remote users, such as FTP, WWW. Please set **Dialing to a Single ISP** first before configuring this web page.

ISDN >> Call Control

Call Control Setup

Dial Retry	<input type="text" value="0"/> times	Remote Activation 1.	<input type="text"/>
Dial Delay Interval	<input type="text" value="0"/> second(s)	2.	<input type="text"/>
		3.	<input type="text"/>
		4.	<input type="text"/>
		5.	<input type="text"/>

PPP/MP Dial-Out Setup

Basic Setup		Bandwidth On Demand (BOD) Setup	
Link Type	<input type="text" value="Dialup BOD"/>	High Water Mark	<input type="text" value="7000"/> cps
PPP Authentication	<input type="text" value="PAP or CHAP"/>	High Water Time	<input type="text" value="30"/> second(s)
TCP Header Compression	<input type="text" value="None"/>	Low Water Mark	<input type="text" value="6000"/> cps
Idle Timeout	<input type="text" value="180"/> second(s)	Low Water Time	<input type="text" value="30"/> second(s)

OK

Dial Retry

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

Dial Delay Interval

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

Remote Activation

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

Link Type

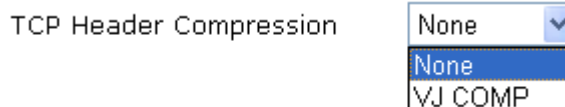
Because ISDN has two B channels (64Kbps/per channel), you can specify whether you would like to have single B channel, two B channels or BOD (Bandwidth on Demand). Four options are available: Link Disable, Dialup 64Kbps, Dialup 128Kbps, Dialup BOD.

Link Type

<input type="text" value="Dialup BOD"/>
Link Disable
Dialup 64Kbps
Dialup 128Kbps
Dialup BOD

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

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



Idle Timeout Because our ISDN link type is “Dial On Demand”, the connection will be initiated only when needed.

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

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

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

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

3.13 Wireless LAN

This function is used for G models only.

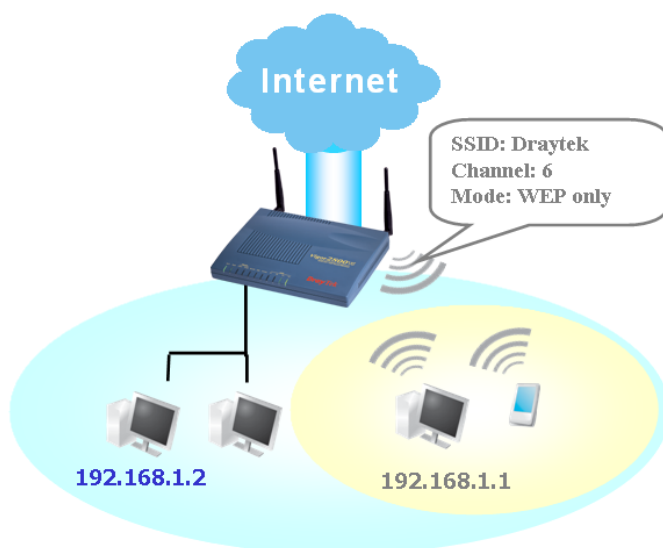
3.13.1 Basic Concepts

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

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

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

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



Security Overview

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

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

WEP (Wired Equivalent Privacy) is a legacy method to encrypt each frame transmitted via radio using either a 64-bit 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.

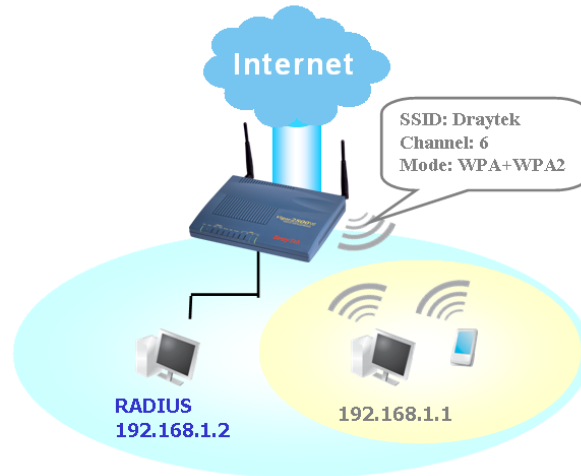
Example 1



Example 2



Example 3



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

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

Below shows the menu items for Wireless LAN.



3.13.2 General Settings

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

Wireless LAN >> General Setup

General Setting (IEEE 802.11)

☒ Enable Wireless LAN

Mode : Mixed(11b+11g)

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

SSID : default

Channel : Channel 6, 2437MHz

Note: If SuperG mode is enabled, channel is fixed at 6.

☐ Hide SSID

☐ Long Preamble

Hide SSID : prevent SSID from being scanned.

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

OK Cancel

Enable Wireless LAN

Check the box to enable wireless function.

Mode

Select an appropriate wireless mode.

Mixed (11b+11g+SuperG) - The radio can support IEEE802.11b, IEEE802.11g and SuperG protocols simultaneously.

Mixed (11b+11g) - The radio can support both IEEE802.11b and IEEE802.11g protocols simultaneously.

SuperG - The radio only supports SuperG.

11g only - The radio only supports IEEE802.11g.

11b only - The radio only supports IEEE802.11b.

Mode : Mixed(11b+11g)

- Mixed(11b+11g+SuperG)
- Mixed(11b+11g)
- SuperG Only
- 11g Only
- 11b Only

Index(1-15)

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

SSID

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

Channel

The channel of frequency of the wireless LAN. The default channel is 6. You may switch channel if the

selected channel is under serious interference.

Channel :

Channel 6, 2437MHz	▼
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	

Hide SSID

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

Long Preamble

This option is to define the length of the sync field in 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.

3.13.3 Security

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

Wireless LAN >> Security Settings

Security Settings

Mode : WEP Only

Set up **RADIUS Server** if 802.1x is enabled.

WPA:

Type: ☒ Mixed(WPA+WPA2) ☐ WPA2 Only

Pre-Shared Key(PSK)

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

WEP:

Encryption Mode: 64-Bit

Use WEP Key

☐ Key 1 :

☒ Key 2 :

☐ Key 3 :

☐ Key 4 :

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

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

OK Cancel

Mode

There are several modes provided for you to choose.

Mode :

- WEP Only
- Disable
- WEP Only
- WEP/802.1x Only
- WEP or WPA/PSK
- WEP/802.1x or WPA/802.1x
- WPA/PSK Only
- WPA/802.1x Only

Disable - Turn off the encryption mechanism.

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

WEP/802.1x Only - Accept WEP clients with 802.1x authentication. Since the key will be auto-negotiated during authentication, the field of key setting below will be not available for input.

WEP or WPA/PSK - Accepts WEP and WPA clients with legal key accordingly. Only Mixed (WPA+WPA2) is applicable if you select WPA/PSK.

WEP/802.1x or WPA/802.1x - Accept WEP or WPA clients with 802.1x authentication. Only Mixed(WPA+WPA2) is applicable if you select WPA/PSK. Since the key will be auto-negotiated during authentication, the field of key setting below will be not available for input.

WPA/PSK Only - Accepts WPA clients and the encryption key should be entered in PSK. Remember to select WPA type to define either Mixed or WPA2 only in the field below.

WPA/802.1x Only - Accept WPA clients with 802.1x authentication. Remember to select WPA type to define

either Mixed or WPA2 only in the field below. Since the key will be auto-negotiated during authentication, the field of key setting below will be not available for input.

WPA

The WPA encrypts each frame transmitted from the radio using the key, which either PSK entered manually in this field below or automatically negotiated via 802.1x authentication.

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

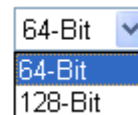
Pre-Shared Key (PSK) - Either **8~63** ASCII characters, such as 012345678...(or 64 Hexadecimal digits leading by 0x, such as "0x321253abcde...").

WEP

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

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

Encryption Mode:



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.

3.13.4 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 | [Set to Factory Default](#)

☒ Enable Access Control

Policy : Activate MAC address filter

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 Access Control

Select to enable the MAC Address access control feature.

Policy

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

Policy : Activate MAC address filter

- Activate MAC address filter
- Isolate WLAN from LAN

MAC Address Filter

Display all MAC addresses that are edited before. Four buttons (Add, Remove, **Client's MAC Address** - Manually enter the MAC address of wireless client.

Attribute

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

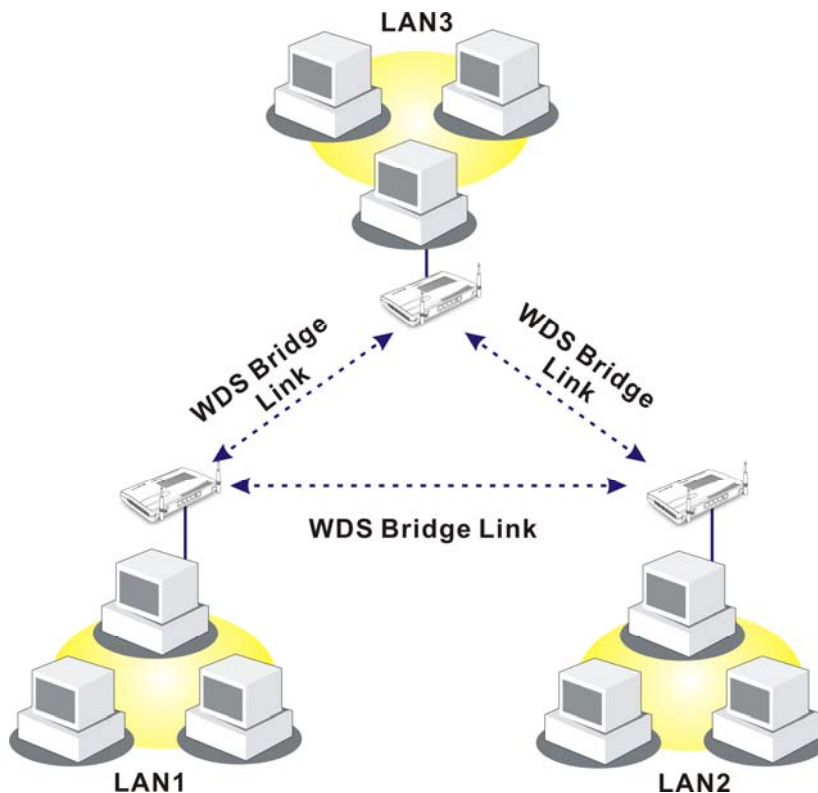
Clean all entries in the MAC address list.

3.13.5 WDS

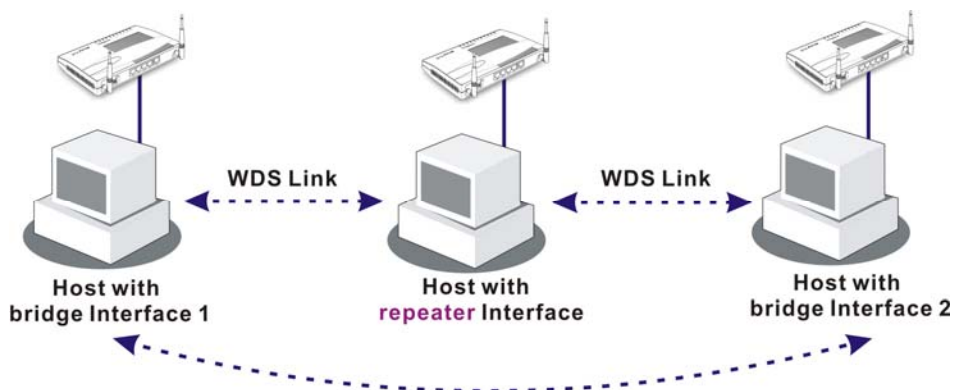
WDS means Wireless Distribution System. It is a protocol for connecting two access points (AP) wirelessly. Usually, it can be used for the following application:

- Provide bridge traffic between two LANs through the air.
- Extend the coverage range of a WLAN.

To meet the above requirement, two WDS modes are implemented in Vigor router. One is **Bridge**, the other is **Repeater**. Below shows the function of WDS-bridge interface:

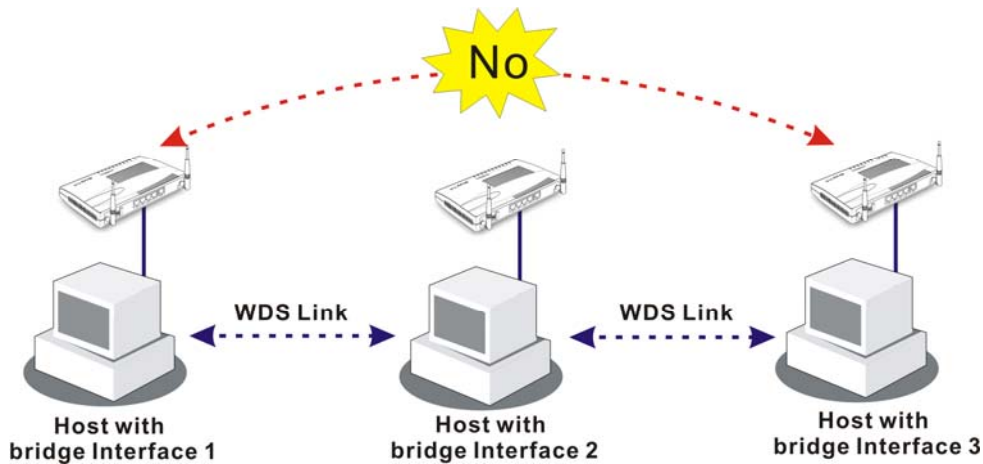


The application for the WDS-Repeater mode is depicted as below:



The major difference between these two modes is that: while in **Repeater** mode, the packets received from one peer AP can be repeated to another peer AP through WDS links. Yet in **Bridge** mode, packets received from a WDS link will only be forwarded to local wired or wireless hosts. In other words, only Repeater mode can do WDS-to-WDS packet forwarding.

In the following examples, hosts connected to Bridge 1 or 3 can communicate with hosts connected to Bridge 2 through WDS links. However, hosts connected to Bridge 1 CANNOT communicate with hosts connected to Bridge 3 through Bridge 2.



Click **WDS** from **Wireless LAN** menu. The following page will be shown.

Wireless LAN >> WDS Settings

WDS Settings
[Set to Factory Default](#)

<p>Mode: Disable</p> <hr/> <p>Security:</p> <p> <input checked="" type="radio"/> Disable <input type="radio"/> WEP <input type="radio"/> Pre-shared Key </p> <hr/> <p>WEP:</p> <p> <input type="checkbox"/> Use the same WEP key set in Security Settings. </p> <p> Encryption Mode : 64-bit Key index : 1 </p> <p><small>The key index is fixed if the security mode is not "WEP Only".</small></p> <p> Key : ***** </p> <p><small>The key format is the same as the one used in Security Settings.</small></p> <hr/> <p>Pre-shared Key:</p> <p> Type : TKIP Key : ***** </p> <p><small>Type 8~63 ASCII characters or 64 hexadecimal digits leading by "0x", for example "cfgs01a2..." or "0x655abcd....".</small></p>	<p>Bridge</p> <p>Enable <input type="checkbox"/> Peer MAC Address</p> <table border="1" style="width: 100%; border-collapse: collapse;"> <tr><td><input type="checkbox"/></td><td>:</td><td>:</td><td>:</td><td>:</td><td>:</td></tr> <tr><td><input type="checkbox"/></td><td>:</td><td>:</td><td>:</td><td>:</td><td>:</td></tr> <tr><td><input type="checkbox"/></td><td>:</td><td>:</td><td>:</td><td>:</td><td>:</td></tr> <tr><td><input type="checkbox"/></td><td>:</td><td>:</td><td>:</td><td>:</td><td>:</td></tr> <tr><td><input type="checkbox"/></td><td>:</td><td>:</td><td>:</td><td>:</td><td>:</td></tr> <tr><td><input type="checkbox"/></td><td>:</td><td>:</td><td>:</td><td>:</td><td>:</td></tr> </table> <p><small>Note: Disable unused links to get better performance.</small></p> <hr/> <p>Repeater</p> <p>Enable <input type="checkbox"/> Peer MAC Address</p> <table border="1" style="width: 100%; border-collapse: collapse;"> <tr><td><input type="checkbox"/></td><td>:</td><td>:</td><td>:</td><td>:</td><td>:</td></tr> <tr><td><input type="checkbox"/></td><td>:</td><td>:</td><td>:</td><td>:</td><td>:</td></tr> </table> <hr/> <p>Access Point Function:</p> <p> <input checked="" type="radio"/> Enable <input type="radio"/> Disable </p> <hr/> <p>Status:</p> <p><input type="checkbox"/> Send "Hello" message to peers.</p> <p style="text-align: center;">Link Status</p> <p><small>Note: The status is valid only when the peer also supports this function.</small></p>	<input type="checkbox"/>	:	:	:	:	:	<input type="checkbox"/>	:	:	:	:	:	<input type="checkbox"/>	:	:	:	:	:	<input type="checkbox"/>	:	:	:	:	:	<input type="checkbox"/>	:	:	:	:	:	<input type="checkbox"/>	:	:	:	:	:	<input type="checkbox"/>	:	:	:	:	:	<input type="checkbox"/>	:	:	:	:	:
<input type="checkbox"/>	:	:	:	:	:																																												
<input type="checkbox"/>	:	:	:	:	:																																												
<input type="checkbox"/>	:	:	:	:	:																																												
<input type="checkbox"/>	:	:	:	:	:																																												
<input type="checkbox"/>	:	:	:	:	:																																												
<input type="checkbox"/>	:	:	:	:	:																																												
<input type="checkbox"/>	:	:	:	:	:																																												
<input type="checkbox"/>	:	:	:	:	:																																												

OK
Clear
Cancel

Mode

Choose the mode for WDS setting. **Disable** mode will not invoke any WDS setting. **Bridge** mode is designed to fulfill the first type of application. **Repeater** mode is for the second one.

Mode:

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.
Settings	<p>Encryption Mode - If you checked the box of Use the same WEP key ..., you do not need to choose 64-bit or 128-bit as the Encryption Mode. If you do not check that box, you can set the WEP key now in this page.</p> <p>Key Index - Choose the key that you want to use after selecting the proper encryption mode.</p> <p>Key - Type the content for the key.</p>
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. Six 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. Two 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.

3.13.6 AP Discovery

Vigor router can scan all regulatory channels and find working APs in the neighborhood. Based on the scanning result, users will know which channel is clean for usage. Also, it can be used to facilitate finding an AP for a WDS link. Notice that during the scanning process (about 5 seconds), no client is allowed to connect to Vigor.

This page is used to scan the existence of the APs on the wireless LAN. Yet, only the AP which is in the same channel of this router can be found. Please click **Scan** to discover all the connected APs.

Access Point List

BSSID	Channel	SSID

See [Statistics](#).

Note: During the scanning process (~5 seconds), no station is allowed to connect with the router.

Add to [WDS Settings](#) :

AP's MAC address : : : : :

☒ Bridge ☐ Repeater

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.

3.13.7 Station List

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

Station List

Status	MAC Address
--------	-------------

Refresh

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

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

Add to **Access Control** :

Client's MAC address : : : : :

Add

Refresh

Click this button to refresh the status of station list.

Add

Click this button to add current selected MAC address into **Access Control**.

3.13.8 Station Rate Control

This page allows you to control the upload and download rate of each wireless client (station). Please check the box of **Enable** to invoke this setting. The range for the rate is between 100 ~ 30,000 kbps.

Wireless LAN >> Station Rate Control

Station Rate Control

☒ Enable

Upload Rate : 00 Kbps

Download Rate : 00 Kbps

Note:
1. Range: 100~30,000 Kbps, Increment: 100 Kbps.
2. The specified rates are applied to each associated wireless client.

OK

Cancel

3.14 VLAN

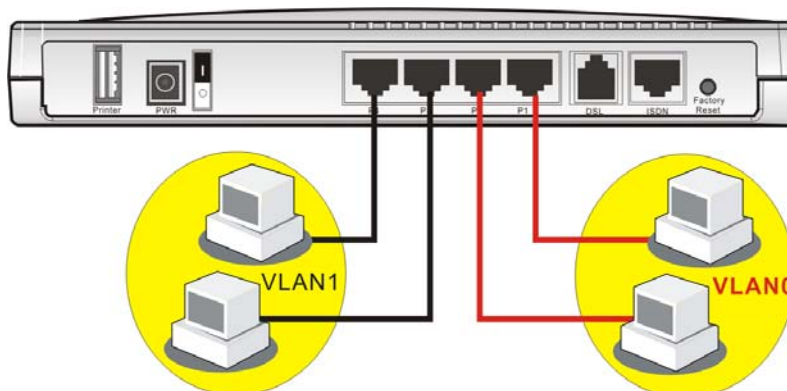
Virtual LAN function provides you a very convenient way to manage hosts by grouping them based on the physical port.

VLAN

- ▶ Wired VLAN
- ▶ Wireless VLAN
- ▶ VLAN Cross Setup
- ▶ Wireless Rate Control

3.14.1 Wired VLAN

PCs connected to Ethernet ports of the router can be divided into different groups and formed VLAN. PCs under the same groups can share each other information through the router and will not be peeked by other groups.



The **VLAN >> Wired VALN** allows you to configure VLAN settings through wired connection to achieve the above intention. Simply check P1 and P2 boxes on the line of VLAN0; and check P3 and P4 boxes on the line of VLAN1.

VLAN >> Wired VLAN Configuration

Wired VLAN Configuration

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

OK Clear Cancel

Enable

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

P1 – P4

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

VLAN0-3

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

Note: If WAN2 interface has been enabled, the P1 boxes will serve as WAN interface and cannot be checked as shown in the following diagram.

Wired VLAN Configuration

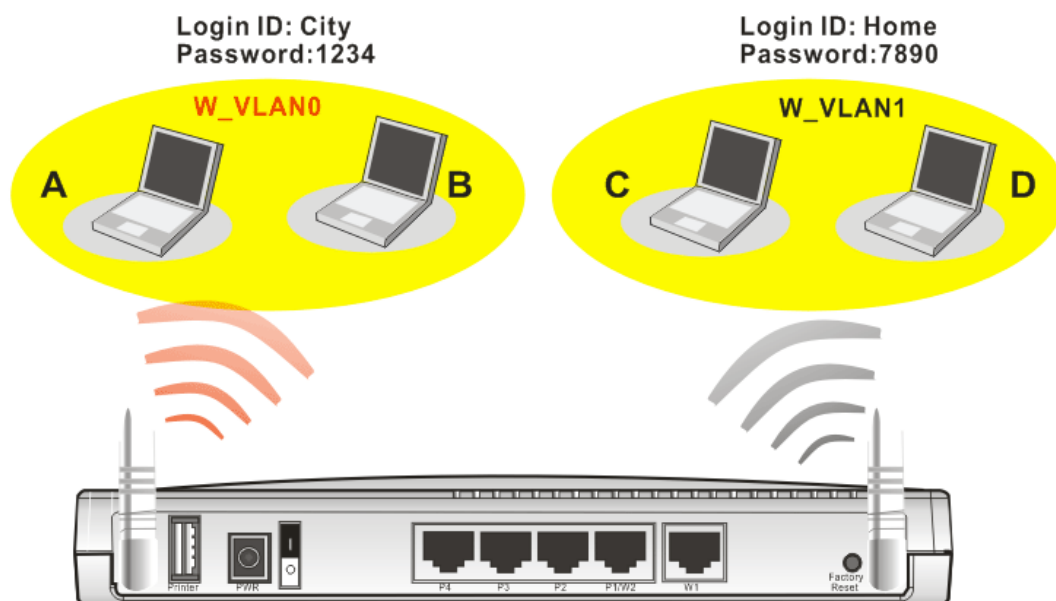
<input checked="" type="checkbox"/> Enable				
	P1	P2	P3	P4
VLAN0	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
VLAN1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
VLAN2	<input type="checkbox"/>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

OK Clear Cancel

3.14.2 Wireless VLAN

PCs (equipped with wireless network cards) connected to the router through wireless interface can be divided into different groups and formed W_VLAN. PCs under the same groups can share each other information through the router and will not be peeked by other groups.

PCs under the same groups can use same Login ID and password to access into Internet. For example, see the following graphic. Both A and B use the same login ID (City) and password (1234). Therefore, they are grouped in the same W_VLAN.



The **VLAN >> Wireless VLAN** allows you to configure Wireless VLAN settings through wireless connection to achieve the above intention. Simply type Login ID and password with **City** and **1234** in the boxes of W_VLAN0. And type Login ID and password with **Home** and **7890** in the boxes of W_VLAN1. Users can configure fifteen groups of wireless VLAN in this page.

VLAN >> Wireless VLAN Setup

Wireless VLAN Configuration

☒ Enable View [Online Station Table](#)

W_VLAN	Login ID	Password	Attributes	W_VLAN	Login ID	Password	Attributes
0	City	1234	Details	8			Details
1	Home	7890	Details	9			Details
2			Details	10			Details
3			Details	11			Details
4			Details	12			Details
5			Details	13			Details
6			Details	14			Details
7			Details	15			Details

☐ Disable broadcast and multicast traffic.

Notes:
 1. Login ID: 1~11 characters, Password: 1~11 characters.
 2. Disable broadcast and multicast traffic to maximize wireless VLAN security; however, the WLAN throughput will be reduced.
 3. Login URL for wireless clients:
<http://www.draytek.vlan/login.htm> or [http://\(Vigor IP Address\)/login.htm](http://(Vigor IP Address)/login.htm)

OK

Cancel

Enable

Check this box to invoke wireless VLAN function.

Login ID

Type Login ID for different groups of W_VLAN with 1 to 11 characters.

Password

Type password for different groups of W_VLAN with 1 to 11 characters.

Details

Click this button to set additional attributes settings for W_VLAN.

W_VLAN0 Attributes

Activated Date:	2006	1	1
Expired Date:	2010	1	1
<input checked="" type="checkbox"/> Connect all WDS links with this VLAN group.			
<input checked="" type="checkbox"/> Isolate each member in this VLAN group.			

OK

Cancel

Activated Date – Use the drop down lists to set the activated date for the wireless VLAN. The wireless VLAN function will be available when the time is arrival.

Expired Date – Use the drop down lists to set the expired date for the wireless VLAN. This function will be invalid when the time is arrival.

Connect all WDS links with this VLAN group – Check this box to activate this connection.

Isolate each member in this VLAN group – Check this box to isolate all the members in this VLAN group and not allow the information sharing among them.

Disable broadcast and multicast traffic

Check this box to prevent broadcast and multicast traffic forwarding to all W_VLAN.

How can you (wireless client) access into Internet?

After finishing the configuration of wireless VLAN, the wireless clients connecting to this router must do the following steps to access into Internet.

1. Open a browser and type <http://www.draytek.vlan/login.htm> or [http://\(vigor router's IP address\)/login.htm](http://(vigor router's IP address)/login.htm) on the address line.
2. The following screen will appear.

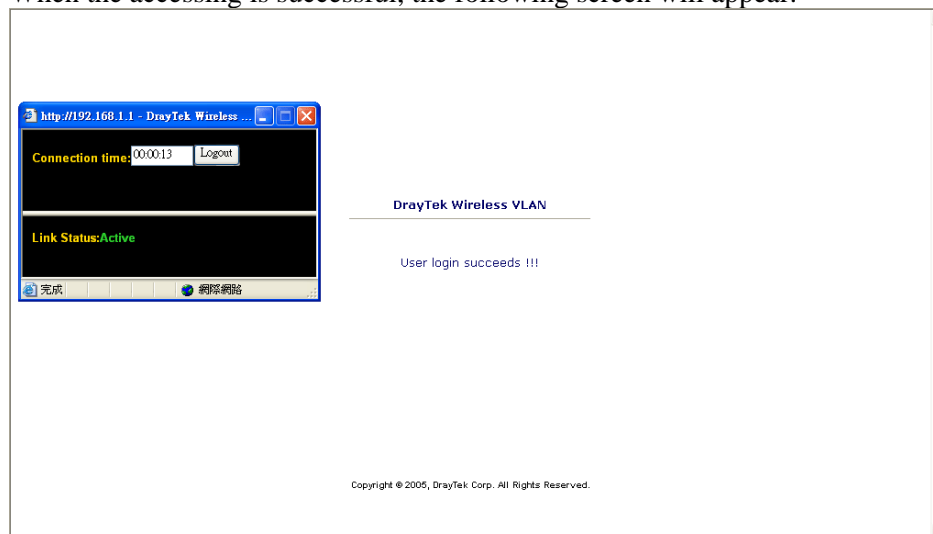
DrayTek Wireless VLAN

Login ID	City
Password	•••••

OK

3. Type in Login ID and Password that was configured in Wireless VLAN Setup page. In this case, we choose the configuration set in first group of W_VLAN (City and 1234).

4. When the accessing is successful, the following screen will appear.



Note: The floating window with connection time will be shown on the screen till you logout.

5. You can go to **Diagnostics>>Wireless VLAN Online Station Table** for viewing the connection status whenever you want.

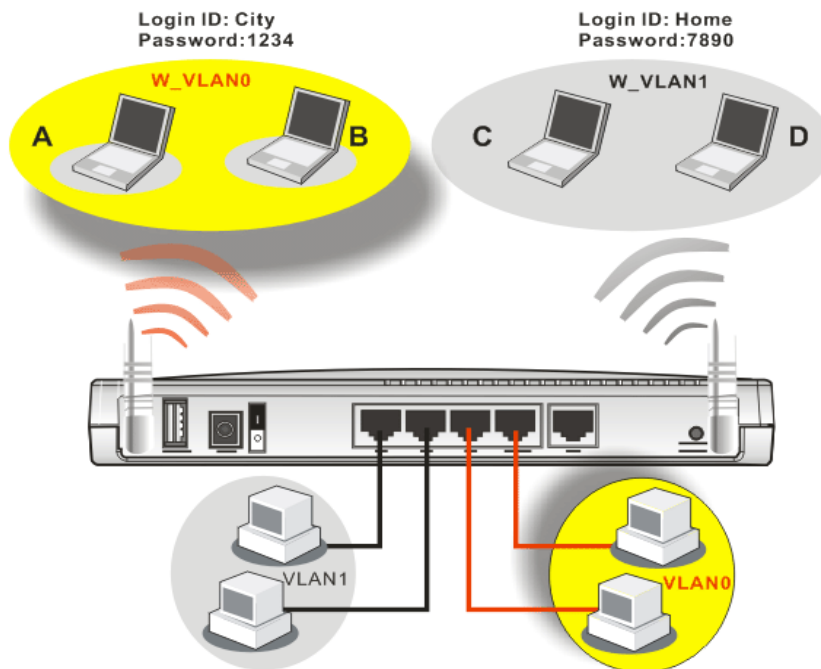
Diagnostics >> Wireless VLAN Online Station

Wireless VLAN Online Station Table | [Refresh](#)

IP Address	MAC Address	Login ID
192.168.1.15	00-14-85-26-00-8C	City
192.168.1.16	00-0E-35-A8-A4-E7	Home

3.14.3 VLAN Cross Setup

This function allows the router to integrate VLAN and W_VLAN for managing different computers (notebooks). See the following picture for an example. With **VLAN Cross Setup**, notebook A/B and PCs on VLAN0 can share resources without difficulty.



The **VLAN >> VALN Cross Setup** allows you to set a communication bridge between computers in Wireless VLAN and wired VLAN. To achieve the intention of the above illustration, simply check the box under VLAN0 on the line of W_VLAN0.

VLAN >> VLAN Cross Setup

VLAN Cross Configuration

<input checked="" type="checkbox"/> Enable				
	VLAN0	VLAN1	VLAN2	VLAN3
W_VLAN0	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
W_VLAN1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
W_VLAN2	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
W_VLAN3	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
W_VLAN4	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
W_VLAN5	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
W_VLAN6	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
W_VLAN7	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
W_VLAN8	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
W_VLAN9	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
W_VLAN10	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
W_VLAN11	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
W_VLAN12	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
W_VLAN13	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
W_VLAN14	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
W_VLAN15	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
WDS	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Notes:

1. W_VLANi: wireless VLAN i, see **Wireless VLAN Setup** for details.
2. All WDS links belong to the same VLAN group.
3. VLANi: wired VLAN i, see **Wired VLAN Setup** for details.
4. Both wired and wireless VLANs must be enabled for VLAN cross settings to be effective.

OK

Cancel

Enable	Check this box to invoke VLAN Cross Setup function.
VLAN0-3	It represents the groups of virtual LAN connected by Ethernet interface.
W_VLAN0-15	It represents the groups of wireless VLAN communicated by wireless interface.

3.14.4 Wireless Rate Control

Rate Control manages the transmission rate of data in and out through the router. You can also manage the in/out rate of each wireless VLAN. Go to **VLAN** menu and select **Wireless Rate Control**. The following page will appear. Click **Enable** to invoke VLAN function.

For the rate control of wireless connection, please open VLAN menu and choose **Wireless Rate Control**. The following page will be shown for you to adjust.

VLAN >> Wireless VLAN Rate Control

Wireless VLAN Rate Control

☒ Enable

Range : 100~30,000 Kbps, Increment : 100 Kbps

W_VLAN	Upload Rate (Kbps)	Download Rate (Kbps)	W_VLAN	Upload Rate (Kbps)	Download Rate (Kbps)
0	300 00	300 00	8	300 00	300 00
1	300 00	300 00	9	300 00	300 00
2	300 00	300 00	10	300 00	300 00
3	300 00	300 00	11	300 00	300 00
4	300 00	300 00	12	300 00	300 00
5	300 00	300 00	13	300 00	300 00
6	300 00	300 00	14	300 00	300 00
7	300 00	300 00	15	300 00	300 00

Note: Specified rate is an aggregate rate for the VLAN group.

OK

Cancel

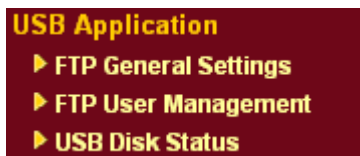
Enable Check this box to enable this function (for Rate Control). The rate control will limit the transmission rate for upload and download.

Upload Rate It decides the rate of data transmission for output. The default setting is 300. The range must be between 100 kbps to 20,000kbps. Adjust the values according to your necessity.

Download Rate It decides the rate of data transmission for input. The default setting is 300. The range must be between 100 kbps to 20,000kbps. Adjust the values according to your necessity.

3.15 USB Application

USB diskette can be regarded as an FTP server. By way of Vigor router, clients on LAN can access, write and read data stored in USB diskette. After setting the configuration in **USB Application**, you can type the IP address of the Vigor router and username/password created in **USB Application>>FTP User Management** on the FTP client software. Thus, the client can use the FTP site (USB diskette) through Vigor router.



3.15.1 FTP General Settings

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

USB Application >> FTP General Settings

FTP General Settings

Concurrent FTP Connection	<input type="text" value="5"/> (Maximum 6)
Default Charset	<input type="button" value="Default"/> ▼

Note: If charset is set to "default", only long file name (in English) will be supported.

Concurrent FTP Connection

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

Default Charset

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

Default ▼
Default
GB2312
BIG5

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

3.15.2 FTP User Management

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

FTP User Management

[Set to Factory Default](#)

Index	Username	Home Folder	Index	Username	Home Folder
1.			9.		
2.			10.		
3.			11.		
4.			12.		
5.			13.		
6.			14.		
7.			15.		
8.			16.		

Click index number to access into configuration page.

USB Application >> FTP User Management

Profile Index: 1

FTP User	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Username	<input type="text" value="carrie"/>
Password	<input type="password" value="•••••"/>
Confirm Password	<input type="password" value="•••••"/>
Home Folder	<input type="text" value="temp_storag"/>
Access Rule	
File	<input type="checkbox"/> Read <input type="checkbox"/> Write <input type="checkbox"/> Delete
Directory	<input type="checkbox"/> List <input type="checkbox"/> Create <input type="checkbox"/> Remove

Note: The folder name can only contain the following characters: A-Z a-z 0-9 \$ % ' - _ @ ~ ` ! () \ and space.

FTP User

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

Disable – Click this button to disable such profile.

Username

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

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

Password

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

Confirm Password

Type the password again to make confirmation.

Home Folder

It determines the range for the client to access into. The user can enter a directory name in this field. Then,

after clicking OK, the router will create the specific/new folder in the USB diskette. In addition, if the user types “/” here, he/she can access into all of the disk folders and files in USB diskette.

Note: When write protect status for the USB diskette is **ON**, you cannot type any new folder name in this field. Only “/” can be used in such case.

Access Rule

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

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

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

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

3.15.3 USB Disk Status

This page is to monitor the status for the FTP users who accessing into FTP server (USB diskette) via the Vigor router.

[USB Application >> USB Disk Status](#)

USB Mass Storage Device Status

Connection Status: **No Disk Connected**

[Disconnect USB Disk](#)

Disk Capacity: 0 MB

Free Capacity: 0 MB [Refresh](#)

FTP User Connected

[Refresh](#)

Index	Username	IP Address
1.		
2.		
3.		
4.		
5.		
6.		

Note: If the write protect switch of USB disk is turned on, the USB disk is in **READ-ONLY** mode. No data can be written to it.

Connection Status

If there is no USB diskette connected to Vigor router, “**No Disk Connected**” will be shown here.

Disk Capacity

It displays the total capacity of the USB diskette.

Free Capacity

It displays the free space of the USB diskette. Click **Refresh** at any time to get new status for free capacity.

Username

It displays the username that user uses to login to the FTP server.

IP Address

It displays the IP address of the user’s host which connecting to the FTP server.

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

Once the USB diskette has been found, the connection status will display “**Disk Connected**” and the web page will be shown as follows:

USB Application >> USB Disk Status

USB Mass Storage Device Status

Connection Status: **Disk Connected** Disconnect USB Disk

Write Protect Status: **No**

Disk Capacity: 1967 MB

Free Capacity: 1610 MB [Refresh](#)

FTP User Connected | [Refresh](#) |

Index	Username	IP Address
1.		
2.		
3.		
4.		
5.		
6.		

Note: If the write protect switch of USB disk is turned on, the USB disk is in **READ-ONLY** mode. No data can be written to it.

3.16 System Maintenance

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

Below shows the menu items for System Maintenance.



3.16.1 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 : DrayTek Vigor2910
Firmware Version : 3.2.1_RC2
Build Date/Time : Tue Jul 29 18:35:51.48 2008

System	
CPU Usage	: 2 %
Total Memory	: 16M
Memory usage	: 60 %

LAN	
MAC Address	: 00-50-7F-DD-15-18
1st IP Address	: 192.168.1.1
1st Subnet Mask	: 255.255.255.0
DHCP Server	: Yes
Primary DNS	:
Secondary DNS	:

VoIP	
Port	: 1 2
SIP registrar	:
Account ID	: change_me change_me
Register	:
Codec	:
In Calls	: 0 0
Out Calls	: 0 0

WAN 1	
Link Status	: Connected
MAC Address	: 00-50-7F-DD-15-19
Connection	: Static IP
IP Address	: 172.16.3.229
Default Gateway	: 172.16.3.4
Primary DNS	:
Secondary DNS	:

WAN 2	
Link Status	: Disconnected
MAC Address	: 00-50-7F-DD-15-1A
Connection	: ---
IP Address	: ---
Default Gateway	: ---
Primary DNS	:
Secondary DNS	:

Wireless LAN	
MAC Address	: 00-14-85-08-69-19
Frequency Domain	: Europe
Firmware Version	: v2.01.10.10.5.4

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.
MAC Address	Display the MAC address of the LAN Interface.
1st IP Address	Display the IP address of the LAN interface.
1st Subnet Mask	Display the subnet mask address of the LAN interface.
DHCP Server	Display the current status of DHCP server of the LAN interface.
MAC Address	Display the MAC address of the WAN Interface.
IP Address	Display the IP address of the WAN interface.
Default Gateway	Display the assigned IP address of the default gateway.
DNS	Display the assigned IP address of the primary DNS.
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 card.

3.16.2 TR-069 Setting

Vigor router with TR-069 is available for matching with VigorACS server. Such page provides VigorACS and CPE settings under TR-069 protocol. All the settings configured here is for CPE to be controlled and managed with VigorACS server. Users need to type URL, username and password for the VigorACS server that such device will be connected. However URL, username and password under CPE client are fixed that users cannot change

it. The default CPE username and password are "vigor" and "password". You will need it when you configure VigorACS server.

System Maintenance >> TR-069 Setting

ACS and CPE Settings

ACS Server	
URL	<input type="text"/>
Username	<input type="text"/>
Password	<input type="password"/>
CPE Client	
<input checked="" type="radio"/> Enable <input type="radio"/> Disable	
URL	<input type="text" value="http://172.16.3.229:8069/cwm/CRN.html"/>
Port	<input type="text" value="8069"/>
Username	<input type="text" value="vigor"/>
Password	<input type="password" value="password"/>

Periodic Inform Settings

<input type="radio"/> Disable <input checked="" type="radio"/> Enable	
Interval Time	<input type="text" value="900"/> second(s)

OK

ACS Server

Such data must be typed according to the ACS (Auto Configuration Server) you want to link. Please refer to VigorACS user's manual for detailed information.

URL - Type the URL for VigorACS server.

If the connected CPE needs to be authenticated, please set URL as the following and type username and password for VigorACS server:

http://{IP address of VigorACS}:8080/ACSServer/services/ACSServlet

If the connected CPE does not need to be authenticated please set URL as the following:

http://{IP address of VigorACS}:8080/ACSServer/services/UnAuthACSServlet

Username/Password - Type username and password for ACS Server for authentication. For example, if you want to use such CPE with VigorACS, you can type as the following:

Username: *acs*

Password: *password*

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

Disable – The system will not send inform message to ACS server.

Enable – The system will send inform message to ACS server periodically (with the time set in the box of interval time).

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.

3.16.3 Administrator Password

This page allows you to set new password.

System Maintenance >> Administrator Password Setup

Administrator Password

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

Old Password

Type in the old password. The factory default setting for password is blank.

New Password

Type in new password in this field.

Confirm New 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.

3.16.4 Configuration Backup

Backup the Configuration

Follow the steps below to backup your configuration.

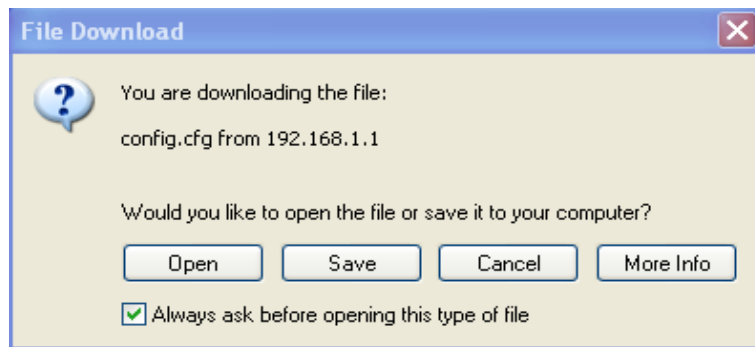
1. Go to **System Maintenance >> Configuration Backup**. The following windows will be popped-up, as shown below.

System Maintenance >> Configuration Backup

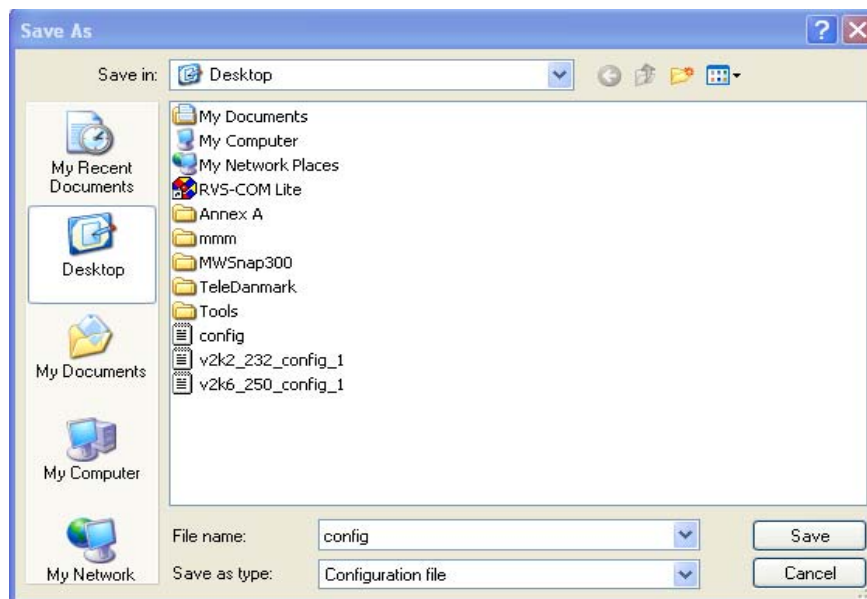
Configuration Backup / Restoration

Restoration	
Select a configuration file.	
<input type="text"/>	<input type="button" value="Browse.."/>
Click Restore to upload the file.	
<input type="button" value="Restore"/>	
Backup	
Click Backup to download current running configurations as a file.	
<input type="button" value="Backup"/>	<input type="button" value="Cancel"/>

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



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



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

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

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

Restore Configuration

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

Configuration Backup / Restoration

Restoration	
Select a configuration file.	<input type="text"/> <input type="button" value="Browse.."/>
Click Restore to upload the file.	<input type="button" value="Restore"/>
Backup	
Click Backup to download current running configurations as a file.	<input type="button" value="Backup"/> <input type="button" value="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.

3.16.5 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.

SysLog / Mail Alert Setup

SysLog Access Setup <input checked="" type="checkbox"/> Enable Router Name <input type="text"/> Server IP Address <input type="text"/> Destination Port <input type="text" value="514"/> Enable syslog message: <input checked="" type="checkbox"/> Firewall Log <input checked="" type="checkbox"/> VPN Log <input checked="" type="checkbox"/> User Access Log <input checked="" type="checkbox"/> Call Log <input checked="" type="checkbox"/> WAN Log <input checked="" type="checkbox"/> Router/DSL information	Mail Alert Setup <input type="checkbox"/> Enable SMTP Server <input type="text"/> Mail To <input type="text"/> Return-Path <input type="text"/> <input type="checkbox"/> Authentication User Name <input type="text"/> Password <input type="text"/>
--	--

Enable

Click "**Enable**" to activate this function.

Router Name

Assign a name for the router.

Server IP

The IP address of the Syslog server.

Destination Port

Assign a port for the Syslog protocol.

Enable syslog message

Check the box listed on this web page to send the corresponding message of firewall, VPN, User Access, Call, WAN, Router/DSL information to Syslog.

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.

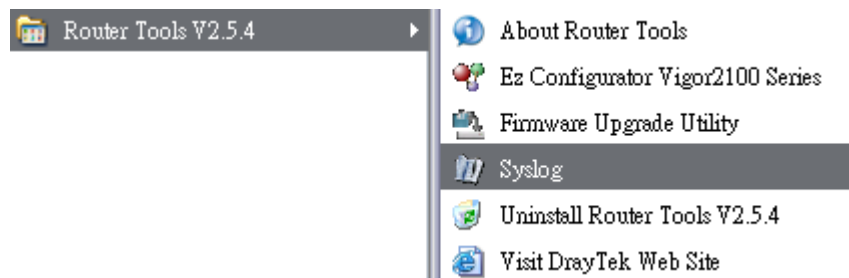
Password

Type the password for authentication.

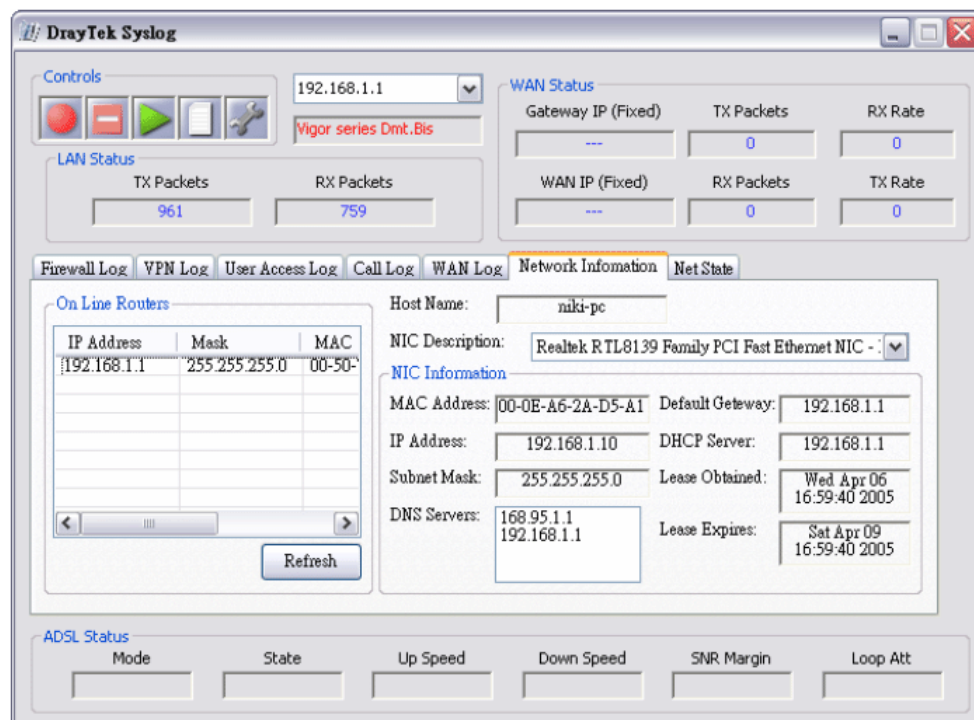
Click **OK** to save these settings.

For viewing the Syslog, please do the following:

1. Just set your monitor PC's IP address in the field of Server IP Address
2. Install the Router Tools in the **Utility** within provided CD. After installation, click on the **Router Tools>>Syslog** from program menu.



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



3.16.6 Time and Date

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

System Maintenance >> Time and Date

Time Information

Current System Time	2006 Jun 12 Mon 8 : 45 : 0	Inquire Time
---------------------	----------------------------	--------------

Time Setup

<input type="radio"/> Use Browser Time	
<input checked="" type="radio"/> 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	<input type="checkbox"/>
Automatically Update Interval	30 min ▼

OK	Cancel
----	--------

Current System Time

Click **Inquire Time** to get the current time.

Use Browser Time

Select this option to use the browser time from the remote administrator PC host as router's system time.

Use Internet Time

Select to inquire time information from Time Server on the Internet using assigned protocol.

Time Protocol

Select a time protocol.

Server IP Address

Type the IP address of the time server.

Time Zone

Select the time zone where the router is located.

Enable Daylight Saving

Such function is useful for some area.

Automatically Update Interval

Select a time interval for updating from the NTP server.

Click **OK** to save these settings.

3.16.7 Management

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

System Maintenance >> Management

Management Setup

Management Access Control <input checked="" type="checkbox"/> Allow management from the Internet <input type="checkbox"/> FTP Server <input checked="" type="checkbox"/> HTTP Server <input checked="" type="checkbox"/> HTTPS Server <input checked="" type="checkbox"/> Telnet Server <input type="checkbox"/> SSH Server <input checked="" type="checkbox"/> Disable PING from the Internet	Management Port Setup <input checked="" type="radio"/> User Define Ports <input type="radio"/> Default Ports Telnet Port <input type="text" value="23"/> (Default: 23) HTTP Port <input type="text" value="80"/> (Default: 80) HTTPS Port <input type="text" value="443"/> (Default: 443) FTP Port <input type="text" value="21"/> (Default: 21) SSH Port <input type="text" value="22"/> (Default: 22)
Access List List IP Subnet Mask 1 <input type="text"/> <input type="text"/> 2 <input type="text"/> <input type="text"/> 3 <input type="text"/> <input type="text"/>	SNMP Setup <input type="checkbox"/> Enable SNMP Agent Get Community <input type="text" value="public"/> Set Community <input type="text" value="private"/> Manager Host IP <input type="text"/> Trap Community <input type="text" value="public"/> Notification Host IP <input type="text"/> Trap Timeout <input type="text" value="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.

User Defined Ports

Check to specify user-defined port numbers for the Telnet and HTTP servers.

Default Ports

Check to use standard port numbers for the Telnet and HTTP servers.

Enable SNMP Agent

Check it to enable this function.

Get Community

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

Set Community	Set community by typing a proper name. The default setting is private .
Manager Host IP	Set one host as the manager to execute SNMP function. Please type in IP address to specify certain host.
Trap Community	Set trap community by typing a proper name. The default setting is public .
Notification Host IP	Set the IP address of the host that will receive the trap community.
Trap Timeout	The default setting is 10 seconds.

3.16.8 Reboot System

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

System Maintenance >> Reboot System

Reboot System

Do You want to reboot your router ?

☒ Using current configuration
☐ Using factory default configuration

OK

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

3.16.9 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](ftp://ftp.draytek.com).

Click **System Maintenance>> Firmware Upgrade** to launch the Firmware Upgrade Utility.

System Maintenance >> Firmware Upgrade

Web Firmware Upgrade

Select a firmware file.

Click Upgrade to upload the file.

TFTP Firmware Upgrade from LAN

Current Firmware Version: 3.2.1_RC2

Firmware Upgrade Procedures:

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

Do you want to upgrade firmware ?

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

System Maintenance >> Firmware Upgrade



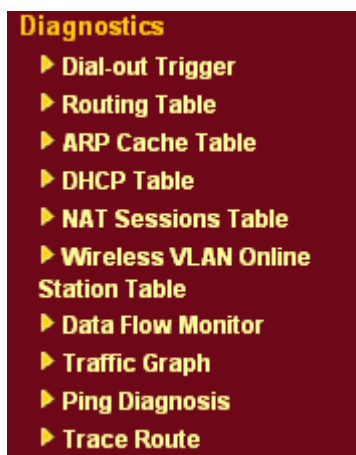
TFTP server is running. Please execute a Firmware Upgrade Utility software to upgrade router's firmware. This server will be closed by itself when the firmware upgrading finished.

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

3.17 Diagnostics

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

Below shows the menu items for Diagnostics.



3.17.1 Dial-out Trigger

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

Diagnostics >> Dial-out Trigger

Dial-out Triggered Packet Header

| [Refresh](#) |

HEX Format:

00 00 00 00 00 00-00 00 00 00 00 00-00 00

00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00

Decoded Format:

0.0.0.0 -> 0.0.0.0
Pr 0 len 0 (0)

Decoded Format

It shows the source IP address (local), destination IP (remote) address, the protocol and length of the package.

Refresh

Click it to reload the page.

3.17.2 Routing Table

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

[Diagnostics >> View Routing Table](#)

Current Running Routing Table

| [Refresh](#) |

Key: C - connected, S - static, R - RIP, * - default, ~ - private			
*	0.0.0.0/	0.0.0.0 via 172.16.3.1,	WAN1
C~	192.168.1.0/	255.255.255.0 is directly connected,	LAN
C	172.16.3.0/	255.255.255.0 is directly connected,	WAN1

Refresh

Click it to reload the page.

3.17.3 ARP Cache Table

Click **Diagnostics** and click **ARP Cache Table** to view the content of the ARP (Address Resolution Protocol) cache held in the router. The table shows a mapping between an Ethernet hardware address (MAC Address) and an IP address.

[Diagnostics >> View ARP Cache Table](#)

Ethernet ARP Cache Table

| [Clear](#) | [Refresh](#) |

IP Address	MAC Address
192.168.1.10	00-0E-A6-2A-D5-A1
172.16.3.112	00-40-CA-6B-56-BA
172.16.3.132	00-05-5D-E4-ED-86
172.16.3.20	00-0D-60-6F-83-BC
172.16.3.121	00-0C-6E-E7-79-99
172.16.3.141	00-11-2F-C7-39-0B
172.16.3.133	00-50-7F-23-4D-B1
172.16.3.179	00-11-2F-4B-15-F2
172.16.3.21	00-05-5D-A1-2B-FF
172.16.3.2	00-11-D8-68-0D-AE
172.16.3.18	00-50-FC-2F-3D-17
172.16.3.151	00-50-7F-2F-33-FF
172.16.3.19	00-0D-60-6F-89-CA

Refresh

Click it to reload the page.

Clear

Click it to clear the whole table.

3.17.4 DHCP Table

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

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

[Diagnostics >> View DHCP Assigned IP Addresses](#)

DHCP IP Assignment Table					Refresh
DHCP server: Running					
Index	IP Address	MAC Address	Leased Time	HOST ID	
1	192.168.1.10	00-0E-A6-2A-D5-A1	0:00:02.630	ok-lccgjyiy075u	

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

3.17.5 NAT Sessions Table

Click **Diagnostics** and click **NAT Sessions Table** to open the setup page.

[Diagnostics >> NAT Sessions Table](#)

NAT Active Sessions Table							Refresh
Private IP	:Port	#Pseudo Port	Peer IP	:Port	Interface		
192.168.1.11	2491	52078	24.9.93.189	443	WAN1		
192.168.1.11	2493	52080	207.46.25.2	80	WAN1		
192.168.1.10	3079	52665	207.46.5.10	80	WAN1		

Private IP:Port	It indicates the source IP address and port of local PC.
#Pseudo Port	It indicates the temporary port of the router used for NAT.

Peer IP:Port	It indicates the destination IP address and port of remote host.
Interface	It indicates the interface of the WAN connection.
Refresh	Click it to reload the page.

3.17.6 Wireless VLAN Online Station Table

Click **Diagnostics** and click **Wireless VLAN Online Station Table** to open the web page. It will display the IP address, MAC address and Login ID information for all the Wireless VLAN stations.

[Diagnostics >> Wireless VLAN Online Station](#)

Wireless VLAN Online Station Table			Refresh
IP Address	MAC Address	Login ID	
192.168.1.15	00-14-85-26-00-8C	City	
192.168.1.16	00-0E-35-A8-A4-E7	Home	

IP Address	Display the IP address of the wireless station.
MAC Address	Display the MAC address of the wireless station.
Login ID	Display the login ID that the wireless station belongs to.

3.17.7 Data Flow Monitor

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

[Bandwidth Management >> Sessions Limit](#)

Sessions Limit

☒ **Enable**
☐ **Disable**

Default Max Sessions:

Limitation List

Index	Start IP	End

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

☐ Enable Data Flow Monitor

Refresh Seconds: 10 Page: 1

[Refresh](#)

Index	IP Address	TX rate(Kbps)	RX rate(Kbps)	Sessions	Action
		Current / Peak / Speed	Current / Peak / Speed	Current / Peak	
WAN1	172.16.3.229	1 / 10 / Auto	2 / 59 / Auto	---	
WAN2	---	0 / 0 / Auto	0 / 0 / Auto	---	
Total		1 / 10 / Auto	2 / 59 / Auto	4 / 80	

Note: 1. Click "Block" to prevent specified PC from surfing Internet for 5 minutes.
 2. The IP blocked by the router will be shown in red, and the session column will display the remaining time that the specified IP will be blocked.
 3. (Kbps): shared bandwidth
 Current/Peak are average.

Enable Data Flow Monitor

Refresh Seconds

Check this box to enable this function.

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

Refresh

Click this link to refresh this page manually.

Index

Display the number of the data flow.

IP Address

Display the IP address of the monitored device.

TX rate (kbps)

Display the transmission speed of the monitored device.

RX rate (kbps)

Display the receiving speed of the monitored device.

Sessions

Display the session number that you specified in Limit Session web page.

Action

Block - can prevent specified PC accessing into Internet within 5 minutes.
 Page: 1 [Refresh](#)

Sessions	Action
1 / 100	Block

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

Page: 1 | [Refresh](#)

Sessions	Action
blocked / 299	Unblock

Current /Peak/Speed

Current means current transmission rate and receiving rate for WAN1/WAN.

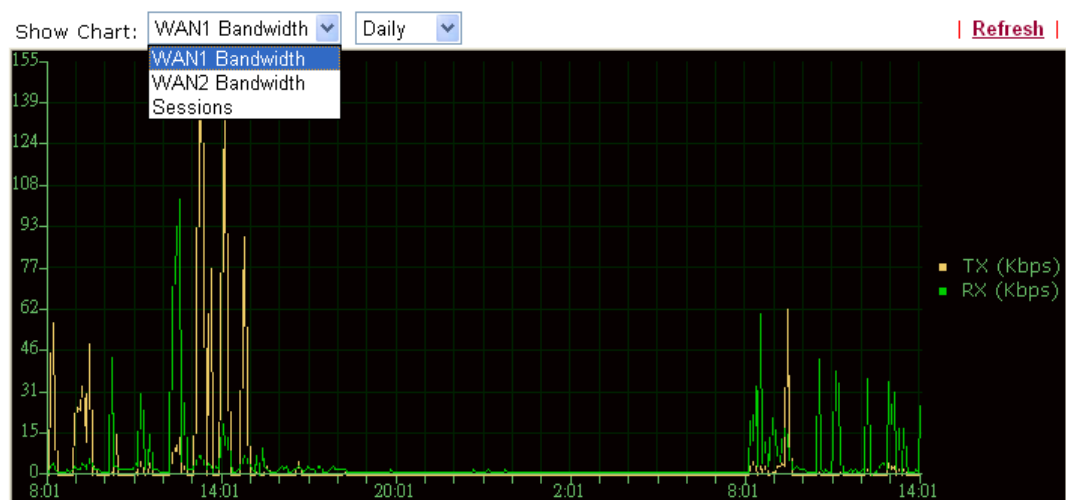
Peak means the highest peak value detected by the router in data transmission.

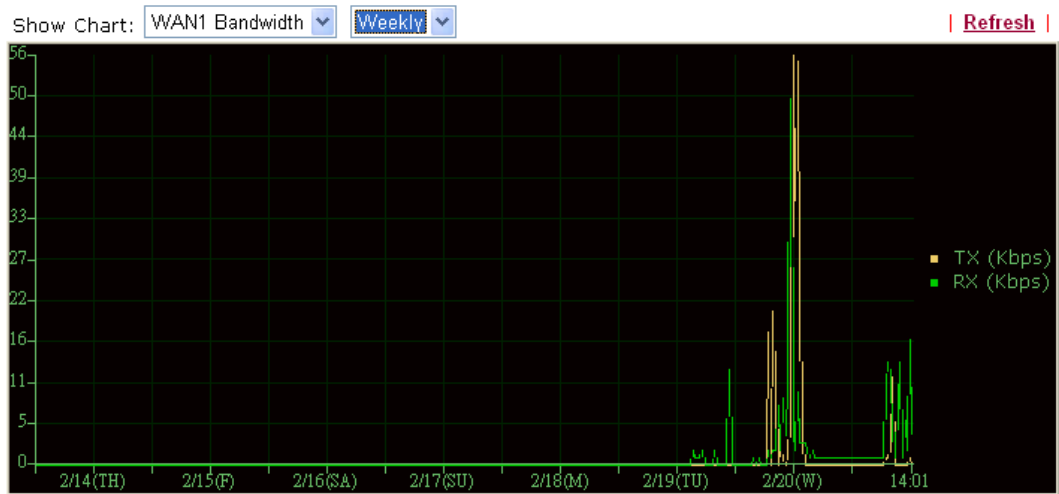
Speed means line speed specified in **WAN>>General**. If you do not specify any rate at that page, here will display **Auto** for instead.

3.17.8 Traffic Graph

Click **Diagnostics** and click **Traffic Graph** to pen the web page. Choose WAN1 Bandwidth/WAN2 Bandwidth, Sessions, daily or weekly for viewing different traffic graph. Click **Refresh** to renew the graph at any time. The following two figures display different charts by daily and weekly.

[Diagnostics >> Traffic Graph](#)





The horizontal axis represents time. Yet the vertical axis has different meanings. For WAN1/WAN2 Bandwidth chart, the numbers displayed on vertical axis represent the numbers of the transmitted and received packets in the past.

For Sessions chart, the numbers displayed on vertical axis represent the numbers of the NAT sessions during the past.

3.17.9 Ping Diagnosis

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

[Diagnostics >> Ping Diagnosis](#)

Ping Diagnosis

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

Ping through:

Ping to: IP Address:

Result [Clear](#)

GateWay1
GateWay2
DNS

Ping through

Use the drop down list to choose the WAN interface that you want to ping through or choose **Unspecified** to be determined by the router automatically.

Ping through:

WAN1
WAN2

Ping to

Use the drop down list to choose the destination that you would like 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.

3.17.10 Trace Route

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

Trace Route

Trace through:

WAN1

Host / IP Address:

Run

Result

| [Clear](#) |

Trace through WAN1.
tracert to 172.16.3.229, 30 hops max
1 Request timed out. *
2 Request timed out. *
Trace complete.

Ping through

Use the drop down list to choose the WAN interface that you want to ping through or choose **Unspecified** to be determined by the router automatically.

Host/IP Address

It indicates the IP address of the host.

Run

Click this button to start route tracing work.

Clear

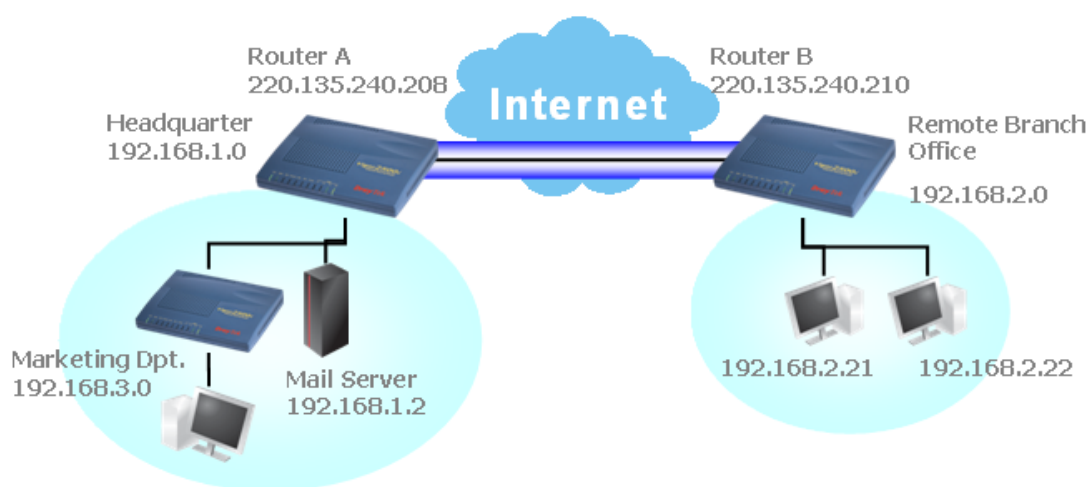
Click this link to remove the result on the window.

This page is left blank.

4 Application and Examples

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

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



Settings in Router A in headquarter:

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

VPN and Remote Access >> PPP General Setup

PPP General Setup	
PPP/MP Protocol	IP Address Assignment for Dial-In Users
Dial-In PPP Authentication	Start IP Address
<div>PAP or CHAP</div>	<div>192.168.1.200</div>
Dial-In PPP Encryption (MPPE)	
<div>Optional MPPE</div>	
Mutual Authentication (PAP)	
<div><input type="radio"/> Yes <input checked="" type="radio"/> No</div>	
Username	
Password	
<div>OK</div>	

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

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

VPN and Remote Access >> IPSec General Setup

VPN IKE/IPSec General Setup

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

IKE Authentication Method	
Pre-Shared Key
Confirm Pre-Shared Key
IPSec Security Method	
<input checked="" type="checkbox"/> Medium (AH)	
Data will be authentic, but will not be encrypted.	
High (ESP)	<input checked="" type="checkbox"/> DES <input checked="" type="checkbox"/> 3DES <input checked="" type="checkbox"/> AES
Data will be encrypted and authentic.	

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

Profile Index : 1

1. Common Settings

Profile Name <input type="text" value="Branch1"/> <input type="checkbox"/> Enable this profile VPN Connection Through: <input type="text" value="WAN1 First"/>	Call Direction <input checked="" type="radio"/> Both <input type="radio"/> Dial-Out <input type="radio"/> Dial-In <input type="checkbox"/> Always on Idle Timeout <input type="text" value="300"/> second(s) <input type="checkbox"/> Enable PING to keep alive PING to the IP <input type="text"/>
Netbios Naming Packet <input checked="" type="radio"/> Pass <input type="radio"/> Block Multicast via VPN <input type="radio"/> Pass <input checked="" type="radio"/> Block (for some IGMP,IP-Camera,DHCP Relay..etc.)	

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

2. Dial-Out Settings

Type of Server I am calling <input type="radio"/> ISDN <input type="radio"/> PPTP <input checked="" type="radio"/> IPSec Tunnel <input type="radio"/> L2TP with IPSec Policy None		Link Type 64k bps Username ??? Password PPP Authentication PAP/CHAP VJ Compression <input checked="" type="radio"/> On <input type="radio"/> Off
Dial Number for ISDN or Server IP/Host Name for VPN. (such as 5551234, draytek.com or 123.45.67.89) <input type="text" value="220.135.240.210"/>		IKE Authentication Method <input checked="" type="radio"/> Pre-Shared Key IKE Pre-Shared Key ***** <input type="radio"/> Digital Signature(X.509) None
		IPSec Security Method <input checked="" type="radio"/> Medium(AH) <input type="radio"/> High(ESP) DES without Authentication <input type="button" value="Advanced"/>
		Index(1-15) in Schedule Setup: <input type="text"/> <input type="text"/> <input type="text"/> <input type="text"/>
		Callback Function (CBCP) <input type="checkbox"/> Require Remote to Callback <input type="checkbox"/> Provide ISDN Number to Remote

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

2. Dial-Out Settings

Type of Server I am calling <input type="radio"/> ISDN <input checked="" type="radio"/> PPTP <input type="radio"/> IPSec Tunnel <input type="radio"/> L2TP with IPSec Policy None		Link Type 64k bps Username draytek Password ***** PPP Authentication PAP/CHAP VJ Compression <input checked="" type="radio"/> On <input type="radio"/> Off
Dial Number for ISDN or Server IP/Host Name for VPN. (such as 5551234, draytek.com or 123.45.67.89) <input type="text" value="220.135.240.210"/>		IKE Authentication Method <input checked="" type="radio"/> Pre-Shared Key IKE Pre-Shared Key ***** <input type="radio"/> Digital Signature(X.509) None
		IPSec Security Method <input checked="" type="radio"/> Medium(AH) <input type="radio"/> High(ESP) DES without Authentication <input type="button" value="Advanced"/>
		Index(1-15) in Schedule Setup: <input type="text"/> <input type="text"/> <input type="text"/> <input type="text"/>
		Callback Function (CBCP) <input type="checkbox"/> Require Remote to Callback <input type="checkbox"/> Provide ISDN Number to Remote

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

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

3. Dial-In Settings

Allowed Dial-In Type <input type="checkbox"/> ISDN <input type="checkbox"/> PPTP <input checked="" type="checkbox"/> IPSec Tunnel <input type="checkbox"/> L2TP with IPSec Policy None		Username <input type="text" value="???"/> Password <input type="password"/> VJ Compression <input checked="" type="radio"/> On <input type="radio"/> Off
<input checked="" type="checkbox"/> Specify ISDN CLID or Remote VPN Gateway Peer ISDN Number or Peer VPN Server IP <input type="text" value="220.135.240.210"/> or Peer ID <input type="text"/>		IKE Authentication Method <input checked="" type="checkbox"/> Pre-Shared Key <input type="button" value="IKE Pre-Shared Key"/> <input type="text"/> <input type="checkbox"/> Digital Signature(X.509) None
		IPSec Security Method <input checked="" type="checkbox"/> Medium (AH) High (ESP) <input checked="" type="checkbox"/> DES <input checked="" type="checkbox"/> 3DES <input checked="" type="checkbox"/> AES
		Callback Function (CBCP) <input type="checkbox"/> Enable Callback Function <input type="checkbox"/> Use the Following Number to Callback Callback Number <input type="text"/> Callback Budget <input type="text" value="0"/> minute(s)

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

3. Dial-In Settings

Allowed Dial-In Type <input type="checkbox"/> ISDN <input checked="" type="checkbox"/> PPTP <input type="checkbox"/> IPSec Tunnel <input type="checkbox"/> L2TP with IPSec Policy None		Username <input type="text" value="draytek"/> Password <input type="password" value="*****"/> VJ Compression <input checked="" type="radio"/> On <input type="radio"/> Off
<input checked="" type="checkbox"/> Specify ISDN CLID or Remote VPN Gateway Peer ISDN Number or Peer VPN Server IP <input type="text" value="220.135.240.210"/> or Peer ID <input type="text"/>		IKE Authentication Method <input checked="" type="checkbox"/> Pre-Shared Key <input type="button" value="IKE Pre-Shared Key"/> <input type="text"/> <input type="checkbox"/> Digital Signature(X.509) None
		IPSec Security Method <input checked="" type="checkbox"/> Medium (AH) High (ESP) <input checked="" type="checkbox"/> DES <input checked="" type="checkbox"/> 3DES <input checked="" type="checkbox"/> AES
		Callback Function (CBCP) <input type="checkbox"/> Enable Callback Function <input type="checkbox"/> Use the Following Number to Callback Callback Number <input type="text"/> Callback Budget <input type="text" value="0"/> minute(s)

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

4. TCP/IP Network Settings

My WAN IP	<input type="text" value="0.0.0.0"/>	RIP Direction	Disable
Remote Gateway IP	<input type="text" value="0.0.0.0"/>	From first subnet to remote network, you have to do	
Remote Network IP	<input type="text" value="192.168.2.0"/>	Route	
Remote Network Mask	<input type="text" value="255.255.255.0"/>		
<input type="button" value="More"/>		<input type="checkbox"/> Change default route to this VPN tunnel (Only single WAN supports this)	

Settings in Router B in the remote office:

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

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

VPN and Remote Access >> PPP General Setup

PPP General Setup	
PPP/MP Protocol Dial-In PPP Authentication: PAP or CHAP Dial-In PPP Encryption (MPPE): Optional MPPE Mutual Authentication (PAP): <input type="radio"/> Yes <input checked="" type="radio"/> No Username: <input type="text"/> Password: <input type="text"/>	IP Address Assignment for Dial-In Users Start IP Address: 192.168.2.200

OK

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

VPN and Remote Access >> IPSec General Setup

VPN IKE/IPSec General Setup	
Dial-in Set up for Remote Dial-in users and Dynamic IP Client (LAN to LAN).	
IKE Authentication Method Pre-Shared Key: <input type="text"/> Confirm Pre-Shared Key: <input type="text"/>	
IPSec Security Method <input checked="" type="checkbox"/> Medium (AH) Data will be authentic, but will not be encrypted. High (ESP): <input checked="" type="checkbox"/> DES <input checked="" type="checkbox"/> 3DES <input checked="" type="checkbox"/> AES Data will be encrypted and authentic.	

OK Cancel

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

Profile Index : 1	
1. Common Settings	
Profile Name: Branch1 <input type="checkbox"/> Enable this profile VPN Connection Through: WAN1 First Netbios Naming Packet: <input checked="" type="radio"/> Pass <input type="radio"/> Block Multicast via VPN: <input type="radio"/> Pass <input checked="" type="radio"/> Block (for some IGMP, IP-Camera, DHCP Relay..etc.)	Call Direction: <input checked="" type="radio"/> Both <input type="radio"/> Dial-Out <input type="radio"/> Dial-In <input type="checkbox"/> Always on Idle Timeout: 300 second(s) <input type="checkbox"/> Enable PING to keep alive PING to the IP: <input type="text"/>

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

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

connection.

2. Dial-Out Settings

Type of Server I am calling <input type="radio"/> ISDN <input type="radio"/> PPTP <input checked="" type="radio"/> IPsec Tunnel <input type="radio"/> L2TP with IPsec Policy None		Link Type 64k bps Username ??? Password PPP Authentication PAP/CHAP VJ Compression <input checked="" type="radio"/> On <input type="radio"/> Off
Dial Number for ISDN or Server IP/Host Name for VPN. (such as 5551234, draytek.com or 123.45.67.89) <input type="text" value="220.135.240.208"/>		IKE Authentication Method <input checked="" type="radio"/> Pre-Shared Key IKE Pre-Shared Key ***** <input type="radio"/> Digital Signature(X.509) None
		IPsec Security Method <input checked="" type="radio"/> Medium(AH) <input type="radio"/> High(ESP) DES without Authentication <input type="button" value="Advanced"/>
		Index(1-15) in Schedule Setup: <input type="text"/> , <input type="text"/> , <input type="text"/> , <input type="text"/>
		Callback Function (CBCP) <input type="checkbox"/> Require Remote to Callback <input type="checkbox"/> Provide ISDN Number to Remote

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

2. Dial-Out Settings

Type of Server I am calling <input type="radio"/> ISDN <input checked="" type="radio"/> PPTP <input type="radio"/> IPsec Tunnel <input type="radio"/> L2TP with IPsec Policy None		Link Type 64k bps Username draytek Password ***** PPP Authentication PAP/CHAP VJ Compression <input checked="" type="radio"/> On <input type="radio"/> Off
Dial Number for ISDN or Server IP/Host Name for VPN. (such as 5551234, draytek.com or 123.45.67.89) <input type="text" value="220.135.240.208"/>		IKE Authentication Method <input checked="" type="radio"/> Pre-Shared Key IKE Pre-Shared Key ***** <input type="radio"/> Digital Signature(X.509) None
		IPsec Security Method <input checked="" type="radio"/> Medium(AH) <input type="radio"/> High(ESP) DES without Authentication <input type="button" value="Advanced"/>
		Index(1-15) in Schedule Setup: <input type="text"/> , <input type="text"/> , <input type="text"/> , <input type="text"/>
		Callback Function (CBCP) <input type="checkbox"/> Require Remote to Callback <input type="checkbox"/> Provide ISDN Number to Remote

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

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

3. Dial-In Settings

Allowed Dial-In Type <input type="checkbox"/> ISDN <input type="checkbox"/> PPTP <input checked="" type="checkbox"/> IPsec Tunnel <input type="checkbox"/> L2TP with IPsec Policy None <input checked="" type="checkbox"/> Specify ISDN CLID or Remote VPN Gateway Peer ISDN Number or Peer VPN Server IP <input type="text" value="220.135.240.208"/> or Peer ID <input type="text"/>	Username <input type="text" value="???"/> Password <input type="text"/> VJ Compression <input checked="" type="radio"/> On <input type="radio"/> Off IKE Authentication Method <input checked="" type="checkbox"/> Pre-Shared Key <input type="button" value="IKE Pre-Shared Key"/> <input type="text"/> <input type="checkbox"/> Digital Signature(X.509) None IPsec Security Method <input checked="" type="checkbox"/> Medium (AH) High (ESP) <input checked="" type="checkbox"/> DES <input checked="" type="checkbox"/> 3DES <input checked="" type="checkbox"/> AES Callback Function (CBCP) <input type="checkbox"/> Enable Callback Function <input type="checkbox"/> Use the Following Number to Callback Callback Number <input type="text"/> Callback Budget <input type="text" value="0"/> minute(s)
--	--

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

3. Dial-In Settings

Allowed Dial-In Type <input type="checkbox"/> ISDN <input checked="" type="checkbox"/> PPTP <input type="checkbox"/> IPsec Tunnel <input type="checkbox"/> L2TP with IPsec Policy None <input checked="" type="checkbox"/> Specify ISDN CLID or Remote VPN Gateway Peer ISDN Number or Peer VPN Server IP <input type="text" value="220.135.240.208"/> or Peer ID <input type="text"/>	Username <input type="text" value="draytek"/> Password <input type="text" value="*****"/> VJ Compression <input checked="" type="radio"/> On <input type="radio"/> Off IKE Authentication Method <input checked="" type="checkbox"/> Pre-Shared Key <input type="button" value="IKE Pre-Shared Key"/> <input type="text"/> <input type="checkbox"/> Digital Signature(X.509) None IPsec Security Method <input checked="" type="checkbox"/> Medium (AH) High (ESP) <input checked="" type="checkbox"/> DES <input checked="" type="checkbox"/> 3DES <input checked="" type="checkbox"/> AES Callback Function (CBCP) <input type="checkbox"/> Enable Callback Function <input type="checkbox"/> Use the Following Number to Callback Callback Number <input type="text"/> Callback Budget <input type="text" value="0"/> minute(s)
--	--

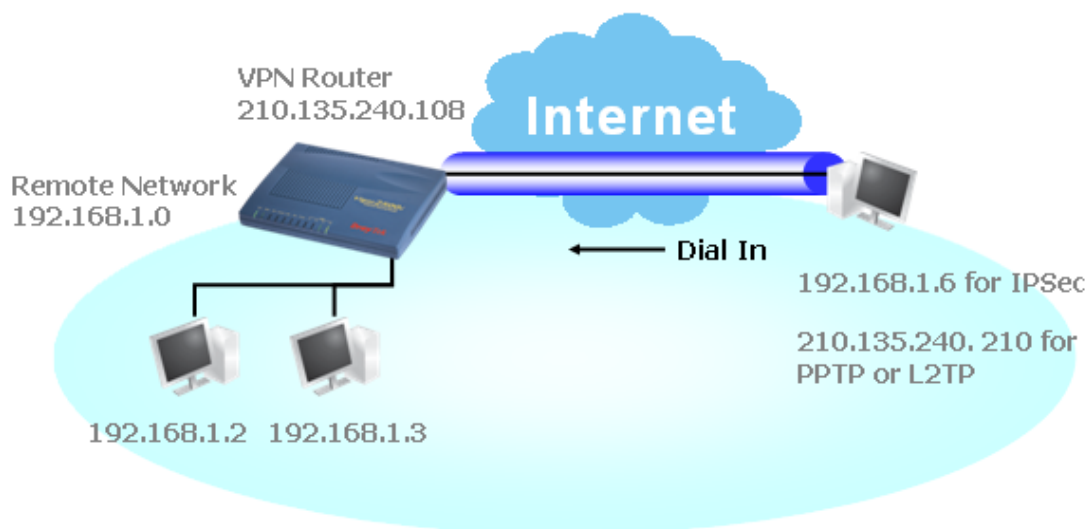
7. At last, set the remote network IP/subnet in **TCP/IP Network Settings** so that Router B can direct the packets destined to the remote network to Router A via the VPN connection.

4. TCP/IP Network Settings

My WAN IP <input type="text" value="0.0.0.0"/> Remote Gateway IP <input type="text" value="0.0.0.0"/> Remote Network IP <input type="text" value="192.168.1.0"/> Remote Network Mask <input type="text" value="255.255.255.0"/> <input type="button" value="More"/>	RIP Direction Disable From first subnet to remote network, you have to do Route <input type="checkbox"/> Change default route to this VPN tunnel (Only single WAN supports this)
---	---

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

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



Settings in VPN Router in the enterprise office:

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

PPP General Setup

PPP/MP Protocol		IP Address Assignment for Dial-In Users	
Dial-In PPP Authentication	PAP or CHAP	Start IP Address	192.168.1.200
Dial-In PPP Encryption (MPPE)	Optional MPPE		
Mutual Authentication (PAP)	<input type="radio"/> Yes <input checked="" type="radio"/> No		
Username			
Password			

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

VPN and Remote Access >> IPSec General Setup

VPN IKE/IPSec General Setup

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

IKE Authentication Method	
Pre-Shared Key
Confirm Pre-Shared Key
IPSec Security Method	
<input checked="" type="checkbox"/> Medium (AH) Data will be authentic, but will not be encrypted.	
High (ESP)	<input checked="" type="checkbox"/> DES <input checked="" type="checkbox"/> 3DES <input checked="" type="checkbox"/> AES Data will be encrypted and authentic.

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

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

VPN and Remote Access >> Remote Dial-in User

Index No. 1

User account and Authentication	
<input type="checkbox"/> Enable this account	
Idle Timeout	300 second(s)
Allowed Dial-In Type	
<input type="checkbox"/> ISDN <input type="checkbox"/> PPTP <input checked="" type="checkbox"/> IPSec Tunnel <input type="checkbox"/> L2TP with IPSec Policy None	
<input checked="" type="checkbox"/> Specify Remote Node	
Remote Client IP or Peer ISDN Number 210.136.240.210	
or Peer ID	
Netbios Naming Packet <input checked="" type="radio"/> Pass <input type="radio"/> Block	
Multicast via VPN <input type="radio"/> Pass <input checked="" type="radio"/> Block (for some IGMP, IP-Camera, DHCP Relay..etc.)	
IKE Authentication Method	
<input checked="" type="checkbox"/> Pre-Shared Key	
IKE Pre-Shared Key	
<input type="checkbox"/> Digital Signature (X.509)	
None	
IPSec Security Method	
<input checked="" type="checkbox"/> Medium (AH)	
High (ESP)	
<input checked="" type="checkbox"/> DES <input checked="" type="checkbox"/> 3DES <input checked="" type="checkbox"/> AES	
Local ID (optional)	
Callback Function	
<input type="checkbox"/> Check to enable Callback function	
<input type="checkbox"/> Specify the callback number	
Callback Number	
<input checked="" type="checkbox"/> Check to enable Callback Budget Control	
Callback Budget 30 minute(s)	

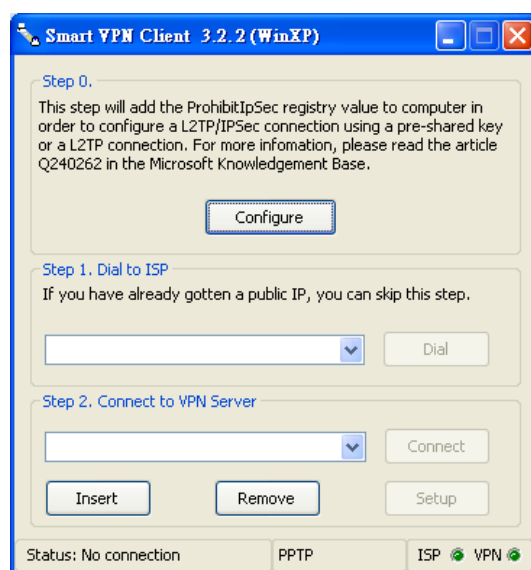
If a **PPP-based** service is selected, you should further specify the remote peer IP Address, Username, Password, and VJ Compression for this Dial-In connection.

Index No. 1

User account and Authentication <input type="checkbox"/> Enable this account Idle Timeout <input type="text" value="300"/> second(s)		Username <input type="text" value="draytek"/> Password <input type="password" value="••••••"/>
Allowed Dial-In Type <input type="checkbox"/> ISDN <input checked="" type="checkbox"/> PPTP <input type="checkbox"/> IPsec Tunnel <input type="checkbox"/> L2TP with IPsec Policy <input type="text" value="None"/>		IKE Authentication Method <input checked="" type="checkbox"/> Pre-Shared Key IKE Pre-Shared Key <input type="text"/> <input type="checkbox"/> Digital Signature (X.509) <input type="text" value="None"/>
<input checked="" type="checkbox"/> Specify Remote Node Remote Client IP or Peer ISDN Number <input type="text" value="210.136.240.210"/> or Peer ID <input type="text"/> Netbios Naming Packet <input checked="" type="radio"/> Pass <input type="radio"/> Block Multicast via VPN <input type="radio"/> Pass <input checked="" type="radio"/> Block (for some IGMP, IP-Camera, DHCP Relay..etc.)		IPsec Security Method <input checked="" type="checkbox"/> Medium (AH) High (ESP) <input checked="" type="checkbox"/> DES <input checked="" type="checkbox"/> 3DES <input checked="" type="checkbox"/> AES Local ID <input type="text"/> (optional)
		Callback Function <input type="checkbox"/> Check to enable Callback function <input type="checkbox"/> Specify the callback number Callback Number <input type="text"/> <input checked="" type="checkbox"/> Check to enable Callback Budget Control Callback Budget <input type="text" value="30"/> minute(s)

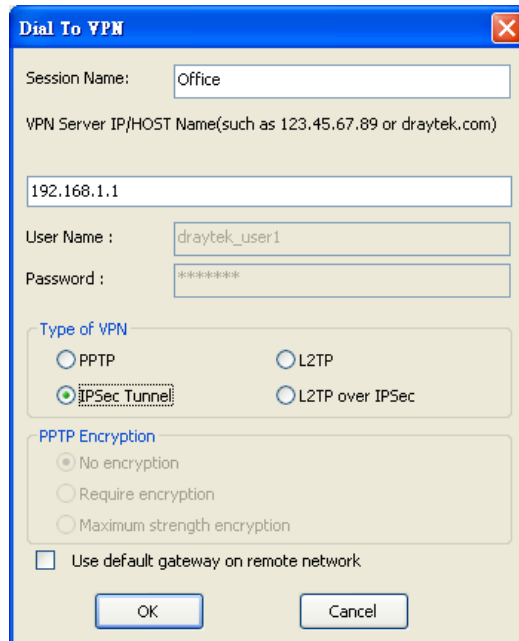
Settings in the remote host:

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



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,

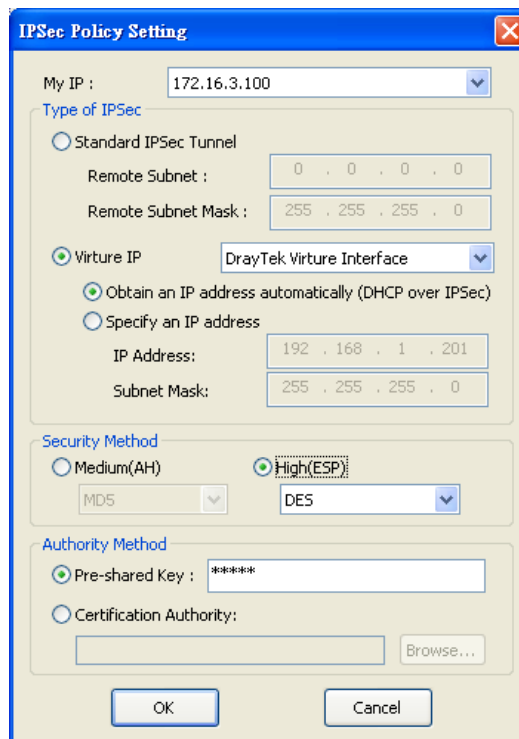


The 'Dial To VPN' dialog box is shown with the following settings:

- Session Name: Office
- VPN Server IP/HOST Name(such as 123.45.67.89 or draytek.com): 192.168.1.1
- User Name : draytek_user1
- Password : *****
- Type of VPN:
 - ☐ PPTP
 - ☒ IPSec Tunnel
 - ☐ L2TP
 - ☐ L2TP over IPSec
- PPTP Encryption:
 - ☒ No encryption
 - ☐ Require encryption
 - ☐ Maximum strength encryption
- ☐ Use default gateway on remote network

Buttons: OK, Cancel

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



The 'IPSec Policy Setting' dialog box is shown with the following settings:

- My IP : 172.16.3.100
- Type of IPSec:
 - ☐ Standard IPSec Tunnel
 - Remote Subnet : 0 . 0 . 0 . 0
 - Remote Subnet Mask : 255 . 255 . 255 . 0
 - ☒ Virture IP
 - DrayTek Virture Interface
 - ☒ Obtain an IP address automatically (DHCP over IPSec)
 - ☐ Specify an IP address
 - IP Address: 192 . 168 . 1 . 201
 - Subnet Mask: 255 . 255 . 255 . 0
- Security Method:
 - ☐ Medium(AH)
 - ☒ High(ESP)
 - MD5
 - DES
- Authority Method:
 - ☒ Pre-shared Key : *****
 - ☐ Certification Authority:
 - Browse...

Buttons: OK, Cancel

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

server then forwarded to Internet. This will make the remote host seem to be working in the enterprise network.

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

4.3 QoS Setting Example

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

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

Bandwidth Management >> Quality of Service

General Setup

Index	Status	Bandwidth	Direction	Class 1	Class 2	Class 3	Others	UDP Bandwidth Control	
WAN1	Disable	10000Kbps/10000Kbps		25%	25%	25%	25%	Inactive	Setup
WAN2	Disable	10000Kbps/10000Kbps		25%	25%	25%	25%	Inactive	Setup

Class Rule

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

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

☒ **Enable the QoS Control** BOTH

WAN Inbound Bandwidth

WAN Outbound Bandwidth

- Set Inbound/Outbound bandwidth.

Bandwidth Management >> Quality of Service

WAN1 General Setup

☒ **Enable the QoS Control** BOTH

WAN Inbound Bandwidth 10000 Kbps

WAN Outbound Bandwidth 10000 Kbps

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

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

Bandwidth Management >> Quality of Service

Class Index #1

Name E-mail

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

Add
Edit
Delete

OK
Cancel

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

Bandwidth Management >> Quality of Service

WAN1 General Setup

☒ **Enable the QoS Control** BOTH

WAN Inbound Bandwidth 10000 Kbps

WAN Outbound Bandwidth 10000 Kbps

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

☐ Enable UDP Bandwidth Control

☐ Outbound TCP ACK Prioritize

Limited_bandwidth Ratio 25 %

OK
Clear
Cancel

6. 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.

Bandwidth Management >> Quality of Service

Class Index #2

Name

NO	Status	Local Address	Remote Address	DiffServ CodePoint	Service Type
1 <input type="radio"/>	Active	Any	Any	ANY	ANY

7. Click **Setup** link for WAN1.

Bandwidth Management >> Quality of Service

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

Index	Status	Bandwidth	Direction	Class 1	Class 2	Class 3	Others	UDP Bandwidth Control	
WAN1	Disable	10000Kbps/10000Kbps		25%	25%	25%	25%	Inactive	Setup
WAN2	Disable	10000Kbps/10000Kbps		25%	25%	25%	25%	Inactive	Setup

Class Rule

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

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

Bandwidth Management >> Quality of Service

WAN1 General Setup

☒ Enable the QoS Control

WAN Inbound Bandwidth		<input type="text" value="10000"/> Kbps
WAN Outbound Bandwidth		<input type="text" value="10000"/> Kbps

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

☒ Enable UDP Bandwidth Control

Limited_bandwidth Ratio %

[Online Statistics](#)

9. 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 reserve bandwidth for 1 VPN tunnel.



10. Click edit to open a new window.

Bandwidth Management >> Quality of Service

Class Index #1

Name

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

11. First, check the **ACT** box. Then click **Edit** of **Local Address** to set a worker's subnet address. Click **Edit** of **Remote Address** to set headquarter's subnet address. Leave other fields and click **OK**.

Bandwidth Management >> Quality of Service

Rule Edit

☒ ACT

Local Address

Remote Address

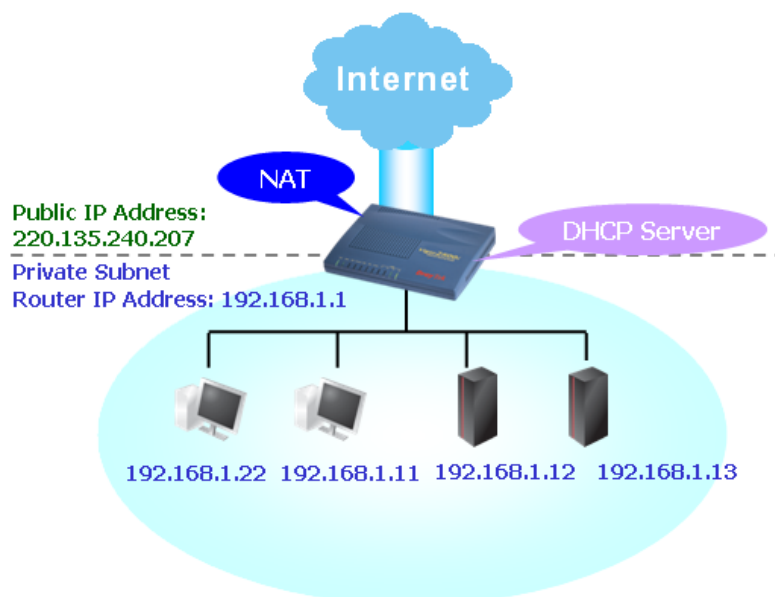
DiffServ CodePoint

Service Type

Note: Please choose/setup the **Service Type** first.

4.4 LAN – Created by Using NAT

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



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

LAN >> General Setup

Ethernet TCP / IP and DHCP Setup

LAN IP Network Configuration

For NAT Usage

1st IP Address

1st Subnet Mask

For IP Routing Usage ☐ Enable ☒ Disable

2nd IP Address

2nd Subnet Mask

RIP Protocol Control

DHCP Server Configuration

☒ Enable Server ☐ Disable Server

Relay Agent: ☐ 1st Subnet ☐ 2nd Subnet

Start IP Address

IP Pool Counts

Gateway IP Address

DHCP Server IP Address for Relay Agent

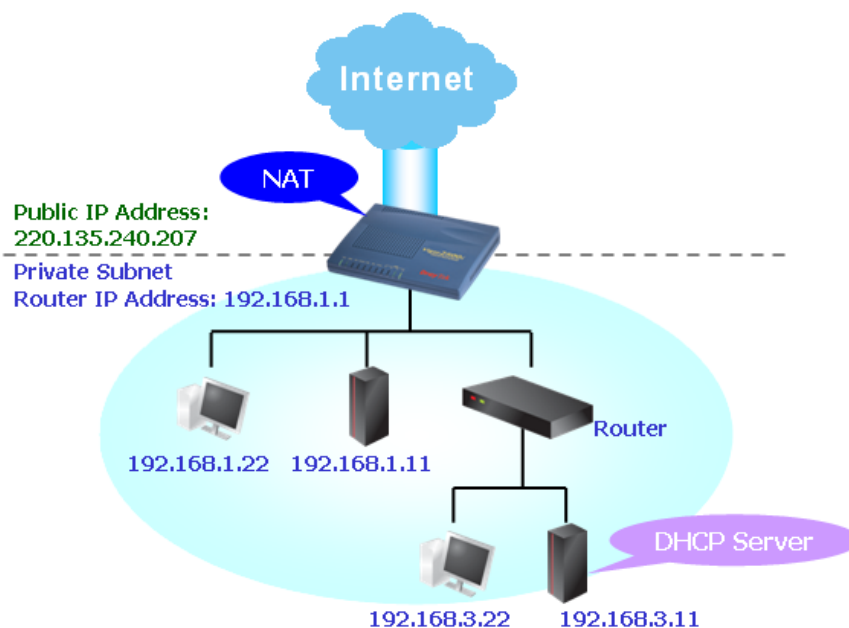
DNS Server IP Address

☐ Force DNS manual setting

Primary IP Address

Secondary IP Address

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



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

LAN >> General Setup

Ethernet TCP / IP and DHCP Setup

LAN IP Network Configuration

For NAT Usage

1st IP Address

1st Subnet Mask

For IP Routing Usage ☐ Enable ☒ Disable

2nd IP Address

2nd Subnet Mask

RIP Protocol Control

DHCP Server Configuration

☐ Enable Server ☒ Disable Server

Relay Agent: ☐ 1st Subnet ☐ 2nd Subnet

Start IP Address

IP Pool Counts

Gateway IP Address

DHCP Server IP Address for Relay Agent

DNS Server IP Address

☐ Force DNS manual setting

Primary IP Address

Secondary IP Address

4.5 Calling Scenario for VoIP function

4.5.1 Calling via SIP Sever

Example 1: Both John and David have SIP Addresses from different service providers.

John's SIP URL: 1234@draytel.org, David's SIP URL: 4321@iptel.org

Settings for John

DialPlan index 1
Phone Number: 1111
Display Name: David
SIP URL: 4321@iptel.org

SIP Accounts Settings ---

Profile Name: draytel1
Register via: Auto
SIP Port: 5060 (default)
Domain/Realm: draytel.org
Proxy: draytel.org
Act as outbound proxy:
unchecked
Display Name: John
Account Number/Name: 1234
Authentication ID: unchecked
Password: ****
Expiry Time: (use default value)

CODEC/RTP/DTMF ---

(Use default value)

Settings for David

DialPlan index 1
Phone Number: 2222
Display Name: John
SIP URL: 1234@draytel.org

SIP Accounts Settings ---

Profile Name: iptel 1
Register via: Auto
SIP Port: 5060 (default)
Domain/Realm: iptel.org
Proxy: iptel.org
Act as outbound proxy:
unchecked
Display Name: David
Account Name: 4321
Authentication ID: unchecked
Password: ****
Expiry Time: (use default value)

CODEC/RTP/DTMF ---

(Use default value)

Phone Book Index No. 1

<input checked="" type="checkbox"/> Enable	Phone Number	1111
	Display Name	David
	SIP URL	4321@iptel.org
	Loop through	None
	Backup Phone Number	

OK Clear Cancel

VoIP >> SIP Accounts

SIP Account Index No. 1

Profile Name	draytel1	(11 char max.)
Register via	Auto	<input type="checkbox"/> make call without register
SIP Port	5060	
Domain/Realm	draytel.org	(63 char max.)
Proxy	draytel.org	(63 char max.)
<input type="checkbox"/> Act as outbound proxy		
Display Name	John	(23 char max.)
Account Number/Name	1234	(63 char max.)
<input type="checkbox"/> Authentication ID		(63 char max.)
Password	****	(63 char max.)
Expiry Time	1 hour	3600 sec
NAT Traversal Support	None	
Ring Port	<input checked="" type="checkbox"/> VoIP1	<input type="checkbox"/> VoIP2 <input type="checkbox"/> ISDN
Ring Pattern	1	

OK Cancel

John calls David ---

He picks up the phone and dials 1111#. (DialPlan Phone Number for David)

Phone Book Index No. 1

<input checked="" type="checkbox"/> Enable	Phone Number	2222
	Display Name	John
	SIP URL	1234@draytel.org
	Loop through	None
	Backup Phone Number	

OK Clear Cancel

VoIP >> SIP Accounts

SIP Account Index No. 1

Profile Name	iptel 1	(11 char max.)
Register via	Auto	<input type="checkbox"/> make call without register
SIP Port	5060	
Domain/Realm	iptel.org	(63 char max.)
Proxy	iptel.org	(63 char max.)
<input type="checkbox"/> Act as outbound proxy		
Display Name	David	(23 char max.)
Account Number/Name	4321	(63 char max.)
<input type="checkbox"/> Authentication ID		(63 char max.)
Password	****	(63 char max.)
Expiry Time	1 hour	3600 sec
NAT Traversal Support	None	
Ring Port	<input checked="" type="checkbox"/> VoIP1	<input type="checkbox"/> VoIP2 <input type="checkbox"/> ISDN
Ring Pattern	1	

OK Cancel

David calls John

He picks up the phone and dials 2222# (DialPlan Phone Number for John)

Example 2: Both John and David have SIP Addresses from the same service provider.

John's SIP URL: 1234@draytel.org , David's SIP URL: 4321@draytel.org

Settings for John

DialPlan index 1

Phone Number: 1111

Display Name: David

SIP URL: 4321@draytel.org



SIP Accounts Settings ---

Profile Name: draytel 1

Register via: Auto

SIP Port: 5060 (default)

Domain/Realm: draytel.org

Proxy: draytel.org

Act as outbound proxy: unchecked

Display Name: John

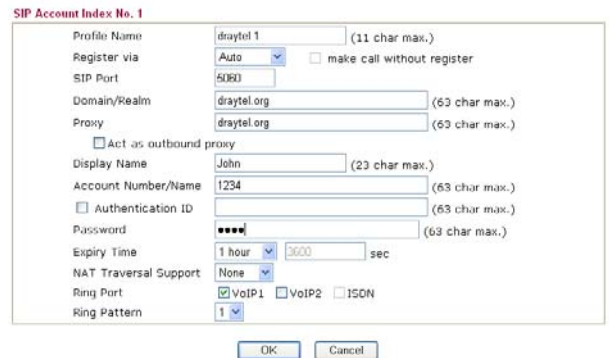
Account Number/Name: 1234

Authentication ID: unchecked

Password: ****

Expiry Time: (use default value)

VoIP >> SIP Accounts



John calls David

He picks up the phone and dials 1111#. (DialPlan Phone Number for David) Or,

He picks up the phone and dials 4321#. (David's Account Name)

CODEC/RTP/DTMF ---

(Use default value)

Settings for David

DialPlan index 1

Phone Number: 2222

Display Name: John

SIP URL: 1234@draytel.org



SIP Accounts Settings ---

Profile Name: John

Register via: Auto

SIP Port: 5060 (default)

Domain/Realm: draytel.org

Proxy: iptel.org

Act as outbound proxy: unchecked

Display Name: David

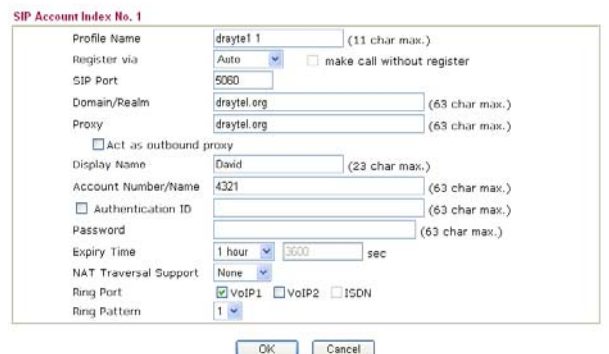
Account Name: 4321

Authentication ID: unchecked

Password: ****

Expiry Time: (use default value)

VoIP >> SIP Accounts



CODEC/RTP/DTMF---

(Use default value)

David calls John

He picks up the phone and dials 2222# (DialPlan Phone Number for John) Or,

He picks up the phone and dials 1234# (John's Account Name)

4.5.2 Peer-to-Peer Calling

Example 3: Arnor and Paulin have Vigor routers respectively. They can call each other *without* SIP Registrar. First they must have each other's IP address and assign an Account Name for the port used for calling.

Arnor's SIP URL: 1234@214.61.172.53 Paulin's SIP URL: 4321@ 203.69.175.24

Settings for Arnor

DialPlan index 1

Phone Number: 1111

Display Name: paulin

SIP URL: 4321@ 203.69.175.24

SIP Accounts Settings ---

Profile Name: Paulin

Register via: None

SIP Port: 5060(default)

Domain/Realm: (blank)

Proxy: (blank)

Act as outbound proxy: unchecked

Display Name: Arnor

Account Name: 1234

Authentication ID: unchecked

Password: (blank)

Expiry Time: (use default value)

CODEC/RTP/DTMF---

(Use default value)

Phone Book Index No. 1

<input checked="" type="checkbox"/> Enable	Phone Number	1111
	Display Name	paulin
	SIP URL	4321 @203.69.175.24
	Loop through	None
	Backup Phone Number	

OK Clear Cancel

VoIP >> SIP Accounts

SIP Account Index No. 1

Profile Name	Paulin	(11 char max.)
Register via	None	<input type="checkbox"/> make call without register
SIP Port	5060	
Domain/Realm		(63 char max.)
Proxy		(63 char max.)
<input type="checkbox"/> Act as outbound proxy		
Display Name	Arnor	(23 char max.)
Account Number/Name	1234	(63 char max.)
<input type="checkbox"/> Authentication ID		(63 char max.)
Password		(63 char max.)
Expiry Time	1 hour	3600 sec
NAT Traversal Support	None	
Ring Port	<input checked="" type="checkbox"/> VoIP1 <input type="checkbox"/> VoIP2 <input type="checkbox"/> ISDN	
Ring Pattern	1	

OK Cancel

Arnor calls Paulin

He picks up the phone and dials **1111#**. (DialPlan Phone Number for Arnor)

VoIP >> DialPlan Setup

Phone Book Index No. 1

<input checked="" type="checkbox"/> Enable	Phone Number	2222
	Display Name	Arnor
	SIP URL	1234 @214.61.172.53
	Loop through	None
	Backup Phone Number	

VoIP >> SIP Accounts

SIP Account Index No. 1

Profile Name	Arnor	(11 char max.)
Register via	None	<input type="checkbox"/> make call without register
SIP Port	5060	
Domain/Realm		(63 char max.)
Proxy		(63 char max.)
<input type="checkbox"/> Act as outbound proxy		
Display Name	Paulin	(23 char max.)
Account Number/Name	4321	(63 char max.)
<input type="checkbox"/> Authentication ID		(63 char max.)
Password		(63 char max.)
Expiry Time	1 hour	3600 sec
NAT Traversal Support	None	
Ring Port	<input checked="" type="checkbox"/> VoIP1 <input type="checkbox"/> VoIP2 <input type="checkbox"/> ISDN	
Ring Pattern	1	

OK Cancel

Settings for Paulin

DialPlan index 1

Phone Number:2222

Display Name: Arnor

SIP URL: 1234@214.61.172.53

SIP Accounts Settings ---

Profile Name: Arnor

Register via: None

SIP Port: 5060(default)

Domain/Realm: (blank)

Proxy: (blank)

Act as outbound proxy: unchecked

Display Name: Paulin

Account Name: 4321

Authentication ID: unchecked

Password: (blank)

Expiry Time: (use default value)

CODEC/RTP/DTMF---

(Use default value)

Paulin calls Arnor

He picks up the phone and dials **2222#** (DialPlan Phone Number for John)

4.6 Upgrade Firmware for Your Router

Before upgrading your router firmware, you need to install the Router Tools. The **Firmware Upgrade Utility** is included in the tools.

1. Insert CD of the router to your CD ROM.
2. From the webpage, please find out **Utility** menu and click it.
3. On the webpage of Utility, click **Install Now!** (under Syslog description) to install the corresponding program.

Please remember to set as follows in your DrayTek Router :

- Server IP Address : IP address of the PC that runs the Syslog
- Port Number : Default value 514

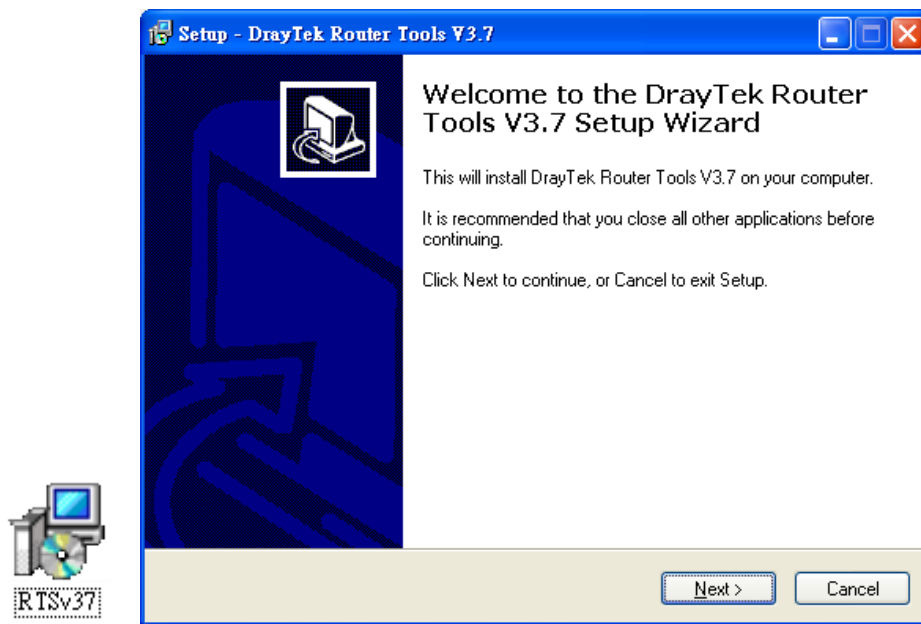


4. The file **RTSxxx.exe** will be asked to copy onto your computer. Remember the place of storing the execution file.
5. Go to **www.draytek.com** to find out the newly update firmware for your router.
6. Access into **Support Center >> Downloads**. Find out the model name of the router and click the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

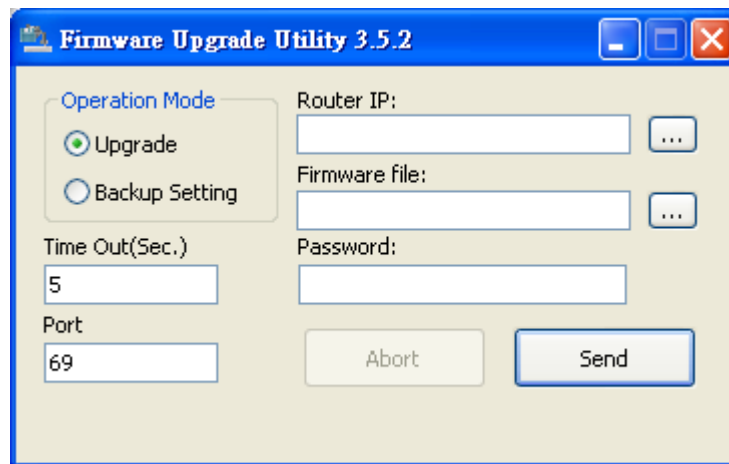
Tools Name	Released Date	Version	OS	Support Model	Download
Router Tools	21/12/2006	3.5.1	MS-Windows	All Model	zip
SmartVPN Client	18/08/2006	3.2.6	MS-Windows	All Model	zip
LPR	27/06/2005	1.0	MS-Windows	For Print Function	zip
VTA	15/09/2005	2.8	Windows2000/XP	For ISDN Model	zip
DialPlan	26/01/2006	2.5_lite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

7. Choose the one that matches with your operating system and click the corresponding link to download correct firmware (zip file).
8. Next, decompress the zip file.

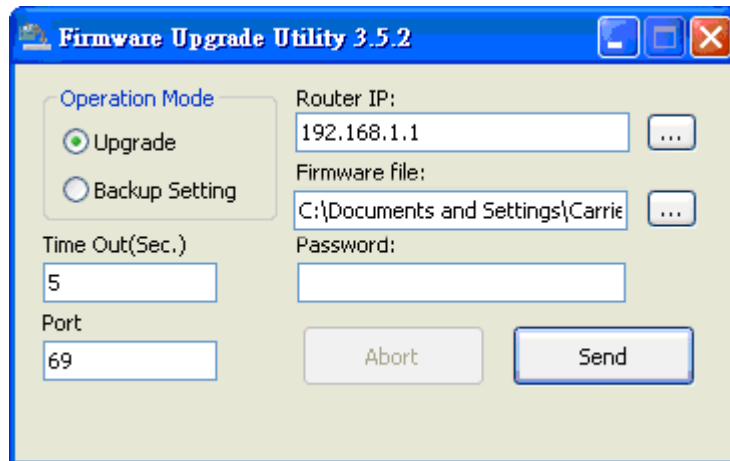
9. Double click on the icon of router tool. The setup wizard will appear.



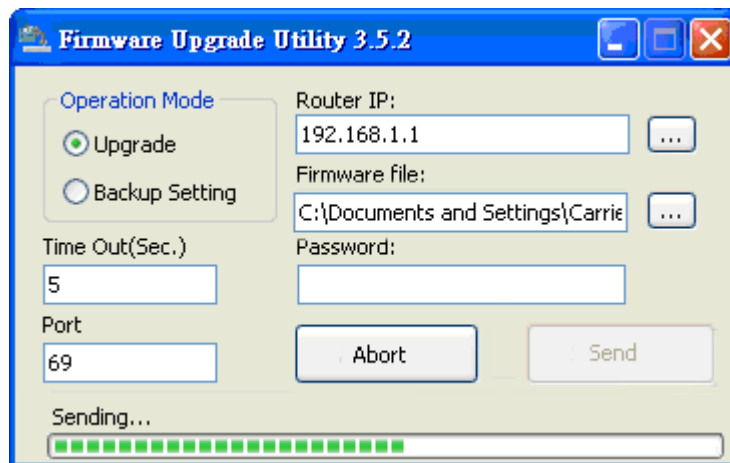
10. Follow the onscreen instructions to install the tool. Finally, click **Finish** to end the installation.
11. From the **Start** menu, open **Programs** and choose **Router Tools XXX >> Firmware Upgrade Utility**.



12. Type in your router IP, usually **192.168.1.1**.
13. Click the button to the right side of Firmware file typing box. Locate the files that you download from the company web sites. You will find out two files with different extension names, **xxxx.all** (keep the old custom settings) and **xxxx.rst** (reset all the custom settings to default settings). Choose any one of them that you need.

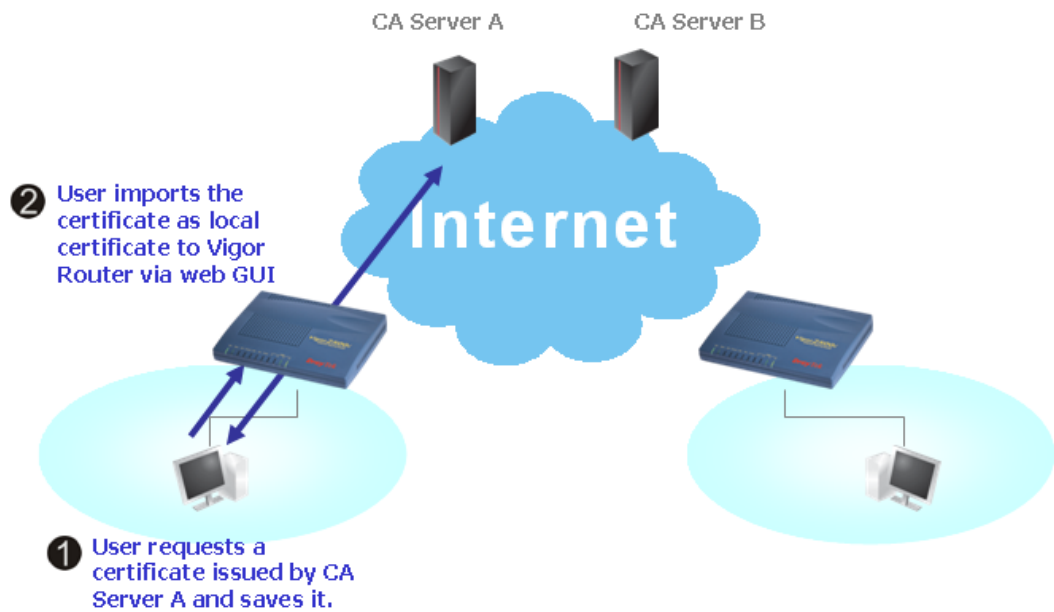


14. Click **Send**.



15. Now the firmware update is finished.

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



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

Certificate Management >> Local Certificate

X509 Local Certificate Configuration

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

X509 Local Certificate

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

Certificate Management >> Local Certificate

Generate Certificate Request

Subject Alternative Name

Type: Domain Name

Domain Name: draytek.com

Subject Name

Country (C): TW

State (ST):

Location (L):

Organization (O): Draytek

Organization Unit (OU):

Common Name (CN):

Email (E): press@draytek.com

Key Type: RSA

Key Size: 1024 Bit

Generate

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

Certificate Management >> Local Certificate

X509 Local Certificate Configuration

Name	Subject	Status	Modify
Local	/C=TW/O=Draytek/emailAddress...	Requesting	View Delete

[GENERATE](#) [IMPORT](#) [REFRESH](#)

X509 Local Certificate Request

```
-----BEGIN CERTIFICATE REQUEST-----
MIIBqjCCARMAQAwQTELMAkGA1UEBhMCVFcxEDAOBgNVBAAoTBORyYX10ZWsxIDAe
BgkqhkiG9wOBCQEWEXByZXRyYX10ZWsuY29tMIGfMAOGCSqGSIb3DQEBAQUA
A4GNADCBiQKBgQDPioahu/gfQaYB1ce5OERSDfWknIdHb1o1kt9cTdLUDaFk6e8d
3wDeQytoV1LBjz2IDF0xjX6ip7ev187twwTsg4lg26Qk/rGhuVTkd9j6P1crnkP7
du84t23tWBdMD4W5c8VmSyDjShLhjdXVYPWpNKVlrOT2RZjkRMAHEUpVpwIDAQABo
CkwJwYJKoZIhvcNAQkOMRowGDAWBgNVHREEDzANggtkcmF5dGVrLnNvbTANBgkq
hkiG9wOBAQUFAA0BgQAUuSBRUGt4W1hH9N6/HwToem1tHQbcwjXvg/t7kF1zTJiHh
uRLq4CiE16nV4hMRytcx2pE26sMar3gRREr86RoO8JxOI45560xCZ/N1Gh9VQ9I1
I9FqkjJNihp4TCjecSNNZjmQo5WU+Bce8TG+SCBCyejqu/fo/4JQFajB7Gviw==
-----END CERTIFICATE REQUEST-----
```

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

Microsoft Certificate Services -- vigor [Home](#)

Welcome

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

Select a task:

- ☐ Retrieve the CA certificate or certificate revocation list
- ☒ Request a certificate
- ☐ Check on a pending certificate

[Next >](#)

Select **Advanced request**.

Microsoft Certificate Services -- vigor Home

Choose Request Type

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

☐ User certificate request

☒ Advanced request

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 Request text file. Select **Router (Offline request)** or **IPSec (Offline request)** below.

Microsoft Certificate Services -- vigor Home

Submit A Saved Request

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

Saved Request:

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

```
-----BEGIN CERTIFICATE REQUEST-----
MIIBqjCCARhCAQAwQTElMAkGA1UEBhMCVFcxEDAO
BgkqhkiG9w0BCQEWEVB7ZmZfFhN9/IeQnG03Xk++
A4GNADCB1QKBgQDQYB7wmZFfFhN9/IeQnG03Xk++
hX4bp89cUF9d1oACGG1M/tcB0ckdcZdPFFvIXcP3
x/G0A7CTvO/fQzpxroCw1JTjLSjS0/Bn9v50951G
-----
```

Browse for a file to insert.

Certificate Template:

Administrator

Additional Attributes:

Authenticated Session

Basic EFS

EFS Recovery Agent

User

IPSEC (Offline request)

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 “-----BEGIN CERTIFICATE-----.....”
Certificate Management >> Local Certificate

X509 Local Certificate Configuration

Name	Subject	Status	Modify
Local	/C=TW/O=Draytek/emailAddress...	Not Valid Yet	View Delete

[GENERATE](#)
[IMPORT](#)
[REFRESH](#)

X509 Local Certificate Request

```

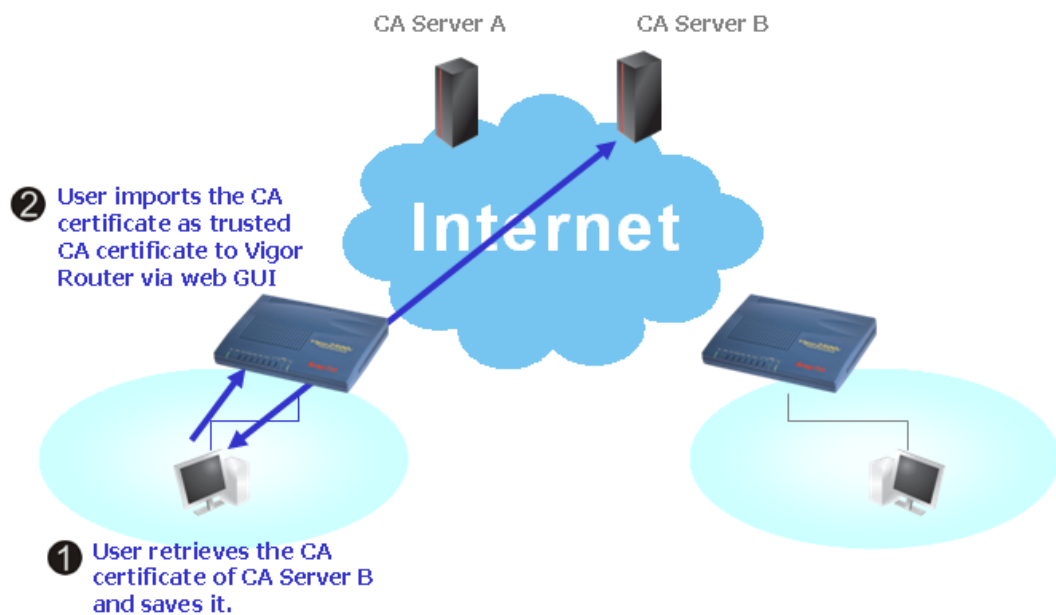
-----BEGIN CERTIFICATE REQUEST-----
MIIBqjCCARMCAQAwQTELMakGA1UEBhMCVFcxEDAOBgNVBAoTBORyYX10ZWsxIDAe
BgkqhkiG9wOBCQEWEYyZXNzQGRyYX10ZWsuY29tMIGfMA0GCSqGSIb3DQEBAQUA
A4GNADCBiQKBgQDPioahu/gFQaYB1ce5OERSDfWknIdHb1o1kt9cTdLUDaFk6s8d
3wDeQytoV1LBJz2IDF0xjX6ip7ev187twwTsg4lgZ6Qk/rGhuVTKd9j6PlcrnkP7
du84t23tWBdMD4W5c8VmSyDjShLhjdVYPWpNKVTrOT2RZjkRMaHEWpVpWIDAQAB
oCkwJwYJKoZIhvcNAQkOMRowGDAWBgNVHREEDzANggtkcmF5dGVrLnNvbTANBgkq
hkiG9wOBAQUFAAOBgQAuSBRUGt4W1hH9N6/HwToemltHQbcwjXvg/t7kFlzTjiHh
uRLq4CiEi6nV4hMRytcxZpEZ6sMarSgRREr86RoO8JxOI45560xCZ/N1Gh9VQ9I1
I9FqkjJNihp4TCjecSNNZjmQo5WU+Bce8TG+SCBCyejqu/fo/AJQFajB7Gviw==
-----END CERTIFICATE REQUEST-----

```

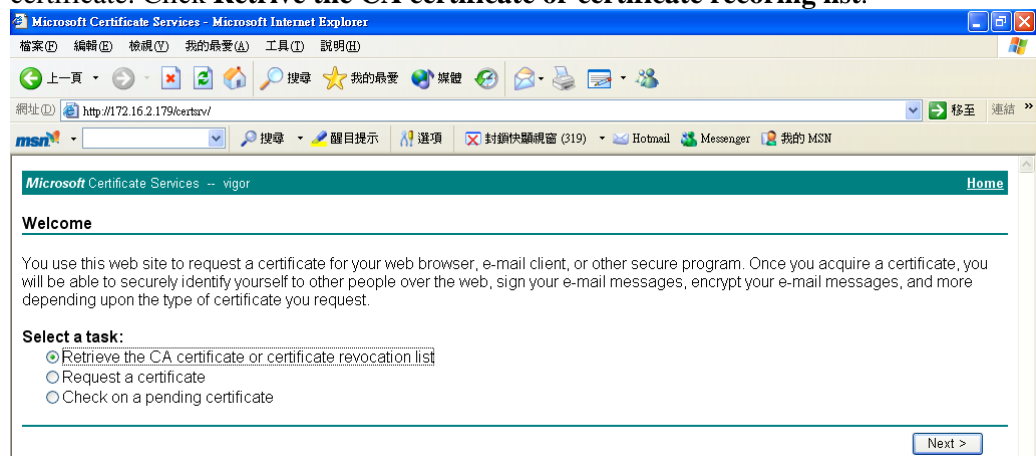
- You may review the detail information of the certificate by clicking **View** button.

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

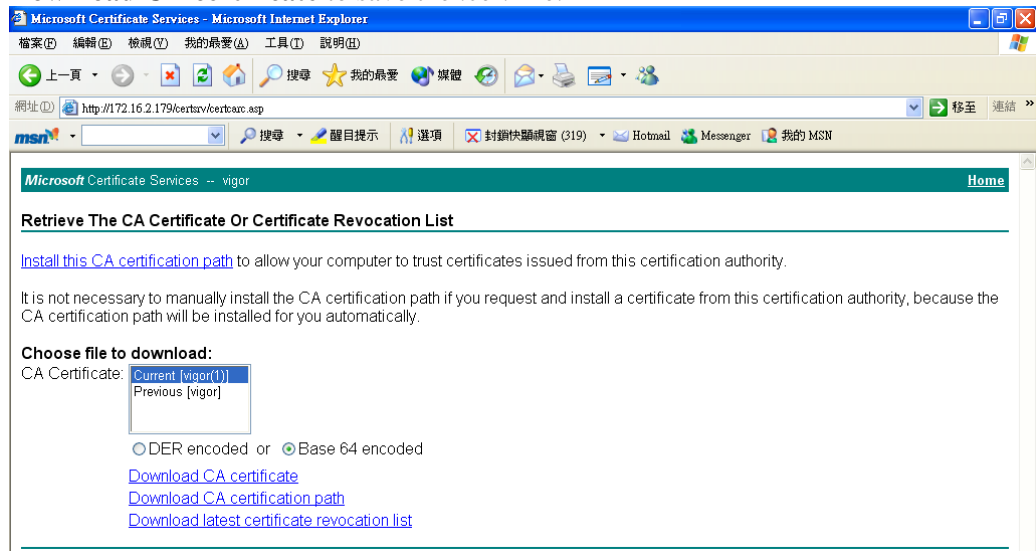
4.8 Request a CA Certificate and Set as Trusted on Windows CA Server



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



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



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

Certificate Management >> Trusted CA Certificate

X509 Trusted CA Certificate Configuration

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

[IMPORT](#)

[REFRESH](#)

- 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.

4.9 VPN Backup Application

You can change, disable or delete VPN Backup profile(s). Yet, the relational web pages in LAN to LAN also will be changed slightly. Please refer to the following explanation.

Change the name of VPN Backup profile(s)

1. Click any one of the items from Backup profile list.
2. Type a new name in the field of **Profile Name**.
3. Click **Edit**.

Disable VPN Backup profile(s)

1. Click any one of the items from Backup profile list.
2. Click **Disable** (as current status).
3. Click **Edit**.
4. The selected profile will be disabled.
5. To check if the profile has been disabled or not, open LAN to LAN. The name with red color means it has joined VPN Backup profile; the name with black color means it does not join VPN Backup profile or is disabled in VPN Backup profile.

LAN-to-LAN Profiles:

Index	Name	Status
<u>1.</u>	2.5	√
<u>2.</u>	2.5-1	√
<u>3.</u>	2.29	√
<u>4.</u>	2.229	√
<u>5.</u>	26	√
<u>6.</u>	27	√
<u>7.</u>	28	√
<u>8.</u>	29	√
<u>9.</u>	30	√

LAN-to-LAN Profiles:

Index	Name	Status
<u>1.</u>	2.5	√
<u>2.</u>	2.5-1	√
<u>3.</u>	2.29	√
<u>4.</u>	2.229	√
<u>5.</u>	2.2	√
<u>6.</u>	27	√
<u>7.</u>	28	√
<u>8.</u>	29	√
<u>9.</u>	30	√

Delete VPN Backup profile(s)

1. Click any one of the items from Backup profile list.
2. Click **Delete**.
3. Click **Edit**.
4. The selected profile will be deleted.

Web Page Changes for VPN Backup

Corresponding web page (LAN to LAN) will be changed if VPN Backup is enabled. Refer to the following figures.

Dial-in call direction and Idle Timeout will be dimmish and cannot be used.

1. Common Settings

Profile Name <input type="text" value="2.29"/>	Call Direction <input type="radio"/> Both <input checked="" type="radio"/> Dial-Out <input type="radio"/> Dial-In
<input checked="" type="checkbox"/> Enable this profile	<input type="checkbox"/> Always on
VPN Connection Through: <input type="text" value="WAN1 Only"/>	Idle Timeout <input type="text" value="0"/> second(s)
	<input type="checkbox"/> Enable PING to keep alive
	PING to the IP <input type="text"/>

All the items in Allowed Dial-in Type will be dimmish and cannot be used.

Allowed Dial-In Type <input checked="" type="checkbox"/> ISDN <input checked="" type="checkbox"/> FFTP <input checked="" type="checkbox"/> IPsec Tunnel <input checked="" type="checkbox"/> L2TP with IPsec Policy <input type="text" value="Must"/> <input type="checkbox"/> Specify Remote VPN Gateway Peer VPN Server IP <input type="text"/> or Peer ID <input type="text"/>	Username <input type="text"/> Password <input type="text"/> VJ Compression <input checked="" type="radio"/> On <input type="radio"/> Off IKE Authentication Method <input checked="" type="checkbox"/> Pre-Shared Key IKE Pre-Shared Key <input type="text"/> <input type="checkbox"/> Digital Signature(X.509) <input type="text" value="None"/> IPsec Security Method <input checked="" type="checkbox"/> Medium (A-I) -high (ESP) <input checked="" type="checkbox"/> DES <input checked="" type="checkbox"/> 3DES <input checked="" type="checkbox"/> AES Callback Function (CBCP) <input type="checkbox"/> Enable Callback Function <input type="checkbox"/> Use the Following Number to Callback Callback Number <input type="text"/> Callback Budget <input type="text"/> minute(s)
--	---

My WAN IP and Remote Gateway IP will be dimmish and cannot be used.

4. TCP/IP Network Settings

My WAN IP <input type="text" value="0.0.0.0"/>	RIP Direction <input type="text" value="Disable"/>
Remote Gateway IP <input type="text" value="0.0.0.0"/>	From first subnet to remote network, you have to do <input type="text" value="Route"/>
Remote Network IP <input type="text" value="192.168.1.0"/>	
Remote Network Mask <input type="text" value="255.255.255.0"/>	<input type="checkbox"/> Change default route to this VPN tunnel (Only single WAN supports this)
<input type="button" value="More"/>	

In addition, after configuring VPN Backup profile(s), the Connection Management in VPN and Remote Access will be changed. Before adding a new VPN Backup profile, the webpage will be shown as the following:

VPN and Remote Access >> Connection Management

Dial-out Tool Refresh Seconds : 10 Refresh

General Mode: (2.5) 192.168.2.5 Dial

Backup Mode: Dial

VPN Connection Status

Current Page: 1

Page No. Go >>

VPN	Type	Remote IP	Virtual Network	Tx Pkts	Tx Rate	Rx Pkts	Rx Rate	UpTime
-----	------	-----------	-----------------	---------	---------	---------	---------	--------

After adding a new VPN Backup profile, it will be listed in Backup Mode drop-down list for you to choose for dialing.

VPN and Remote Access >> Connection Management

Dial-out Tool Refresh Seconds : 10 Refresh

General Mode: (2.2) 192.168.2.2 Dial

Backup Mode: (VpnLB) 192.168.2.103 Dial

VPN Connection Status

Current Page: 1

Page No. Go >>

VPN	Type	Remote IP	Virtual Network	Tx Pkts	Tx Rate	Rx Pkts	Rx Rate	UpTime
-----	------	-----------	-----------------	---------	---------	---------	---------	--------

Examples for VPN Backup Profile

Here provides two situations that you can take advantages of VPN Backup profile mechanism.

Example 1: A VPN Backup profile with member 1 (IPSec type) and Member 2(L2TP over IPSec) has been created for Router A for connecting with Router B. In general, Router A connects to Router B through Member 1 VPN tunnel (with IPSec type).

VPN and Remote Access >> VPN Backup Management

Backup Profile List | Set to Factory Default |

Note: [Active:NO]The LAN-to-LAN Profile is disable or under Dial-In(Call Direction) at present.

No.	Status	Name	Member1(Active)Type	Member2(Active)Type
1	v	VpnBackup	3(YES)IPSec	4(YES)L2TP over IPSec(MUST)
2	v	PptpBackup	1(YES)PPTP	2(YES)PPTP

Status ☒ Enable ☐ Disable

Profile Name

Member1

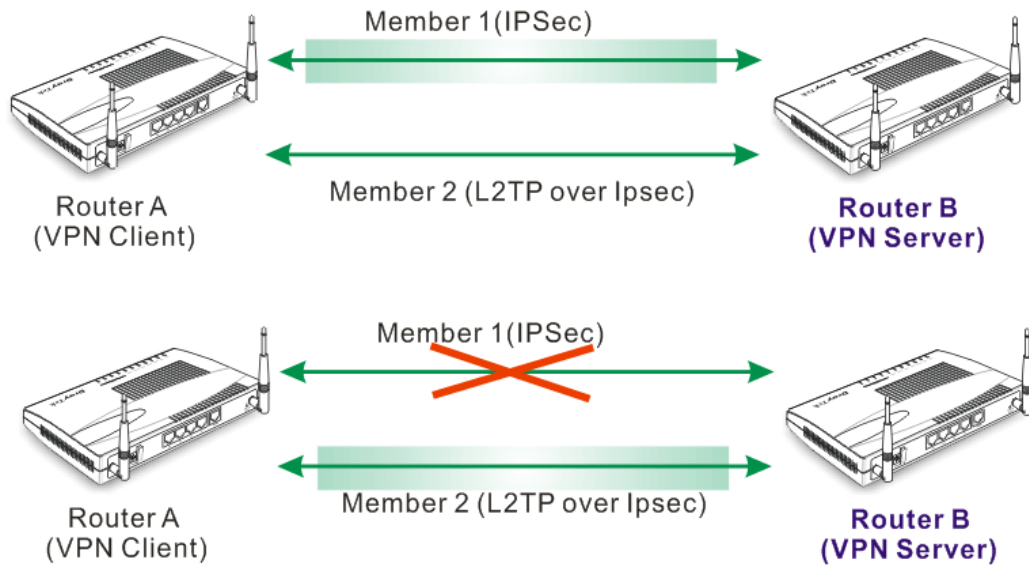
Please choose the combination that you want.

Member2

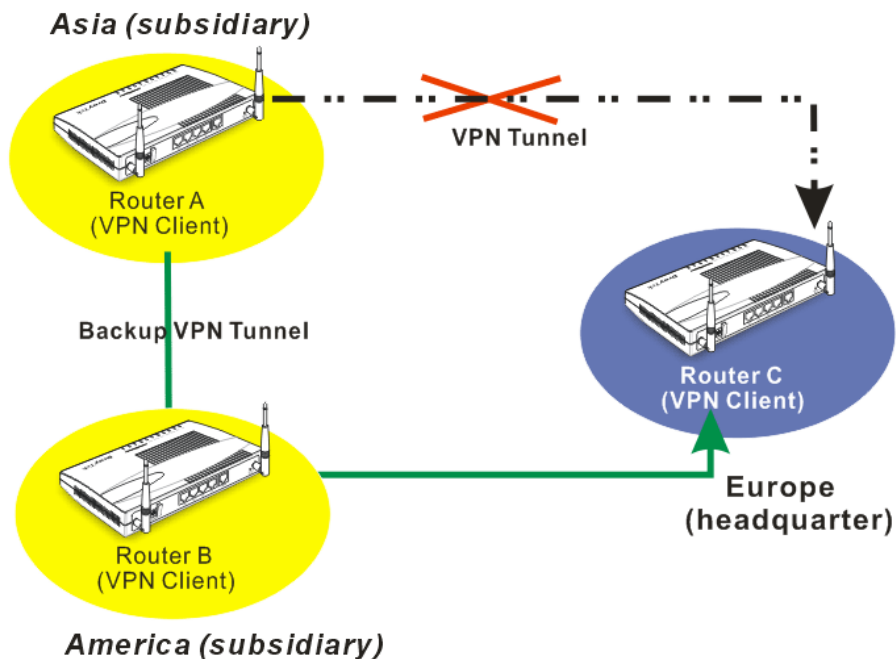
Please choose the combination that you want.

No.	<Name>	<Connection-Type>	<VPN ServerIP(Private Network)>
5	2.2	L2TP	192.168.2.2(192.168.26.0)
6	27	IPSec	192.168.0.27(192.168.27.0)
7	28	PPTP	192.168.0.28(192.168.28.0)
8	29	L2TP over IPSec(NICE)	192.168.0.29(192.168.29.0)
9	30	L2TP over IPSec(NICE)	192.168.0.30(192.168.30.0)
10	31	L2TP over IPSec(NICE)	192.168.0.31(192.168.31.0)
11	32	L2TP over IPSec(NICE)	192.168.0.32(192.168.32.0)

However, if the connection is off-line, Router A will use Member 2 VPN tunnel (with L2TP over IPsec) instead to connect Router B right away.



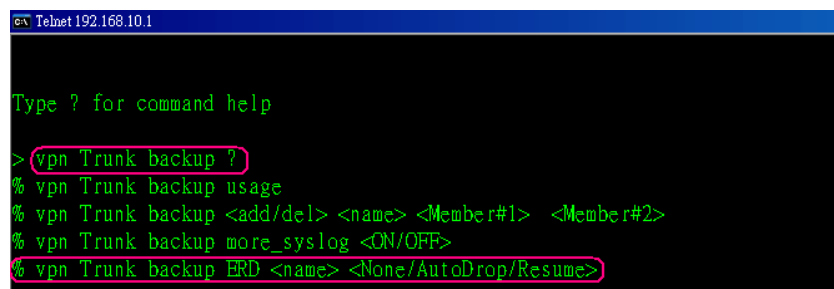
Example 2: Subsidiary in Asia can use vigor router as VPN client. Every day it should transmit ERP, Mail or order information to headquarter in Europe. The Vigor router can build another backup VPN tunnel to subsidiary in America through LAN to LAN, and the VPN server in the subsidiary in American can build Routing /RIP. When the VPN tunnel is off-line, the subsidiary in Asia can send the data (that should transmit to headerquarter in Europe) to the subsidiary in America, then the subsidiary in America transmit the data to headerquarter in Europe through VPN server by using VPN tunnel backup connection.



4.10 ERD Mechanism for VPN Backup

To use ERD (Environment Recovery Detection) mechanism for VPN Backup, please follow the steps listed below:

1. Click **Start >> Run** and type **Telnet 192.168.1.1** in the Open box as below. Note that the IP address in the example is the default address of the router. If you have changed the default, enter the current IP address of the router.
2. Click **OK**. The Telnet terminal will be open. If an administrator password has not already been assigned, follow the on-screen instructions to assign one.
3. After assigning a password, type **?**. You will see a list of valid/common commands depending on the router that you use.
4. For using ERD mechanism, please type “vpn Trunk backup?”. The available commands will be shown as the following figure.



```
cn Telnet 192.168.10.1

Type ? for command help

> vpn Trunk backup ?
% vpn Trunk backup usage
% vpn Trunk backup <add/del> <name> <Member#1> <Member#2>
% vpn Trunk backup more_syslog <ON/OFF>
% vpn Trunk backup ERD <name> <None/AutoDrop/Resume>
```

(1) To inquire current ERD setting

```
> vpn Trunk backup ERD VpnBackup -----> (name of Trunk profile)
```

(2) None Mode (Default Setting)

Such mode makes all of the dial-out VPN Backup profiles being activated alternately. Request Background: Some of users think if VPN tunnel connected again, it is Environment Recovery Detection. For such users, use None mode.

To set ERD None mode

```
> vpn Trunk backup ERD VpnBackup None
```

(3) Resume Mode

When VPN connection breaks down, Member1 is a top priority for the system to do VPN connection again.

Request Background: Some of users hope the connection can be continuous and not breaking down (maybe they will have thousands of orders coming within one minute). If the network connection breaks down, the users must connect from the first VPN server and spend lots of time. Such mode can solve their problems.

To set ERD Resume mode

```
> vpn Trunk backup ERD VpnBackup Resume
```

(4) AutoDrop Mode

Detect VPN connection periodically (by setting value for “second”). If VPN server for Member 1 has completed the network connection, current VPN Tunnel backup connection will be off-line.

Request Background: Some of users think it is not really environment recovery detection to borrow VPN tunnels from branches for connecting with the headquarters. The system should connect to headquarters automatically and that is called ERD.

To set ERD AutoDrop mode

- To check current status of AutoDrop

```
> vpn Trunk backup ERD VpnBackup AutoDrop
```

- To set AutoDrop

```
> vpn Trunk backup ERD VpnBackup AutoDrop 3600
```

- Why use <second> - AutoDrop might cause unstable condition for data transmitting. To solve the problem, you can set value for second to specify valid time for sending data out.
- When set value for <second> with “0”: VPN tunnel that does not join Member1 will try to connect with VPN server of Member1 for every six seconds. Once the connection is successful, current transmitting data (mail, video conference, or other) will be dropped immediately.
- When set value for <second> with “1 ~ 4294967295”: The administrator can try to connect with VPN server within certain time. Once the connection is successful, current transmitting data (mail, video conference, or other) will be dropped immediately. For example, if you type “3600” as the value for <second>, AutoDrop will be done with 30 seconds (3531 ~ 3600) for the backup VPN tunnel. If you set “30” as the value for <second>, it will be regarded as “0”.

5

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.

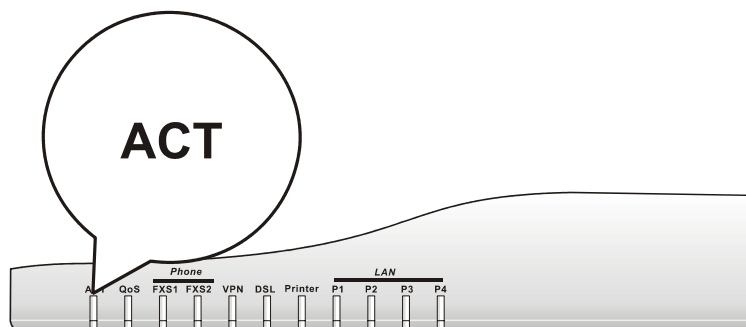
- Checking if the hardware status is OK or not.
- Checking if the network connection settings on your computer are OK or not.
- Pinging the router from your computer.
- Checking if the ISP settings are OK or not.
- Backing to factory default setting if necessary.

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.

5.1 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 “**2.1 Hardware Installation**” to execute the hardware installation again. And then, try again.

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

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

For Windows

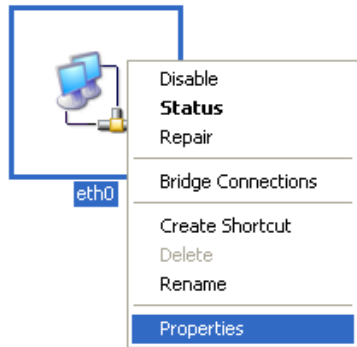


The example is based on Windows XP. As to the examples for other operation systems, please refer to the similar steps or find support notes in www.draytek.com.

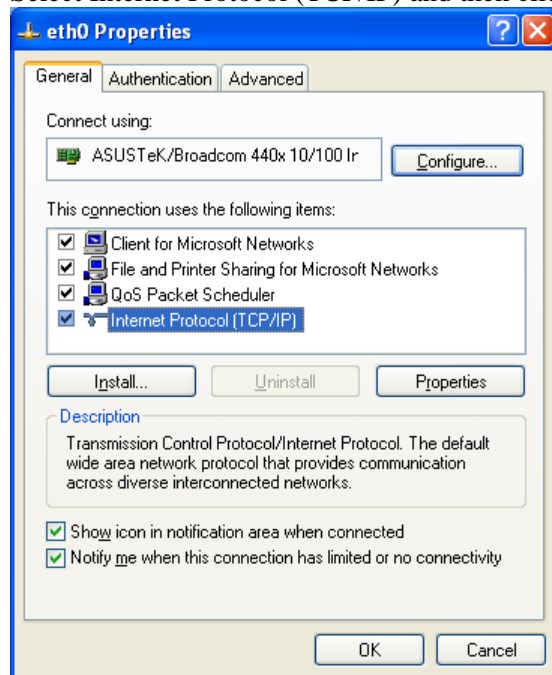
1. Go to Control Panel and then double-click on Network Connections.



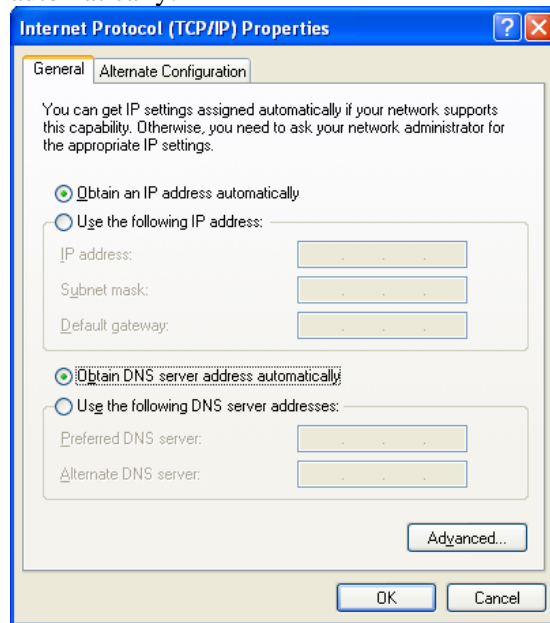
2. Right-click on Local Area Connection and click on Properties.



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

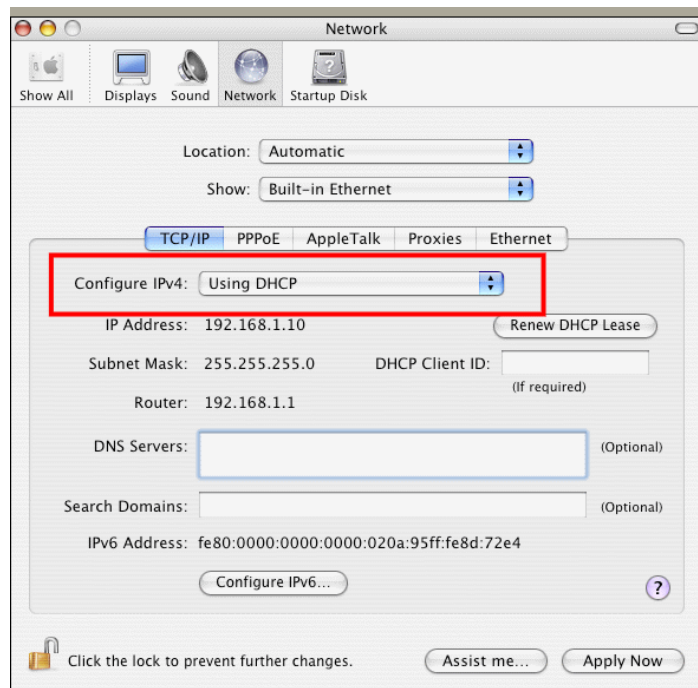


4. Select Obtain an IP address automatically and Obtain DNS server address automatically.



For MacOs

1. Double click on the current used MacOs on the desktop.
2. Open the **Application** folder and get into **Network**.
3. On the **Network** screen, select **Using DHCP** from the drop down list of Configure IPv4.



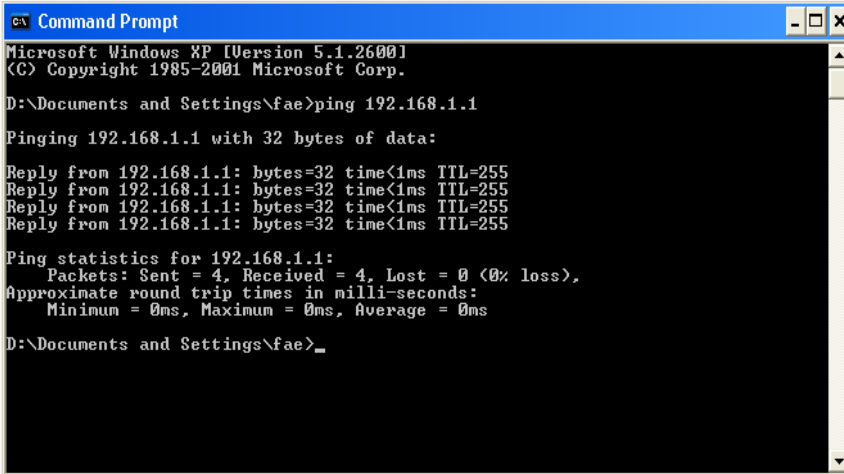
5.3 Pinging the Router from Your Computer

The default gateway IP address of the router is 192.168.1.1. For some reason, you might need to use “ping” command to check the link status of the router. **The most important thing is that the computer will receive a reply from 192.168.1.1.** If not, please check the IP address of your computer. We suggest you setting the network connection as **get IP automatically**. (Please refer to the section 4.2)

Please follow the steps below to ping the router correctly.

For Windows

1. Open the **Command Prompt** window (from **Start menu> Run**).
2. Type **command** (for Windows 95/98/ME) or **cmd** (for Windows NT/ 2000/XP). The DOS command dialog will appear.



```

C:\ Command Prompt
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

D:\Documents and Settings\fae>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:

Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

D:\Documents and Settings\fae>_

```

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

For MacOs (Terminal)

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


```
Terminal — bash — 80x24
Last login: Sat Jan  3 02:24:18 on ttty1
Welcome to Darwin!
Vigor10:~ draytek$ ping 192.168.1.1
PING 192.168.1.1 (192.168.1.1): 56 data bytes
64 bytes from 192.168.1.1: icmp_seq=0 ttl=255 time=0.755 ms
64 bytes from 192.168.1.1: icmp_seq=1 ttl=255 time=0.697 ms
64 bytes from 192.168.1.1: icmp_seq=2 ttl=255 time=0.716 ms
64 bytes from 192.168.1.1: icmp_seq=3 ttl=255 time=0.731 ms
64 bytes from 192.168.1.1: icmp_seq=4 ttl=255 time=0.72 ms
^C
--- 192.168.1.1 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 0.697/0.723/0.755 ms
Vigor10:~ draytek$
```

5.4 Checking If the ISP Settings are OK or Not

Click **WAN>> Internet Access** and then check whether the ISP settings are set correctly.

WAN >> Internet Access

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

Static or Dynamic IP

None

PPPoE

Static or Dynamic IP

PPTP/L2TP

For PPPoE Users

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

WAN >> Internet Access

WAN 1

PPPoE Client Mode

☐ Enable ☒ Disable

ISP Access Setup

Username

Password

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

=> , , ,

ISDN Dial Backup Setup

Dial Backup Mode

WAN Connection Detection

Mode

Ping IP

TTL:

MTU (Max: 1492)

PPP/MP Setup

PPP Authentication

Idle Timeout second(s)

IP Address Assignment Method (IPCP)

Fixed IP: ☐ Yes ☒ No (Dynamic IP)

Fixed IP Address

☒ Default MAC Address

☐ Specify a MAC Address

MAC Address:

For Static/Dynamic IP Users

1. Check if the **Enable** option is selected.
2. Check if **IP address**, **Subnet Mask** and **Gateway** are entered with correct values that you **got from** your **ISP**.

WAN 1

Static or Dynamic IP (DHCP Client) <input checked="" type="radio"/> Enable <input type="radio"/> Disable		WAN IP Network Settings WAN IP Alias	
ISDN Dial Backup Setup Dial Backup Mode: None		<input type="radio"/> Obtain an IP address automatically Router Name: <input type="text"/> * Domain Name: <input type="text"/> * <small>* : Required for some ISPs</small>	
Keep WAN Connection <input type="checkbox"/> Enable PING to keep alive PING to the IP: <input type="text"/> PING Interval: 0 minute(s)		<input checked="" type="radio"/> Specify an IP address IP Address: 172.16.3.229 Subnet Mask: 255.255.0.0 Gateway IP Address: 172.16.3.4	
WAN Connection Detection Mode: ARP Detect Ping IP: <input type="text"/> TTL: <input type="text"/>		DNS Server IP Address Primary IP Address: <input type="text"/> Secondary IP Address: <input type="text"/>	
MTU 1442 (Max: 1500)		<input checked="" type="radio"/> Default MAC Address <input type="radio"/> Specify a MAC Address MAC Address: 00 50 7F DD 15 19	
RIP Protocol <input type="checkbox"/> Enable RIP			

OK

Cancel

5.5 Problems for 3G Network Connection

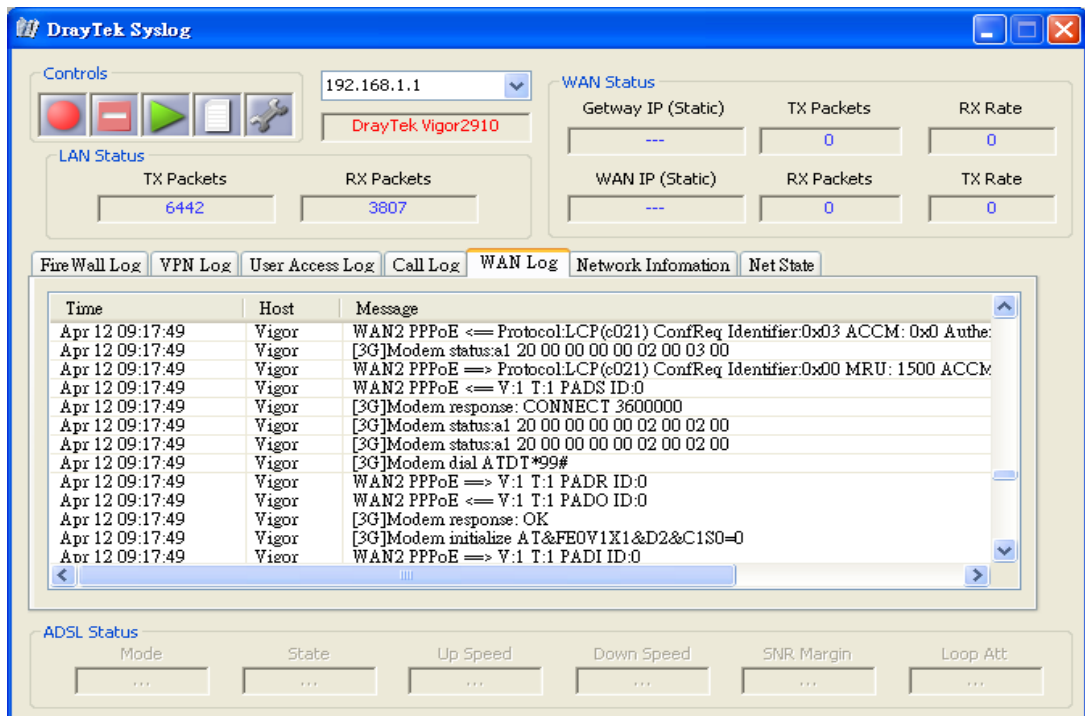
When you have trouble in using 3G network transmission, please check the following:

Check if USB LED lights on or off

You have to wait about 15 seconds after inserting 3G USB Modem into your Vigor2910. Later, the USB LED will light on which means the installation of USB Modem is successful. If the USB LED does not light on, please remove and reinsert the modem again. If it still fails, restart Vigor2910.

USB LED lights on but the network connection does not work

Check the PIN Code of SIM card is disabled or not. Please use the utility of 3G USB Modem to disable PIN code and try again. If it still fails, it might be the compliance problem of system. Please open DrayTek Syslog Tool to capture the connection information (WAN Log) and send the page (similar to the following graphic) to the service center of DrayTek.



Transmission Rate is not fast enough

Please connect your Notebook with 3G USB Modem to test the connection speed to verify if the problem is caused by Vigor2910. In addition, please refer to the manual of 3G USB Modem for LED Status to make sure if the modem connects to Internet via HSDPA mode. If you want to use the modem indoors, please put it on the place near the window to obtain better signal receiving.

5.6 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.

Reboot System

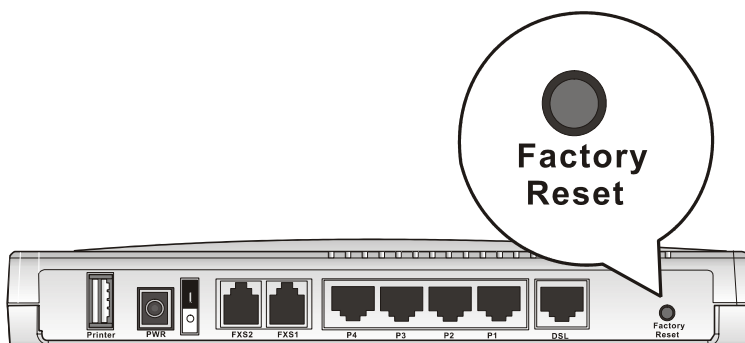
Do You want to reboot your router ?

- ☒ Using current configuration
- ☐ Using factory default configuration

OK

Hardware Reset

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



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

5.7 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.