

VigorIPPBX 2820 Series



Your reliable networking solutions partner

User's Guide

Vigor*IPPBX* 2820 Series User's Guide

Version: 2.01 Date: 24/09/2009

Copyright Information

Copyright Declarations	Copyright 2009 All rights reserved. This publication contains information that is protected by copyright. No part may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language without written permission from the copyright holders.			
Trademarks	 The following trademarks are used in this document: Microsoft is a registered trademark of Microsoft Corp. Windows, Windows 95, 98, Me, NT, 2000, XP, Vista and Explorer are trademarks of Microsoft Corp. Apple and Mac OS are registered trademarks of Apple Inc. Other products may be trademarks or registered trademarks of their respective manufacturers. 			

Safety Instructions and Approval

Safety Instructions	 Read the installation guide thoroughly before you set up the router. The router is a complicated electronic unit that may be repaired only be authorized and qualified personnel. Do not try to open or repair the router yourself. Do not place the router in a damp or humid place, e.g. a bathroom. The router should be used in a sheltered area, within a temperature range of +5 to +40 Celsius. Do not expose the router to direct sunlight or other heat sources. The housing and electronic components may be damaged by direct sunlight or heat sources.
	 Do not deploy the cable for LAN connection outdoor to prevent electronic shock hazards. Keep the package out of reach of children. When you want to dispose of the router, please follow local regulations on conservation of the environment.
Warranty	We warrant to the original end user (purchaser) that the router will be free from any defects in workmanship or materials for a period of two (2) years from the date of purchase from the dealer. Please keep your purchase receipt in a safe place as it serves as proof of date of purchase. During the warranty period, and upon proof of purchase, should the product have indications of failure due to faulty workmanship and/or materials, we will, at our discretion, repair or replace the defective products or components, without charge for either parts or labor, to whatever extent we deem necessary tore-store the product to proper operating condition. Any replacement will consist of a new or re-manufactured functionally equivalent product of equal value, and will be offered solely at our discretion. This warranty will not apply if the product is modified, misused, tampered with, damaged by an act of God, or subjected to abnormal working conditions. The warranty does not cover the bundled or licensed software of other vendors. Defects which do not significantly affect the usability of the product will not be covered by the warranty. We reserve the right to revise the manual and online documentation and to make changes from time to time in the contents hereof without obligation to notify any person of such revision or changes.
Be a Registered Owner	Web registration is preferred. You can register your Vigor router via http://www.draytek.com.
Firmware & Tools Updates	Due to the continuous evolution of DrayTek technology, all routers will be regularly upgraded. Please consult the DrayTek web site for more information on newest firmware, tools and documents.
	http://www.draytek.com

European Community Declarations

Manufacturer: DrayTek Corp.

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

Product: Vigor*IPPBX* 2820

DrayTek Corp. declares that VigorIPPBX 2820 of routers are in compliance with the following essential requirements and other relevant provisions of R&TTE Directive 1999/5/EEC.

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

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

Regulatory Information

Federal Communication Commission Interference Statement

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

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

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

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

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

Please visit http://www.draytek.com/user/AboutRegulatory.php.



This product is designed for DSL, ISDN, and POTS 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

Chapter	1: Preface	1
	1.1 Web Configuration Buttons Explanation	1
	1.2 LED Indicators and Connectors	2
	1.2.1 For VigorIPPBX 2820 1.2.2 For VigorIPPBX 2820n	
	1.3 Hardware Installation	7
	1.4 ISDN Phone Adapter Installation	
	1.5 Printer Installation	9
Chapter	2: Configuring Basic Settings	15
	2.1 Changing Password	15
	2.2 Quick Start Wizard	17
	2.2.1 PPPoE/PPPoA 2.2.2 1483 Bridged IP 2.2.3 1483 Routed IP	
	2.3 IPPBX Wizard	
	2.3.1 Extension & Group Setup 2.3.2 SIP Trunk Setup 2.3.3 Office Hours Setup	
	2.4 Online Status	
	2.5 Saving Configuration	
Chapter	3: Applications	31
	3.1 The Registration of 50 IP-based Telephone/Extensions	
	3.2 The IP Registration from Remote Site (through WAN Connection)	
	3.3 The Integration IP Registration with SIP Server	33
	3.4 The Integration VoIP Communications via SIP Server	
	3.5 The Integration with PSTN telephony	
	3.6 The Added ISDN Telephony	
	3.7 The Integrated ISDN line	
	3.8 The 4 B Channels of Two ISDN Lines	

	00
3.9 The Integration of ISDN PBX with One ISDN Line	39
3.10 The Deployment of ISDN PBX and PSTN Network	40
3.11 The Integration of ISDN Telephony and PSTN Network	41
3.12 The Integration of ISDN Telephony, PSTN Network and VoIP Connection	42

Chapter 4: Other Applications	.43
4.1 Create a LAN-to-LAN Connection Between Remote Office and Headquarter	. 43
4.2 Create a Remote Dial-in User Connection Between the Teleworker and Headquarter	. 50

	4.3 QoS Setting Example	54
	4.4 LAN – Created by Using NAT	
	4.5 Upgrade Firmware for Your Router	59
	4.6 Request a certificate from a CA server on Windows CA Server	62
	4.7 Request a CA Certificate and Set as Trusted on Windows CA Server	66
Chan	oter 5: Reference - Advanced Web Configuration	60
Спар	5.1 WAN	
	5.1.1 Basics of Internet Protocol (IP) Network 5.1.2 Network Connection by 3G USB Modem	
	5.1.3 General Setup	
	5.1.4 Internet Access	
	5.1.5 Multi-PVCs	
	5.1.6 Load-Balance Policy	
	5.2 LAN	
	5.2.1 Basics of LAN	-
	5.2.2 General Setup	
	5.2.3 Static Route	
	5.2.5 Bind IP to MAC	
	5.3 NAT	
	5.3.1 Port Redirection	
	5.3.2 DMZ Host	
	5.3.3 Open Ports	109
	5.4 Firewall	111
	5.4.1 Basics for Firewall	
	5.4.2 General Setup	
	5.4.3 Filter Setup 5.4.4 DoS Defense	
	5.5 Objects Settings	
	5.5.1 IP Object	
	5.5.2 IP Group 5.5.3 Service Type Object	
	5.5.4 Service Type Group	
	5.5.5 Keyword Object	
	5.5.6 Keyword Group	
	5.5.7 File Extension Object 5.5.8 IM Object	
	5.5.9 P2P Object	
	5.5.10 Misc Object	
	5.6 CSM	138
	5.6.1 IM/P2P Filter Profile	
	5.6.2 URL Content Filter Profile	
	5.6.3 Web Content Filter Profile	
	5.7 Bandwidth Management	
	5.7.1 Sessions Limit	
	5.7.2 Bandwidth Limit 5.7.3 Quality of Service	
	5.8 Applications	
	o.o Applications	



5.8.1 Dynamic DNS	
5.8.2 Schedule	
5.8.3 RADIUS 5.8.4 UPnP	
5.8.5 IGMP	
5.8.6 Wake on LAN	
5.9 VPN and Remote Access	
5.9.1 Remote Access Control	165
5.9.2 PPP General Setup	
5.9.3 IPSec General Setup	
5.9.4 IPSec Peer Identity	. 168
5.9.5 Remote Dial-in User	
5.9.6 LAN to LAN	
5.9.7 Connection Management	. 181
5.10 Certificate Management	
5.10.1 Local Certificate	
5.10.2 Trusted CA Certificate	
5.10.3 Certificate Backup	. 185
5.11 ISDN	. 185
5.11.1 Basic Concept	. 185
5.11.2 General Setup	
5.11.3 Dial to Single ISP	. 189
5.11.4 Dial to Dual ISPs	
5.11.5 Call Control	. 191
5.12 IP PBX	. 193
5.12.1 Extension	. 193
5.12.2 Line Setting	
5.12.3 Dial Plan	
5.12.4 PBX System	
5.12.5 PBX Status	. 230
5.13 Wireless LAN	-
5.13.1 Basic Concepts	
5.13.2 General Setup	
5.13.3 Security	
5.13.4 Access Control.	
5.13.5 WPS 5.13.6 WDS	
5.13.7 Advanced Setting	
5.13.8 AP Discovery	
5.13.9 Station List	
5.14 System Maintenance	. 247
5.14.1 System Status	. 247
5.14.2 TR-069	. 248
5.14.3 Administrator Password	. 249
5.14.4 Configuration Backup	
5.14.5 Syslog/Mail Alert	
5.14.6 Time and Date	
5.14.7 Management	
5.14.8 Reboot System 5.14.9 Firmware Upgrade	
5.15 Diagnostics	
5.15.1 Dial-out Trigger	
5.15.2 Routing Table	. ∠၁୪



5.15.3 ARP Cache Table 2	58
5.15.4 DHCP Table 2	59
5.15.5 NAT Sessions Table 2	
5.15.6 Ping Diagnosis	
5.15.7 Data Flow Monitor	
5.15.8 Traffic Graph	
5.15.9 Trace Route	03
apter 6: Trouble Shooting	65
6.1 Checking If the Hardware Status Is OK or Not 2	65
6.2 Checking If the Network Connection Settings on Your Computer Is OK or Not 2	66
6.3 Pinging the Router from Your Computer 2	68
6.4 Checking If the ISP Settings are OK or Not2	70
6.5 Problems for 3G Network Connection 2	73
6.6 Backing to Factory Default Setting If Necessary 2	74
6.7 Contacting Your Dealer 2	74
opendix: Hardware Specifications2	75

Chapter 1: Preface

VigorIPPBX 2820 is an ADSL and broadband router with WAN interface. It provides policy-based load-balance, fail-over and BOD (Bandwidth on Demand), also it integrates IP layer QoS, NAT session/bandwidth management to help users control works well with large bandwidth.

By adopting hardware-based VPN platform and hardware encryption of AES/DES/3DS, the router increases the performance of VPN greatly, and offers several protocols (such as IPSec/PPTP/L2TP) with up to 32 VPN tunnels.

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

VigorIPPBX 2820 can provide up to 50 extensions setup to let all registered IP phones in LAN or remote sites around the world to have unlimited free calls through Internet. Moreover, VigorIPPBX 2820 is able to establish multiple networking architectures corresponding to your current desire and future needs of growing communication. Its ISDN/PSTN compatibility lets you move from simple VoIP solution such as IP phone and Softphone to integrate with comprehensive networking infrastructure, such as ISDN and Analog phone line any time you need.

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

1.1 Web Configuration Buttons Explanation

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

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

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

1.2 LED Indicators and Connectors

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

The displays of LED indicators and connectors for the routers are different slightly. The following sections will introduce them respectively. If the model of router you have does not support ISDN and/or VoIP function, simply ignore the relational description.

Definitions for ISDN Ports

Below shows the names that displayed on front panel of the device and the WEB UI of this device.

Both **ISDN1 and ISDN2** port on front panel of the device are configurable for connecting phone or accessing Internet according to the settings that you adjust on WEB UI.

ISDN1-TE /**ISDN2-TE** (shown on WEB UI) is a port that used to connect ISDN line.

ISDN1-S0/ISDN2-S0 (shown on WEB UI) is a port that used to connect ISDN phone.

Please refer to **IP PBX>>PBX System>>Phone Settings** in User's Guide for detailed information.



Warning: When the orange LED lights (means ISDN NT mode), the ISDN port can be used to connect phone only. Wrong ISDN connection might cause severe damage on your device.

1.2.1 For VigorIPPBX 2820



LED		Status	Explanation
ACT (Activity)		Blinking	The router is powered on and running normally.
		Off	The router is powered off.
USB		On	A USB device is connected and active.
		Blinking	The data is transmitting.
CSM		On	The profile of CSM (Content Security Management) fo IM/P2P application is enabled from Firewall >> General Setup . (Such profile is established under CSM menu).
VPN		On	VPN tunnel is up and down.
DSL		On	The router is ready to access Internet through DSL link.
		Blinking	Slowly: The modem is ready. Quickly: The connection is training.
WAN 2		On	The WAN2 connection is ready.
		Blinking	It will blink while transmitting data.
Line		On	A PSTN phone call comes (in and out). However, when the phone call is disconnected, the LED will be off about six seconds later.
		Off	There is no PSTN phone call.
Phone		On	The phone connected to this port is off-hook.
		Off	The phone connected to this port is on-hook.
		Blinking	A phone call comes.
QoS		On	The QoS function is active.
LED on Con	nector		
ISDN1/2	Left LED (Orange)	On	ISDN-S0 (ISDN-NT) mode is active configured from IP PBX>>PBX System>>Phone Settings and an ISDN phone adapter is connected.
		Blinking	ISDN S0 (ISDN-NT) mode configured from IP
		C	PBX>>PBX System>>Phone Settings is active and ar ISDN phone adapter is not connected.
		Off	It means ISDN TE mode is active which is configured from IP PBX>>PBX System>>Phone Settings .
	Right LED (Green)	On	A phone adapter with phone set has been connected (ISDN-S0) or ISDN line has been connected

(ISDN-TE).

call) is transmitting.

The port is connected.

The port is disconnected.

The data is transmitting.

off-hook or a phone call comes.

Blinking

Off

On

Off

On

Off

Blinking

Left LED

Right LED

(Green)

(Green)

ISDN-S0 (ISDN-NT) mode, it means an ISDN phone is

In ISDN-TE mode, it means data, fax or voice (phone

It will be off if there is nothing connected.

The port is connected with 1000Mbps.

The port is connected with 10/100Mbps.

LAN 1(Giga)



	Left LED	On	The port is connected.
LAN 2/3/4	(Green)	Off	The port is disconnected.
		Blinking	The data is transmitting.
	Right LED	On	The port is connected with 100Mbps.
	(Green)	Off	The port is connected with 10Mbps.
	Left LED	On	The port is connected.
WAN 2	(Green)	Off	The port is disconnected.
		Blinking	The data is transmitting.
	Right LED	On	The port is connected with 100Mbps.
	(Green)	Off	The port is connected with 10Mbps.



Interface	Description		
Factory Reset	Restore the default settings.		
	Usage: Turn on the router (ACT LED is blinking). Press the hole and keep for more than 5 seconds. When you see the ACT LED begins to blink rapidly		
	than usual, release the button. Then the router will restart with the factory		
	default configuration.		
ISDN1/2	Connecter for ISDN line or ISDN phone adapter in particular condition.		
	Refer to section 2.2 for more details.		
Phone	Connecter for PSTN phone.		
Line	Connector for PSTN life line.		
LAN (1-4)	Connecters for local networked devices.		
DSL	Connecter for accessing the Internet through ADSL2/2+.		
WAN 2	Connecter for remote networked devices.		
USB	Connecter for a USB device (for 3G USB Modem or printer).		
PWR	Connecter for a power adapter.		
ON/OFF	Power Switch.		

1.2.2 For VigorIPPBX 2820n



LED	Status	Explanation
ACT (Activity)	Blinking	The router is powered on and running normally.
	Off	The router is powered off.
USB	On	A USB device is connected and active.
	Blinking	The data is transmitting.
CSM	On	The profile of CSM (Content Security Management) for IM/P2P application is enabled from Firewall >> General Setup . (Such profile is established under CSM menu).
WLAN	On	Wireless access point is ready.
	Blinking	It will blink while wireless traffic goes through. If ACT and WLAN LEDs blink simultaneously when WPS is working, and it will return to normal condition after two minutes. (You need to setup WPS within 2 minutes.)
DSL	On	The router is ready to access Internet through DSL link.
	Blinking	Slowly: The modem is ready. Quickly: The connection is training.
WAN 2	On	The WAN2 connection is ready.
	Blinking	It will blink while transmitting data.
Line	On	A PSTN phone call comes (in and out). However, when the phone call is disconnected, the LED will be off about six seconds later.
	Off	There is no PSTN phone call.
Phone	On	The phone connected to this port is off-hook.
	Off	The phone connected to this port is on-hook.
	Blinking	A phone call comes.
QoS	On	The QoS function is active.
LED on Connector		

ISDN1/2	Left LED (Orange)	On	ISDN-S0 (ISDN-NT) mode is active configured from IP PBX>>PBX System>>Phone Settings and an ISDN phone adapter is connected.
		Blinking	ISDN S0 (ISDN-NT) mode configured from IP PBX>>PBX System>>Phone Settings is active and an ISDN phone adapter is not connected.
		Off	It means ISDN TE mode is active which is configured from IP PBX>>PBX System>>Phone Settings .
	Right LED (Green)	On	A phone adapter with phone set has been connected (ISDN-S0) or ISDN line has been connected (ISDN-TE).
		Blinking	ISDN-S0 (ISDN-NT) mode, it means an ISDN phone is off-hook or a phone call comes. In ISDN-TE mode, it means data, fax or voice (phone call) is transmitting.
		Off	It will be off if there is nothing connected.



	Left LED	On	The port is connected.
LAN 1(Giga)	LAN 1(Giga) (Green)		The port is disconnected.
		Blinking	The data is transmitting.
	Right LED	On	The port is connected with 1000Mbps.
	(Green)	Off	The port is connected with 10/100Mbps.
	Left LED	On	The port is connected.
LAN 2/3/4	(Green)	Off	The port is disconnected.
		Blinking	The data is transmitting.
	Right LED	On	The port is connected with 100Mbps.
	(Green)	Off	The port is connected with 10Mbps.
	Left LED	On	The port is connected.
WAN 2	(Green)	Off	The port is disconnected.
		Blinking	The data is transmitting.
	Right LED	On	The port is connected with 100Mbps.
	(Green)	Off	The port is connected with 10Mbps.

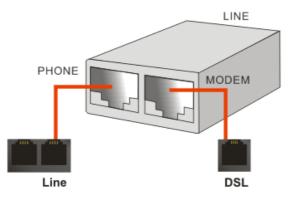


Interface	Description
Factory Reset	Restore the default settings.
	Usage: Turn on the router (ACT LED is blinking). Press the hole and keep
	for more than 5 seconds. When you see the ACT LED begins to blink rapidly
	than usual, release the button. Then the router will restart with the factory
	default configuration.
ISDN1/2	Connecter for ISDN line or ISDN phone adapter in particular condition.
	Refer to section 2.2 for more details.
Phone	Connecter for PSTN phone.
Line	Connector for PSTN life line.
LAN (1-4)	Connecters for local networked devices.
DSL	Connecter for accessing the Internet through ADSL2/2+.
WAN 2	Connecter for remote networked devices.
USB	Connecter for a USB device (for 3G USB Modem or printer).
PWR	Connecter for a power adapter.
ON/OFF	Power Switch.

1.3 Hardware Installation

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

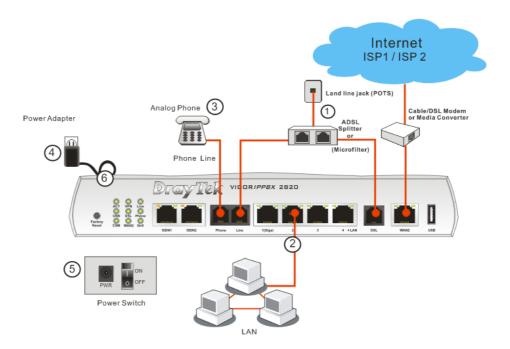
1. Connect the ADSL interface to the external ADSL splitter with an ADSL line cable. Also, connect Line interface to an external ADSL splitter.



For second WAN, connect the cable Modem/DSL Modem/Media Converter to WAN2 port of router with Ethernet cable (RJ-45).

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

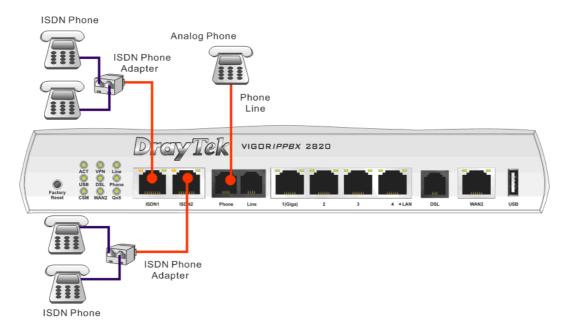
(For the detailed information of LED status, please refer to section 1.2.)



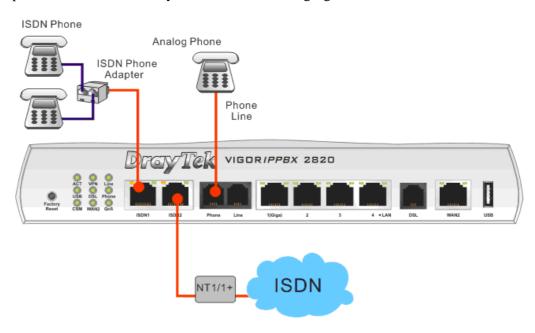
Caution: Each of the Phone ports can be connected to an analog phone only. Do not connect the phone ports to the telephone wall jack. Such connection might damage your router.

1.4 ISDN Phone Adapter Installation

ISDN1/2 port is configurable as NT or TE mode. When the user configures ISDN port as NT mode in **IP PBX>>PBX System>>Phone Settings**, the **orange** LED will light on to indicate **ISDN-NT** is selected. And by using ISDN phone adapters (coming from the router package), the user can connect several phones to the router for communication. Refer to the following figure for reference.



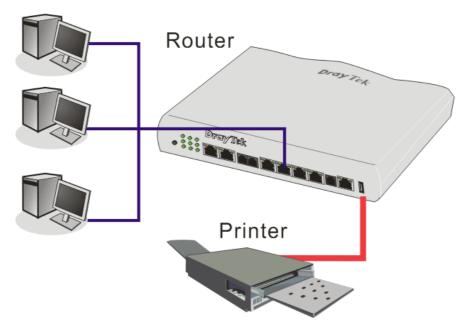
Yet, if the user configures ISDN port as TE Mode in **IP PBX>>PBX System>>Phone Settings**, the **green** LED will light on to indicate **ISDN-TE** is selected. Then, the port is specified for ISDN line only. Refer to the following figure for reference.



1.5 Printer Installation

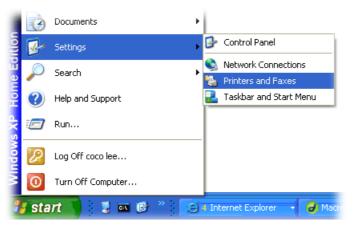
You can install a printer onto the router for sharing printing. All the PCs connected this router can print documents via the router. The example provided here is made based on Windows XP/2000. For Windows 98/SE, please visit <u>www.draytek.com</u>.

Printer Name: 192.168.1.1 Port Name: IP_192.168.1.1



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**.

Select the port you want y new port.	your printer to use. If the port is not listed, you	can create a
Use the following port:	LPT1: (Recommended Printer Port)	~
5	250	

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

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

7. Click Standard and choose Generic Network Card.

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

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



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

Install Printer Softwa The manufacturer a	re Id model determine which printer software to use.	
	cturer and model of your printer. If your printer ca isk. If your printer is not listed, consult your printe software.	
Manufacturer	Printers	
AST AT&T	Brother HL-1060 BR-Script2	-
Brother	Brother HL-1070 BR-Script2	
Bull Canon	BIOMER HL-TOPS7DPS	
→ → This driver is digitally s		e <u>H</u> ave Disk

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

Brother HL-1070 Properties	? 🛛
General Sharing Ports Advanc	ed Device Settings
Brother HL-1070	
Print to the following port(s). Docume checked port.	ents will print to the first free
Port Description	Printer
□ 3.250 Standard TCP/IP Por □ IP_1 Standard TCP/IP Por	
IP_1 Standard TCP/IP Por IP_1 Standard TCP/IP Por IP_1 Standard TCP/IP Por	t 📳 📗
IP_1 Standard TCP/IP Por	
IP_1 Standard TCP/IP Por PDF Local Port	PDE995
	PDF355
Add Por <u>t</u> <u>D</u> ele	te Port Configure Port
Enable bidirectional support	
	K Cancel Apply

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

ort Name:	IP_192.168.1.1
Printer Name or IP <u>A</u> ddress:	192.168.1.1
Protocol O <u>R</u> aw	<u>● L</u> PR
Raw Settings	
Port Number: 91	00
LPR Settings	
Queue Name: p1	
LPR Byte Counting Enab	led
SNMP Status Enabled	
Community Name: pul	blic
SNMP Device Index: 1	

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



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

FAQ - Basic	FAQ
01. What are the differences among these firmware file formats ?	Basic
02. How could I get the telnet command for routers ?	Advanced
03. How can I backup/restore my configuration settings ?	VPN
04. How do I reset/clear the router's password ?	DHCP
05. How to bring back my router to its default value ?	Wireless
06. How do I tell the type of my Vigor Router is AnnexA or AnnexB? (For ADSL model only	
07. Ways for firmware upgrade.	QoS
08. Why is SNMP removed in firmware 2.3.6 and above for Vigor2200 Series routers?	
09. I failed to upgrade Vigor Router's firmware from my Mac machine constantly, what shou I do?	Id Printer Servei
10. How to upgrade firmware of Vigor Router remotely ?	USB ISDN TA
1. How do I configure LPR printing on Windows2000/XP ?	IICR
AQ - Printer Server 1. How do I configure LPR printing on Windows2000/XP ? 2. How do I configure LPR printing on Windows98/Me ?	
1. How do I configure LPR printing on Windows2000/XP ?	
1. How do I configure LPR printing on Windows2000/XP ? 2. How do I configure LPR printing on Windows98/Me ?	
1. How do I configure LPR printing on Windows2000/XP ? 2. How do I configure LPR printing on Windows98/Me ? 3. How do I configure LPR printing on Linux boxes ? 4. Why there are some strange print-out when I try to print my d P / 2300's print server?	
 How do I configure LPR printing on Windows2000/XP ? How do I configure LPR printing on Windows98/Me ? How do I configure LPR printing on Linux boxes ? Why there are some strange print-out when I try to print my d P / 2300's print server? What types of printers are compatible with Vigor router? 	ocuments through Vigor210
 How do I configure LPR printing on Windows2000/XP ? How do I configure LPR printing on Windows98/Me ? How do I configure LPR printing on Linux boxes ? Why there are some strange print-out when I try to print my d P / 2300's print server? What types of printers are compatible with Vigor router? What are the limitations in the USB Printer Port of Vigor Rout 	ocuments through Vigor210
1. How do I configure LPR printing on Windows2000/XP ? 2. How do I configure LPR printing on Windows98/Me ? 3. How do I configure LPR printing on Linux boxes ? 4. Why there are some strange print-out when I try to print my d	ocuments through Vigor210

This page is left blank.

Chapter 2: Configuring Basic Settings

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

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

2.1 Changing Password

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

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



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

2. Open a web browser on your PC and type **http://192.168.1.1.** A pop-up window will open to ask for username and password. Please type "admin" as the username and leave blank for the password on the window. Next click **OK** for next screen.



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

Vigor <i>IPPE</i>	3X 2820)			Dray Tel www.draytek.com
Quick Start Wizard IPPBX Wizard Online Status	System Star Model Name Firmware Ver	: \	/igor2820 PBX		
WAN	Build Date/Tin		Sep 8 2009 18:07:32 11801 A Annex A		
LAN NAT					WAN 1
Firewall	MAC Addr	LAN	0-7F-94-E7-80	Link Status	: Disconnected
Objects Setting	1st IP Add		168.1.1	MAC Address	: 00-50-7E-94-E7-81
CSM	1st IP Aut		255.255.0	Connection	. 00-30-7F-94-E7-81
Bandwidth Management	DHCP Ser			IP Address	
Applications	DNS		95.1.1	Default Gateway	
/PN and Remote Access	DIVO	. 100.	55.1.1	Deladic Gateway	•
Certificate Management SDN		SIP Trun	k		WAN 2
P PBX	Index	Profile	Status	Link Status	: Connected
Wireless LAN	1.			MAC Address	: 00-50-7F-94-E7-82
System Maintenance	2.			Connection	: DHCP Client
Diagnostics	3.			IP Address	: 192.168.5.27
	4.			Default Gateway	: 192.168.5.1
	5.				
	6.	6		Wireless LAN	
				MAC Address	: 00-50-7F-94-E7-80
				Frequency Domain	: Europe
All Rights Reserved.				Firmware Version	: 1.8.1.0
				SSID	: default

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

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

System Maintenance >> Administrator Password Setup

Old Password	
New Password	
Confirm Password	

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

Connect to 192.1	68.1.1 🛛 💽 🔀
	GR
Login to the Router V	Veb Configurator
User name:	🛃 admin 🛛 💟
Password:	••••
	Remember my password
	OK Cancel

2.2 Quick Start Wizard

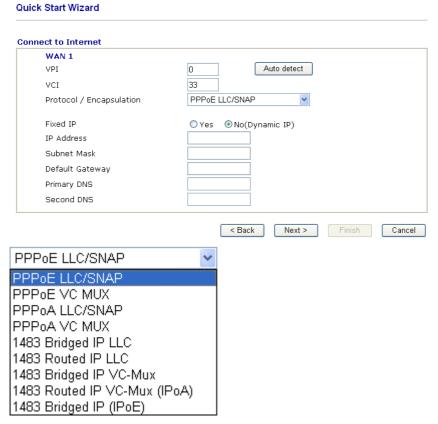
If your router can be under an environment with high speed NAT, the configuration provide here can help you to deploy and use the router quickly. The first screen of **Quick Start Wizard** is entering login password. After typing the password, please click **Next**.

Quick Start Wizard	
Enter login password	
Please enter an alpha-numeric	string as your Password (Max 23 characters).
New Password	••••
Confirm Password	••••
	<pre>< Back Next > Finish Cancel</pre>

On the next page as shown below, please select the WAN interface (WAN 1 or WAN2) that you use. If DSL interface is used, please choose WAN1; if WAN2 interface is used, please choose WAN2. Choose **Auto negotiation** as the physical type for your router. Then click **Next** for next step.

Interface	
WAN Interface:	WAN1 💌
Display Name:	
Physical Mode:	ADSL 💌
Physical Type:	Auto negotiation 👻

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



In the **Quick Start Wizard**, you can configure the router to access the Internet with different protocol/modes such as **PPPoE/PPPoA**, **1483 Bridged IP** or **1483 Routed IP**. The router supports the DSL WAN interface for Internet access.

2.2.1 PPPoE/PPPoA

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

84005756@hinet.net
•••••
••••••
<pre>< Back Next > Finish Cancel</pre>

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

Click Next for viewing summary of such connection.

Quick Start Wizard

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 1483 Bridged IP

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

Quick Start Wizard

WAN 1	
VPI	0 Auto detect
VCI	33
Protocol / Encapsulation	1483 Bridged IP LLC
Fixed IP	○Yes ⓒNo(Dynamic IP)
IP Address	
Subnet Mask	
Default Gateway	
Primary DNS	168.95.1.1
Second DNS	

Click Next for viewing summary of such connection.

Quick Start Wizard

e confirm your settings:	
WAN Interface: Physical Mode: Physical Type: VPI: VCI: Protocol / Encapsulation: Fixed IP: Primary DNS: Secondary DNS:	WAN1 ADSL Auto negotiation 0 33 1483 Bridge LLC No 168.95.1.1
	< Back Next > Finish Ca

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 1483 Routed IP

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

Quick Start Wizard

WAN 1	
VPI	0 Auto detect
VCI	33
Protocol / Encapsulation	1483 Routed IP VC-Mux (IPoA) 🔽
cius di to	
Fixed IP	○Yes ⊙No(Dynamic IP)
IP Address	
Subnet Mask	
Default Gateway	
Primary DNS	168.95.1.1
Second DNS	168.95.1.10

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

Quick Start Wizard

ase confirm your settings:	
WAN Interface:	WAN1
Physical Mode:	ADSL
Physical Type:	Auto negotiation
VPI:	0
VCI:	33
Protocol / Encapsulation:	1483 Route VCMUX
Fixed IP:	No
Primary DNS:	168.95.1.1
Secondary DNS:	168.95.1.10
	<pre>< Back Next > Finish Cance</pre>

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 IPPBX Wizard

IPPBX Wizard can guide the user to configure the required settings for this router within several steps. All the settings, also, can be configured by using **IP PBX** menu. However, the wizard is the most convenient and easy method for users.

Vigor <i>IPPB</i>	X 2820				Dray T www.draytek.	
	System Status					
IPPBX Wizard Online Status WAN	Model Name Firmware Version Build Date/Time ADSL Firmware Versi	: 3.5.3 : Sep (2820 PBX 8 2009 18:07:32 01_A Annex A			
NAT Firewall		LAN			WAN 1	
Objects Setting CSM Bandwidth Management Applications VPN and Remote Access Certificate Management	MAC Address 1st IP Address 1st Subnet Mask DHCP Server DNS	: 192.168	.255.0	Link Status MAC Address Connection IP Address Default Gateway	: Disconnected : 00-50-7F-94-E7-81 : : :	
SDN		SIP Trunk			WAN 2	
IP PBX Wireless LAN System Maintenance Diagnostics	Index Pr 1 2 3 4 5	ofile - - - -	Status 	Link Status MAC Address Connection IP Address Default Gateway	: Connected : 00-50-7F-94-E7-82 : DHCP Client : 192.168.5.27 : 192.168.5.1	
	6	-		Wir	eless LAN	
All Rights Reserved.				MAC Address Frequency Domain Firmware Version SSID	: 00-50-7F-94-E7-80 : Europe : 1.8.1.0 : default	

2.3.1 Extension & Group Setup

Click **IPPBX Wizard**. You can get the first screen as shown below.

IPPBX Wizard

Extension & Groups Setup : Index 1		
Extension Group Name:		(for example : sales)
Extension Group Number:		(for example : 100)
Start Number of the extension Group:		(for example : 101)
Number of extensions in this group:		(for example : 10, max = 20)
	ОК	

Index	Group Name	Group Extension	Hunt List(Max 20 Extension)
<u>1.</u>			
<u>2.</u>			
<u>3.</u>			
<u>4.</u>			
<u>5.</u>			
<u>6.</u>			
<u>7.</u>			
<u>8.</u>			
<u>9.</u>			
<u>10.</u>			
		< Bac	ck Next > Finish Cancel

Extension Group NameType a name as a display for this extension group.Extension Group NumberType the number of extension for such group.

Start Number of the extension Group	Type the start extension number for such group.
Number of extension in this group	Type the total number of the extension for such group.

When you finish the settings of group name, group number, start number, number of extension fields, please click **OK** to save them. The new added group will be displayed on the screen. You can set 10 groups for using in different conditions. Then click **Next** to access into next web page.

2.3.2 SIP Trunk Setup

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

IPPBX Wizard

Sip Trunk Setup : Index 1		
Profile Name:		(11 characters max.)
Domain/Realm:		(63 characters max.)
Proxy:		(63 characters max.)
Account Number/Name:		(63 characters max.)
Password:		(63 characters max.)
Trunk number:	001	(3 characters max.)
	OK	

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

< Back

Next >

Finish

Cancel

Profile Name	Type a name for this profile for identifying.
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)
Account Number/Name	Enter your account name of SIP Address, e.g. every text before @.
Password	The password provided to you when you registered with a SIP service.
Trunk Number	There are two ways to dial outside lines for an extension number. First, dial a short number and wait for a while. When dial tone appears, please dial the real outside line number. Second, dial a short number and then the real outside line number without waiting for dial tone. The short number is defined here as Trunk Number.



When you finish the settings of profile name, domain/realm, proxy, account number/name, password and trunk number fields, please click **OK** to save them. The new added profile will be displayed on the screen.

Index	Profile Name	Domain/Realm	Proxy	Account Number/Name	Trunk Number
<u>1.</u>	SalesMarket	192.168.1.55	nat.draytel.org:5065	salesgroup	001
<u>2.</u>					002
<u>3.</u>					003
<u>4.</u>					004
<u>5.</u>					005
<u>6.</u>					006
			< Back	Next > Finish	Cancel

You can set 6 profiles for using in different conditions. Then click **Next** to access into next web page.

2.3.3 Office Hours Setup

This page allows you to set office hours including starting point, ending point on duty day(s).

IPPBX Wizard

Now, You can make the work time schedule of your office	e.		
	Hour :	Min	
When do you start working in the morning	00 🔽	00 🛩	
When do you have a rest at noon	00 🛩	00 🛩	
When do you start working in the afternoon	00 🛩	00 🛩	
When do you leave the office	00 🔽	00 🛩	
Is this schedule available at weekend?	○ Yes	No	

When do you start workingUse the drop down menu to choose the time as the startingin the morningpoint in the morning.

When do you have a rest at noon	Use the drop down menu to choose the time as the ending point in the morning.
When do you start working in the afternoon	Use the drop down menu to choose the time as the starting point in the afternoon.
When do you leave the office	Use the drop down menu to choose the time as the ending point in the afternoon.
Is this schedule available at the weekend	If such schedule will be available in the weekend, simply click Yes , otherwise, click No .

work time schedule of your office.			
	Hour :	Min	
ing in the morning	08 🛰	00 🛰	
at noon	12 💌	00 🐱	
ing in the afternoon	13 💌	00 🐱	
office	17 💌	30 💌	
e at weekend?	○Yes	💿 No	
< Back Ne	ext >	Finish	Cancel

When you finish the settings, click **Finish** to save the settings and exit the wizard.

2.4 Online Status

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

Online status for PPPoE (WAN2)

Online Status

System Status				Sy	stem Up	time: 3:18:44
Primary		S	econdary			
LAN Status		Primary DNS:	192.168.66.1	Seconda	ry DNS:	168.95.1.1
IP Address	ТХ Р	ackets I	RX Packets			
192.168.1.1	749		552			
WAN 1 Status						>> <u>Release</u>
Enable	Line	Name	e Mode	Up Tim	e	
Yes	ADSL		DHCP C	lient 0:00:00	D	
IP	GW IP	TX Pa	ickets - TX Rate	e(Bps) RX Pac	kets R)	(Rate(Bps)
192.168.66.10	192,168.6	6.1 1	9	1	0	
WAN 2 Status					>	> <u>Drop PPPoE</u>
Enable	Line	Name	e Mode	Up Tim	e	
Yes	Ethernet		PPPoE	0:00:22	2	
IP	GW IP	TX Pa	ickets - TX Rate	e(Bps) RX Pac	kets R)	(Rate(Bps)
218,160,234,238	61.216.11	6.254 14	16	15	41	
ADSL Information	(ADSL	. Firmware Versio	n: 211011_A)			
ATM Statistics	TX Blocks	RX Bloc	ks Co	rrected Blocks	Uncorre	ected Blocks
:	18	23	0		0	
ADSL Status Mod	de Stat	e Up Sp	oeed Down	Speed SNR M	argin I	_oop Att.
G.D	мт ѕно	WTIME 10240	000 11936	000 0)

Online status for PPTP (for WAN2)

Online Status

System Status					System	Uptime: 3:18:44
Primary		Secondary				
LAN Status		Primary D	NS: 168.95	.1.1	Secondary DN	S: 168.95.1.1
IP Address	ТХ Р	ackets	RX Pac	kets		
192.168.1.1	480		339			
WAN 1 Status						
Enable	Line	r	Name	Mode	Up Time	
Yes	ADSL			Static IP	0:00:00	
IP	GW IP	1	TX Packets	TX Rate(Bps)	RX Packets	RX Rate(Bps)
192.168.66.52	192,168,6	6.1 :	L	9	1	16
WAN 2 Status						>> <u>Release</u>
Enable	Line	r	Vame	Mode	Up Time	
Yes	Ethernet			PPTP	0:00:28	
IP	GW IP	٦	TX Packets	TX Rate(Bps)	RX Packets	RX Rate(Bps)
192.168.129.11	192,168,1	29.1 8	3	12	10	9
ADSL Information	(ADSL	. Firmware V	/ersion: 211	011_A)		
ATM Statistics T	X Blocks	RX	Blocks	Corrected	Blocks Unco	orrected Blocks
4		З		0	2	
ADSL Status Mod	le Stat	e I	Up Speed	Down Speed	SNR Margin	Loop Att.
G.DM	ит ѕно	WTIME	1024000	12000000	8	0

Online status for Static IP (for WAN1)

Online Status

System Status 👘				System	Uptime: 3:18:44
Primary		Secon	dary		
LAN Status		Primary DNS: 168.9	95.1.1	Secondary DN	S: 168.95.1.1
IP Address	TX Pa	ckets RX Pa	ickets		
192.168.1.1	480	339			
WAN 1 Status					
Enable	Line	Name	Mode	Up Time	
Yes	ADSL		Static IP	0:00:00	
IP	GW IP	TX Packets	s TX Rate(Bps)	RX Packets	RX Rate(Bps)
192.168.66.52	192,168,66.	1 1	9	1	16
WAN 2 Status					>> <u>Release</u>
Enable	Line	Name	Mode	Up Time	
Yes	Ethernet		PPTP	0:00:28	
IP	GW IP	TX Packets	s TX Rate(Bps)	RX Packets	RX Rate(Bps)
192,168,129,11	192,168,129	9.1 8	12	10	9
ADSL Information	(ADSL F	irmware Version: 2:	11011_A)		
ATM Statistics	FX Blocks	RX Blocks	Corrected	l Blocks Unco	orrected Blocks
4	4	3	0	2	
ADSL Status Mod	de State	Up Speed	Down Speed	SNR Margin	Loop Att.
G.DI	MT SHOW	TIME 1024000	1200000	8	0

Online status for DHCP (WAN1)

Online Status

System Status				System	Uptime: 3:18:44
Primary		Seconda	ary		
LAN Status	Pr	imary DNS: 192.16	8.66.1	Secondary DN	IS: 168.95.1.1
IP Address	TX Pack	ets RX Pac	kets		
192.168.1.1	749	552			
WAN 1 Status					>> <u>Release</u>
Enable	Line	Name	Mode	Up Time	
Yes	ADSL		DHCP Client	0:00:00	
IP	GW IP	TX Packets	TX Rate(Bps)	RX Packets	RX Rate(Bps)
192.168.66.10	192,168,66,1	1	9	1	0
WAN 2 Status					>> <u>Drop PPPoE</u>
Enable	Line	Name	Mode	Up Time	
Yes	Ethernet		PPPoE	0:00:22	
IP	GW IP	TX Packets	TX Rate(Bps)	RX Packets	RX Rate(Bps)
218.160.234.238	61,216,116,2	54 14	16	15	41
ADSL Information	(ADSL Fir	mware Version: 211	011_A)		
ATM Statistics T	X Blocks	RX Blocks	Corrected	l Blocks – Unc	orrected Blocks
1	.8	23	0	0	
ADSL Status Mod	le State	Up Speed	Down Speed	SNR Margin	Loop Att.
G.DI	NT SHOWT	IME 1024000	11936000	0	0

Online status for ISDN enabled

Enable Yes	LIT	ne hernet	Nē	ime	M ode Static IP	<mark>uр ніт</mark> 00:00:0		
IP		V IP	тх	Packets			ets RX Rate	e(Bps)
172.17.3.4		2.17.3.2	0		0	0	0	
ADSL Infor	mation	(ADSL Fir	mware Ve	rsion: 212	1501_A)			
ATM Stati	istics TX B	locks	RX E	locks	Correct	ed Blocks	Uncorrected	Blocks
	0		0		0		0	
ADSL Sta	tus Mode	State	U	o Speed	Down Spe	ed SNR Ma	argin Loop	Att.
		READY	0		0	0	0	
ISDN Statu	IS				>> <u>Dia</u>	al ISDN >>	Drop B1 >>	Drop B2
Channel	Active Cor	nnection	TX Pkts	TX Rate (Bps)	RX Pkts	RX Rate (Bps)	Up Time	AOC
ISDN1- B1	Idle []		0	0	0	0	0:0:0	0
ISDN1- B2	Idle []		0	0	0	0	0:0:0	0
ISDN1-D	UP							
ISDN2- B1	2930 [192.	168.3.10]	19	9	10	3	0:0:36	0
ISDN2- B2	Idle []		0	0	0	0	0:0:0	0
ISDN2-D	UP							

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.
ISDN Status	
Channel Active Conn.	Displays the active connection status for each channel.
TX Pkts	Displays the total transmitted packets at the ISDN interface.
TX Rate	Displays the speed of transmitted octets at the ISDN interface.

RX Pkts	Displays the total number of received packets at the ISDN interface.
RX Rate	Displays the speed of received octets at the ISDN interface.
Up Time	Displays the total uptime of the interface.
AOC	Displays the charge information of the 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.

2.5 Saving Configuration

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

Status: Ready

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

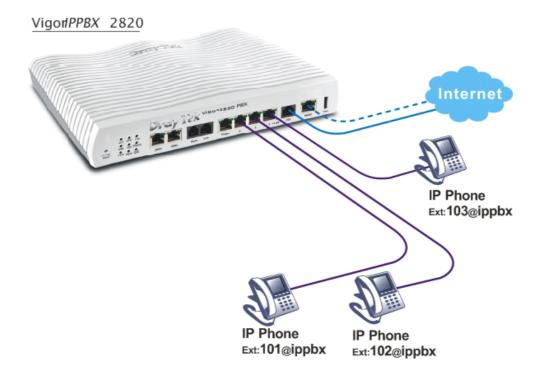
Settings Saved means your settings are saved once you click Finish or OK button.

This page is left blank.

Chapter 3: Applications

This chapter shows several scenarios for your reference to configure IP PBX for different purposes.

3.1 The Registration of 50 IP-based Telephone/Extensions



- The establishment through DSL Internet.
- Flexible second WAN for back-up.
- IP-based telephones are connected to LAN ports and set with ext. no. 101, 102 & 103.
- The IP-based telephones (101, 102, 103) are registered on the Vigor*IPPBX* 2820.

3.2 The IP Registration from Remote Site (through WAN Connection)

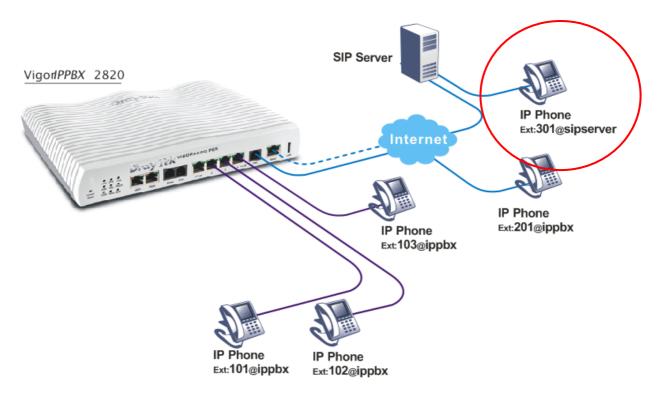
VigodPPBX 2820 Internet Internet IP Phone Ext:103@ippbx IP Phone Ext:101@ippbx IP Phone Ext:102@ippbx

- The establishment through DSL Internet.
- Flexible second WAN for back-up.
- IP-based telephones are connected to LAN ports and set with ext. no. 101, 102 & 103.
- The IP-based telephones (101, 102, 103) and remote IP-based phone are registered on the Vigor*IPPBX* 2820.
- The IP-based phone with ext. no. 201 is at remote site.

3.3 The Integration IP Registration with SIP Server

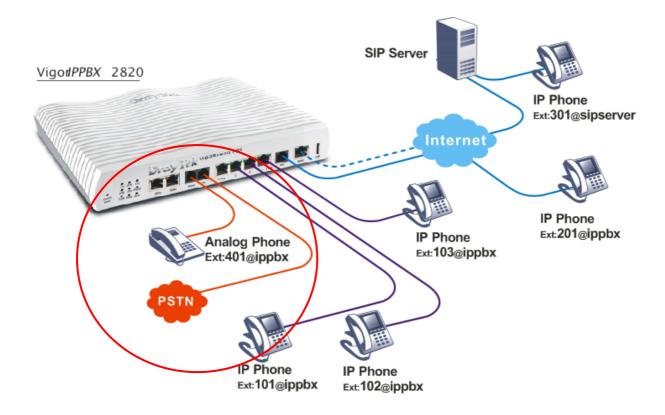
- The establishment through DSL Internet.
- Flexible second WAN for back-up.
- IP-based telephones are connected to LAN ports and set with ext. no. 101, 102 & 103.
- The IP-based telephones (101, 102, 103) and remote IP-based phone are registered on the Vigor*IPPBX* 2820.
- The IP-based phone with ext. no. 201 is at remote site.
- The Vigor*IPPBX* 2820 seamlessly integrate with ITSP services (allow you to register at a SIP server).

3.4 The Integration VoIP Communications via SIP Server



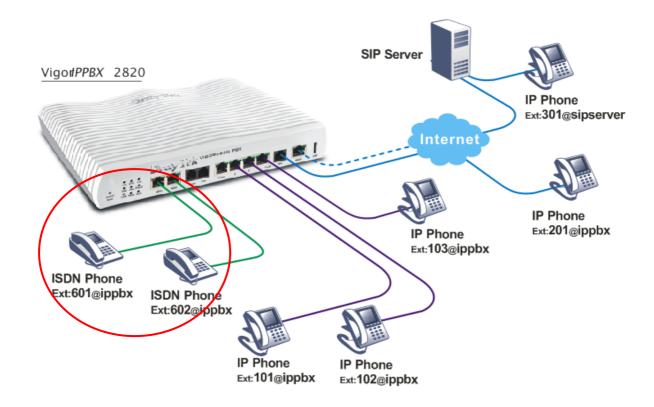
- The establishment through DSL Internet.
- Flexible second WAN for back-up.
- IP-based telephones are connected to LAN ports and set with ext. no. 101, 102 & 103.
- The IP-based telephones (101, 102, 103) and remote IP-based phone are registered on the Vigor*IPPBX* 2820.
- The IP-based phone with ext. no. 201 is at remote site.
- The Vigor*IPPBX* 2820 seamlessly integrate with ITSP services (allow you to register at a SIP server).
- The remote IP-based phone with ext. 301 is registered at a SIP server.

3.5 The Integration with PSTN telephony



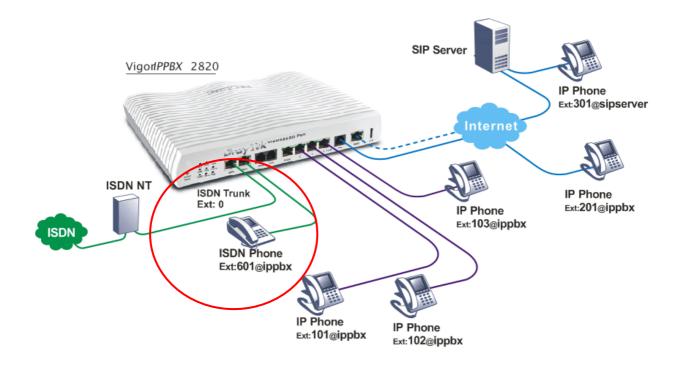
- The establishment through DSL Internet.
- Flexible second WAN for back-up.
- IP-based telephones are connected to LAN ports and set with ext. no. 101, 102 & 103.
- The IP-based telephones (101, 102, 103) and remote IP-based phone are registered on the Vigor*IPPBX* 2820.
- The IP-based phone with ext. no. 201 is at remote site.
- The Vigor*IPPBX* 2820 seamlessly integrate with ITSP services (allow you to register at a SIP server).
- The remote IP-based phone with ext. 301 is registered at a SIP server.
- The analog land line is connected to the "Line" port.
- The analog phone is connected to the "Phone" port and is using ext. no. 401 at the Vigor*IPPBX* 2820.

3.6 The Added ISDN Telephony



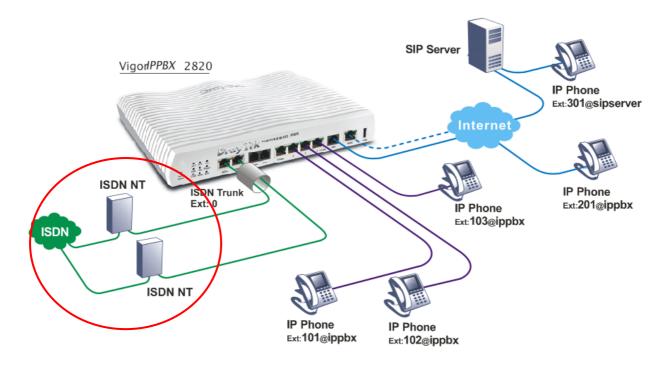
- The establishment through DSL Internet.
- Flexible second WAN for back-up.
- IP-based telephones are connected to LAN ports and set with ext. no. 101, 102 & 103.
- The IP-based telephones (101, 102, 103) and remote IP-based phone are registered on the Vigor*IPPBX* 2820.
- The IP-based phone with ext. no. 201 is at remote site.
- The Vigor*IPPBX* 2820 seamlessly integrate with ITSP services (allow you to register at a SIP server).
- The remote IP-based phone with ext. 301 is registered at a SIP server.
- The ISDN phones with ext. no. 601 and 602 are connected to NT-interface of the Vigor*IPPBX* 2820.

3.7 The Integrated ISDN line



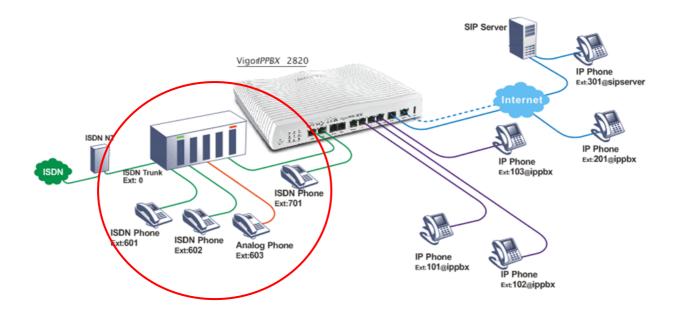
- The establishment through DSL Internet.
- Flexible second WAN for back-up.
- IP-based telephones are connected to LAN ports and set with ext. no. 101, 102 & 103.
- The IP-based telephones (101, 102, 103) and remote IP-based phone are registered on the Vigor*IPPBX* 2820.
- The IP-based phone with ext. no. 201 is at remote site.
- The Vigor*IPPBX* 2820 seamlessly integrate with ITSP services (allow you to register at a SIP server).
- The remote IP-based phone with ext. 301 is registered at a SIP server.
- The ISDN line is connected to TE-interface of the Vigor*IPPBX* 2820.
- The ISDN phone with ext. no. 601 is connected to NT-interface of the Vigor*IPPBX* 2820.

3.8 The 4 B Channels of Two ISDN Lines



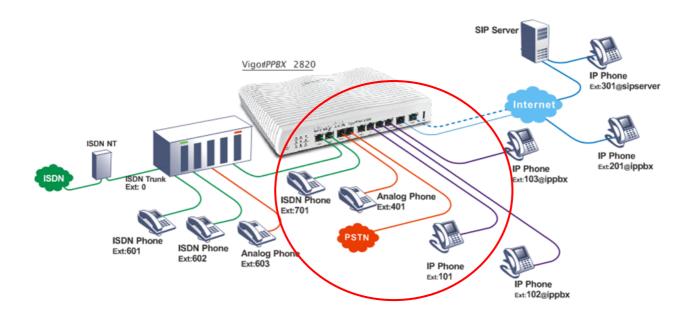
- The establishment through DSL Internet.
- Flexible second WAN for back-up.
- IP-based telephones are connected to LAN ports and set with ext. no. 101, 102 & 103.
- The IP-based telephones (101, 102, 103) and remote IP-based phone are registered on the Vigor*IPPBX* 2820.
- The IP-based phone with ext. no. 201 is at remote site.
- The Vigor*IPPBX* 2820 seamlessly integrate with ITSP services (allow you to register at a SIP server).
- The remote IP-based phone with ext. 301 is registered at a SIP server.
- The two ISDN lines are connected to two TE-interfaces of the *VigorIPPBX* 2820.

3.9 The Integration of ISDN PBX with One ISDN Line



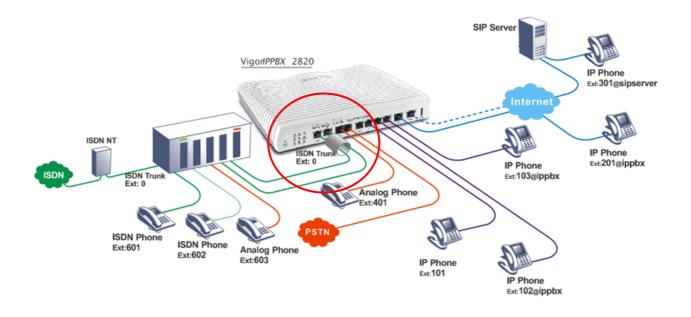
- The establishment through DSL Internet.
- Flexible second WAN for back-up.
- IP-based telephones are connected to LAN ports and set with ext. no. 101, 102 & 103.
- The IP-based telephones (101, 102, 103) and remote IP-based phone are registered On the Vigor*IPPBX* 2820.
- The IP-based phone with ext. no. 201 is at remote site.
- The Vigor*IPPBX* 2820 seamlessly integrate with ITSP services (allow you to register at a SIP server).
- The remote IP-based phone with ext. 301 is registered at a SIP server.
- The ISDN phone with ext. no. 701 is connected to NT-interface of the Vigor*IPPBX* 2820.
- The ISDN PBX is connected to TE-interface of the Vigor*IPPBX* 2820. The ISDN phones with ext. no. 601 and 602 are connected to ISDN PBX.
- The ISDN PBX also provides analog extensions to allow analog phones to be connected. The analog phone with ext. no. 603 is connected at the ISDN PBX.

3.10 The Deployment of ISDN PBX and PSTN Network



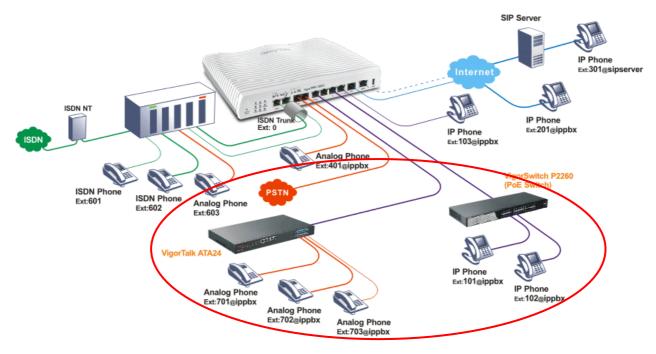
- The establishment through DSL Internet.
- Flexible second WAN for back-up.
- IP-based telephones are connected to LAN ports and set with ext. no. 101, 102 & 103.
- The IP-based telephones (101, 102, 103) and remote IP-based phone are registered on the Vigor*IPPBX* 2820.
- The IP-based phone with ext. no. 201 is at remote site.
- The Vigor*IPPBX* 2820 seamlessly integrate with ITSP services (allow you to register at a SIP server).
- The remote IP-based phone with ext. 301 is registered at a SIP server.
- The ISDN phone with ext. no. 701 is connected to NT-interface of the Vigor*IPPBX* 2820.
- The ISDN PBX is connected to TE-interface of the Vigor*IPPBX* 2820. The ISDN phones with ext. no. 601 and 602 are connected to ISDN PBX.
- The ISDN PBX also provides analog extensions to allow analog phones to be connected. The analog phone with ext. no. 603 is connected at the ISDN PBX.
- The analog land line is connected to the "Line" port.
- The analog phone is connected to the "Phone" port and is using ext. no. 401 at the Vigor*IPPBX* 2820.

3.11 The Integration of ISDN Telephony and PSTN Network



- The establishment through DSL Internet.
- Flexible second WAN for back-up.
- IP-based telephones are connected to LAN ports and set with ext. no. 101, 102 & 103.
- The IP-based telephones (101, 102, 103) and remote IP-based phone are registered on Vigor*IPPBX* 2820.
- The IP-based phone with ext. no. 201 is at remote site.
- The Vigor*IPPBX* 2820 seamlessly integrate with ITSP services (allow you to register at a SIP server).
- The remote IP-based phone with ext. 301 is registered at a SIP server.
- The ISDN phones with ext. no. 601 and 602 are connected to ISDN PBX.
- The ISDN PBX also provides analog extensions to allow analog phones to be connected. The analog phone with ext. no. 603 is connected at the ISDN PBX.
- The analog land line is connected to the "Line" port.
- The analog phone is connected to the "Phone" port and is using ext. no. 401 at Vigor*IPPBX* 2820.
- The ISDN PBX's two internal lines are connected to the TE-interfaces of the Vigor*IPPBX* 2820.

3.12 The Integration of ISDN Telephony, PSTN Network and VoIP Connection

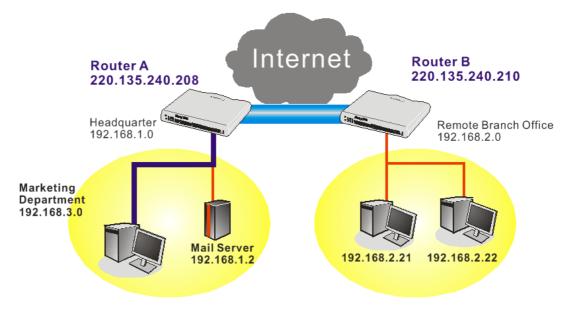


- The establishment through DSL Internet.
- Flexible second WAN for back-up.
- IP-based telephones with ext. no. 101 & 102 are connected to LAN ports of the VigorSwitch. Analog telephones with ext. no. 701, 702 & 703 are connected to the VigorTalk ATA24 and are registered at the VigorIPPBX 2820.
- The IP-based telephone with ext. no. 103 and remote IP-based phone ext. no. 201 are registered on the Vigor*IPPBX* 2820.
- The IP-based phone with ext. no. 201 is at remote site.
- The Vigor*IPPBX* 2820 seamlessly integrate with ITSP services (allow you to register at a SIP server).
- The remote IP-based phone with ext. 301 is registered at a SIP server.
- The ISDN phones with ext. no. 601 and 602 are connected to ISDN PBX.
- The ISDN PBX also provides analog extensions to allow analog phones to be connected. The analog phone with ext. no. 603 is connected at the ISDN PBX.
- The analog land line is connected to the "Line" port.
- The analog phone is connected to the "Phone" port and is using ext. no. 401 at Vigor*IPPBX* 2820.
- The ISDN PBX's two internal lines are connected to the TE-interfaces of the Vigor*IPPBX* 2820.

Chapter 4: Other Applications

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

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



Settings in Router A in headquarter:

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

.....

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

PPP General Setup			
PPP/MP Protocol		IP Address Assignmer	
Dial-In PPP	PAP or CHAP 🗸	(When DHCP Disable s	set)
Authentication		Start IP Address	192.168.1.200
Dial-In PPP Encryption (MPPE)	Optional MPPE		
Mutual Authentication	(PAP) 🔘 Yes 💽 No		
Username			
Password			

For using IPSec-based service, such as IPSec or L2TP with IPSec Policy, you have to



set general settings in **IPSec General Setup**, such as the pre-shared key that both parties have known.

VPN and Remote Access >> IPSec Ge	neral Setup
VPN IKE/IPSec General Setup Dial-in Set up for Remote Dial-in users and	Dynamic IP Client (LAN to LAN).
IKE Authentication Method	
Pre-Shared Key	••••
Confirm Pre-Shared Key	•••••
IPSec Security Method	
Medium (AH)	
Data will be authentic, but will	not be encrypted.
High (ESP) 🛛 DES 🗹 3DES	AES
Data will be encrypted and aut	nentic.
	OK Cancel

- 3. Go to LAN-to-LAN. Click on one index number to edit a profile.
- 4. Set **Common Settings** as shown below. You should enable both of VPN connections because any one of the parties may start the VPN connection.

VPN and Remote Access >> LAN to LAN

Profile Index : 1 1. Common Settings	
Profile Name Branch1	Call Direction 🛛 💿 Both 🔿 Dial-Out 🔘 Dial-In
Enable this profile	Always on
	Idle Timeout 300 second(s)
VPN Connection Through: WAN1 First 🌱	Enable PING to keep alive
Netbios Naming Packet 💿 Pass 🔘 Block	PING to the IP

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

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

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

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

Type of Server I am calling	Link Type	64k bps 💉	
O ISDN	Username	draytek	
• РРТР	Password		
O IPSec Tunnel	PPP Authentication		
L2TP with IPSec Policy None	VJ Compression	⊙ On ○ Off	
Dial Number for ISDN or Server IP/Host Name for VPN. (such as 5551234, draytek.com or 123.45.67.89)	IKE Authentication M • Pre-Shared Key	lethod	
220.135.240.210	IKE Pre-Shared Key		
	O Digital Signature(X.5)	609)	
	None 🗸		
	IPSec Security Metho	od	
	Medium(AH) High(ESP) DES without Authentication Advanced Index(1-15) in <u>Schedule</u> Setup: ,,,,		
	Callback Function (C		
	Require Remote to		
	Provide ISDN Num	ber to Remote	

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

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

3. Dial-In Settings	
Allowed Dial-In Type	
ISDN	Username ???
РРТР	Password
IPSec Tunnel	VJ Compression On Off
L2TP with IPSec Policy None	
·	IKE Authentication Method
Specify ISDN CLID or Remote VPN Gateway	Pre-Shared Key
Peer ISDN Number or Peer VPN Server IP	IKE Pre-Shared Key
220.135.240.210	Digital Signature(X.509)
or Peer ID	None 💙
	IPSec Security Method
	Medium (AH)
	High (ESP)
	🗹 DES 🗹 3DES 🗹 AES
	Collhash Superior (CB CB)
	Callback Function (CBCP)
	Enable Callback Function
	Use the Following Number to Callback
	Callback Number
	Callback Budget 0 minute(s)

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

Allowed Dial-In Type			
ISDN	Username	draytek	
V PPTP	Password	*****	
IPSec Tunnel	VJ Compression	💿 On 🔘 Off	
L2TP with IPSec Policy None	IKE Authentication	Method	
Specify ISDN CLID or Remote VPN Gateway	🗹 Pre-Shared Key		
Peer ISDN Number or Peer VPN Server IP	IKE Pre-Shared Key		
220.135.240.210	Digital Signature(X.	509)	
or Peer ID	None 🛩		
	IPSec Security Meth	nod	
	🗹 Medium (AH)		
	High (ESP)		
	🗹 DES 🗹 3D	es 🗹 Aes	
	Callback Function (CBCP)	
	Enable Callback Function		
	Use the Following	Number to Callback	
	Callback Number		
	Callback Budget	0 minute(s)	

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

4. TCP/IP Network Sett	ings			
My WAN IP	0.0.0.0		RIP Direction	Disable 👻
Remote Gateway IP	0.0.0.0		From first subnet to rem do	note network, you have to
Remote Network IP	192.168.2.0			Route 💌
Remote Network Mask	255.255.255.0			
	More		Change default route single WAN supports this	to this VPN tunnel (Only)
OK Clear Cancel				



Settings in Router B in the remote office:

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

PPP General Setup		
PPP/MP Protocol	IP Address Assignment for	Dial-In Users
Dial-In PPP PAP or CHAP	(When DHCP Disable set)	
Authentication	Start IP Address	192.168.2.200
Dial-In PPP Encryption Optional MPPE 👻		
Mutual Authentication (PAP) 🛛 🔿 Yes 💿 No		
Username		
Password		

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

VPN and Remote Access >> IPSec General Setup		
VPN IKE/IPSec General Setup		
Dial-in Set up for Remote Dial-in users	s and Dynamic IP Client (LAN to LAN).	
IKE Authentication Method		
Pre-Shared Key	•••••	
Confirm Pre-Shared Key	•••••	
IPSec Security Method		
Medium (AH)		
Data will be authentic, but	t will not be encrypted.	
·····	3DES 🔽 AES	
Data will be encrypted and	d authentic.	
	OK Cancel	

- 3. Go to LAN-to-LAN. Click on one index number to edit a profile.
- 4. Set **Common Settings** as shown below. You should enable both of VPN connections because any one of the parties may start the VPN connection.

VPN and Remote Access >> LAN to LAN		
Profile Index : 1 1. Common Settings		
Profile Name Branch1	Call Direction 💿 Both 🔿 Dial-Out 🔿 Dial-Ir	
Enable this profile	🔲 Always on	
	Idle Timeout 300 second(s)	
VPN Connection Through: 🛛 WAN1 First 😪	Enable PING to keep alive	
Netbios Naming Packet 💿 Pass 🔘 Block	PING to the IP	



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

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

2. Dial-Out Settings		
Type of Server I am calling	Link Type	64k bps 💙
O ISDN	Username	draytek
О РРТР	Password	
IPSec Tunnel	PPP Authentication	PAP/CHAP V
C L2TP with IPSec Policy None	VJ Compression	On Off
Dial Number for ISDN or Server IP/Host Name for VPN. (such as 5551234, draytek.com or 123.45.67.89)	IKE Authentication Me	ethod
220.135.240.208	IKE Pre-Shared Key	
	Digital Signature(X.50)	J [] 19)
	None 🗸	
	IPSec Security Metho	d
	Medium(AH)	1. A. 11. 12. 12.
	O High(ESP) DES with	out Authentication
	Advanced	
	Index(1-15) in <u>Schedule</u>	Setup:
	Callback Function (CB	ICP)
	Require Remote to	Callback
	Provide ISDN Numb	er 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.

Type of Server I am calling	Link Type	64k bps 😽
O ISDN	Username	draytek
PPTP	Password	
O IPSec Tunnel	PPP Authentication	
L2TP with IPSec Policy None	VJ Compression	💿 On 🔘 Off
Dial Number for ISDN or Server IP/Host Name for VPN.	IKE Authentication Me Pre-Shared Key	thod
(such as 5551234, draytek.com or 123.45.67.89) 220.135.240.208	IKE Pre-Shared Key	
	O Digital Signature(X.50	9)
	IPSec Security Method Medium(AH) High(ESP) DES without Advanced	
	Index(1-15) in <u>Schedule</u>	
	Callback Function (CB	· ·
	🗌 Require Remote to (Callback
	Provide ISDN Number	er to Remote

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

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

3. Dial-In Settings		
Allowed Dial-In Type	_	
ISDN	Username	draytek
PPTP	Password	
🗹 IPSec Tunnel	VJ Compression	🖲 On 🔾 Off
L2TP with IPSec Policy None	IKE Authentication Meth	od
☑ Specify ISDN CLID or Remote VPN Gateway	Pre-Shared Key	
Peer ISDN Number or Peer VPN Server IP	IKE Pre-Shared Key	
220.135.240.208	Digital Signature(X.509)	
or Peer ID	None 🗸	
	IDCon Convity Mathed	
	IPSec Security Method Medium (AH)	
	High (ESP)	
	- · ·	AES
	Callback Function (CBCF	")
	🗌 Enable Callback Functi	on
	Use the Following Num	ber to Callback
	Callback Number	
	Callback Budget	minute(s)

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

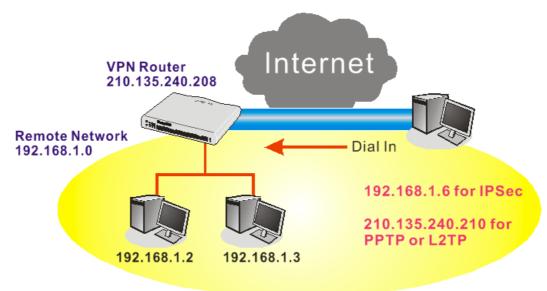
3. Dial-In Settings	
Allowed Dial-In Type	
ISDN	Username draytek
PPTP	Password ••••••
🗌 IPSec Tunnel	VJ Compression 💿 On 🔘 Off
L2TP with IPSec Policy None	IKE Authentication Method
Specify ISDN CLID or Remote VPN Gateway	🗹 Pre-Shared Key
Peer ISDN Number or Peer VPN Server IP	IKE Pre-Shared Key
220.135.240.208	Digital Signature(X.509)
or Peer ID	None 🗸
	IPSec Security Method
	Medium (AH)
	High (ESP)
	🗹 DES 🗹 3DES 🗹 AES
	Callback Function (CBCP)
	Enable Callback Function
	Use the Following Number to Callback
	Callback Number
	Callback Budget 0 minute(s)

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 Sett	ings	
My WAN IP	0.0.0.0	RIP Direction Disable 💌
Remote Gateway IP	0.0.0.0	From first subnet to remote network, you have to do
Remote Network IP	192.168.1.0	Route 💌
Remote Network Mask	255.255.255.0	
	More	□ Change default route to this VPN tunnel (Only single WAN supports this)
	OK [Clear Cancel

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:

VPN and Remote Access >> PPP General Setup

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

PPP/MP Protocol		IP Address Assignment for	Dial-In Use <mark>rs</mark>
Dial-In PPP	PAP or CHAP 🔽	(When DHCP Disable set)	
Authentication		Start IP Address	192.168.1.200
Dial-In PPP Encryption (MPPE)	Optional MPPE 🛛 👻]	
Autual Authentication (P/	AP) 🔘 Yes 💿 No		
Username			
Password			

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



VPN and Remote Access >> IPSec General Setup

VPN IKE/IPSec General Setup

Dial-in Set up	for Remote Dia	al-in users a	and Dynamic II	P Client (LAN	to LAN).

IKE Authentication Method	
Pre-Shared Key	•••••
Confirm Pre-Shared Key	•••••
IPSec Security Method	
🗹 Medium (AH)	
Data will be authentic, but will n	ot be encrypted.
High (ESP) 🛛 🗹 DES 🗹 3DES	▼ AES
Data will be encrypted and authe	entic.
	OK Cancel

- 3. Go to **Remote Dial-In User**. Click on one index number to edit a profile.
- 4. Set **Dial-In** settings to as shown below to allow the remote user dial-in to build VPN connection.

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

Jser account and Authentication	
Enable this account	Username ???
Idle Timeout 300 second(s)	Password
Allowed Dial-In Type	IKE Authentication Method
ISDN ISDN	Pre-Shared Key
PPTP	IKE Pre-Shared Key
🗹 IPSec Tunnel	Digital Signature (X.509)
🔲 L2TP with IPSec Policy None 🔛	None 💌
 ✓ Specify Remote Node Remote Client IP or Peer ISDN Number 220.135.240.210 or Peer ID 	IPSec Security Method ✓ Medium (AH) High (ESP) ✓ DES ✓ 3DES ✓ AES Local ID (optional)
	Callback Function
	Check to enable Callback function
	Specify the callback number
	Callback Number
	Check to enable Callback Budget Control
	Callback Budget 30 minute(s)

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

VPN and Remote Access >> Remote Dial-in User



VPN and Remote Access >> Remote Dial-in User

Index No. 1	
User account and Authentication	
🗹 Enable this account	Username draytek
Idle Timeout 300 second(s)	Password
Allowed Dial-In Type	IKE Authentication Method
ISDN ISDN	🗹 Pre-Shared Key
PPTP	IKE Pre-Shared Key
🔲 IPSec Tunnel	Digital Signature (X.509)
L2TP with IPSec Policy None	None 👻
✓ Specify Remote Node Remote Client IP or Peer ISDN Number 220.135.240.210 or Peer ID	IPSec Security Method ✓ Medium (AH) High (ESP) ✓ DES ✓ 3DES ✓ AES Local ID Callback Function Check to enable Callback function Specify the callback number Callback Number Check to enable Callback Budget Control
	Callback Budget 30 minute(s)
ОК С	lear Cancel

Settings in the remote host:

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

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

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

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

Dial To VPN	
Session Name:	Office
VPN Server IP/HOST	Name(such as 123.45.67.89 or draytek.com)
192.168.1.1	
User Name :	draytek_user1
Password :	www.www.
Type of VPN	
○ PPTP	◯ L2TP
IPSec Tunne	L2TP over IPSec
PPTP Encryption	
No encryptio Require encr	
	ength encryption
	ateway on remote network
OK	Cancel

You may further specify the method you use to get IP, the security method, and authentication method. If the Pre-Shared Key is selected, it should be consistent with the one set in VPN router.

IPSec Policy Setti	ng	×
My IP : Type of IPSec —	172.16.3.100	· · ·
Standard IPS	iec Tunnel	
Remote Su	bnet :	0.0.0.0
Remote Su	bnet Mask :	255 , 255 , 255 , 0
💿 Virture IP	Dray1	Fek Virture Interface 🛛 👻
	n IP address a an IP address	automatically (DHCP over IPSec)
IP Addr	ess:	192 . 168 . 1 . 201
Subnet	Mask:	255 . 255 . 255 . 0
Security Method Medium(AH)	0	High(ESP)
MD5	~	DES
Authority Method		
 Certification 	Authority:	
		Browse
0	к	Cancel

If a PPP-based service is selected, you should further specify the remote VPN server IP address, Username, Password, and encryption method. The User Name and Password should be consistent with the one set up in the VPN router. To use default gateway on remote network means that all the packets of remote host will be directed to VPN



server then forwarded to Internet. This will make the remote host seem to be working in the enterprise network.

Dial To VPN	
Session Name:	office
VPN Server IP/HOST	Name(such as 123.45.67.89 or draytek.com)
192.168.1.1	
User Name :	draytek_user1
Password :	****
PPTP	O L2TP
O IPSec Tunnel	OL2TP over IPSec
PPTP Encryption	
O No encryptio	
Require encr	
O Maximum str	ength encryption
🗹 Use default ga	ateway on remote network
ОК	Cancel

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

4.3 QoS Setting Example

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

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

Index	Status	Bandwidth	Directon	Class 1	Class 2	Class 3	Others	UDP Bandwidth Control	
WAN1	Enable	10000Kbps/10000Kbps	Outbound	25%	25%	25%	25%	Inactive	Setu
WAN2	Enable	10000Kbps/10000Kbps	Outbound	25%	25%	25%	25%	Inactive	Setu
Class F Inde		N	ame				Rule	Service	Туре
	вх	N	ame				Rule <u>Edit</u>	Service	Туре
	вж 5 1	N	ame					Service	

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

Bandwidth Management >> Quality of Service

WAN1 General Setup

~	Enable the (QoS Control	OUT	*	
	Index				ame
	Class 1		BOTH		
	Class 2				

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

Bandwidth Management >> Quality of Service

Bandwidth Management >> Quality of Service

Class I Name	n dex #1 E-mail				
NO	Status	Local Address	Remote Address	DiffServ CodePoint	Service Type
1	Empty	-	-	-	-
		[Add Edit Dele	te	
		[OK Cancel		

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

WAN1 General S	QoS Control BOTH 🔽	
Index	Class Name	Reserved_bandwidth Ratio
Class 1	E-mail	25 %
Class 2		25 %
Class 3		25 %
	Others	25 %
Enable UDP 8	Bandwidth Control	Limited_bandwidth Ratio 25 %
Outbound T	CP ACK Prioritize	Online Statistics
	OK Clear	Cancel

 Return to previous page. Enter the Name of Index Class 2 by clicking Edit link. In this index, the user will set reserved bandwidth for HTTPS. And click OK. Bandwidth Management>> Quality of Service

IS Local Address	Remote Address	DiffServ CodePoint	Service Type
/e Any	Any	ANY	ANY
[Add Edit Delet	е	
		Add Edit Delet	

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

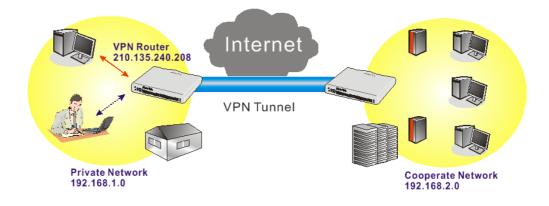
Bandwidth Management >> Quality of Service

Index	Status	Bandwidth	Directon	Class 1	Class 2	Class 3	Others	UDP Bandwidth Control	
WAN1	Enable	10000Kbps/10000Kbps	Both	25%	25%	25%	25%	Inactive	<u>Setup</u>
WAN2	Enable	10000Kbps/10000Kbps	Outbound	25%	25%	25%	25%	Inactive	<u>Setup</u>
Class F Inde		N	ame				Rule	Service	Туре
	ex		ame -mail				Rule <u>Edit</u>	Service	Туре
Inde	ex 5 1	E						Service	

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

WAN1 General S	Setup						
☑ Enable the QoS Control BOTH ▼							
Index	Class Name	Reserved_bandwidth Ratio					
Class 1	E-mail	25 %					
Class 2	HTTPS	25 %					
Class 3		25 %					
	Others	25 %					
	Bandwidth Control CP ACK Prioritize	Limited_bandwidth Ratio 25 % Online Statistics					
	OK Clear	Cancel					

8. If the worker has connected to the headquarter using host to host VPN tunnel. (Please refer to Chapter 3 VPN for detail instruction), he may set up an index for it. Enter the Class Name of Index 3. In this index, he will set reserved bandwidth for 1 VPN tunnel.



Bandwidth Management >> Quality of Service

Bandwidth Management >> Quality of Service

Bandwidth Management >> Quality of Service

me	VPN							
NO	Status	Local Address	Remote Address	DiffServ CodePoint	Service Type			
1 🔿	Inactive	Any	Any	ANY	undefined			
Add Edit Delete								

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

🗹 ACT			
Local Address	Any		Edit
Remote Address	Any		Edit
DiffServ CodePoint	ANY	~	
Service Type	ANY	~	
Note: Please choose	e/setup the <u>Service Ty</u>	pe first.	

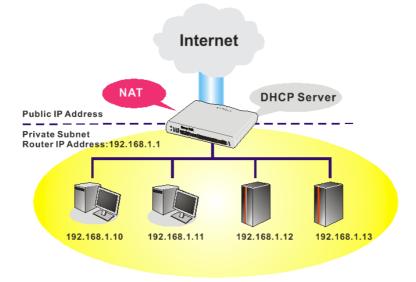
10. Then click **Edit** of **Local Address** to set a worker's subnet address. Click **Edit** of **Remote Address** to set headquarter's IP address. Leave other fields and click **OK**.

🗹 ACT		
Local Address	192.168.1.10	Edit
Remote Address	192.168.2.0	Edit
DiffServ CodePoint	ANY	*
Service Type	ANY	*
ote: Please choose/se		first.

4.4 LAN - Created by Using NAT

LAN >> General Setup

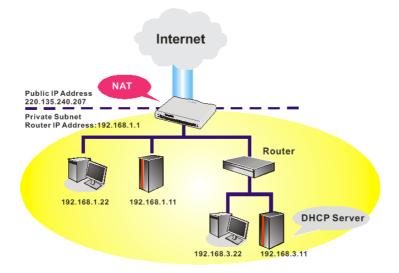
An example of default setting and the corresponding deployment are shown below. The default Vigor router private IP address/Subnet Mask is 192.168.1.1/255.255.255.0. The built-in DHCP server is enabled so it assigns every local NATed host an IP address of 192.168.1.x starting from 192.168.1.10.



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

LAN IP Network Config	juration	DHCP Server Configura	tion
For NAT Usage		💿 Enable Server 🔘 Disat	ole Server
1st IP Address	192.168.1.1	Relay Agent: 🔘 1st Subr	iet 🔾 2nd Subnet
1st Subnet Mask	255.255.255.0	Start IP Address	192.168.1.10
For IP Routing Usage 🤇) Enable 💿 Disable	IP Pool Counts	50
2nd IP Address	192.168.2.1	Gateway IP Address	192.168.1.1
2nd Subnet Mask	255.255.255.0	DHCP Server IP Address	
	2nd Subnet DHCP Server	for Relay Agent	
		DNS Server IP Address	
RIP Protocol Control	Disable 🚩	🔲 Force DNS manual se	tting
		Primary IP Address	
		Secondary IP Address	

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

LAN IP Network Confi	uration	DHCP Server Configura	ation
For NAT Usage	garación	O Enable Server I Disa	
1st IP Address	192.168.1.1	Relay Agent: 🔘 1st Sub	net O 2nd Subnet
1st Subnet Mask	255.255.255.0	Start IP Address	192.168.1.10
For IP Routing Usage 🤇) Enable 💿 Disable	IP Pool Counts	50
2nd IP Address	192.168.2.1	Gateway IP Address	192.168.1.1
2nd Subnet Mask	255.255.255.0	DHCP Server IP Address	
	2nd Subnet DHCP Server	for Relay Agent	
		DNS Server IP Address	;
RIP Protocol Control	Disable 🔽	🔲 Force DNS manual se	etting
		Primary IP Address	
		Secondary IP Address	

4.5 Upgrade Firmware for Your Router

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

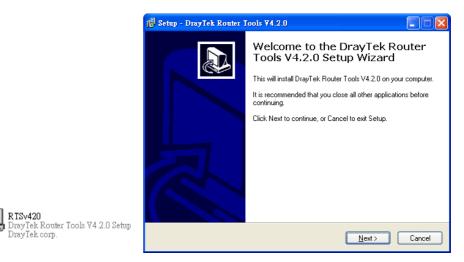
- 1. Go to www.draytek.com.
- 2. Access into **Support** >> **Downloads**. Please find out **Firmware** menu and click it. Search the model you have and click on it to download the newly update firmware for your router.

	About DrayTek	Products	Support	Education	Partners	Contact U
ome > Support > Download	S					
Downloads - Firmware					Downlo	ads
Model Name	Firmware Version	Re	elease Date		Firmware	
Vigor120 series	3.2.2.1	2	6/06/2009		Driver	
Vigor2100 series	2.6.2	26/02/2008			Utility	
Vigor2104 series	2.5.7.3	1	3/02/2008		Utility In	troduction
Vigor2110 series	3.3.0	2	5/06/2009		Datashee	
Vigor2200/X/W/E	2.3.11	2	2/09/2004			ertification
Vigor2200Eplus	2.5.7	1	8/02/2009		KATTEU	ennication
Vigor2200USB	2.3.10	1	6/03/2005			

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

		About	DrayTek Products	s Support I	Education	Partners	Contact Us
ome > Support > Ut	ility						
Jtility						Downlo	ads
Tools Name	Release Date	Version	OS	Support Mo	odel	Firmware	
Router Tools	2009/06/18	4.2.0	MS-Windows	All Module	es		
Syslog Tools	2009/06/18	4.2.0	MS-Windows XP	All Module	es	Driver	
offing room			MS-Vista			Utility	
VigorPro Alert Notice	2009/06/03	1.1.0	MS-Windows XP			Utility In	troduction
Tools		(Multi- language)	MS-Vista			Datashee	t
				VigorPro 5300	series	R&TTE C	ertification
Smart VPN Client	2009/05/25	3.6.3	MS-Windows XP	All Module	es		ontineation
		(Multi-	MS-Vista				
		language)					
Smart Monitor	2009/03/25	2.0	MS-Windows XP	Vigor2950 s			

- 4. Click on the link of **Router Tools** to download the file. After downloading the files, please decompressed the file onto your host.
- 5. Double click on the icon of router tool. The setup wizard will appear.



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



Time Out(Sec.) Router IP:	
5)
Port Firmware file:	
69]
Password: Abort Send]

- 8. Type in your router IP, usually **192.168.1.1**.
- 9. Click the button to the right side of Firmware file typing box. Locate the files that you download from the company web sites. You will find out two files with different extension names, **xxxx.all** (keep the old custom settings) and **xxxx.rst** (reset all the custom settings to default settings). Choose any one of them that you need.

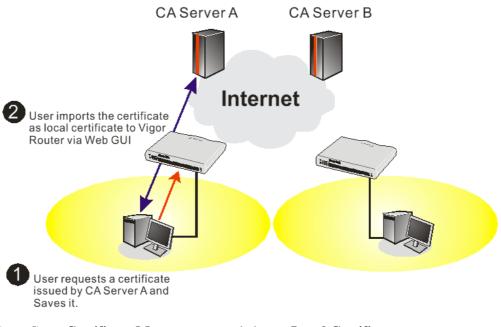
🛍 Firmware Upgrad	le Utility 3.5.1	
Time Out(Sec.)	Router IP:	
5	192.168.1.1	
Port	Firmware file:	
69	C:\Documents and Settings\Carrie	
Password:		
	Abort Ser	nd

10. Click Send.

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

11. Now the firmware update is finished.

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



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

Name	Subject	Status	Modify
Local			View Delete
GENERATE	IMPORT REFRESH		
X509 Local C	ertificate		
			~
			~

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

Subject Alternative Name		
Туре	Domain Name 💌	
IP	draytek.com	
Subject Name		
Country (C)	TW	
State (ST)		
Location (L)		
Orginization (O)	Draytek	
Orginization Unit (OU)		
Common Name (CN)		
Email (E)	press@draytek.com	
Кеу Туре	RSA 🕶	
Key Size	1024 Bit 💌	

Certificate Management >> Local Certificate

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

Local /C=TW/ST=HS/O=Draytek/OU=RD/ ENERATE IMPORT REFRESH X509 Local Certificate Request BEGIN CERTIFICATE REQUEST MIIBnTCCAQYCAQAWXTELMAkGA1UEBhMCVFcxCzAJI EwdEcmF5dGVrMcgwCQTDVQQLEwJSRDEIMCAGC3qG3			lete
X509 Local Certificate Request		RAWDGYDVQQK	^
MIIBnTCCAQYCAQAwXTELMAkGA1UEBhMCVFcxCzAJH		RAwDgYDVQQK	^
cmF5dGVrLmWvbTCBnzANBgkqhkiG9w0BAQEFAA0B: OTSZSZQdw1Re1tv1HNVm/MFC099x+XEwNKG46jd(mASVORtj7HbNOdYn88p1xRrQFgk8nkbMLdAqb10oc dKiyAPfp/Z02OWsCddxh/Hz23Ys8m60CAwEAAAAA AGNB9071V44sgXwiWnXHJvdFLD0dwcQ01ZL1XR+(nacBqEc1W0chKzES0dyDc8mtIf7k+104SseuY7nx: sOvJGBHHwKSkWb1RAZL5xvHjDoMX16czT1ybedZS: EDC CERTIFICATE REOUEST	jQAwgYkCgYEAy GY1LSAvJTduHH c/lsYN/smGb4N MAOGCSqGSIb3D OVdheJjvaISCg swXvPIOn31JMJ	ZELVTVBytix 90z40MWx02G +Pbo4VM01V0 QEBBQUAA4GB iqzJQCKaDQ7	

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**.

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
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
O Retrieve the CA certificate or certificate revocation list
Check on a pending certificate



Select Advanced request.

Microsoft Certificate Services vigor	<u>Home</u>
Choose Request Type	
Please select the type of request you would like to make:	
User certificate request. User Certificate	
 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 Requet text file. Select **Router (Offline request)** or **IPSec (Offline request)** below.

Microsoft Certifica	te Services vigor	Hom
Submit A Save	d Request	
		request or PKCS #7 renewal request generated by an external application (such as a web t to the certification authority (CA).
Saved Request:		
Certificate Request (PKCS #10 or #7):	BEGIN CERTIFICATE REQUI HIIBGJCCARMCAQAwQTELMAKGA1U BgkqhkiGywBCC2EWZK9ZXNZQQX A4GNADCB1QKBgQDQYB7wmZfFhM hX4bp89cUF9d1oACGG1W/tcBOck X/G0A7CTV0/fQ2pxroCw1JTJLSJ; Browse for a file to insert.	EBhMCVFcxEDAO 9/I2QDW3W29t 9/I2QDG03Xk++ dc2QFFFvIXcP3
Certificate Templa		
	Administrator	
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 "-----BEGINE CERTIFICATE-----""

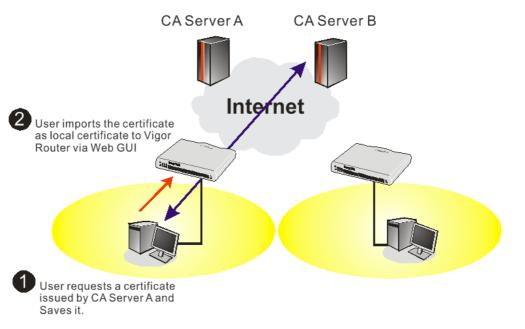
Certificate Management >> Local Certificate

	Name	Subject	Status	Modify
X509 Local Certificate RequestBEGIN CERTIFICATE REQUEST MIIBnTCCAQYCAQAwXTELMAkGA1UEBhMCVFcxCzAJBgNVBAgTAkhTMRAwDgYDVQQK EwdEcmF5dGVrMQswCQYDVQQLEwJSRDEiMCAGCSqGSIb3DQEJARYTc3VwcG9ydEBk cmF5dGVrLmNvbTCBnzANBgkqhkIG9w0BAQEFAAOBjQAwgYkCgYEAyZELVTVBytix OTSZSZQdw1Reltv1HnVwm/MFC0y9x+XEwNKG46jdGY1LSAvJTduHH90z40MWx02G mASVORtj7HbN0dYn88p1xRrQFgk8nkbMLdAqb10oc/lsYN/smGb4N+Pbo4VM01V0 dKiyAPfp/Z020WsCddxh/HzZ3Ys8m60CAwEAAaAAMA0GCSqGSIb3DQEBBQUAA4GB AGNB9071V44sgXw1WnXHJvdFLD0dwcQ01ZL1XRn+0VdheJjvaISCgiqzJQCKaDQ7 nacBqEc1W0chKzESOdyDc8mtIf7k+i045SeuY7nxswXvPIOn31JMJGMZvQSVrTYu s0vJGBHHwKSkWb1RAZL5xvHjD0MX16czT1ybedZSsrJw	Local	/C=TW/ST=HS/O=Draytek/OU=RD/	Requesting	View Delete
BEGIN CERTIFICATE REQUEST MIIBATCCAQYCAQAwXTELMAkGA1UEBhMCVFcxCzAJBgNVBAgTAkhTMRAwDgYDVQQK EwdEcmF5dGVrMQswCQYDVQQLEwJSRDEiMCAGCSqGSIb3DQEJARYTc3VwcG9ydEBk cmF5dGVrLmNvbTCBnzANBgkqhkiG9wOBAQEFAAOBjQAwgYkCgYEAyZELVTVBytix OTSZ5ZQdwlReltvlHnVwm/MFCOy9x+XEwMKG46jdGY1LSAvJTduHH90z4OMWx02G mASVORtj7HbNOdYn88p1xRrQFgk8nkbMLdAqbl0cc/lsYN/smGb4N+Pb04VM01V0 dKiyAPfp/Z02OWsCddxh/HzZ3Ys8m60CAwEAAAAMA0GCSqGSIb3DQEBBQUAA4GB AGNB9071V44sgXw1WnXHJvdFLD0dwcQ01ZL1XRn+0VdheJjvaISCgiqzJQCKaDQ7 nacEqEc1W0chKzESOdyDc6mtIf7k+i045SeuY7nxswXvPIOn31JMJGMZvQSVrTYu sOvJGBHHwKSkWb1RAZL5xvHjD0MX16czT1ybedZSsrJw	GENERATE	IMPORT REFRESH		
MIIBnTCCAQYCAQAwXTELMAkGA1UEBhMCVFcxCzAJBgNVBAgTAkhTMRAwDgYDVQQK EwdEcmF5dGVrMQswCQYDVQQLEwJSRDEiMCAGCSqGSIb3DQEJARYTc3VwcG9ydEBk cmF5dGVrLmNvbTCBnzANBgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEAyZELVTVBytix OTSZ5ZQdwlReltvlHnVwm/MFC0y9x+XEwNKG46jdGY1LSAvJTduHH9Oz4OMWx02G mASVORtjTbNOdYn88p1xRrQFgk8nkbMLdAqb10oc/lsXvJTduHH9Oz4OMWx02G dKiyAPfp/Z02OWsCddxh/HzZ3Ys8m60CAwEAAaAAMAOGCSqGSIb3DQEBBQUAA4GB AGNB9071V44sgXw1WnXHJvdFLD0dwcQ01ZL1XRn+0VdheJjvaISCgiqzJQCKaDQ7 nacBqEclWOchKzESOdyDc8mtIf7k+iO45SeuY7nxswXvPIOn31JMJGMZvQSVrTYu sOvJGBHHwKSkWb1RAZL5xvHjD0MX16czT1ybedZSsrJw	X509 L	ocal Certificate Request		
	F			

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

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

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



1. Use web browser connecting to the CA server that you would like to retrieve its CA certificate. Click **Retrive the CA certificate or certificate recoring list**.

Microsoft Certificate Services - Microsoft Internet Explorer	- J 7 🔀
當案(F) 編輯(E) 檢視(Y) 我的最愛(A) 工具(I) 説明(H)	At
🌍 上—頁 • 🕥 · 🛃 😰 🏠 🔎 搜尋 🌟 我的最爱 🔮 媒體 🚱 🔗 - 🌺 🚍 • 🦓	
時世 ① 🥘 http://172.16.2.179/certsrv/	▶ 移至 連結
nsn 🕅 🔹 📝 建厚 🔹 🥜 提厚 🔹 🥜 超目提示 🛛 🕅 遵項 🛛 🔀 封鎖快顯視窗 (319) 🔹 🖂 Hotmail 👗 Messe	mger [2 我的 MSN
Microsoft Certificate Services vigor	<u>Home</u>
Welcome	
You use this web site to request a certificate for your web browser, e-mail client, or other secure progra will be able to securely identify yourself to other people over the web, sign your e-mail messages, encry	
Welcome You use this web site to request a certificate for your web browser, e-mail client, or other secure progra will be able to securely identify yourself to other people over the web, sign your e-mail messages, encry depending upon the type of certificate you request. Select a task:	
You use this web site to request a certificate for your web browser, e-mail client, or other secure progra will be able to securely identify yourself to other people over the web, sign your e-mail messages, encry depending upon the type of certificate you request. Select a task:	
You use this web site to request a certificate for your web browser, e-mail client, or other secure progra will be able to securely identify yourself to other people over the web, sign your e-mail messages, encry depending upon the type of certificate you request.	

- 2. In Choose file to download, click CA Certificate Current and Base 64 encoded, and Download CA certificate to save the .cer. file.
 - 🚰 Microsoft Certificate Services Microsoft Internet Explorer ΒX 🔇 上一頁 🔹 💿 · 🖹 😰 🏠 🔎 搜尋 📌 我的最爱 🔮 媒體 🚱 🔗 - 🌺 🔜 • 🍪 網址 (D) 🍓 http://172.16.2.179/certsrv/certcarc.asp 🗸 🄁 移至 🏾 連結 💙 msn^M • 🗸 🔎 搜尋 🔹 🥒 醒目提示 🛛 🚶 選項 🛛 🔀 封鎖快顯視窗 (319) 🔹 🔤 Hotmail 🎎 Messenger 12 我的 MSN Retrieve The CA Certificate Or Certificate Revocation List Install this CA certification path to allow your computer to trust certificates issued from this certification authority. It is not necessary to manually install the CA certification path if you request and install a certificate from this certification authority, because the CA certification path will be installed for you automatically. Choose file to download: CA Certificate: Current [vigor(1)] Previous [vigor] ○DER encoded or ●Base 64 encoded Download CA certificate Download CA certification path Download latest certificate revocation list
- 3. Back to Vigor router, go to **Trusted CA Certificate**. Click **IMPORT** button and browse the file to import the certificate (.cer file) into Vigor router. When finished, click refresh and you will find the below illustration.

Certificate Management >> Trusted CA Certificate

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

REFRESH

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

IMPORT

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.

This page is left blank.

Chapter 5: Reference -Advanced Web Configuration

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

5.1 WAN

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

5.1.1 Basics of Internet Protocol (IP) Network

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

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

What are Public IP Address and Private IP Address

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

Get Your Public IP Address from ISP

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

When a router begins to connect to your ISP, a serial of discovery process will occur to ask for a connection. Then a session will be created. Your user ID and password is authenticated



via **PAP** or **CHAP** with **RADIUS** authentication system. And your IP address, DNS server, and other related information will usually be assigned by your ISP.

5.1.2 Network Connection by 3G USB Modem

For 3G mobile communication through Access Point is popular more and more, Vigor2820 adds the function of 3G network connection for such purpose. By connecting 3G USB Modem to the USB port of Vigor2820, it can support HSDPA/UMTS/EDGE/GPRS/GSM and the future 3G standard (HSUPA, etc). Vigor2820 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 802.11n wireless function of Vigor2820n, and enjoy the powerful firewall, bandwidth management, VPN, VoIP features of Vigor2820 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.



5.1.3 General Setup

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

This router supports dual WAN function. It allows users to access Internet and combine the bandwidth of the dual WAN to speed up the transmission through the network. Each WAN port 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 and WAN2 are enabled.



WAN >> General Setup

General Setup				
WAN1		WAN2		
Enable:	Yes 🕶	Enable:	Yes 🕶	
Display Name:		Display Name:		
Physical Mode:	ADSL	Physical Mode:	Ethernet 🔽	
Physical Type:	Auto negotiation 🔽	Physical Type:	Auto negotiation 🐱	
Load Balance Mode:	Auto Weight 🛛 👻	Load Balance Mode:	Auto Weight 🛛 👻	
Line Speed(Kbps):	DownLink	Line Speed(Kbps):	DownLink 🛛	
	UpLink		UpLink	
Active Mode:	Always On 🛛 👻	Active Mode:	Always On 🔽	
Active on demand:		Active on demand:		
🔾 WAN2 Fail		O WAN1 Fail		
WAN2 Upload spe	ed exceed OKbps	WAN1 Upload speed exceed Kbps		
WAN2 Download	speed exceed OKbps	WAN1 Download :	speed exceed OKbps	
1		1		

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	Type the description for the WAN1/WAN2 interface.		
Physical Mode	port; yet the physical of	For WAN1, the physical connection is done through ADSL port; yet the physical connection for WAN2 is done through an Ethernet port (P1) or USB port. You cannot change it.		
	Physical Mode:	Ethernet 💌		

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

3G USB Modem

WAN >>	Internet	Access

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

Physical Type

This setting is available for WAN2 only. You can change the physical type for WAN2 or choose **Auto negotiation** for

determined by the system.

Physical Type:

Auto negotiation	Y
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: Auto Weigh Auto Weigh According to Line Speed Line Speed If your choose According to Line Speed as the Load **Balance Mode**, please type the line speed for downloading and uploading through WAN1/WAN2. The unit is kbps. **Active Mode** Choose Always On to make the WAN connection (WAN1/WAN2) being activated always; or choose Active on demand to make the WAN connection (WAN1/WAN2) activated if it is necessary. Active Mode: Active on demand 🛰 Always On Active on demand

> If you choose Active on demand, the Idle Timeout will be available for you to set for PPPoE and PPTP access modes in the Details Page of WAN>>Internet Access. In addition, there are three selections for you to choose for different purposes. **WAN2 Fail** – It means the connection for WAN1 will be activated when WAN2 is failed.

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

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

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

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

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

5.1.4 Internet Access

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

WAN >> Internet Access

Index	Display Name	Physical Mode	Config Information
WAN1		ADSL	Channel:1, VPI:0, VCI:33, Protocol:PPPoE/LLC/SNAP, Modulation:Multimode, Dynamic IP
WAN2		Ethernet	IP Address:172.16.3.229, Subnet Mask:255.255.0.0, Gateway IP:172.16.3.4

Inter	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 port for WAN1/WAN2.
Config Information	It shows brief configuration information for WAN1/WAN2 interface.

WAN1 and WAN2 support different protocols. WAN1 supports PPPoE/PPPoA and MPoA. WAN2 supports PPPoE, Static or Dynamic IP and PPTP. According to physical connection of your router, please choose suitable WAN interface link to set detailed information.

PPPoE/PPPoA for WAN1

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

WAN >> Internet Access

		-
N		

PPPoE / PPPoA	MPoA (RFC1	483/2684)	
🔘 Enable 🛛 💿 Dis	able	ISP Access Setup	
		Username	
DSL Modem Settings Multi-PVC channel VPI VCI Encapsulating Type Protocol Modulation	Channel 1 8 35 VC MUX PPPoA Multimode	Fixed IP Address	PAP or CHAP PAP or CHAP PAP or CHAP PAP or CHAP PAP or CHAP PAP or CHAP
PPPoE Pass-through For Wired LAN For Wireless LAN		 Default MAC Address Specify a MAC Address MAC Address: 00 .50 	955
ISDN Dial Backup Setu Dial Backup Mode	P None	Index(1-15) in <u>Schedule</u> =>, , ,	2 Setup:
WAN Connection Dete	ction		
Mode	ARP Detect 💌		
Ping IP			
TTL:			

Enable/Disable	Click Enable for activating this function. If you click Disable , this function will be closed and all the settings that you adjusted in this page will be invalid.
DSL Modem Settings	 Set up the DSL parameters required by your ISP. These are vital for building DSL connection to your ISP. Multi-PVC channel - The selections displayed here are determined by the page of Internet Access – Multi PVCs. Select M-PVCs Channel means no selection will be chosen. VPI - Type in the value provided by ISP. VCI - Type in the value provided by ISP. Encapsulating Type - Drop down the list to choose the type provided by ISP. Protocol - Drop down the list to choose the one provided by ISP. If you have already used Quick Start Wizard to set the protocol, then it is not necessary for you to change any settings in this group. Modulation – Default setting is Multimode. Choose the one that

fits the requirement of your router.

Modulation

Multimode	~
T1.413	
G.Lite	
G.DMT	
ADSL2(G.992.3)	
ADSL2 annex M	
ADSL2+(G.992.5)	
ADSL2+ annex M	
Multimode	

PPPoE Pass-throughThe router offers PPPoE dial-up connection. Besides, you also can
establish the PPPoE connection directly from local clients to your
ISP via the Vigor router. When PPPoA protocol is selected, the
PPPoE package transmitted by PC will be transformed into PPPoA
package and sent to WAN server. Thus, the PC can access Internet
through such direction.
For Wired LAN – If you check this box, PCs on the same network

can use another set of PPPoE session (different with the Host PC) to access into Internet.

For Wireless LAN – If you check this box, PCs on the same wireless network can use another set of PPPoE session (different with the Host PC) to access into Internet.

ISDN Dial BackupThis 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 ISDN > Dialing to
a Single ISP to create the backup profile.

Dial Backup Mode

None	*
None	
Packet Trigger	
Always On	

Note: This feature is available for ISDN 2 port only.

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.
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.

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**

WAN Connection

Detection



On.

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

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

IP Address From ISP Usually ISP dynamically assigns IP address to you each time you connect to it and request. In some case, your ISP provides service to always assign you the same IP address whenever you request. In this case, you can fill in this IP address in the Fixed IP field. Please contact your ISP before you want to use this function. WAN IP Alias - If you have multiple public IP addresses and would like to utilize them on the WAN interface, please use WAN IP Alias. You can set up to 8 public IP addresses other than the current one you are using. Notice that this setting is available for WAN1 only. Type the additional WAN IP address and check the Enable box. Then click OK to exit the dialog.

) http://19	http://192.168.1.1 - WAN IP Alias - Microsoft Internet Explorer 🛛 🔲 🔀				
WAN IP Alias (Multi-NAT)					
Index	Enable	Aux, WAN IP	Join NAT IP Pool		
1.	v		v		
2.					
з.					
4.					
5.					
6.					
7.					
8.					
		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.

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

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

MPoA for WAN1

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

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

PPPoE / PPPoA	MPoA (RFC	1483/2684)
🔘 Enable 🛛 💿 Disa	ble	WAN IP Network Settings WAN IP Alias
		○ Obtain an IP address automatically
DSL Modem Settings Multi-PVC channel	Channel 2	Router Name
	Channel 2	Domain Name
Encapsulation	Bridged IP LLC	*
		Specify an IP address
VPI	8	IP Address
VCI	88	
Modulation	Multimode 🗸 🗸	Subnet Mask
		Gateway IP Address
ISDN Dial Backup Setu	p	
Dial Backup Mode	None 👻	Oefault MAC Address
		 Specify a MAC Address
WAN Connection Detec		MAC Address: 00 .50 .7F :94 .E7 .81
Mode	ARP Detect 👻	
Ping IP		DNS Server IP Address
TTL:		Primary IP Address
		Secondary IP Address
RIP Protocol		
Enable RIP		
n-ide e Mede		-
Bridge Mode		
Enable Bridge Mode		

DSL Modem SettingsSet up the DSL parameters required by your ISP. These are vital
for building DSL connection to your ISP.
Multi-PVC channel - The selections displayed here are
determined by the page of Internet Access – Multi PVCs. Select
M-PVCs Channel means no selection will be chosen.
Encapsulating Type - Drop down the list to choose the type
provided by ISP.
VPI - Type in the value provided by ISP.
VCI - Type in the value provided by ISP.

Modulation –Default setting is Multimode. Choose the one that

	fits the requirement of your router.				
	Modulation	Multimode T1.413 G.Lite G.DMT ADSL2(G.992.3) ADSL2 annex M ADSL2+(G.992.5) ADSL2+ annex M Multimode			
ISDN Dial Backup Setup	only. Before utilizing the IS	the routers supporting ISDN function DN dial backup feature, you must first. Please click ISDN > Dialing to ackup profile.			
	Dial Backup Mode Note: This feature is availab	None None Packet Trigger Always On Dele for ISDN 2 port only.			
	None - Disable the backup f	function. p line is not on until a packet from a			
	the backup line will be activ until the broadband connect	nd connection is no longer available, ated automatically and always on ion is restored. We recommend you to st a web server for your customers'			
WAN Connection Detection	alive or not through ARP De Mode – Choose ARP Detection. execute for WAN detection. Ping IP – If you choose Pin to type IP address in this field	t or Ping Detect for the system to g Detect as detection mode, you have ld for pinging. lays value for your reference. TTL			
RIP Protocol	-	bl is abbreviated as RIP (RFC1058) ange routing tables information. Click his function.			
Bridge Mode	•	s the protocol, you can check this box router will work as a bridge modem.			
WAN IP Network Settings	This group allows you to ob allows you type in IP addres	tain an IP address automatically and as manually.			
	the IP address automatically Router Name – Type in the Domain Name – Type in th Specify an IP address – Cli data. WAN IP Alias - If you have	matically – Click this button to obtain router name provided by ISP. e domain name that you have assigned. ick this radio button to specify some e multiple public IP addresses and n the WAN interface, please use WAN			

IP Alias. You can set up to 8 public IP addresses other than the current one you are using. Notice that this setting is available for WAN1 only. Type the additional WAN IP address and check the Enable box. Then click OK to exit the dialog.

2	🖹 http://192.168.1.1 - WAN IP Alias - Microsoft Internet Explorer 💦 🔲 🗙							
			RALIA: RIAT N					
		Enable	Multi-NAT) Aux. WAN IP	Join NAT IP Pool				
	1.	v		v				
	2.							
	з.							
	4.							
	5.							
	6.							
	7.							
	8.							
	-		OK Clear All	Close				

IP Address – Type in the private IP address.
Subnet Mask – Type in the subnet mask.
Gateway IP Address – Type in gateway IP address.
Default MAC Address Type in MAC address for the router. You can use Default MAC Address or specify another MAC address for your necessity.
MAC Address – Type in the MAC address for the router manually.

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

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

PPPoE for WAN2

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

WAN >> Internet Access

WAN 2				
PPPoE	Static or D	Oynamic IP	PPTP/L2TP	
🔘 Enab	le 💿 Disable		PPP/MP Setup	
			- PPP Authentication	PAP or CHAP 🔽
ISP Access	Setup		Idle Timeout	-1 second(s)
Username			IP Address Assign	ment Method (IPCP)
Password			WAN IP Alias	
Index(1-15)	in <u>Schedule</u> Setup): 	Fixed IP: 🔘 Yes 🤅	🖲 No (Dynamic IP)
=>	,,	,	Fixed IP Address	
ISDN Dial Backup Setup				
Dial Backup	Mode None	~	Oefault MAC Add	dress
			— O Specify a MAC A	Address
WAN Conne	ection Detection		MAC Address: 00	.50 .7F 94 .E7 .82
Mode	ARP	Detect 💙	MAC Address.	
Ping IP				
TTL:				

Enable/Disable Click Enable for activating this function. If you click Disable, this function will be closed and all the settings that you adjusted in this page will be invalid. **ISP** Access Setup Enter your allocated username, password and authentication parameters according to the information provided by your ISP. 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. This setting is available for the routers supporting ISDN function **ISDN Dial Backup** only. Before utilizing the ISDN dial backup feature, you must Setup create a dial backup profile first. Please click **ISDN** > **Dialing to** a Single ISP to create the backup profile. None Dial Backup Mode None Packet Trigger Note: This feature is available for ISDN 2 port only. 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 Such function allows you to verify whether network connection is alive or not through ARP Detect or Ping Detect. Detection Mode – Choose ARP Detect or Ping Detect for the system to execute for WAN detection. **Ping IP** – If you choose Ping Detect as detection mode, you have to type IP address in this field for pinging. TTL (Time to Live) – Displays value for your reference. TTL

value is set by telnet command.

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

index	Enable	Aux. WAN IP	Join NAT IP Pool
1.	v		v
2.			
з.			
4.			
5.			
6.			
7.			
8.			

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

Static or Dynamic IP for WAN2

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, select **Static or Dynamic IP** mode. The following web page will appear.

PPPoE	Static or Dynamic IP	PPTP/L2TP
Enable	O Disable	WAN IP Network Settings WAN IP Alias
ISDN Dial Backı Dial Backup Mod		Obtain an IP address automatically Router Name Domain Name
Keep WAN Con	nection	* : Required for some ISPs
Enable PING	to keep alive	○ Specify an IP address
PING to the IP		IP Address
PING Interval	0 minute(s)	Subnet Mask
WAN Connectio	on Detection	Gateway IP Address
Mode Ping IP TTL:	ARP Detect	 Default MAC Address Specify a MAC Address MAC Address: 00 .50 .7F .94 .E7 .82
RIP Protocol		DNS Server IP Address Primary IP Address Secondary IP Address

WAN >> Internet Access

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

ISDN Dial BackupThis 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 ISDN > Dialing to
a Single ISP to create the backup profile.

Dial Backup Mode

None	*
None	
Packet Trigger	
Always On	

Note: This feature is available for ISDN 2 port only.

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	because some within certain box to activat PING to the the IP address	s function is designed for I ISPs will drop connection periods of time. Check Er e this function. IP - If you enable the PING for the system to PING it al - Enter the interval for th on.	s if there is no traffic able PING to keep alive G function, please specify for keeping alive.			
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. 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. Ping IP – If you choose Ping Detect as detection mode, you have to type IP address in this field for pinging. TTL (Time to Live) – Displays value for your reference. TTL value is set by telnet command. 					
RIP Protocol	specifying ho	mation Protocol is abbrevi w routers exchange routing or activating this function.	g tables information. Click			
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. Type the additional WAN IP address and check the Enable box. Then click OK to exit the dialog. 					
	WAN IP Alia: Index Enab	s (Multi-NAT) le Aux. WAN IP	Join NAT IP Pool			
	1. v		V			
	2. 🗆					
	з. 🗖					
	4. 🗖					
	5.					
	6. 🗌					
	7. 🗆					
	8. 🗆					
		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. <i>Router Name:</i> Type in the router name provided by ISP. <i>Domain Name:</i> 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. <i>IP Address:</i> Type the IP address. <i>Subnet Mask:</i> Type the subnet mask. <i>Gateway IP Address:</i> Click this radio button to use default MAC address for the router. <i>Specify a MAC Address:</i> Some Cable service providers specify a specific MAC address for access authentication. In such cases you need to click the Specify a 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.

PPTP/L2TP for WAN2

To use **PPTP/L2TP** as the accessing protocol of the Internet, select **PPTP/L2TP** mode. The following web page will appear.

WAN >> Internet Access

VAN 2 PPPoE	Stati	c or Dynan	nic IP	PPTP/L2TP	
	_		-	PPP Setup	
O Enab	le PPTP OEr	hable L2TP	• Disable		
Server Addr	ess			PPP Authentication	PAP or CHAP
Specify Gat	eway IP Addre	ess		Idle Timeout	-1 second(s)
				IP Address Assignme	nt Method (IPCP)
				WAN IP Alias	
ISP Access	Setup			Fixed IP: 🔘 Yes 💿 I	No (Dynamic IP)
Username				Fixed IP Address	
Password				WAN IP Network Setti	ngs
Index(1-15)	in <u>Schedule</u>	Setup:		Obtain an IP addres	s automatically
=>	,,	,		Specify an IP addre	SS
ISDN Dial B	ackup Setup			IP Address	
Dial Backup	Mode	None	*	Subnet Mask	

Enable/ Disable	Click Enable PPTP/L2TP 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.
PPTP Server	Specify the IP address of the PPTP 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	only. Be create a	fore utili dial back	izing the ISDN dial bac	supporting ISDN function ckup feature, you must click ISDN > Dialing to le.	
	Dial Bac Note: Th	·	ode None None Packet Tr re is available for ISD		
	Packet 1	Frigger -	he backup function. -The backup line is no s the router to establish	on until a packet from a a connection.	L
PPP Setup	Idle Tin passing t only whe	neout - S hrough t en the A	Set the timeout for brea		fter
IP Address Assignment Method(IPCP)	connect to alway In this ca	to it and s assign ase, you	request. In some case, you the same IP addre	lress to you each time yo your ISP provides servic ss whenever you request. ess in the Fixed IP field. at to use this function.	ce
	would life IP Alias current of WAN1 of Enable b	ke to util You can one you a only. Typ oox. Then	lize them on the WAN n set up to 8 public IP are using. Notice that the pe the additional WAN n click OK to exit the o		r
			- WAN IP Alias - Microsoft Int Multi-NAT)	ernet Explorer 📃 🗌 🗙	
		Enable	Aux. WAN IP	Join NAT IP Pool	
	1.	v		v	
	2.				
	з.				
	4.				
	5.				
	6.				
	7.				
	8.				
	Click V		OK Clear All	Close	he

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

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

WAN IP Network Settings	Obtain an IP address automatically – Click this button to obtain the IP address automatically.
	 Specify an IP address – Click this radio button to specify some data. IP Address – Type the IP address. Subnet Mask – Type the subnet mask.

PPP for WAN2

Such mode is active only **3G USB Modem** was chosen as the physical mode in General Setup.

WAN >> Internet Access

PPP Client Mode	🔘 Enable 💿 Disable	
SIM PIN code		
Modem Initial String	AT&FE0V1X1&D2&C1S0=0 (De	fault:AT&FEOV1X1&D2&C1SO=0)
APN Name		Apply
Modem Dial String	ATDT*99# (De	fault:ATDT*99#)
PPP Username	(Op	tional)
PPP Password	(Opti	onal)
Index(1-15) in <u>Schee</u>	<u>ule</u> 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(Access Point Name) is provided by your ISP for identifying different access points. Simply click Apply to apply such name. Finally, you have to click OK to save the setting. Apply – Activate the function of identification.
Modem Dial String	Such value is used to dial through USB mode. Please use the default value. If you have any question, please contact to your ISP.
PPP Username	Type the PPP username (optional).
PPP Password	Type the PPP password (optional).
	Index (1-15) Set the PCs on LAN to work at certain time interval only. You may choose up to 4 schedules out of the 15 schedules pre-defined in Applications >> Schedule setup. The default setting of this filed is blank and the function will always work.

5.1.5 Multi-PVCs

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

General

Internet Access >> Multi-PVCs

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

General	ATM Q	oS	Port	-based	Brid	ge	
hannel	Enable	VPI	VCI	QoS T	ype	Protocol	Encapsulation
1.	✓	8	35	UBR	*	PPPoA 🛩	VC MUX 🔽
2.		8	88	UBR	*	MPoA 💌	1483 Bridged IP LLC
з. <u>WAN</u>		1	43	UBR	\sim	PPPoA 💌	VC MUX 🗸
4. <u>WAN</u>		1	44	UBR	~	PPPoA 🗸	VC MUX 🗸
5. <u>WAN</u>		1	45	UBR	~	PPPoA 🗸	VC MUX 🗸
6.		1	46	UBR	~	PPPoA v	VC MUX 🔽
7.		1	47	UBR	~	PPPoA 🗸	VC MUX 🗸
8.		1	48	UBR	~	PPPoA V	VC MUX 🔽

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

ОК	Clear	Cancel
----	-------	--------

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

Encapsulation

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

	Encapsulation		
	1483 Route IP LLC	*	
Encapsulation	1483 Bridged IP LLC		
	1483 Route IP LLC		
VC MUX 🛛 🗠	1483 Bridged IP VC-Mux		
VC MUX	1483 Routed IP VC-Mux(IPoA)		
	1483 Bridged IP(IPoE)		

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

WAN >> Multi-PVCs >> PVC Channel	Channel	'VC Cha	PVC	VCs>>	Multi-P	WAN >>
----------------------------------	---------	---------	-----	-------	---------	--------

🖲 Enable 🔘 Disable	
DSL Modem Settings	
VPI 1 QoS T	ype UBR 💌
VCI 43 Protoc	ol PPPoA 💌
Encap	sulation 🛛 VC MUX 💌
PPPoE/PPPoA Client	MPoA (RFC1483/2684)
ISP Access Setup	Obtain an IP address automatically
ISP Name	Router Name
Username	Domain Name
Password	*: Required for some ISPs
PPP Authentication PAP or CHAP 🗸	Specify an IP address
✓ Always On	IP Address
Idle Timeout -1 second(s)	Subnet Mask
IP Address From ISP	Gateway IP Address
Fixed IP 🛛 🔿 Yes 💿 No (Dynamic IP)	DNS Server IP Address
Fixed IP Address	Primary IP Address
	Secondary IP Address
Ok	Cancel

Router-borne Application	 Management - It can be specified for general management (Web configuration/telnet/TR069). If you choose Management, the configuration for this PVC will be effective for Web configuration/telnet/TR069. VoIP - It can be specified for VoIP only. If you choose VoIP, the configuration for this PVC will be effective for VoIP data transmitting and receiving.
Enable/Disable	Click Enable for activating this function. If you click Disable , this function will be closed and all the settings that you adjusted in this page will be invalid.

DSL Modem Settings	 Set up the DSL parameters required by your ISP. These are vital for building DSL connection to your ISP. VPI - Type in the value provided by ISP. VCI - Type in the value provided by ISP. QoS Type -Select a proper QoS type for the channel. Protocol - Select a proper protocol for this channel. There are three options, PPPoE, PPPoA and MPoA for you to select. The following settings will be changed according to the protocol selected here. Encapsulating Type - Drop down the list to choose the type provided by ISP.
ISP Access Setup	Enter your allocated username, password and authentication parameters according to the information provided by your ISP. If you want to connect to Internet all the time, you can check Always On . Username – Type in the username provided by ISP in this field. Password – Type in the password provided by ISP in this field. PPP Authentication – Select PAP only or PAP or CHAP for PPP. Idle Timeout – Set the timeout for breaking down the Internet after passing through the time without any action. This setting is active only when the Always On option is note selected.
IP Address from ISP	Fixed IP - Click Yes to use this function and type in a fixed IP address in the box of Fixed IP Address . Fixed IP Address - Type a fixed IP address.
Obtain an IP address automatically	Click this button to obtain the IP address automatically. Router Name – Type in the router name provided by ISP. Domain Name – Type in the domain name that you have assigned.
Specify an IP address	Click this radio button to specify some data. IP Address – Type in the private IP address. Subnet Mask – Type in the subnet mask. Gateway IP Address – Type in gateway IP address.
DNS Server IP Address	Type in the primary IP address for the router. If necessary, type in secondary IP address for necessity in the future.

ATM QoS

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

Multi-PVCs General	ATM QoS	Port-based	Bridge		
Channel	QoS Type	PCR	SCR	MBS	
1.	UBR 🔽	0	0	0	
2.	UBR 🔽	0	0	0	
з.	UBR 🚩	0	0	0	
4.	UBR 🕑	0	0	0	
5.	UBR 🚩	0	0	0	
6.	UBR 🔽	0	0	0	
7.	UBR 🔽	0	0	0	
8.	UBR 🔽	0	0	0	
	Qo UE CB AB	R R R VBR	r ISP provides.		
CR	It re	It represents Peak Cell Rate. The default setting is "0". It represents Sustainable Cell Rate. The value of SCR mus be smaller than PCR.			
CR CR	It re	epresents Sustai	nable Cell Rate.	e	

Port-based Bridge

WAN >> Multi-PVCs

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

Multi-PVCs General ATM QoS Port-based Bridge Channel Enable **P1 P2** P3 **P4** Service Type Add Tag 1. Normal 🗸 2. Normal 💊 з. \checkmark Normal 💌 4. Normal 🐱 Normal IGMP 5. 6. Normal 🗸 7. Normal 🔽 8. Normal 🔻 Note: 1.Channel 1 to 2 are reserved for Nat/Route use.

2.P1 is reserved for Nat/Route use.

ОК	Clear	Cancel

Enable	Check this box to enable that channel. Only channel 3 to 8 can be set in this page, for channel 1 to 4 are reserved for NAT using.
P1 to P4	It means the LAN port 1 to 4. Check the box to designate the LAN port for channel 3 to 8.
Service Type	 Normally, service type is used for the service of video stream (e.g., IPTV). It can divide the packets from remote control and from video stream into different PVC. In general, the protocol used by remote control is IGMP. Normal Normal IGMP Normal – It means that the PVC can accept all packets except IGMP. IGMP – It means that the PVC can accept packets of IGMP only.
Add Tag	To identify the usage of PVC, check this box to invoke this setting. And type the number for VLAN ID (number).
Clipte Clean to nome	all the configurations in this page if you do not estisfy it. When you

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

5.1.6 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
```

Index	Enable	Proto	col	WAN	Src IP Start	Src IP End	Dest IP Start	Dest IP End	Dest Port End	MOA6	Move Down
1		any	*	WAN1 🔽							<u>Down</u>
<u>2</u>		any	~	WAN1 💌						<u>UP</u>	<u>Down</u>
<u>3</u>		any	~	WAN1 🔽						<u>UP</u>	<u>Down</u>
4		any	~	WAN1 🔽						<u>UP</u>	<u>Down</u>
<u>5</u>		any	~	WAN1 🔽						<u>UP</u>	<u>Down</u>
<u>6</u>		any	~	WAN1 🔽						<u>UP</u>	<u>Down</u>
Z		any	~	WAN1 💌						<u>UP</u>	<u>Down</u>
<u>8</u>		any	~	WAN1 💌						<u>UP</u>	<u>Down</u>
<u>9</u>		any	~	WAN1 💌						<u>UP</u>	<u>Down</u>
<u>10</u>		any	*	WAN1 💌						<u>UP</u>	<u>Down</u>
<< <u>1-10</u>	<u>11-20</u> >	~								1	<u>Vext</u> >:

```
Load-Balance Policy
```

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. any TCP UDP TCP/UDP ICMP IGMP			
WAN	Use the drop-down menu to change the WAN interface.			
Src IP Start	Displays the IP address for the start of the source IP.			
Src IP End	Displays the IP address for the end of the source IP.			
Dest IP Start	Displays the IP address for the start of the destination IP.			

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



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

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

Move UP/Move Down Use Up or Down link to move the order of the policy.

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

WAN >> Load-Balance Policy

🗹 Enable	
Protocol	ТСР
Binding WAN Interface	WAN1 💌
Src IP Start	192.168.1.6
Src IP End	192.168.1.9
Dest IP Start	168.95.0.0
Dest IP End	168.95.1.100
Dest Port Start	80
Dest Port End	100

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 C 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.

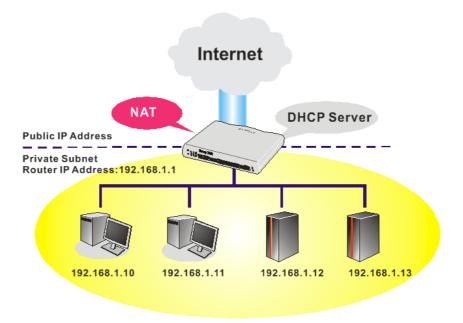
5.2 LAN

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



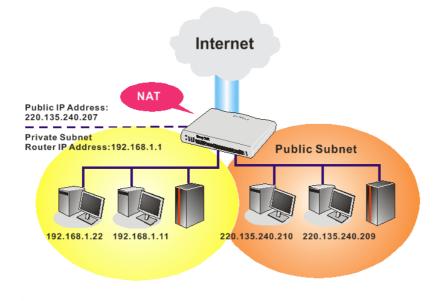
5.2.1 Basics of LAN

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



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





What is Routing Information Protocol (RIP)

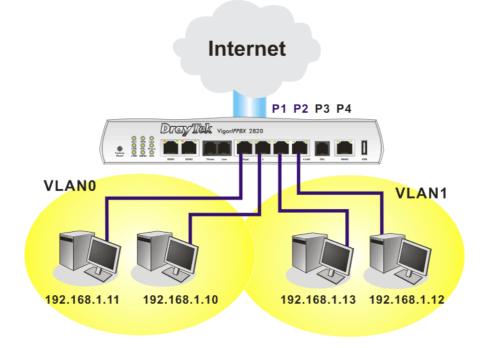
Vigor router will exchange routing information with neighboring routers using the RIP to accomplish IP routing. This allows users to change the information of the router such as IP address and the routers will automatically inform for each other.

What is Static Route

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

What are Virtual LANs

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



5.2.2 General Setup

This page provides you the general settings for LAN.

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

LAN >> General Setup

Ethernet TCP / IP and DHCP Setup						
LAN IP Network Configu	iration	DHCP Server Configuration				
For NAT Usage		⊙Enable Server ○Disable Server				
1st IP Address	192.168.1.1	Relay Agent: 🔘 1st Subr	net 🔾 2nd Subnet			
1st Subnet Mask	255.255.255.0	Start IP Address	192.168.1.10			
For IP Routing Usage 🔘	Enable 💿 Disable	IP Pool Counts	50			
2nd IP Address	192.168.2.1	Gateway IP Address	192.168.1.1			
2nd Subnet Mask	255.255.255.0	DHCP Server IP Address				
2	nd Subnet DHCP Server	for Relay Agent				
		DNS Server IP Address				
RIP Protocol Control	Disable 🚩	🔲 Force DNS manual se	tting			
		Primary IP Address				
		Secondary IP Address				

OK

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

2nd DHCP Server

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

	Start IP Address IP Pool Counts	0 (max. 1	0)
AC Address :	Index Ma	tched MAC Address	given IP Address
Add Delete Edit Cancel	MAC Address :	Delete Edit	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 2^{nd} DHCP server will help router to assign the correct IP address of the correct subnet to the correct host. So those hosts in 2nd subnet won't get an IP address belonging to 1st subnet.

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

RIP Protocol Control

Disable	*
Disable	
1st Subnet	
2nd Subnet	

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

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

DHCP Server DHCP stands for Dynamic Host Configuration Protocol. The Configuration 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 – $(1^{st} subnet/2^{nd} subnet)$ Specify which subnet that DHCP server is located the relay agent should redirect the DHCP request to.

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

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

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

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

DNS Server Configuration

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

Force DNS manual setting - Force Vigor router to use DNS servers in this page instead of DNS servers given by the Internet Access server (PPPoE, PPTP, L2TP or DHCP server). **Primary IP Address -**You must specify a DNS server IP address here because your ISP should provide you with usually more than one DNS Server. If your ISP does not provide it, the router will automatically apply default DNS Server IP address: 194.109.6.66 to this field.

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

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

System Status			System Uptime: 2:10:17
LAN Status	Primary [ONS: 194.109.6.66	Secondary DNS: 168.95.1.1
IP Address	TX Packets	RX Packets	
192.168.1.1	7508	175019	

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

If the IP address of a domain name is already in the DNS cache, the router will resolve the domain name immediately. Otherwise, the

router forwards the DNS query packet to the external DNS server by establishing a WAN (e.g. DSL/Cable) connection.

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

5.2.3 Static Route

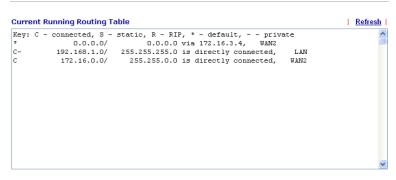
Go to LAN to open setting page and choose Static Route.

LAN >> Static Route Setup

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

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

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



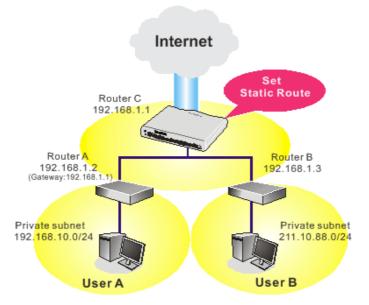
Add Static Routes to Private and Public Networks

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

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

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





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

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

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

Index No. 1

Enable

Destination IP Address
192.168.10.0

Subnet Mask
255.255.0

Gateway IP Address
192.168.1.2

Network Interface
LAN ♥

LAN >> Static Route Setup

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

DrayTek

LAN >> Static Route Setup				
Index No. 2				
🗹 Enable				
	Destination IP Address		211.100.88.0	
	Subnet Mask		255.255.255.0	
	Gateway IP Address		192.168.1.3	
	Network Interface		LAN 🔽	
		OK	Cancel	

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

Diagnostics >> View Routing Table

5.2.4 VLAN

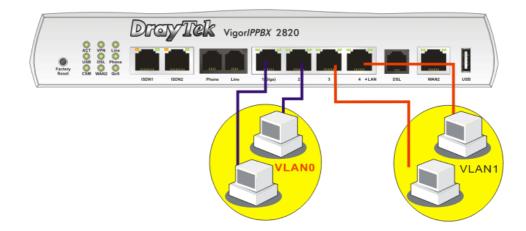
Virtual LAN function provides you a very convenient way to manage hosts by grouping them based on the physical port. You can also manage the in/out rate of each port. Go to LAN page and select VLAN. The following page will appear. Click **Enable** to invoke VLAN function.

Enable				
	P1	P2	P3	P4
VLANO				
VLAN1				
VLAN2				
VLAN3				

LAN >> VLAN Configuration

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

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



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

AN >> VLAN Config	juration				
/LAN Configuration					
	P1	P2	P3	P4	
VLANO		V			
VLAN1					
VLAN2					
VLAN3					

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

5.2.5 Bind IP to MAC

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

Click $\ensuremath{\textbf{LAN}}$ and click $\ensuremath{\textbf{Bind}}$ $\ensuremath{\textbf{IP}}$ to $\ensuremath{\textbf{MAC}}$ to open the setup page.

LAN >> Bind IP to MAC

Note: IP-MAC binding preset	s DHCP Allocat	ions.	
	•	LAN clients cannot acces	ss the Internet.
	Strict Bind		
ARP Table <u>Select All</u> <u>S</u>	<u>iort Refresh </u>	IP Bind List	Select All Sort
IP Address Mac Addre 192.168.1.10 00-0E-A6		Index IP Address	Mac Address
Add and Edit IP Address Mac Address :::::::::::::::::::::::::::::::::::			
	Add	Edit Delete	

Enable	Click this radio button to invoke this function. However, IP/MAC which is not listed in IP Bind List also can connect to Internet.
Disable	Click this radio button to disable this function. All the settings on this page will be invalid.
Strict Bind	Click this radio button to block the connection of the IP/MAC which is not listed in IP Bind List.
ARP Table	This table is the LAN ARP table of this router. The information for IP and MAC will be displayed in this field. Each pair of IP and MAC address listed in ARP table can be selected and added to IP Bind List by clicking Add below.
Add and Edit	 IP Address – Type the IP address that will be used for the specified MAC address. Mac Address – Type the MAC address that is used to bind with the assigned IP address.
Refresh	It is used to refresh the ARP table. When there is one new PC added to the LAN, you can click this link to obtain the newly ARP table information.
IP Bind List	It displays a list for the IP bind to MAC information.



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

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

5.3 NAT

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

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

The benefit of the NAT includes:

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

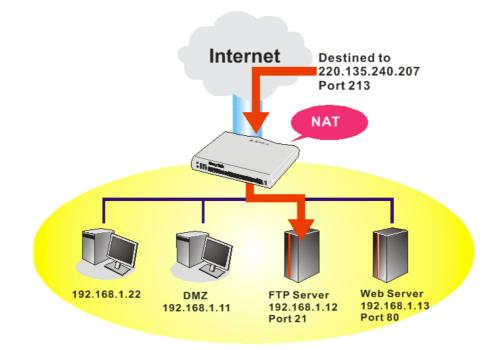
On NAT page, you will see the private IP address defined in RFC-1918. Usually we use the 192.168.1.0/24 subnet for the router. As stated before, the NAT facility can map one or more IP addresses and/or service ports into different specified services. In other words, the NAT function can be achieved by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

Below shows the menu items for NAT.



5.3.1 Port Redirection

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



The port redirection can only apply to incoming traffic.

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

NAT >> Port Redirection	n
-------------------------	---

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

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



NAT >> Port Redirection

Index No. 1				
🗹 Enable				
Mode	Range 💌			
Service Name	Single Range			
Protocol	💙			
WAN IP	1.All			
Public Port	0 -			
Private IP				
Private Port	0			

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

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

Enable	Check this box to enable such port redirection setting.
Mode	Two options (Single and Range) are provided here for you to choose. To set a range for the specific service, select Range . In Range mode, if the public port (start port and end port) and the starting IP of private IP had been entered, the system will calculate and display the ending IP of private IP automatically.
Service Name	Enter the description of the specific network service.
Protocol	Select the transport layer protocol (TCP or UDP).
WAN IP	Select the WAN IP used for port redirection. There are eight WAN IP alias that can be selected and used for port redirection. The default setting is All which means all the incoming data from any port will be redirected to specified range of IP address and port.
Public Port	Specify which port can be redirected to the specified Private IP and Port of the internal host. If you choose Range as the port redirection mode, you will see two boxes on this field. Simply type the required number on the first box. The second one will be assigned automatically later.
Private IP	Specify the private IP address of the internal host providing the service. If you choose Range as the port redirection mode, you will see two boxes on this field. Type a complete IP address in the first box (as the starting point) and the fourth digits in the second box (as the end point).
Private Port	Specify the private port number of the service offered by the internal host.
Active	Check this box to activate the port-mapping entry you have defined.

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

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

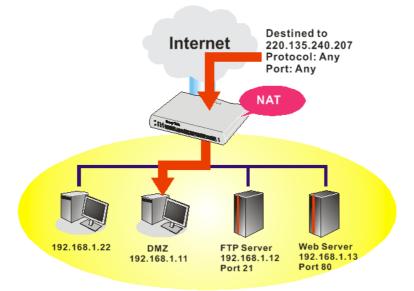


conflict, such as 8080. This can be set in the **System Maintenance** >>**Management Setup**. You then will access the admin screen of by suffixing the IP address with 8080, e.g., http://192.168.1.1:8080 instead of port 80.

Management Access Control			Management Port Setup			
Allow management from the Internet			💿 User Define Ports 🛛 Default Ports			
FTP Server			Telnet Port	23 (Default: 23)		
 HTTP Server HTTPS Server Telnet Server SSH Server 			HTTP Port	80 (Default: 80)		
			HTTPS Port	443 (Default: 443)		
			FTP Port	21 (Default: 21)		
 SSH Server Disable PING from the Internet 		SSH Port	22 (Default: 22)			
Acces	s List		SNMP Setup			
List	IP	Subnet Mask	📃 Enable SNMP Agent			
1		*	Get Community	public		
2		~	Set Community	private		
3		~	Manager Host IP			
			Trap Community	public		
			Notification Host IP			
			Trap Timeout	10 seconds		

5.3.2 DMZ Host

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



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

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

NAT >> DMZ Host Setup

VAN 1	
None 🔽	
Private IP	Choose PC
MAC Address of the True IP	DMZ Host 00 00 00 00 00 00 00
	DMZ Host 00 . 00 . 00 . 00 . 00 . 00 . 00 . 00
Note: When a True-IP DMZ h be always on. YAN 2	ost is turned on, it will force the router's WAN connection to
Note: When a True-IP DMZ h be always on.	

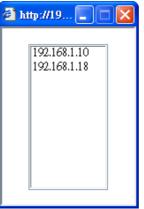
If you previously have set up **WAN Alias** for **PPPoE/PPPoA** or **MPoA** mode, you will find them in **Aux. WAN IP** for your selection.

NAT >> DMZ Host Setup

WAN 1 Index	Enable	Aux. WAN IP	Private IP	
1.		192.168.1.88		Choose PC
WAN 2				
	Enable		Private IP	
				Choose PC
			OK Clear	
nable		Check to en	able the DMZ Host func	ction.

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

WAN 1 Index	Enable	Aux. WAN IP	Private IP	
1.		192.168.1.88	192.168.1.10	Choose PC
WAN 2				
	Enable		Private IP	
				Choose PC

5.3.3 Open Ports

NAT >> 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:

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

IndexIndicate 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.CommentSpecify the name for the defined network service.

VigorIPPBX 2820 Series User's Guide



WAN Interface	N 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

Inde	Index No. 1						
🗹 Enable Open Ports							
Comment			P21	>			
WAN Interface			W	WAN1 🔽			
	Local Computer			2.168.1.10	Cho	iose PC	
	Protocol	Start Port	End Port		Protocol	Start Port	End Port
1.	TCP 🔽	4500	4700	6.	💙	0	0
2.	ТСР 🔽	4500	4700	7.	💙	0	0
з.	💙	0	0	8.	💙	0	0
4.	💌	0	0	9.	🚩	0	0
5.	💙	0	0	10.	💙	0	0

OK	Clear	Cancel

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

5.4 Firewall

5.4.1 Basics for Firewall

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

Firewall Facilities

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

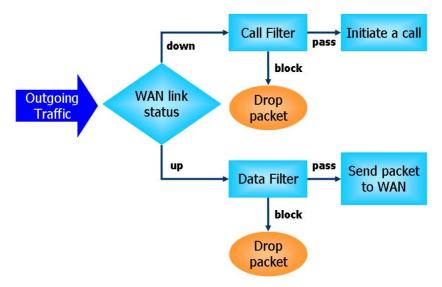
- User-configurable IP filter (Call Filter/ Data Filter).
- Stateful Packet Inspection (SPI): tracks packets and denies unsolicited incoming data
- Selectable Denial of Service (DoS) /Distributed DoS (DDoS) attacks protection

IP Filters

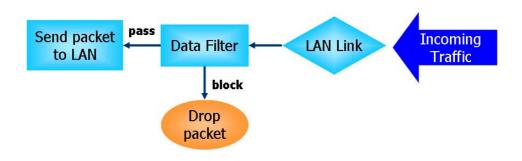
Depending on whether there is an existing Internet connection, or in other words "the WAN link status is up or down", the IP filter architecture categorizes traffic into two: **Call Filter** and **Data Filter**.

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

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



Dray Tek



Stateful Packet Inspection (SPI)

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

Denial of Service (DoS) Defense

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

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

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

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

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

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

Below shows the menu items for Firewall.



Dray Tek

5.4.2 General Setup

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

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

Firewall >> General Setur	Firewa	>>	General	Setu	p
---------------------------	--------	----	---------	------	---

Call Filter	💿 Enable	Start Filter S	et Set#1 💌
	🔘 Disable		
Data Filter	💿 Enable	Start Filter S	et Set#2 💌
	🔘 Disable		
Actions for defa	ult rule:		
Application		Action/Profile	Syslog
Filter		Pass 💌	
IM/P2P Filter		None 💌	
URL Content Filte	Ľ	None 💌	
<u>Web Content Filte</u>	<u>u</u>	None 💌	
Advance Setting		Edit	

OK Cancel

Call Filter	Check Enable to activate the Call Filter function. Assign a start filter set for the Call Filter.
Data Filter	Check Enable to activate the Data Filter function. Assign a start filter set for the Data Filter.
Action/Profile	Select Pass or Block for the packets that do not match with the filter rules.
IM/P2P Filter	Select one of the IM/P2P Filter Profile settings (created in CSM>> IM/P2P Filter) for applying with this router. Please set at least one profile for choosing in CSM>> IM/P2P Filter Profile web page first. For troubleshooting needs, you can specify to record information for IM/P2P Filter Profile by checking the Log box. It will be sent to Syslog server. Please refer to section 5.14.5 Syslog/Mail Alert for more detailed information.
URL Content Filter	Select one of the URL Content Filter Profile settings (created in CSM>> URL Content Filter Profile) for applying with this router. Please set at least one profile for choosing in CSM>> URL Content Filter Profile web page first. For troubleshooting needs, you can specify to record information for URL Content Filter by checking the Log box. It will be sent to Syslog server. Please refer to section 5.14.5 Syslog/Mail Alert for more detailed information.
Web Content Filter	Select one of the Web Content Filter Profile settings (created in CSM>> Web Content Filter Profile) for applying with this router.



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

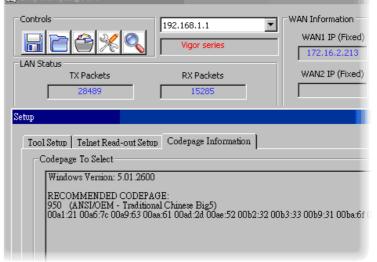
For troubleshooting needs you can specify the filter log and/or CSM log here by checking the box. The log will be displayed on Draytek Syslog window.

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

	utm - Microsoft Internet Exp	plorer
irewall >> General Se	etup	
Advance Setting		
Codepage	ANSI(1253)-Gr	eek 🔽
Window size:	65535	
Session timeout:	1440	Minute
	OK Close	

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

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



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

Syslog

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

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

5.4.3 Filter Setup

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

Firewall >>	Filter	Setup
-------------	--------	-------

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

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

Filter Set 1 Comments :	efault Call Filter			
Filter Rule	Active	Comments	Move Up	Move Down
1	V	Block NetBios		Down
2			<u>UP</u>	<u>Down</u>
3			<u>UP</u>	<u>Down</u>
4			<u>UP</u>	<u>Down</u>
5			<u>UP</u>	Down
6			<u>UP</u>	<u>Down</u>
7			<u>UP</u>	
1			Next Filte	er Set 🛛 None 💌
		OK Clear C	ancel	
filter Rule		Click a button number button will open Edit F information, refer to th	Filter Rule web pa	ge. For the d
ctive		Enable or disable the fi	ilter rule.	
Comment		Enter filter set commen 23–character long.	nts/description. M	aximum len
Move Up/Do	wn	Use Up or Down link t	to move the order	of the filter
Next Filter S	let	Set the link to the next filter run. Do not make		

Firewall >> Filter Setup >> Edit Filter Set



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

Firewall >> Edit Filter Set >> Edit Filter Rule

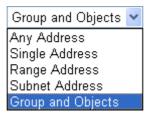
🗹 Check to enable the Filter Rule	9	
Comments:	Block NetBios	
Index(1-15) in <u>Schedule</u> Setup:		
Direction:	LAN -> WAN 🔽	
Source IP:	Any	Edit
Destination IP:	Any	Edit
Service Type:	TCP/UDP, Port: from 137~139 to undefined	Edit
Fragments:	Don't Care 👻	
Application	Action/Profile	Syslog
Application Filter:	Action/Profile Block Immediately	Syslog
		Syslog
Filter:	Block Immediately	Syslog
Filter: Branch to Other Filter Set:	Block Immediately	Syslog
Filter: Branch to Other Filter Set: IM/P2P Filter:	Block Immediately	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 PCs on LAN to work at certain time interval only. You may choose up to 4 schedules out of the 15 schedules pre-defined in Applications >> Schedule setup. The default setting of this filed is blank and the function will always work.
Direction	Set the direction of packet flow (LAN->WAN/WAN->LAN). It is for Data Filter only. For the Call Filter , this setting is not available since Call Filter is only applied to outgoing traffic.
Source/Destination IP	Click Edit to access into the following dialog to choose the source/destination IP or IP ranges.

Dray Tek

art IP Address O.O.O. d IP Address O.O.O. ert Mask O.O.O. ert Selection Occurs
d IP Address 0.0.0.0 onet Mask 0.0.0.0 onet Mask 0.0.0.0 onet Mask 0.0.0.0 onet Selection
onet Mask 0.0.0
ert Selection
No.
Group None 🛩
IP Object None 🛩
IP Object None
IP Object 1-RD Department 2-Finanical Dept.
3-HR Department

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



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

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

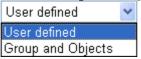
Service Type	Group and Objects 💌
Protocol	
Source Port	= 🗸 137 ~ 139
Destination Port	= 🗸 1 ~ 65535
<u>Service Group</u>	None 💌
or <u>Service Object</u>	None 💌
or Service Object	None 💌
or Service Object	None 1-SIP
ОК	2-RTP

To set the service type manually, please choose **User defined** as the Service Type and type them in this dialog. In addition, if you

Service Type



want to use the service type from defined groups or objects, please choose **Group and Objects** as the Service Type.



Protocol - Specify the protocol(s) which this filter rule will apply to. **Source/Destination Port -**(=) – when the first and last value are the same, it indicates one port; when the first and last values are different, it indicates a range for the port and available for this service type. (!=) – when the first and last value are the same, it indicates all the ports except the port defined here; when the first and last values are different, it indicates that all the ports except the range defined here are available for this service type. (>) – the port number greater than this value is available. (<) – the port number less than this value is available for this profile. Service Group/Object - Use the drop down list to choose the one that you want. **Fragments** Specify the action for fragmented packets. And it is used for Data Filter only. Don't care - No action will be taken towards fragmented packets. Unfragmented - Apply the rule to unfragmented packets. *Fragmented* - Apply the rule to fragmented packets. *Too Short* - Apply the rule only to packets that are too short to contain a complete header. Filter Specifies the action to be taken when packets match the rule. Block Immediately - Packets matching the rule will be dropped immediately. Pass Immediately - Packets matching the rule will be passed immediately. Block If No Further Match - A packet matching the rule, and that does not match further rules, will be dropped. Pass If No Further Match - A packet matching the rule, and that does not match further rules, will be passed through. **Branch to other Filter** If the packet matches the filter rule, the next filter rule will branch Set to the specified filter set. Select next filter rule to branch from the drop-down menu. Be aware that the router will apply the specified filter rule for ever and will not return to previous filter rule any more. **IM/P2P** Filter Select one of the IM/P2P Filter Profile settings (created in **CSM>> IM/P2P Filter**) for applying with this router. Please set at least one profile for choosing in CSM>> IM/P2P Filter Profile web page first. For troubleshooting needs, you can specify to record information for IM/P2P Filter Profile by checking the Log box. It will be sent to Syslog server. Please refer to section System Maintenance>>Syslog/Mail Alert for more detailed information. **URL Content Filter** Select one of the URL Content Filter profile settings (created in **CSM>> URL Content Filter Profile**) for applying with this router. Please set at least one profile for choosing in CSM>> URL Content Filter Profile web page first. For troubleshooting needs,

you can specify to record information for **URL Content Filter** by checking the Log box. It will be sent to Syslog server. Please refer to section **System Maintenance>>Syslog/Mail Alert** for more detailed information.

- Web Content FilterSelect one of the Web Content Filter profile settings (created in
CSM>> Web Content Filter Profile) for applying with this router.
Please set at least one profile for anti-virus in CSM>> Web
Content Filter Profile web page first. For troubleshooting needs,
you can specify to record information for Web Content Filter by
checking the Log box. It will be sent to Syslog server. Please refer
to section System Maintenance>>Syslog/Mail Alert for more
detailed information.
- SysLogFor troubleshooting needs you can specify the filter log and/or CSM
log here. Check the corresponding box to enable the log function.
Then, the filter log and/or CSM log will be shown on Draytek
Syslog window.

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

http://192.168.1.1/doc/ipfgenadv.ht	r://192.168.1.1/doc/ipfgenady.htm - Microsoft Internet Explorer				
Firewall >> General Set	tup				
Advance Setting					
Codepage	ANSI(1253)-Greel	ĸ	~		
Window size:	65535				
Session timeout:	1440	Minute			
	OK Close]			

Codepage - This function is used to compare the characters among different languages. Choose correct codepage can help the system obtaining correct ASCII after decoding data from URL and enhance the correctness of URL Content Filter. The default value for this setting is ANSI 1252 Latin I. If you do not choose any codepage, no decoding job of URL will be processed. Please use the drop-down list to choose a codepage. If you do not have any idea of choosing suitable codepage, please open Syslog. From Codepage Information of Setup dialog, you will see the recommended codepage listed on the dialog box.

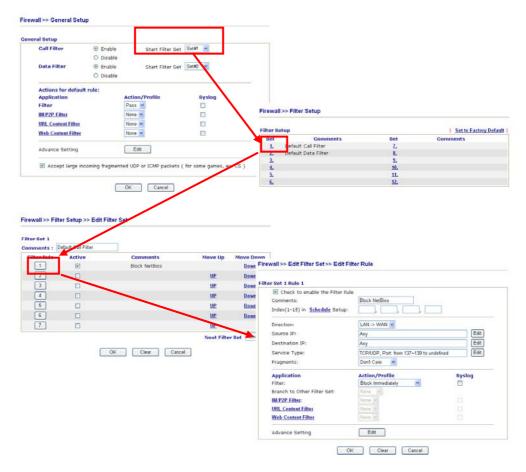
📶 DrayTek Syslog 3.9.1		
Controls	192.168.1.1	WAN Information WAN1 IP (Fixed)
TX Packets	RX Packets	WAN2 IP (Fixed)
28489	15285	
Setup		
Tool Setup Telnet Read-out Setup Codepage To Select	Codepage Information	_
Windows Version: 5.01.2600 RECOMMENDED CODEPA 950 (ANSI/OEM - Tradition 00a1:21 00a6:7c 00a9:63 00a		0b3:33 00b9:31 00ba:6f (

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

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

Example

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



Dray Tek

5.4.4 DoS Defense

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

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

Enable DoS Defense			
🗌 Enable SYN flood defense	Threshold	50	packets / sec
	Timeout	10	sec
Enable UDP flood defense	Threshold	150	packets / sec
	Timeout	10	sec
Enable ICMP flood defense	Threshold	50	packets / sec
	Timeout	10	sec
Enable Port Scan detection	Threshold	150	packets / sec
Block IP options	🔲 Block TCP fl	lag scan	
Block Land	📃 Block Tear (Drop	
🔲 Block Smurf	📃 Block Ping c	of Death	
🔲 Block trace route	📃 Block ICMP	fragment	
🔲 Block SYN fragment	📃 Block Unkno	wnProtocol	
📃 Block Fraggle Attack			
Enable DoS defense function t crackers.	o prevent the attacks	from hack	ter or 📥
			~

Firewall >>	DoS	defense	Setup

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



indicate the protocol type running over the upper layer. However, the protocol types greater than 100 are reserved and undefined at this time. Therefore, the router should have ability to detect and reject this kind of packets.

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

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

System Maintenance >> SysLog / Mail Alert Setup

ysLog Access Setup ✓ Enable ierver IP Address iestination Port nable syslog message: ✓ Firewall Log ✓ VPN Log ✓ User Access Log ✓ Call Log ✓ WAN Log ✓ Router/DSL informa	192.168.1.115 514 tion	Mail Alert Setup Clear Cancel SMTP Server Send a test SMTP Server Mail To Returm-Path Authentication User Name Password Enable E-Mail Alert: IM-P2P Clear Cancel	e-mail
erver IP Address eestination Port inable syslog message: IV Firewall Log IV PN Log IV User Access Log IV Call Log IV WAN Log	514	SMTP Server Mail To Return-Path Authentication User Name Password Enable E-Mail Alert: DoS Attack IM-P2P	
estination Port nable syslog message: V Firewall Log V VPN Log V User Access Log V Call Log V WAN Log	514	Mail To	
nable syslog message: V Firewall Log V VPN Log V User Access Log V Call Log V WAN Log	tion	Return-Path	
Firewall Log VPN Log User Access Log Call Log WAN Log		Authentication User Name Password Enable E-Mail Alert: DoS Attack IM-P2P	
 ✓ VPN Log ✓ User Access Log ✓ Call Log ✓ WAN Log 		User Name Password Enable E-Mail Alert: DoS Attack IM-P2P	
 ✓ User Access Log ✓ Call Log ✓ WAN Log 		Password Enable E-Mail Alert: DoS Attack IM-P2P	
✓ Call Log✓ WAN Log		Enable E-Mail Alert: DoS Attack IM-P2P	
WAN Log		DoS Attack	
-		□ IM-P2P	
Router/DSL information			
	UK	Cancel	
)rayTek Syslog 3.7.0			
ontrols 192.1	.68.1.1 WAN St.		
	/igor2820 Series	Sateway IP (Fixed) TX Packets TX Rate 172.16.3.4 343 3	
AN Status TX Packets	RX Packets	WAN IP (Fixed) RX Packets RX Rate	
4175	3668	172.16.3.229 2558 126	
rewall Log VPN Log User Access L	og Call Log WAN Log Others	Network Information Net State Traffic Graph	
Time Host	Message		
Jan 1 00:00:42 ¥igor Jan 1 00:00:34 ¥igor		2.168.1.115,10605 -> 192.168.1.1,23 PR 6(tcp) len 20 40 -\$ 394375 92.168.1.115 -> 192.168.1.1 PR 1(icmp) len 20 60 icmp 0/8	

5.5 Objects Settings

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

Objects Setting
IP Object
▶ IP Group
Service Type Object
Service Type Group
Keyword Object
Keyword Group
File Extension Object
IM Object
P2P Object
Misc Object

Objects Setting >> IP Object

Objects Setting >> IP Object

5.5.1 IP Object

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

(P Object Profiles:			Set to Factory De	<u>stault</u>
Index	Name	Index	Name	
<u>1.</u>		<u>17.</u>		
<u>2.</u>		<u>18.</u>		
<u>3.</u>		<u>19.</u>		
<u>4.</u>		<u>20.</u>		
<u>5.</u>		<u>21.</u>		
<u>6.</u>		<u>22.</u>		
<u>7.</u>		<u>23.</u>		
<u>8.</u>		<u>24.</u>		
<u>9.</u>		<u>25.</u>		
<u>10.</u>		<u>26.</u>		
<u>11.</u>		<u>27.</u>		
<u>12.</u>		<u>28.</u>		
<u>13.</u>		<u>29.</u>		
<u>14.</u>		<u>30.</u>		
<u>15.</u>		<u>31.</u>		
16.		<u>32.</u>		
101				

Set to Factory Default Clear all profiles.

Click the number under Index column for settings in detail.

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
Invert Selection:	

Name	Type a name for this profile. Maximum 15 characters are allowed.
Interface	Choose a proper interface (WAN, LAN or Any). Interface: Any Any LAN WAN For example, the Direction setting in Edit Filter Rule will ask you specify IP or IP range for WAN or LAN or any IP address. If you choose LAN as the Interface here, and choose LAN as the direction setting in Edit Filter Rule, then all the IP addresses specified with LAN interface will be opened for you to choose in Edit Filter Rule page.
Address Type	 Determine the address type for the IP address. Select Single Address if this object contains one IP address only. Select Range Address if this object contains several IPs within a range. Select Subnet Address if this object contains one subnet for IP address. Select Any Address if this object contains any IP address.
Start IP Address	Type the start IP address for Single Address type.
End IP Address	Type the end IP address if the Range Address type is selected.
Subnet Mask	Type the subnet mask if the Subnet Address type is selected.
Invert Selection	If it is checked, all the IP addresses except the ones listed above will be applied later while it is chosen.

Below is an example of IP objects settings.

Objects Setting >> IP Object

IP Obj	ject I	Profil	es:
--------	--------	--------	-----

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

5.5.2 IP Group

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

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

Objects Setting >> IP Group

Set to Factory Default Clear all profiles.

Click the number under Index column for settings in detail.

Objects Setting >> IP Group

Name:	Administration		
Interface:	Any 💌		
Available IP Objects	Selected IP Objects		
1-RD Department 2-Finanical Dept. 3-HR Department	» «		
	OK Clear Cancel		
Name	Type a name for this profile. Maximum 15 characters are allowed.		
Interface	Choose WAN, LAN or Any to display all the available IP objects with the specified interface.		
Available IP Objects	All the available IP objects with the specified interface chosen above will be shown in this box.		
Selected IP Objects	Click >> button to add the selected IP objects in this box.		

5.5.3 Service Type Object

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

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

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

Set to Factory Default Clear all profiles.

Click the number under Index column for settings in detail.

-	• •	
Profile Index	::1	
	Name	www
	Protocol	ТСР 🖌 6
	Source Port	= 🗸 1 👡 65535
	Destination Port	= 🗸 70 ~ 80
		OK Clear Cancel
Name		Type a name for this profile.
Protocol		Specify the protocol(s) which this profile will apply to.
		TCP 🔽 6
		Any ICMP IGMP
		TCP
		Other
Source/Des	tination 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.

Objects Setting >> Service Type Object Setup

Dray Tek

(=) – 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>	
<u>4.</u>	

5.5.4 Service Type Group

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

```
Objects Setting >> Service Type Group
```

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

Set to Factory Default Clear all profiles.

Click the number under Index column for settings in detail.

Name:	VolP]			
Available Service Typ	e Objects	Sel	ected Service Type	Objects		
1-SIP 2-RTP						
	OK CI	ar	Cancel			
Name	Type a nar	e foi	this profile.			
Available Service Type Objects			e service objects >>Service Type			
Selected Service Type Objects	Click w box.	bı	utton to add the s	elected IP of	objects in t	his

5.5.5 Keyword Object

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

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

Objects Setting >> Keyword Object

Set to Factory Default Clear all profiles.

Click the number under Index column for setting in detail.

Dray Tek

Objects Setting >> I	Keyword Object Setup
Profile Index : 1	
Name	
Contents	(Max 63 characters)
Name	OK Clear Cancel Type a name for this profile, e.g., game.
Contents	Type the content for such profile. For example, type <i>gambling</i> as Contents. When you browse the webpage, the page with gambling information will be watched out and be passed/blocked based on the configuration on Firewall settings.

5.5.6 Keyword Group

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

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

```
Objects Setting >> Keyword Group
```

```
Set to Factory Default Clear all profiles.
```

Click the number under Index column for setting in detail.

Objects Setting >> Keyword Group Setup

Name:	
Available Keyword Objects	Selected Keyword Objects(Max 16 Objects)
1-Keyword-1 2-keyword-2	» «
(OK Clear Cancel
Name	Type a name for this group.
Available Keyword Objects	You can gather keyword objects from Keyword Object page within one keyword group. All the available Keyword objects that you have created will be shown in this box.
Selected Keyword Objects	Click button to add the selected Keyword objects in this box.

5.5.7 File Extension Object

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

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

File Extension Ob	ject Profiles:		Set to Factory Defau	<u>ılt</u>
Profile	Name	Profile	Name	
<u>1.</u>		<u>5.</u>		
<u>2.</u>		<u>6.</u>		
<u>3.</u>		<u>7.</u>		
<u>4.</u>		<u>8.</u>		

Set to Factory Default Clear all profiles.

Objects Setting >> File Extension Object

Click the number under Profile column for configuration in details.

Objects Setting >> File Extension Object Setup

Profile Index: 1		Profile	Name:				
Categories	File Extensions						
Image Select All Clear All	D.bmp	.dib .pcx	.gif] .jpeg. .pict	.jpg .png	.jpg2 . .tif	.jp2 .iff
Video Select All Clear All	.asf .qt	□.avi □.rm	□.mov □.wmv	.mpe .3gp	.mpeg . .3gpp	.mpg .3gpp2	.mp4
Audio Select All Clear All	.aac .ra	□.aiff □.ram	□.au □.vox	.mp3 .wav	.m4a	□.m4p	ogg .
Java Select All Clear All	🗌 .class 🗋 .jse	□.jad □.jsp	□.jar □.jtk	🗆 .jav	🗆 .java	🗆 .jcm	🗆 .js
ActiveX Select All Clear All	🗆 .alx 🗋 .viv	.apb .vrm	.axs	.ocx	🗌 . olb	.ole	.tlb
Compression Select All Clear All	.ace .rar	□.arj □.sit	□.bzip2 □.zip	.bz2	🗌.cab	🗆 .gz	🗆 . gzip
Executation Select All Clear All	.bas .scr	🗌 .bat	.com	.exe	.inf	🗆 .pif	.reg
		OK	Clear	Canc	el		

Profile Name

Type a name for this profile.

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

5.5.8 IM Object

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

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

Objects Setting >> IM Object Profile

Set to Factory Default Clear all profiles.

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

Objects Setting >> IM Object Profile

rofile Name:					
heck for Disallov	v:				
		Advanced	Management		
Activity / Ap	plication	MSN	YahooIM	AIM(<=5.9)	ICQ
Login	1				
Messa	ge				
File Tran	sfer				
Game	9				
Video)				
Voice	9				
Confere	nce				
Other Acti	ivities				
IM Application VoIP					
AIM6	🗖 QQ	🗌 iChat	🗌 Jabb	er/GoogleTalk	Skype
🗌 GoogleChat	🗌 ×Fire	📃 GaduGadı	u 📃 Palta	alk	SIP
🗌 Qnext	🗌 Meetro	POCO/PP:	365 🗌 Ares	Chat	
	14	1-1- TR4 (*			
Web IM (* = more than one address)					
	<u>eMessenger</u> ICQ Java*	<u>WebMSN</u> ICQ Flash*	<u>meebo*</u> goowy*	<u>eBuddy</u> IMhaha*	<u>ILoveIM*</u> getMessenger
📃 WebIM URLs	IMUnitive*	Wablet*	<u>goowy</u> mabber*	MSN2GO*	<u>KoollM</u>
	MessengerFX*		tos <u>WebYahoolM</u>		<u></u>

Profile Name

Type a name for this profile.

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

5.5.9 P2P Object

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

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

Objects Setting >> P2P Object Profile

Set to Factory Default Clear all profiles.

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

file Name:			
eck for Disallow:			
Protocol		Applications	
📃 SoulSeek	SoulSeek		
🗌 eDonkey	eDonkey, eMu	ule, Shareaza	
FastTrack	KazaA, BearS	hare, iMesh	
🗌 OpenFT	KCeasy, FileP	ipe	
🗌 Gnutella	BearShare, Li	BearShare, Limewire, Shareaza, Foxy	
🗌 OpenNap	Lopster, XNa	Lopster, XNap, WinLop	
BitTorrent	BitTorrent, BitSpirit, BitComet		
🗌 Winny	Winny, WinMX, Share		
	Other P2	P Applications	
Xunlei	🗌 Vagaa	PP365	POCO
Clubbox	Ares	🗌 ezPeer	

Objects Setting >> P2P Object Profile



Profile Name Type a name for this profile.

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

5.5.10 Misc Object

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

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

Objects Setting >> Misc Object Profile

Set to Factory Default

Clear all profiles.

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

Objects Setting >> Misc Object Profile

Profile Index: 1				
Profile Name:				
Check for Disallow	e:			
		Tunneling		
Socks4/5	PGPNet	HTTP Proxy	TOR 🗌	VNN VNN
SoftEther	FolderShare	MS TEREDO	📃 Wujie/UltraSurf	🗌 Hamachi
HTTP Tunnel	🗌 Ping Tunnel	🔲 Tiny VPN		
-				
		Streaming		
MMS	RTSP	🗌 TVAnt	s 🔲 F	PPStream
🗌 PPlive	🗌 FeiDian	🗌 UUSee	n 🗌 n	NSPlayer
PCAST	🗌 TVKoo	🗌 SopCa	st 📃 l	JDLiveX
TVUPlayer	MySee	🗌 Joost	F	FlashVideo
		Remote Control		
VNC VNC	🗌 Radmin	🗌 SpyAn	ywhere 🔲 🤋	ShowMyPC
LogMeIn	🗌 TeamViewe	r 📃 Gogrok	< 🗖 F	RemoteControlPro
CrossLoop	🗌 WindowsRD	P 🗌 pcAny	where	
	OK	Clear	Cancel	

Profile Name

Type a name for this profile.

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

5.6 CSM

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

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

IM/P2P Filter

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



URL Content Filter

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

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

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

Web Content Filter

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

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

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



5.6.1 IM/P2P Filter Profile

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

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

CSM >> IM/P2P Filter Profile

Set to Factory Default Clear all profiles.

Click the number under Index column for settings in detail.

CSM >> IM/P2P Filter Profile

Profile Index: 1	
Profile Name:	
IM Object	None 💌
P2P Object	None 💌
<u>Misc Object</u>	None 💌
-	OK Cancel

Profile Name

Type a name for the CSM profile.

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

5.6.2 URL Content Filter Profile

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

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



a job-related only environment hence to increase the employee work efficiency. How can URL Content Filter work better than traditional firewall in the field of filtering? Because it checks the URL strings or some of HTTP data hiding in the payload of TCP packets while legacy firewall inspects packets based on the fields of TCP/IP headers only.

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

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

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

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

URL Content F	ilter Profile Table:		Set to Factory Default
Profile	Name	Profile	Name
<u>1.</u>		<u>5.</u>	
<u>2.</u>		<u>6.</u>	
<u>3.</u>		<u>7.</u>	
<u>4.</u>		<u>8.</u>	
Administratior	1 Message (Max 255 characters)	
-	r> The requested Web ease contact your system ad		

CSM >> URL Content Filter Profile

information.</center></body>

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

OK

CSM >> URL Content Filter Profile

Profile Name:		
Priority:	Both : Pass	Log: None V
1.URL Acces	s Control	
🗌 Enab	le URL Access Control	Prevent web access from IP address
Actio	in:	Group/Object Selections
Pass	~	Edit
2.Web Feat	ure	
🗌 Enab	le Restrict Web Feature	
Actio	n:	
Pass	Cookie Pr	oxy File Extension Profile: None 🗸
	OK	Clear Cancel

Profile Name	Type the name for such profile.
Priority	 It determines the action that this router will apply. Both: Pass – The router will let all the packages that match with the conditions specified in URL Access Control and Web Feature below passing through. When you choose this setting, both configuration set in this page for URL Access Control and Web Feature will be inactive. Both: Block – The router will block all the packages that match with the conditions specified in URL Access Control and Web Feature below. When you choose this setting, both configuration set in this page for URL Access Control and Web Feature below. When you choose this setting, both configuration set in this page for URL Access Control and Web Feature below. When you choose this setting, both configuration set in this page for URL Access Control and Web Feature below. When you choose this setting, both configuration set in this page for URL Access Control and Web Feature will be inactive. Either: URL Access Control First – When all the packages matching with the conditions specified in URL Access Control and Web Feature below, such function can determine the priority for the actions executed. For this one, the router will process the packages matching with the conditions set below for URL first, then Web feature second. Either: Web Feature First – When all the packages matching with the conditions specified in URL Access Control and Web Feature below, such function can determine the priority for the actions executed. For this one, the router will process the packages with the conditions specified in URL Access Control and Web Feature below, such function can determine the priority for the actions executed. For this one, the router will process the packages with the conditions set below for web feature first, then URL second.
	Both : Pass 💙
	Both : Pass Both : Block Either : URL Access Control First Either : Web Feature First
Log	None – There is no log file will be recorded for this profile.

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

Log

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



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

Prevent web access from IP address - Check the box to deny any web surfing activity using IP address, such as http://202.6.5.2. The reason for this is to prevent someone dodges the URL Access Control. You must clear your browser cache first so that the URL content filtering facility operates properly on a web page that you visited before.

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

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

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





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

http://192.168.1.1 - Group/Object Edit -		
Object/Group Edit		
Keyword Object	None 🗸	
or Keyword Object	None 🗸	
or Keyword Object	None 🗸	
or Keyword Object	None 🕶	
or Keyword Object	None 🕶	
or Keyword Object	None 💌	
or Keyword Object	None 💌	
or Keyword Object	None 💌	
or <u>Keyword Group</u>	None 💌	
or Keyword Group	None 💌	
or Keyword Group	None 💌	
or Keyword Group	None 💌	
or Keyword Group	None 💌	
or Keyword Group	None 💌	
or Keyword Group	None 💌	
or Keyword Group	None 💌	
	OK Close	

keyword list the more efficiently the Vigor router perform

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

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

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

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

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

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

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

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



5.6.3 Web Content Filter Profile

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

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

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

Profile	Name	Profile	Name
<u>1.</u>		<u>5.</u>	
<u>2.</u>		<u>6.</u>	
<u>3.</u>		<u>7.</u>	
<u>4.</u>		<u>8.</u>	
Iministration M	lessage (Max 255 charact	ers)	
oody> <center>< ilter.Pleas</center>	br>The requested We se contact your system senter>	eb page has been block	-

CSM >> Web Content Filter Profile

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

CSM >> Web Content Filter Profile

Profile Index : 1			
Profile Name:			
Action : Block 💌		log : Block 💌	
Groups Child Protection Select All Clear All	Categories	Criminal Hacking Violence	Drugs/Alcohol
Leisure Select All Clear All	Advertisements Games Hobbies Personals Sports	Entertainment Glamour Lifestyle Photo Searches Streaming Media	 Food Health Motor Vehicles Shopping Travel
Business Select All Clear All	Computing/Internet Politics Remote proxies	☐ Finance ☐ Real Estate ☐ Search Engine	☐ Job Search/Career ☐ Reference ☐ Web Mail
Others Select All Clear All	 Education News Usenet news 	 Hosting sites Religion uncategorised sites 	☐ Kid Sites ☐ Sex Education
Action	Pass - allow acces categories listed of Block - restrict acc categories listed of If the web pages d	n the box below. cessing into the corre n the box below.	onding webpage with the sponding webpage with specified feature set here
νog	Pass – Only the lo Block – Only the l	-	

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

5.7 Bandwidth Management

Below shows the menu items for Bandwidth Management.

Bandwidth Management	
Sessions Limit	
Bandwidth Limit	
Quality of Service	

5.7.1 Sessions Limit

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

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

	💿 Enat	ole 🔘 Disable					
	Default N	1ax Sessions: 100					
	Limitatio	on List					
	Index	Start IP	End	IP	Max S	essions	
	Start IP:	Limitation		End IP:			
			Add	Edit	Delete		
ne Sch	edule						
		 <u>Schedule</u> Setup: and Idle Timeout se 	ttings w	ill be ignor	, ed.		

Bandwidth Management >> Sessions Limit

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

Enable	Click this button to activate the function of limit session.
Disable	Click this button to close the function of limit session.
Default session limit	Defines the default session number used for each computer in LAN.
Limitation List	Displays a list of specific limitations that you set on this web page.
Start IP	Defines the start IP address for limit session.
End IP	Defines the end IP address for limit session.



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

5.7.2 Bandwidth Limit

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

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

Bandwidth Management >> Bandwidth Li	imit
--------------------------------------	------

Bandwid	Ith Limit
	🔘 Enable 💿 Disable
	Default TX Limit: 200 Kbps Default RX Limit: 800 Kbps
	Limitation List
	Index Start IP End IP TX limit RX limit
	Start IP: End IP:
	TX Limit: Kbps RX Limit: Kbps Add Edit Delete
ime Scl	hedule
Inde	ex(1-15) in <u>Schedule</u> Setup:,,,,
	e: Action and Idle Timeout settings will be ignored.
	OK

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

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

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

5.7.3 Quality of Service

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

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

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

There are two components within Primary configuration of QoS deployment:

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

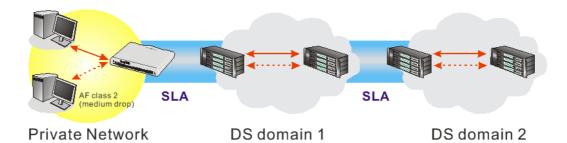
The basic QoS implementation in Vigor routers is to classify and schedule packets based on the service type information in the IP header. For instance, to ensure the connection with the headquarter, a teleworker may enforce an index of QoS Control to reserve bandwidth for HTTPS connection while using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

One more larger-scale implementation of QoS network is to apply DSCP (Differentiated Service Code Point) and IP Precedence disciplines at Layer 3. Compared with legacy IP Precedence that uses Type of Service (ToS) field in the IP header to define 8 service classes, DSCP is a successor creating 64 classes possible with backward IP Precedence compatibility.



In a QoS-enabled network, or Differentiated Service (DiffServ or DS) framework, a DS domain owner should sign a Service License Agreement (SLA) with other DS domain owners to define the service level provided toward traffic from different domains. Then each DS node in these domains will perform the priority treatment. This is called per-hop-behavior (PHB). The definition of PHB includes Expedited Forwarding (EF), Assured Forwarding (AF), and Best Effort (BE). AF defines the four classes of delivery (or forwarding) classes and three levels of drop precedence in each class.

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



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

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

Genera	l Setup						1	<u>Set to Factory D</u>	efault
Index	Status	Bandwidth	Directon	Class 1	Class 2	Class 3	Others	UDP Bandwidth Control	
WAN1	Enable	10000Kbps/10000Kbps	Outbound	25%	25%	25%	25%	Inactive	<u>Setu</u>
WAN2	Enable	10000Kbps/10000Kbps	Outbound	25%	25%	25%	25%	Inactive	Setu

Bandwidth Management >> Quality of Service

Index	Name	Rule	Service Type
Class 1		<u>Edit</u>	
Class 2		<u>Edit</u>	Edit
Class 3		<u>Edit</u>	

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					
	OUT 💌 Class Name	Reserved_bandwidth Ratio			
Class 1		25 %			
Class 2		25 %			
Class 3		25 %			
	Others	25 %			
🔲 Enable UDP Bandwidth Contr	ol	Limited_bandwidth Ratio 25 %			
🔲 Outbound TCP ACK Prioritize		Online Statistics			
	OK Clear	Cancel			
Enable the QoS Control	Please also define whi apply to. IN- apply to incoming OUT- apply to outgoin BOTH- apply to both Check this box and cli	•			
WAN Inbound Bandwidth	It allows you to set the connecting rate of data input for WAN. For example, if your ADSL supports 1M of downstream and 256K upstream, please set 10000kbps for this box. The default value is 10000kbps.				
WAN Outbound Bandwidt	WAN. For example, if	connecting rate of data output for your ADSL supports 1M of upstream, please set 256kbps for this is 10000kbps.			
Reserved Bandwidth Ratio	0	roup index in the form of ratio of to upstream speed and reserved ream speed.			
Enable UDP Bandwidth Control	field. This is a protecti	limited bandwidth ratio on the right on of TCP application traffic since c such as streaming video will exhaust			
Outbound TCP ACK Prioritize	are great in ADSL2+ e might be impacted by	width between download and upload environment. For the download speed the uploading TCP ACK, you can ACK of upload faster to speed the			
Limited_bandwidth Ratio	The ratio typed here is application.	reserved for limited bandwidth of UD			
Online Statistics	- ·	stics for quality of service for your ll be seen only if you click OK in			



WAN1/WAN2 General Setup web page and click Setup again (for WAN1/WAN2) on the **Bandwidth Management>>Quality of Service**.

Bandwidth Management >> Quality of Service

WAN1 O	nline Stati	stics		Refresh Ir	nterval:	5 💌 seconds	Refresh
Inde	× Direction	Class Name	Reserved-bandw	idth Ratio	Outbou	nd Throughput	(Bytes/sec)
1	OUT		25%			0	
2	OUT		25%			0	
3	OUT		25%			0	
4	OUT	Others	25%			0	
		_	hers	5	10 (B)	99)	

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

ienera	al Setup							Set to Factory D	<u>efault</u>
Index	Status	Bandwidth	Directon	Class 1	Class 2	Class 3	Others	UDP Bandwidth Control	
WAN1	Enable	10000Kbps/10000Kbps	Outbound	25%	25%	25%	25%	Inactive	<u>Setup</u>
WAN2	Enable	10000Kbps/10000Kbps	Outbound	25%	25%	25%	25%	Inactive	Setup
Class F Inde		N	ame				Rule	Service	Туре
	51						<u>Edit</u>		
Class	-						<u>Edit</u>	Edit	
Clas: Clas:	52								

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.

Bandwic	lth Manage	ment >> Quality o	f Service		
Class Inc	lex #1				
Name 🔤	Test				
NO	Status	Local Address	Remote Address	DiffServ CodePoint	Service Type
1	Empty	-	-	-	-
Add Edit Delete					
		ſ	OK Cancel	1	

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

🗹 ACT		
ocal Address.	Any	Edit
Remote Address	Any	Edit
DiffServ CodePoint	ANY	*
Service Type	ANY	~
Note: Please choose/se	tup the Service Type	first.

OK]	Cancel
------	--------

ACT	Check this box to invoke these settings.
Local Address	Click the Edit button to set the local IP address (on LAN) for the rule.
Remote Address	Click the Edit button to set the remote IP address (on LAN/WAN) for the rule.
Edit	It allows you to edit source address information. It allows you to edit source address information. It allows you to edit source address information. It allows you to edit source address information. It allows you to edit source address information. It allows you to edit source address information. It allows you to edit 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 CodePointAll the packets of data will be divided with different levels
and will be processed according to the level type by the
system. Please assign one of the levels of the data for
processing with QoS control.Service TypeIt 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 Game 1 Name DiffServ Local Address NO Status **Remote Address** Service Type CodePoint ANY 10 Active Any ANY AF Class4 (High 20 Active TELNET(TCP:23) Any \sim Drop) Add Edit Delete 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

Genera	al Setup						I.	<u>Set to Factory D</u>	efault
Index	Status	Bandwidth	Directon	Class 1	Class 2	Class 3	Others	UDP Bandwidth Control	
WAN1	Enable	10000Kbps/10000Kbps	Outbound	25%	25%	25%	25%	Inactive	<u>Setup</u>
WAN2	Enable	10000Kbps/10000Kbps	Outbound	25%	25%	25%	25%	Inactive	<u>Setup</u>

Class Rule

Index	Name	Rule	Service Type
Class 1		<u>Edit</u>	
Class 2		<u>Edit</u>	<u>Edit</u>
Class 3		<u>Edit</u>	

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

Bandwidth Management >> Quality of Servic	vice
---	------

User Defined Service Type

NO	Name	Protocol	Port
1	Empty	-	-
		Add Edit Delete	
		Cancel	

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

Bandwidth	Management >>	Quality of Service
Daniaria	managementer	adding of contrioo

Service Type Edit		
Service Nam	Э	
Service Type		TCP 6
Port Configu	ation	
Туре		💿 Single 🔘 Range
Port N	umber	0 – 0
Service Name	Type in	OK Cancel a new service for your request.
Service Type	Choose service.	the type (TCP, UDP or TCP/UDP) for the new
have to type in the starting port number a number on the boxes below. Port Number – Type in the starting port		ingle or Range as the Type . If you select Range, you type in the starting port number and the end porting on the boxes below. umber – Type in the starting port number and the end 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.

5.8 Applications

Below shows the menu items for Applications.

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

5.8.1 Dynamic DNS

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

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

Enable the Function and Add a Dynamic DNS Account

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

Applications >> Dynamic DNS Setup

🗹 Enable Dynamic DNS Setup		View Log	Force Update
ccounts:			
Index	WAN Interface	Domain Name	Active
<u>1.</u>	WAN1 First		×
<u>2.</u>	WAN1 First		×
<u>3.</u>	WAN1 First		×

Set to Factory DefaultClear all profiles and recover to factory settings.Enable Dynamic DNS SetupCheck this box to enable DDNS function.IndexClick the number below Index to access into the setting page of DDNS setup to set account(s).

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

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

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

OK

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. 64 characters)
Password	•••••	(max. 23 characters)
📃 Wildcards		
📃 Backup MX		
Mail Extender		

Clear

Cancel

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

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

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

5.8.2 Schedule

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

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

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

Applications >> Schedule

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

Set to Factory Default	Clear all profiles and recover to factory settings.	
Index	Click the number below Index to access into the setting page of schedule.	
Status	Display if this schedule setting is active or inactive.	

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

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

Applications >> Schedule

🗹 Enable :	Schedule Setup	
	Start Date (yyyy-mm-dd)	2000 💙 - 1 💙 - 1 💙
	Start Time (hh:mm)	
	Duration Time (hh:mm)	0 🕶 : 0 💌
	Action	Force On
	Idle Timeout	minute(s).(max. 255, 0 for default)
	How Often	
	🔘 Once	
	💿 Weekdays	
	🗌 Sun 🗹 Mon 🗹	Tue 🗹 Wed 🗹 Thu 🗹 Fri 🔲 Sat

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

Example

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

Office Hour:	$11 \frac{12}{2} \frac{1}{2}$	11 12 1 2 1 2 -9 3 3
(Force On)	87654	87654
Mon - Sun	9:00 am to	6:00 pm

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

5.8.3 RADIUS

Applications >> RADIUS

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

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

RADIUS Setup	
🗹 Enable	
Server IP Ad	dress
Destination F	Port 1812
Shared Secre	et
Confirm Shar	red Secret
(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 mus be configured to use the same shared secret.
Confirm Shared Secret	Re-type the Shared Secret for confirmation.

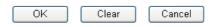
5.8.4 UPnP

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

Applications >> UPnP

UPnP
Enable UPnP Service
Enable Connection control Service
Enable Connection Status Service

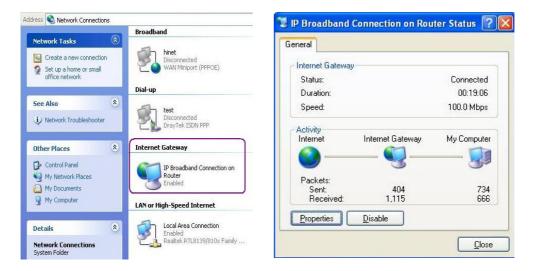
Note: If you intend running UPnP service inside your LAN, you should check the appropriate service above to allow control, as well as the appropriate UPnP settings.



Enable UPNP Service

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

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



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



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

The reminder as regards concern about Firewall and UPnP

Can't work with Firewall Software

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

Security Considerations

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

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

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

5.8.5 IGMP

IGMP is the abbreviation of *Internet Group Management Protocol*. It is a communication protocol which is mainly used for managing the membership of Internet Protocol multicast groups. For invoking IGMP Snooping function, you have to check the Enable IGMP Proxy box first for activating the IGMP proxy function.

Applications >> IGMP

Enable IGMP	Proxy WAN1 🖌			
	to act as a multicast prov / multicast group. But this			
Enable IGMP	Snooping			
	nooping, multicast traffic nooping, multicast traffic			
		OK Can	cel	
				Refres
Working Multicas	t Groups			 <u>Refres</u>

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

WAN1	*
WAN1	
WAN2	
PVC	

Enable IGMP Snooping	Check this box to enable this function. The application of multicast will be executed for the clients in LAN.
Group ID	This field displays the ID port for the multicast group. The available range for IGMP starts from 224.0.0.0 to 239.255.255.254.
P1 to P4	It indicates the LAN port used for the multicast group.
Refresh	Click this link to renew the working multicast group status.

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

5.8.6 Wake on LAN

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

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

Application)>> Wa	ke on	LAN
-------------	--------	-------	-----

Address:	Note : Wake on can wake up thr	LAN integrates with <u>Bind IP to MAC</u> function, only binded PCs ough IP.
AC Address:	Wake by:	MAC Address 🗸
	IP Address:	😵
esult	MAC Address:	Wake Up!
	Result	
		<u>``</u>

Wake by	choose Wake by MAC MAC address of the h	you to wake up the binded IP. If you C Address, you have to type the correct ost in MAC Address boxes. If you ddress, you have to choose the correct IP
	Wake by:	MAC Address MAC Address IP Address
IP Address	Firewall>>Bind IP to	have been configured in MAC will be shown in this drop down lress from the drop down list that you
MAC Address	Type any one of the MAC address of the binded PCs.	
Wake Up	Click this button to wa figure. The result will	ake up the selected IP. See the following be shown on the box.

Application >	> Wake on LAN
---------------	---------------

Wake by: MAC Address IP Address: MAC Address: Wake Up!	
MAC Address: Wake Up!	
Result	

5.9 VPN and Remote Access

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

Below shows the menu items for VPN and Remote Access.

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

5.9.1 Remote Access Control

Enable the necessary VPN service as you need. If you intend to run a VPN server inside your LAN, you should disable the VPN service of Vigor Router to allow VPN tunnel pass through, as well as the appropriate NAT settings, such as DMZ or open port.

VPN and Remote Access >> Remote Access Control Setup

Remote Access Control Se	etup
	Enable PPTP VPN Service
	Enable IPSec VPN Service
	Enable L2TP VPN Service
	Enable ISDN Dial-In

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

|--|

The Vigor router will not accept the ISDN dial-in connection if the box of **Enable ISDN Dial-in** is not checked.

5.9.2 PPP General Setup

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

PPP General Setup			
PPP/MP Protocol Dial-In PPP		IP Address Assignment for (When DHCP Disable set)	Dial-In Users
Authentication	PAP or CHAP 💙	Start IP Address	192.168.1.200
Dial-In PPP Encryption (MPPE)	Optional MPPE		
Mutual Authentication	(PAP) (Yes 💽 No		
Username			
Password			

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 wi 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 schem will be used to encrypt the data. Optional MPPE Require MPPE(40/128 bit) Maximum MPPE(128 bit) Require MPPE (40/128 bit) force the router to encrypt packets by using the MPPE encryption algorithm. In addition, the remote dial-in user wi 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 wituse the MPPE encryption scheme with maximum bits (128-bit) to encrypt the data.			
Mutual Authentication (PAP)	The Mutual Authentication function is mainly used to communicate with other routers or clients who need bi-directional authentication in order to provide stronger security, for example, Cisco routers. So you should enable this function when your peer router requires mutual authentication. You should further specify the User Name and Password of the mutual authentication peer.			
Start IP Address	Enter a start IP address for the dial-in PPP connection. You should choose an IP address from the local private network.			

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

5.9.3 IPSec General Setup

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

There are two phases of IPSec.

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

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

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

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

VPN and Remote Access >> IPSec General Setup

IKE Authentication Method		
Pre-Shared Key	•••••	
Confirm Pre-Shared Key	••••	
IPSec Security Method		
🗹 Medium (AH)		
Data will be authentic, but	will not be encrypted.	
High (ESP) 🗹 DES 🗹	3DES 🗹 AES	
Data will be encrypted and	l authentic.	

IKE Authentication MethodThis 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.**Pro Shared KayCurrently only support Pro Shared Kay**

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

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

5.9.4 IPSec Peer Identity

To use digital certificate for peer authentication in either LAN-to-LAN connection or Remote User Dial-In connection, here you may edit a table of peer certificate for selection. As shown below, the router provides **32** entries of digital certificates for peer dial-in users.

VPN and Remote Access >> IPSec Peer Identity

X509 Peer ID Accounts: Set to Factory Default					
Index	Name	Status	Index	Name	Status
<u>1.</u>	???	Х	<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>	???	Х
<u>8.</u>	???	×	<u>24.</u>	???	X
<u>9.</u>	???	×	<u>25.</u>	???	Х
<u>10.</u>	???	×	<u>26.</u>	???	X
<u>11.</u>	???	×	<u>27.</u>	???	×
<u>12.</u>	???	Х	<u>28.</u>	???	×
<u>13.</u>	???	Х	<u>29.</u>	???	×
<u>14.</u>	???	Х	<u>30.</u>	???	×
<u>15.</u>	???	Х	<u>31.</u>	???	×
<u>16.</u>	???	×	<u>32.</u>	???	×

Set to Factory Default

Index

Click it to clear all indexes.

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

Name

Display the profile name of that index.

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

VPN and Remote Access >> IPSec Peer Identity

Profile Index : 1						
Profile Name ???						
Enable this account						
• Accept Any Peer ID						
O Accept Subject Alternative Nam	ie in the second se					
Туре	IP Address					
IP						
O Accept Subject Name						
Country (C)						
State (ST)						
Location (L)						
Orginization (O)						
Orginization Unit (OU)						
Common Name (CN)						
Email (E)						
	DK Clear Cancel					
Profile Name	Type in a name in this file.					
Accept Any Peer ID	Click to accept any peer regardless of its identity.					
Accept Subject Alternative Name Click to check one specific field of digital signature to acc the peer with matching value. The field can be IP Address Domain, or E-mail Address. The box under the Type with appear according to the type you select and ask you to fill corresponding setting.						

Accept Subject Name Click to check the specific fields of digital signature to accept the peer with matching value. The field includes Country (C), State (ST), Location (L), Organization (O), Organization Unit (OU), Common Name (CN), and Email (E).

5.9.5 Remote Dial-in User

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

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

emote Acce	ss User Accounts:	Set to Factory Default			
Index	User	Status	Index	User	Status
<u>1.</u>	???	X	<u>17.</u>	???	Х
<u>2.</u>	???	×	<u>18.</u>	???	×
<u>3.</u>	???	×	<u>19.</u>	???	X
<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>	???	Х
<u>10.</u>	???	×	<u>26.</u>	???	×
<u>11.</u>	???	×	<u>27.</u>	???	Х
<u>12.</u>	???	×	<u>28.</u>	???	×
<u>13.</u>	???	X	<u>29.</u>	???	×
<u>14.</u>	???	X	<u>30.</u>	???	×
<u>15.</u>	???	Х	<u>31.</u>	???	×
<u>16.</u>	???	×	<u>32.</u>	???	×

VPN and Remote Access >> Remote Dial-in User

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

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

VPN and Remote Access >> Remote Dial-in User

Index No. 1 User account and Authentica	tion	Heername	???			
Enable this account		Username				
Idle Timeout 300	second(s)	Password				
		IKE Authentication M	1ethod			
Allowed Dial-In Type		🗹 Pre-Shared Key				
ISDN		IKE Pre-Shared Key				
✓ РРТР		Digital Signature(X	(.509)			
✓ IPSec Tunnel		None 🗸				
L2TP with IPSec Policy No	ne 💙					
Specify Remote Node		IPSec Security Meth	IPSec Security Method			
Remote Client IP or Peer ISDN N	Number	Medium(AH)				
		5 ()	JDES AES			
or Peer ID		Local ID (optional)				
Netbios Naming Packet 💿 P	ass 🔘 Block	Callback Function				
		Check to enable C	allback function			
		Specify the callba				
		Callback Number				
			allback Budget Control			
		Callback Budget				
			30 minute(s)			
SDN		cout is set to 300 seco				
SDN	set up Ca		n connection. You can further w. You should set the User e dial-in user below			
PPTP	connectio		to make a PPTP VPN et. You should set the User e dial-in user below			
PSec Tunnel		e remote dial-in user on through Internet.	to make an IPSec VPN			
L2TP	connection alone or w None - D connection viewed as Nice to H during ne becomes	on through the Interne- with IPSec. Select free o not apply the IPSec on employed the L2T s one pure L2TP con Iave - Apply the IPS gotiation. Otherwise one pure L2TP conn pecify the IPSec police	c policy. Accordingly, the VP P without IPSec policy can be nection. ec policy first, if it is applicab , the dial-in VPN connection			
Specify Remote Node		al-in user, ISDN nur	n specify the IP address of the nber or peer ID (used in IKE			



	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.
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 Metho	 d This group of fields is applicable for IPSec Tunnels and L2TP with IPSec Policy when you specify the IP address of the remote node. The only exception is Digital Signature (X.509) can be set when you select IPSec tunnel either with or without specify the IP address of the remote node. Pre-Shared Key - Check the box of Pre-Shared Key to invoke this function and type in the required characters (1-63) as the pre-shared key. Digital Signature (X.509) – Check the box of Digital Signature to invoke this function and Select one predefined Profiles set in the VPN and Remote Access >>IPSec Peer Identity.
IPSec Security Method	This group of fields is a must for IPSec Tunnels and L2TP with IPSec Policy when you specify the remote node. Check the Medium, DES, 3DES or AES box as the security method. Medium -Authentication Header (AH) means data will be authenticated, but not be encrypted. By default, this option is invoked. You can uncheck it to disable it. High-Encapsulating Security Payload (ESP) means payload (data) will be encrypted and authenticated. You may select encryption algorithm from Data Encryption Standard (DES), Triple DES (3DES), and AES. Local ID - Specify a local ID to be used for Dial-in setting in the LAN-to-LAN Profile setup. This item is optional and can be used only in IKE aggressive mode.
Callback Function	 The callback function provides a callback service only for the ISDN dial-in user. 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.

5.9.6 LAN to LAN

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

The router supports 2 VPN tunnels and provides up to **32** profiles simultaneously. The following figure shows the summary table.

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

VPN and Remote Access >> LAN to LAN

Set to Factory Default

Click to clear all indexes.

Name

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

Status

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

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

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

VPN and Remote Access >> LAN to LAN

Profile Index : 1 1. Common Settings	
Profile Name ???	Call Direction 💿 Both 🔿 Dial-Out 🔿 Dial-in
VPN Connection Through WAN1 First V Netbios Naming Packet O Pass O Block	Idle Timeout 300 second(s) Enable PING to keep alive PING to the IP
Type of Server I am calling	Link Type 64k bps 💙
 ISDN PPTP IPSec Tunnel L2TP with IPSec Policy None 	Username ??? Password PAP/CHAP V VJ Compression On Off
Dial Number for ISDN or Server IP/Host Name for VPN. (such as 5551234, draytek.com or 123.45.67.89)	IKE Authentication Method Pre-Shared Key KE Pre-Shared Key Digital Signature(X.509) None
	IPSec Security Method Medium(AH) High(ESP) DES without Authentication ▼ Advanced Index(1-15) in <u>Schedule</u> Setup: ,,,,
	Callback Function (CBCP) Require Remote to Callback Provide ISDN Number to Remote

Profile Name	Specify a name for the profile of the LAN-to-LAN connection.				
Enable this profile	Check here to activate this profile.				
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. 				
VPN Connection Through	Use the drop down menu to choose a proper WAN interface for this profile. This setting is useful for dial-out only.				
	VPN Connection Through: WAN1 First WAN1 First 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				

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.
Call Direction	Specify the allowed call direction of this LAN-to-LAN profile. Both:-initiator/responder Dial-Out- initiator only Dial-In- responder only.
Always On or Idle Timeout	Always On-Check to enable router always keep VPN
	connection. Idle Timeout: The default value is 300 seconds. If the connection has been idled over the value, the router will drop the connection.
Enable PING to keep alive	This function is to help the router to determine the status of IPSec VPN connection, especially useful in the case of abnormal VPN IPSec tunnel disruption. For details, please refer to the note below. Check to enable the transmission of PING packets to a specified IP address.
PING to the IP	Enter the IP address of the remote host that located at the other-end of the VPN tunnel.
	Enable PING to Keep Alive is used to handle abnormal IPSec VPN connection disruption. It will help to provide the state of a VPN connection for router's judgment of redial. Normally, if any one of VPN peers wants to disconnect the connection, it should follow a serial of packet exchange procedure to inform each other. However, if the remote peer disconnect without notice, Vigor router will by no where to know this situation. To resolve this dilemma, by continuously sending PING packets to the remote host, the Vigor router can know the true existence of this VPN connection and react accordingly. This is independent of DPD (dead peer detection).
ISDN	Build ISDN LAN-to-LAN connection to remote network. 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.
РРТР	Build a PPTP VPN connection to the server through the Internet. You should set the identity like User Name and Password below for the authentication of remote server.
IPSec Tunnel	Build an IPSec VPN connection to the server through Internet.
L2TP with	 Build a L2TP VPN connection through the Internet. You can select to use L2TP alone or with IPSec. Select from below: None: Do not apply the IPSec policy. Accordingly, the VPN connection employed the L2TP without IPSec policy can be viewed as one pure L2TP connection. Nice to Have: Apply the IPSec policy first, if it is applicable during negotiation. Otherwise, the dial-out VPN connection



	becomes one pure L2TP connection. Must: Specify the IPSec policy to be definitely applied on the L2TP connection.
User Name	This field is applicable when you select 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) - Select one predefined Profiles set in the VPN and Remote Access >> IPSec Peer Identity .
IPSec Security Method	This group of fields is a must for IPSec Tunnels and L2TP with IPSec Policy.
Medium	Authentication Header (AH) means data will be authenticated, but not be encrypted. By default, this option is active.
	 High (ESP-Encapsulating Security Payload)- means payload (data) will be encrypted and authenticated. Select from below: DES without Authentication -Use DES encryption algorithm and not apply any authentication scheme. DES with Authentication-Use DES encryption algorithm and apply MD5 or SHA-1 authentication algorithm. 3DES without Authentication-Use triple DES encryption algorithm and not apply any authentication scheme. 3DES with Authentication-Use triple DES encryption algorithm and apply MD5 or SHA-1 authentication algorithm. AES without Authentication-Use 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 and apply MD5 or SHA-1 authentication scheme.
Advanced	Specify mode, proposal and key life of each IKE phase, Gateway etc. The window of advance setup is shown as below:

🚰 http://192.168.1.1 - IKE advanc	ed settings - Microsoft Internet Explorer
IKE advanced settings	
IKE phase 1 mode	Main mode Aggressive mode
IKE phase 1 proposal	DES_MD5_G1/DES_SHA1_G1/3DES_MD5_G1/3DES_MD5_G2
IKE phase 2 proposal	HMAC_SHA1/HMAC_MD5 🔽
IKE phase 1 key lifetime	28800 (900 ~ 86400)
IKE phase 2 key lifetime	3600 (600 ~ 86400)
Perfect Forward Secret	Oisable
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 nine for **Main** mode. We suggest you select the combination that covers the most schemes.

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

IKE phase 1 key lifetime-For security reason, the lifetime of key should be defined. The default value is 28800 seconds. You may specify a value in between 900 and 86400 seconds. **IKE phase 2 key lifetime-**For security reason, the lifetime of key should be defined. The default value is 3600 seconds. You may specify a value in between 600 and 86400 seconds.

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

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

Callback Function

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.

3. Dial-In Settings							
Allowed Dial-In Type							
ISDN		Username	???				
 ✓ PPTP ✓ IPSec Tunnel 		Password					
		VJ Compression	💿 On 🔘 Off				
L2TP with IPSec Pol	icy None 🔽						
<u>-</u>		→ IKE Authentication Me ✓ Pre-Shared Key	ethod				
🔲 Specify ISDN CLID or		IKE Pre-Shared Key	·				
Peer ISDN Number or Pee	er VPN Server IP						
			Digital Signature(X.509)				
or Peer ID		None 🚩					
		IPSec Security Metho	d				
		🗹 Medium(AH)					
		High(ESP) 🗹 DES	🗹 3DES 🗹 AES				
		Callback Function (CE	3CP)				
		Enable Callback Fun	· ·				
		Use the Following N	umber to Callback				
		Callback Number					
		Callback Budget	0 minute(s)				
4. TCP/IP Network Sett	tinas		i minute(s)				
My WAN IP	0.0.0.0	RIP Direction	Disable 🗸				
,			mote network, you have to				
Remote Gateway IP	0.0.0.0	do					
Remote Network IP	0.0.0.0	Route V Change default route to this VPN tunnel (Only single WAN supports this)					
Remote Network Mask	255.255.255.0						
	More						
1			,				
	ОК	Clear Cancel					
Allowed Dial-In Typ	e Determine th	e dial-in connection wi	ith different types.				
ISDN	Allow the re	mote ISDN LAN-to-LA	AN connection. You				
			word of remote dial-in use				
			tion, you can further set up Callback function				
	below.						
РРТР	Allow the re	mote dial-in user to ma	ke a PPTP VPN				
			ough the Internet. You should set the User				
		assword of remote dial-					
[PSec Tunnel	Allow the re	mote dial-in user to trio	oger an IPSec VPN				
		nrough Internet.	ote dial-in user to trigger an IPSec VPN outputs of the second second second second second second second second				
L2TP		-	ke a I 2TP VPN				
		mote dial-in user to make a L21P VPN rough the Internet. You can select to use L2TP					
			cy. Accordingly, the VPN				
			hout IPSec policy can be				
Allowed Dial-In Type ISDN PPTP IPSec Tunnel L2TP	e Determine the Allow the resistould set the below. In addition below. Allow the resiston the Name and Pa Allow the resiston the Allow the resiston the Allow the resiston the Allow the resiston the alone or with None - Do not	Clear Cancel The dial-in connection with mote ISDN LAN-to-LA the User Name and Passy dition, you can further set mote dial-in user to man mote dial-in user to tright mote dial-in user to tright mote dial-in user to tright mote dial-in user to man mote dial-in user to	ith different types. AN connection. You word of remote dial-in set up Callback funct ke a PPTP VPN u should set the User in user below. gger an IPSec VPN ke a L2TP VPN u can select to use L2 low: cy. Accordingly, the				

	 viewed as one pure L2TP connection. Nice to Have - Apply the IPSec policy first, if it is applicable during negotiation. Otherwise, the dial-in VPN connection becomes one pure L2TP connection. Must - Specify the IPSec policy to be definitely applied on the L2TP connection.
Specify CLID or Remote VPN Gateway	You can specify the IP address of the remote dial-in user or peer ID (should be the same with the ID setting in dial-in type) by checking the box. Enter Peer ISDN number if you select ISDN above. Also, you should further specify the corresponding security methods on the right side.
	If you uncheck the checkbox, the connection type you select above will apply the authentication methods and security methods in the general settings.
User Name	This field is applicable when you select 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	This group of fields is applicable for IPSec Tunnels and L2TP with IPSec Policy when you specify the IP address of the remote node. The only exception is Digital Signature (X.509) can be set when you select IPSec tunnel either with or without specify the IP address of the remote node. Pre-Shared Key - Check the box of Pre-Shared Key to invoke this function and type in the required characters (1-63) as the pre-shared key. Digital Signature (X.509) –Check the box of Digital Signature to invoke this function and select one predefined Profiles set in the VPN and Remote Access >> IPSec Peer Identity .
IPSec Security Method	 This group of fields is a must for IPSec Tunnels and L2TP with IPSec Policy when you specify the remote node. Medium- Authentication Header (AH) means data will be authenticated, but not be encrypted. By default, this option is active. High- Encapsulating Security Payload (ESP) means payload (data) will be encrypted and authenticated. You may select encryption algorithm from Data Encryption Standard (DES), Triple DES (3DES), and AES.
Callback Function	The callback function provides a callback service only for the ISDN LAN-to-LAN connection. The remote user will be charged the connection fee by the telecom. Check to enable Callback function -Enables the callback function. Callback number -The option is for extra security. Once enabled, the router will ONLY call back to the specified Callback Number. Callback budget - By default, the callback function has



	limitation of callback period. Once the callback budget is exhausted, the function will be disabled automatically. Callback Budget (Unit: minutes)- Specify the time budget for the dial-in user. The budget will be decreased automatically per callback connection. The default value 0 means no limitation of callback period.
My WAN IP	This field is only applicable when you select ISDN, PPTP or L2TP with or without IPSec policy above. The default value is 0.0.0.0, which means the Vigor router will get a PPP IP address from the remote router during the IPCP negotiation phase. If the PPP IP address is fixed by remote side, specify the fixed IP address here. Do not change the default value if you do not select ISDN, PPTP or L2TP.
Remote Gateway IP	This field is only applicable when you select ISDN, PPTP or L2TP with or without IPSec policy above. The default value is 0.0.0.0, which means the Vigor router will get a remote Gateway PPP IP address from the remote router during the IPCP negotiation phase. If the PPP IP address is fixed by remote side, specify the fixed IP address here. Do not change the default value if you do not select ISDN, PPTP or L2TP.
Remote Network IP/ Remote Network Mask	Add a static route to direct all traffic destined to this Remote Network IP Address/Remote Network Mask through the VPN connection. For IPSec, this is the destination clients IDs of phase 2 quick mode.
More	Add a static route to direct all traffic destined to more Remote Network IP Addresses/ Remote Network Mask through the VPN connection. This is usually used when you find there are several subnets behind the remote VPN router.
RIP Direction	The option specifies the direction of RIP (Routing Information Protocol) packets. You can enable/disable one of direction here. Herein, we provide four options: TX/RX Both, TX Only, RX Only, and Disable.
From first subnet to remote network, you have to do	If the remote network only allows you to dial in with single IP, please choose NAT , otherwise choose Route .
Change default route to this VPN tunnel	Check this box to change the default route with this VPN tunnel. Be aware that this setting is available only for one WAN interface is enabled. It is not available when both WAN interfaces are enabled. You have to disable one WAN interface (WAN 1 or WAN 2) on WAN >> General Setup for enabling such setting.

5.9.7 Connection Management

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

VPN and Remote Acc	cess >> Connec	tion Manage	ment				
Dial-out Tool				Refre	sh Sec	onds : 10	Refresh
				✓ Dial]		
VPN Connection Statu Current Page: 1	s				Pa	ge No.	Go >>
VPN Type	Remote IP	Virtual Network	Tx Pkts	Tx Rate (Bps)	Rx Pkts	Rx Rate (Bps)	UpTime
1				×××××× : C ×××××× : C			
Dial	Clic	k this butto	n to exe	cute dia	l out f	unction.	
Refresh Seconds	Cho and		for ref	fresh the	dial ii	nformati	on among 5,
Refresh	Clic	k this butto	n to refi	resh the	whole	connect	ion status.

5.10 Certificate Management

A digital certificate works as an electronic ID, which is issued by a certification authority (CA). It contains information such as your name, a serial number, expiration dates etc., and the digital signature of the certificate-issuing authority so that a recipient can verify that the certificate is real. Here Vigor router support digital certificates conforming to standard X.509.

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

Here you can manage generate and manage the local digital certificates, and set trusted CA certificates. Remember to adjust the time of Vigor router before using the certificate so that you can get the correct valid period of certificate.

Below shows the menu items for Certificate Management.



5.10.1 Local Certificate

Certificate Management >> Local Certificate

X509 Local Certificate Configuration

Name	Subject	Status	Modify
Local			View Delete
GENERATE	IMPORT REFRESH		

Generate

Click this button to open Generate Certificate Request window.

Cartificate	Management >>		Certificate
Certificate	management >>	Local	Certificate

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

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

Name Subject		Status	Modify
Local /C=TW/ST=HS/O=Draytek/OU=RD/		Requesting	View Delete
GENERATE	IMPORT REFRESH		
X509 Lo	ocal Certificate Request		
MIIBnT EwdEcmi cmF5dG OTS2S2 mASVOR	EGIN CERTIFICATE REQUEST CCAQVCAQAwXTELMAkGAIUEBHMCVFcxCZAJ F5GGVrMQswCQYDVQQLEwJSRDEiMCAGCSqG JrLmNvbTCBnzANBgkqhkiG9w0BAQEFAAOB QdwlReltvlHnVwm/MFC0y9x+XEwNKG46jd j7HbNOdYn88plxRrCPgk8nkbMLdAgb10o; Ep/2020WsCddxh/HzZ3Ys8m60CAwEAAAAA	SIb3DQEJARYTC jQAwgYkCgYEAy GY1LSAvJTduHH c/lsYN/smGb4N MAOGCSqGSIb3D	3VwcG9ydEBk ZELVTVBytix 90z40MWx02G +Pbo4VM01V0
AGNB90 nacBqE sOvJGB	71V44sgXwiWnXHJvdFLDOdwcQO1ZL1XRn+; z1WOchKzESOdyDc8mtIf7k+iO45SeuY7nx; HHwKSkWb1RAZL5xvHjDoMX16czT1ybedZS; ND CERTIFICATE REOUEST	swXvPIOn31JMJ	•

X509 Local Certificate Configuration

5.10.2 Trusted CA Certificate

Trusted CA certificate lists three sets of trusted CA certificate.

Certificate Ma	anagement >>	Trusted	CA	Certificate
----------------	--------------	---------	----	-------------

X509 Trusted CA Certificate Configuration

 	View Delete
 	View Delete
 	View Delete

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

Certificate Management >> Trusted CA Certificate

Import X509 Trusted CA Certificate		
Select a trusted CA certificate file.		
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.

🌈 Certificate Information - Windows Internet Explorer				
🤌 http	://192.168.1.1/doc/XCaCfVi1.htm		~	
			^	
	Certific	cate Detail Information		
	Certificate Name:	Trusted CA-1		
	Issuer:			
	Subject:			
	Subject Alternative Name:			
	Valid From:			
	Valid To:			
		Close	~	

5.10.3 Certificate Backup

Local certificate and Trusted CA certificate for this router can be saved within one file. Please click **Backup** on the following screen to save them. If you want to set encryption password for these certificates, please type characters in both fields of **Encrypt password** and **Confirm password**.

Also, you can use **Restore** to retrieve these two settings to the router whenever you want.

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

5.11 ISDN

5.11.1 Basic Concept

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 for ISDN.

ISDN

General Setup

Dialing to a Single ISP

Dialing to Dual ISPs

Call Control

VigorIPPBX 2820 Series User's Guide



5.11.2 General Setup

This page provides some basic ISDN settings such as enabling the ISDN port or not, MSN numbers and blocked MSN numbers, etc.

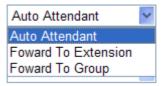
ISDN Setup			-		
ISDN Port	💿 Enable 🔘	Disable	Blocked MSN numb	ers for the router	
Country Code	International	~	1.		
D-Channel Mode			2.		
ISDN1	O Point-to-P	oint	3.		
	Point-to-M		4.		
ISDN2	O Point-to-P		5.		
	Point-to-Multipoint				
	eans that the router SDN number when it				
Index	MSN numbers for the router		Answer mode	Phone C	LIR/CLIP
0.		Au	to Attendant 🛛 👻		
1.		Au	to Attendant 🛛 👻		
2.		Au	to Attendant 🗸		
3.		Au	to Attendant 🗸 🗸		
4.		Au	to Attendant 🗸 🗸		
5.		Au	to Attendant 🗸 🗸		
6.			to Attendant		
7.			to Attendant		
			to Attendant		_
8.					
9.	neans that the router		to Attendant 🛛 👻		
	uld be supported by				addition,
		OK	Cancel		
SDN Port		Click Ena it.	ble to open the 1	ISDN port and D	isable to
ountry Code			r operation on yo pose the correct	our local ISDN n country code.	etwork, y
		Internat Argenti Austral Austria Banglad Belgiun Brasil	tional 🔨 na ia desh		
-Channel Moo	le			ISDN layer2 pro e ISDN port to u	

Dray Tek

(Terminal Endpoint Identifier).

	Point-to-Multipoint - Configure ISDN port to use Dynamic TEI.
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.
Answer mode	Specify the way to process incoming phone calls which

le Specify the way to process incoming phone calls which matched the MSN number for router.



Auto Attendant - The incoming call would be picked by router automatically. You could hear IVR voice to remind you to dial extension number you want to reach.

Forward to Extension - The incoming call would be forwarded to the extension number you setup directly.

Forward to Group - If you have setup group extension number in web page "Hunt Group", the incoming call could be forwarded to the group extension number you selected.

Phone CLIR/CLIPCheck this box to hide or present the caller ID to
remote user.

Example:

Below shows an example of TE port MSN number:

Index	MSN numbers for the router	Answer mode	Pho CLIR/	A CONTRACTOR OF
0.	5972727	Auto Attendant		
1.	5972728	Foward To Extension 💌 1 - 100 💌 Extension	Γ	~
2.	5972729	Foward To Group 💌 1 - 300 💌 Group	Г	•
3.		Auto Attendant		
4.		Auto Attendant	Г	
5.		Auto Attendant		
6.		Auto Attendant		
7.		Auto Attendant		
8.		Auto Attendant		
9.		Auto Attendant	Г	

"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.

Refer to the following explanation:

- a. If you setup "MSN numbers for the router" as the above figure, it means the Vigor router only accepts MSN numbers of **5972727 / 5972728 / 5972729**.
- b. If someone dials to the router with **5972727**, the call would be picked up automatically. You could hear IVR voice to remind you to dial the extension number you want to reach.
- c. If someone dials to the router with **5972728**, the call would be forwarded to extension 100 directly.
- d. If someone dials to the router with **5972729**, the call would be forwarded to group extension 300.
- e. If you use a phone with extension 100 to dial an ISDN call, the remote ISDN phone would see the **caller ID: 5972728** (for the Phone CLIP is checked).
- f. If you use any extension number included in Group extension 300 to dial an ISDN call, the remote ISDN phone would see the **caller ID: 5972729** (for the Phone CLIP is checked).

5.11.3 Dial to Single ISP

Select **Dialing to a Single ISP** if you access the Internet via a single ISP.

ISDN >> Dialing	g to a Single ISP
-----------------	-------------------

Single ISP			
ISP Access Setup	PPP/MP Setup		
ISP Name	Link Type	Dialup BOD 🛛 👻	
Dial Number	PPP Authentication	PAP or CHAP 🔽	
	Idle Timeout	180 second(s)	
Username	IP Address Assignment Method (IPCP)		
Password	Fixed IP	🔘 Yes 💿 No (Dynamic IP)	
Require ISP callback (CBCP)	Fixed IP Address		
Index(1-15) in <u>Schedule</u> Setup:			
=>,,,			
Г	ок		

ISP Access Setup	 ISP Name - Enter your ISP name such as Seednet, Hinet and so on. 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. Refer to section 5.8.2 Schedule for detailed configuration.
PPP/MP Setup	 Link Type – There are three link types provided here for different purpose. Link Disable disables the ISDN dial-out function. Dialup 64Kbps allows you to use one ISDN B channel for Internet access. Dialup 128Kbps allows you to use both ISDN B channels for Internet access. Dialup BOD (for detailed information of configuration, please refer to section 5.12.4) 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 section of Call Control. PPP Authentication - PAP only allows you to configure the PPP session to use the PAP protocol to negotiate the username and password with the ISP. PAP or CHAP is to 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.

ISP Access Setu



IP Address Assignment
Method (IPCP)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 and enter the IP address in the field of
Fixed IP Address.

5.11.4 Dial to Dual ISPs

Select **Dialing to Dual ISPs** if you have more than one ISP. 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). 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	PPP/MP Setup
1. 🗌 Enable Dual ISPs Function	Link Type Dialup BOD 💌
2. 🔲 Require ISP callback (CBCP)	PPP Authentication PAP or CHAP 💌
	Idle Timeout 180 second(s)
Primary ISP Setup	Secondary ISP Setup
ISP Name	ISP Name
Dial Number	Dial Number
Username	Username 84005755@hinet.net
Password	Password ••••••
IP Address Assignment Method (IPCP)	IP Address Assignment Method (IPCP)
Fixed IP 🛛 🔿 Yes 💿 No (Dynamic IP)	Fixed IP 🛛 🔿 Yes 💿 No (Dynamic IP)
Fixed IP Address	Fixed IP Address

ΟK

Common SettingsEnable Dual ISPs Function - Check to enable the Dual ISPs
function. Require ISP Callback (CBCP) -If your ISP
supports the callback function, check this box to activate the
Callback Control Protocol during the PPP negotiation.PPP/MP SetupLink Type – There are three link types provided here for
different purpose. Link Disable disables the ISDN dial-out
function. Dialup 128Kbps allows you to use both ISDN B

channels for Internet access. **Dialup BOD** (for detailed information of configuration, please refer to section **5.12.4**) 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.

PPP Authentication - PAP only allows you to configure the PPP session to use the PAP protocol to negotiate the username and password with the ISP. **PAP or CHAP** can 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.
Primary ISP Setup	 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.
IP Address Assignment Method (IPCP) for primary ISP setup	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 and enter the IP address in the field of Fixed IP Address .
Secondary ISP Setup)	 ISP Name - Enter the secondary ISP name. Dial Number -Enter the ISDN access number provided by the ISP. Username - Enter the username provided by your ISP. Password - Enter the password provided by your ISP.
IP Address Assignment Method (IPCP) for secondary ISP setup	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 and enter the IP address in the field of Fixed IP Address .

5.11.5 Call Control

Some applications require that the router 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.

Dial Retry	0 times	Remote Activation	
Dial Delay Interval 0 second(s)			
PPP/MP Dial-Out Setup			
Basic Setup		Bandwidth On Demand	(BOD) Setup
Link Type	Dialup BOD 🛛 👻	High Water Mark	7000 cps
PPP Authentication	PAP or CHAP 🔒	High Water Time	30 second(s)
TCP Header Compression	None 🔽	Low Water Mark	6000 cps
Idle Timeout	180 second(s)	Low Water Time	30 second(s)

Call Control Setup

ISDN >> Call Control

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 can help users who would like to access the server which is off the Internet in the head office. To remotely make the server to be available on the Internet, i.e. make the router in the head office activating its Internet access either by dialing-up or starting broadband connection, users can make a regular phone call (the number is set in the Remote Activation field) to the router as signaling it for activation. The phone call will be soon disconnected once the router is on line. 			
	Note that Dialing to a Single ISP should be pre-configured properly.			
Basic Setup	Link Type - Because ISDN has t channel), you can specify whethe single B channel, two B channels Demand). Four options are availa 64Kbps, Dialup 128Kbps, Dialup	r you would like to have or BOD (Bandwidth on ble: Link Disable, Dialup		
	Link Type	Dialup BOD Link Disable Dialup 64Kbps Dialup 128Kbps Dialup BOD		
	 PPP Authentication - It specifies method for PPP/MP connections. PAP/CHAP for better compatibilit TCP Header Compression - VJ TCP/IP protocol header compress to improve bandwidth utilization. Idle Timeout - Because our IDSN Demand, the connection will be in 	Normally you can set it to ity. Compression : It is used for sion. Normally it is set to Yes N link type is Dial On		
Bandwidth-On-Demand (BOD) Setup	 Bandwidth-On-Demand is for Multiple-Link PPP \(ML-PPP or MP). The parameters are only applied when you set the Link Type to Dialup BOD. The ISDN usually use 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. High Water Mark and High Water Time - 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 Wat specify the situation in which the dropped. In terms of the two B ch under the Low Water Mark and th used over the High Water Time, t dropped. As a result, the total link	second channel will be annels, if their utilization is nese two channels are being he additional channel will be		

B channel).

5.12 IP PBX

IP PBX (*IP -Private Branch eXchange*) is a private telephone network used within an enterprise. Users of the PBX can share a certain number of outside lines for making telephone calls external to the PBX.

IP PBX integrates the benefits of VoIP and transfers the message from IP phone into the data that can be accepted by traditional PBX through IP network. It is a new platform that enterprises can use data network to deliver voice. Additionally, to move the IP phone set(s), users just need to plug into another network connector. Such thing simplifies the procedure of moving, increasing, changing and deleting phone settings; also it can join with other system such as CALL center to be a multi-functional communication platform. Moreover, it can save large cost in communication for the enterprise.

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

Below shows menu items for IP PBX:

IP PBX	
Extension	
Line Setting	
Dial Plan	
PBX System	
PBX Status	

5.12.1 Extension

The system allows you to set 50 extension numbers. Please open **IP PBX>>Extension** to get the following pages.

Index	Ext.	Name	Email Address	Outgoing Call	Status
<u>1.</u>				SIP1 SIP2 SIP3 SIP4 SIP5 SIP6 ISDN2-TE	x
<u>2.</u>				SIP1 SIP2 SIP3 SIP4 SIP5 SIP6 ISDN2-TE	x
<u>3.</u>				SIP1 SIP2 SIP3 SIP4 SIP5 SIP6 ISDN2-TE	x
<u>4.</u>				SIP1 SIP2 SIP3 SIP4 SIP5 SIP6 ISDN2-TE	x
<u>5.</u>				SIP1 SIP2 SIP3 SIP4 SIP5 SIP6 ISDN2-TE	x
<u>6.</u>				SIP1 SIP2 SIP3 SIP4 SIP5 SIP6 ISDN2-TE	x
<u>7.</u>				SIP1 SIP2 SIP3 SIP4 SIP5 SIP6 ISDN2-TE	x
<u>8.</u>				SIP1 SIP2 SIP3 SIP4 SIP5 SIP6 ISDN2-TE	x
<u>9.</u>				SIP1 SIP2 SIP3 SIP4 SIP5 SIP6 ISDN2-TE	x
<u>10.</u>				SIP1 SIP2 SIP3 SIP4 SIP5 SIP6 ISDN2-TE	x

IP PBX >> Extension

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

IP PBX >> Extension Profile

Internal Phone Exte	nsion Index 1			
Internal Phone Exten	sion Active	O Enable	🖲 Disable	
Extension Number				
User Name				
Authentication				
Password		•••		
E-mail Address				Send a test e-mail
Voice mail Password		•••		
MWI				
 Notify User who Subscribed 		O Force Not	tify User	
Outgoing Call Use				
SIP1 SIP2 S	IP3 🗌 SIP4 🔲 SIP5	SIP6 IS	DN1-TE 📃 IS	DN2-TE
Answer Mode				
No answer after	120 sec then	Keep Ring	*	
Busy then	Do Nothing	*		
Not on-line	Do Nothing	*		
1				

ΟK

Cancel

Internal Phone Extension Active	Click Enable to invoke such profile.
Extension Number	Type the number of extension for such index.
User Name	Type a name as a display for this extension profile.
Authentication	Check this box to make the IP PBX executing authentication while the number is dialed.
Password	Type a number for the IP PBX to execute authentication. When an IP phone connects to network, IP PBX will use such password for authentication.
E-mail Address	Type an e-mail address to receive media (voice) file sent by incoming calls. Send a test e-mail : Click this button to send a test e-mail to the mail box you typed here.
Voice Mail Password	Type a password here. When the user want to listen the voice mail, he/she muse use such password to open it.
MWI (Message Waiting Indicator)	There are two types of MWI for users to choose. Please click the one according to the real application.
	Notify User who Subscribed - The user needs to send out SUBSCRIBE message first. When IPPBX detects new voice message from some extension number or the condition of the voice message is changed, it will transfer "NOTIFY" message to the users within the valid time subscribed.

Force Notify User- The user does not send out SUBSCRIBE

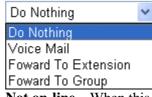
message automatically. The IPPBX will deliver "NOTIFY" message to the users if there is a new message or the user registers on IPPBX again.

Outgoing Call Use There are six outside lines (SIP accounts) and two ISDN lines (available based on the Phone Setting configuration) for you to specify for such extension. Please check the one(s) you want.

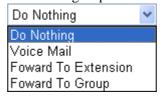
Answer ModeSpecify the way to process incoming phone calls.
No answer after – When the incoming phone call is not
picked up, it will be processed by keeping, forwarding to
certain extension or group. Please specify the waiting time and
determine the way you want to process.



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



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



5.12.2 Line Setting

There are six SIP outside lines and one ISDN line provided by this IP PBX device. Users can set them respectively from SIP Trunk and ISDN Trunk.

IP PBX >> Line Setting		
Line Setting		
	SIP Trunk	
	ISDN Trunk	

DID (Direct Inward Dialing) is a service provided by SIP providers. It allows one main SIP account (**SIP Trunk**) attached with several sub-accounts (defined in **Alias List** under **SIP Turnk**). When the main accounts have been registered on VigorIPPBX 2820, it means the router owns these sub-accounts at the same time. That is, people can dial main SIP accounts or sub-accounts via VigorIPPBX 2820.

5.12.2.1 SIP Trunk

This page allows you to set profiles for 6 SIP outside lines (main account) at one time with 50 alias names (sub account).

IP PBX >> SIP Trunk List

SIP Trun	ik List			Refresh Seconds: 5	*	<u>Refresh</u>
Index	Profile Name	Domain/Realm	Proxy	Account Number/Name	Trunk Number	Status
<u>1.</u>					001	-
<u>2.</u>					002	-
<u>3.</u>					003	-
<u>4.</u>					004	-
<u>5.</u>					005	-
<u>6.</u>					006	-

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

Alias List

Profile Name	Display the name for such main account.	
Domain/Realm	Display domain name or IP address of the SIP Registrar server.	
Proxy	Display the domain name or IP address of SIP proxy server.	
Account Number/Name	Display the account name of SIP Address.	
Trunk Number	Display the short number for such account.	
Status	Display current status for the account (successful registration or failed registration).	
Alias List	Allows you to set sub accounts for the main accounts in SIP Trunk.	

Please click any number under Index to set detailed configuration.



IP PBX >> SIP Trunk List

Profile Name	(11 char max.)
Register via	Auto 💌
SIP Local Port	5070
Domain/Reallm	(63 char max.)
Proxy	(63 char max.)
Proxy Port	5060 (63 char max.)
Display Name	(23 char max.)
Account Number/Name	(63 char max.)
Authentication ID	(63 char max.)
Password	(63 char max.)
Expiry Time	1 hour 💙 3600 sec
Trunk number	001 (3 char max.)
Office hours answer mode	Auto Attendant
Non-Office hours answer mode	Auto Attendant
Note:SIP Local Port can not be equal to F	PBX Proxy Port.
	OK Cancel

Profile Name	Assign a name for this profile for identifying. You can type similar name with the domain. For example, if the domain name is <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. Choosing Auto is recommended. The system will select a proper way for your VoIP call.	
	None V None Auto WAN1 WAN2	
SIP Port	Set the port number for sending/receiving SIP message for building a session. The default value is 6060 . Your peer must set the same value in his/her Registrar.	
Domain/Realm	Set the domain name or IP address of the SIP Registrar server.	
Proxy	Set domain name or IP address of SIP proxy server. By the time you can type :port number after the domain name to specify that port as the destination of data transmission (e.g., nat.draytel.org:5065)	
Proxy Port	Set port number for the proxy server.	
Display Name	The caller-ID that you want to be displayed on your friend's screen.	
Account Number/Name	Enter your account name of SIP Address, e.g. every text before @	



Authentication ID	Check the box to invoke this function and enter the name or number used for SIP Authorization with SIP Registrar. If this setting value is the same as Account Name, it is not necessary for you to check the box and set any value in this field.	
Password	The password provided to you when you registered with a SIP service.	
Expiry Time	It is the time duration that your SIP Registrar server keeps your registration record. Before the time expires, the router will send another register request to SIP Registrar again.	
Trunk Number	There are two ways to dial outside lines for an extension number. First, dial a short number and wait for a while. When the dial tone appears, please dial the real outside line number. Second, dial a short number and then the real outside line number without waiting for dial tone. The short number is defined here as Trunk Number.	
Office hours answer mode	Set the answering mode for such outside line in office time. You can specify it with Auto Attendant (AA), or forward it to any Extension or Group directly. Auto Attendant Foward To Extension Foward To Group	
Non-office hours answer mode	Set the answering mode for such outside line in non-office time. You can specify it with Auto Attendant (AA), or forward it to any Extension or Group directly. Auto Attendant Foward To Extension Foward To Group	

Alias List

Click the Alias List link to access into the configuration page as shown below.

```
IP PBX >> Alias
```

Index	Profile Name	Number	Office Hours	Non Office Hours	Active	Trunk
<u>1.</u>			Auto Attendant	Auto Attendant	No	
<u>2.</u>			Auto Attendant	Auto Attendant	No	
<u>3.</u>			Auto Attendant	Auto Attendant	No	
<u>4.</u>			Auto Attendant	Auto Attendant	No	
<u>5.</u>			Auto Attendant	Auto Attendant	No	
<u>6.</u>			Auto Attendant	Auto Attendant	No	
<u>7.</u>			Auto Attendant	Auto Attendant	No	
<u>8.</u>			Auto Attendant	Auto Attendant	No	
<u>9.</u>			Auto Attendant	Auto Attendant	No	
<u>10.</u>			Auto Attendant	Auto Attendant	No	

<< 1-10 | 11-20 | 21-30 | 31-40 | 41-50 >>

<u>Next</u> >>

Profile Name

Display the alias name for such sub account.



Number	Display the phone number of such account.
Office Hours	Display the selected answer mode for office hours.
Non Office Hours	Display the selected answer mode for non office hours.
Active	Display current activation status for such account, enabled or disabled.
Trunk	Display the SIP Trunk for such sub account attached.

You can set 50 profiles as alias for SIP Trunk list. Click the number under Index to set detailed configuration.

IP PBX >> Alias

Alias 1.	
Active	●Enable ○Disable
Alias Name	
Alias Number	
Alias of SIP Trunk	1 - ??? 💌
Answer Mode	
Office hours answer mode	Auto Attendant
Non-Office hours answer mode	Auto Attendant
	OK Clear Cancel
Active	Click Enable to activate this entry. Or, click Disable to inactive this entry.
Alias	Type a name for such account.
Alias Number Type a number for such account.	
Alias of SIP Trunk	Choose one of the items listed in SIP Trunk List for this alias profile.
Office hours answer mode	Set the answering mode for such outside line in office time. You can specify it with Auto Attendant (AA), or forward it to any Extension or Group directly. Auto Attendant Foward To Extension Foward To Group
Non-office hours answer mode	Set the answering mode for such outside line in non-office time. You can specify it with Auto Attendant (AA), or forward it to any Extension or Group directly. Auto Attendant Foward To Extension Foward To Group

5.12.2.2 ISDN Trunk

This page allows you to set profile for ISDN outside line.

IP PBX >> ISDN Trunk

ISDN Trunk	
Office hours answer mode	Auto Attendant
Non-Office hours answer mode	Auto Attendant
ISDN Trunk Auto Hunt	
	OK Cancel
Office hours answer mode	Set the answering mode for such outside line in office time. You can specify it with Auto Attendant (AA), or forward it to any Extension or Group directly. Auto Attendant Foward To Extension Foward To Group
Non-office hours answer mode	Set the answering mode for such outside line in non-office time. You can specify it with Auto Attendant (AA), or forward it to any Extension or Group directly. AA AA Foward To Extension Foward To Group
ISDN Trunk Auto Hunt	When both ISDN ports set to TE mode, you can specify an auto hunt number. When people want to dialing to I SDN network via this number by using extension, the router will auto hunt an available line for it.
Dial Plan	

IP PBX >> Dial Plan		
Dial Plan Configuration		
	<u>Digit Map</u>	
	<u>Call Barring</u>	

5.12.3.1 Digit Map

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

5.12.3

IP PBX >> DialPlan Setup

#	Enable	Prefix Number	Mod	е	OP Number	Min Len	Max Len	Interface
1			None	*		0	0	ISDN1-TE 💌
2			None	~		0	0	ISDN1-TE ISDN2-TE
З			None	~		0	0	ISDN1-TE 🔽
4			None	~		0	0	ISDN1-TE 🔽
5			None	~		0	0	ISDN1-TE 🔽
6			None	~		0	0	ISDN1-TE 🔽
7			None	~		0	0	ISDN1-TE 🔽
8			None	~		0	0	ISDN1-TE 🔽
9			None	~		0	0	ISDN1-TE 🔽
10			None	~		0	0	ISDN1-TE 🔽
11			None	~		0	0	ISDN1-TE 🔽
12			None	~		0	0	ISDN1-TE 🔽
13			None	~		0	0	ISDN1-TE 🔽
14			None	~		0	0	ISDN1-TE 🔽
15			None	~		0	0	ISDN1-TE 🔽
16			None	~		0	0	ISDN1-TE 🔽
17			None	~		0	0	ISDN1-TE 🔽
18			None	×		0	0	ISDN1-TE 🔽
19			None	~		0	0	ISDN1-TE 🔽
20			None	~		0	0	ISDN1-TE

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

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 OP number of 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 "031111111" will be changed to "8863111111"

	SIP server. Mode Replace None Add Strip Replace
OP Number	The front number you type here is the first part of the account number that you want to execute special function (according to the chosen mode) by using the prefix number.
Min Len	Set the minimal length of the dial number for applying the prefix number settings. Take the above picture (Prefix Table Setup web page) as an example, if the dial number is between 7 and 9, that number can apply the prefix number settings here.
Max Len	Set the maximum length of the dial number for applying the prefix number settings.
Interface	Choose the one that you want to enable the prefix number settings from the saved SIP accounts. Please set up one SIP account first to make this interface available. This item will be changed according to the port settings configured in IP PBX>>PBX System>>Phone Settings and IP PBX>>Line Settings>>SIP Trunk .

Index	Port	Call Feature	Codec	٦
1	Phone	CW,CT,	G.729A/B	De
2	ISDN1-S0 💌		G.729A/B	D
<u>3</u>	ISDN2-TE		G.729A/B	De

IP PBX >> PBX System

esh Seconds: 5	~	Refresh
Account nber/Name	Trunk Number	Status
	001	-
	002	-
	003	-
	004	-
	005	-
	006	-

5.12.3.2 Call Barring

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

IP PBX >> DialPlan Setup

Call Ba	rring Setup				Set to F	actory Default
Index	Call Direction	Barring Type	Barring Number/URL/URI	Interface	Schedule	Status
<u>1.</u>						×
<u>2.</u>						×
<u>3.</u>						×
<u>4.</u>						×
<u>5.</u>						×
<u>6.</u>						×
<u>7.</u>						×
<u>8.</u>						×
<u>9.</u>						×
<u>10.</u>						×
<< <u>1-10</u>	<u> 11-20</u> >>					<u>Next</u> >>

Advanced: <u>Block Anonymous</u> <u>Block Unknown Domain</u>

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

```
IP PBX >> DialPlan Setup
```

Call Barring Index No. 1			
🗹 Enable			
Call Direction	IN 💌		
Barring Type	Specific URI/URL 💌		
Specific URI/URL			
Interface	All		
Index(1-15) in <u>Sch</u>	edule Setup All ISDN1-TE , , , , , , , , , , , , , , , , , , ,		
-	ISDN2-TE OK Cancel		
Enable	Click this to enable this entry.		
Call Direction	Determine the direction for the phone call, IN – incoming call, OUT-outgoing call, IN & OUT – both incoming and outgoing calls. IN OUT IN & OUT IN & OUT		
Barring Type	Determine the type of the VoIP phone call, URI/URL or number. It will bring out different setting options. Specific URI/URL Specific URI/URL Specific Number		
Specific Number/Specific URI/URL	This field will be changed based on the type you selected for barring Type. Please type numbers or URI/URL		
Interface	"All" means all the phone calls (including ISDN1/2 & SIP) will be blocked with such mechanism. Or you can specify certain port to be blocked by choosing from the drop down list.		



Index (1-15) in Schedule

Enter the index of schedule profiles to control the call barring according to the preconfigured schedules. Refer to section **Application** >>**Schedule** for detailed configuration.

Additionally, you can set advanced settings for call barring such as **Block Anonymous**, **Block Unknown Domain** or **Block IP Address**. Simply click the relational links to open the web page.

For **Block Anonymous** – this function can block the incoming calls without caller ID on the interface specified in the following window. Such controlling also can be done based on preconfigured schedules.

IP PBX >> DialPlan Setup

Call Barri	ng Block Anonymous	
	Index(1-15) in <u>Schedule</u> Setup	
	, , , ,	
Note:Block	< the incoming calls which do not	have the caller ID.
		OK Cancel

For **Block Unknown Domain** – this function can block incoming calls from unrecognized domain that is not specified in SIP accounts. Such controlling also can be done based on preconfigured schedules.

IP PBX >> DialPlan Setup	
Call Barring Block Unknown Domain	
🗹 Enable	
Index(1-15) in <u>Schedule</u> Setup	
Note: If the domain of the incoming call is different should be blocked.	erent from the domain found in SIP accounts,the call



5.12.4 PBX System

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

IP PBX >> PBX System

PBX System

<u>SIP Proxy Setting</u>	
Hunt Group	
Voice Mail Configuration	
Office Hours	
Auto Attendant Wizard	
Prompt Maintenance	
Phone Setting	



5.12.4.1 SIP Proxy Setting

To make the IP phone to be registered in IP PBX device successfully, it is necessary for the users to configure settings in this page.

IP PBX >> PBX System

(nil) (nil)	
SIP Local Port	5060
SIP Proxy Realm	PBX.com
Parking Server Number	777
RTP Local Port Start	15050
RTP Local Port End	20000

SIP Local Port	Set a port number as SIP local port. The default setting is 5060.		
SIP Proxy Realm	Type SIP service domain name. In full SIP URI, such is the part after @ symbol.		
Parking Server Number	This number is used to communicate with the parking server and invoke the parking function. The default setting number is "777".		
	1.	When you receive a phone call and need to go to the remote end to talk with the same caller, you have to hold the phone call and transfer the call to this number from VoIP phone set.	
	2.	The parking sever will give you another voice number (e.g., your parking number is XXXX). Please remember it and hang up the phone set.	
	3.	Next, use another phone set in remote end to communicate with that caller again by dialing the voice number (XXXX).	
RTP Local Port Start/ RTP Local Port End	RTP If your VoIP service provider gave you such inforplease type the port number for RTP traffic. Other the default setting. For one port number used, typ port number in RTP Local Port Start and RTP Local fields. To set a range for port numbers type oport numbers in RTP Local Port Start and RTP L End fields.		

5.12.4.2 Hunt Group

This page allows you to make several extension numbers under certain group. Thus, when a phone call incomes, all the extension numbers under such group will ring.

IP PBX >> PBX System

Hunt Group

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

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

Index

	information.	
Group Name	Display the name of such group.	
Group Extension	Display the extension number of such group.	
Hunt List	Display the members inside the group.	

Click any index number to display the hunt group setup page.

IP PBX >> PBX System

Hunt Groups Index 1		
Hunt Group Name		
Hunt Group Extension		
Hunt Rule	Simultaneously 😪	
Hunt List (Maximum Of Group Mem	ber:20)	
Available	-	Chosen
34 35 36 37 38 39 40 41 42 43 44 45 46 47 48 48 50 51 - FXS PHONE-901 52 - ISDN PHONE1-903 ▼	Add » Add All Remove « Remove All Move Up Move Down	
	OK Cancel	

Hunt Group Name	Type suitable name for such group.
Hunt Group Extension	Type extension number for such group.
Hunt Rule	Use the drop down menu to choose rule for such group. Simultaneously – Choose such rule can make all the phones in the groups ring while receiving incoming calls. Sequentially - Choose such rule can make all the phones in the groups ring one by one while receiving incoming calls.
Add>>	Click this button to move the selected item in Available area to Chosen area.
Add All	Click this button to move all of the items in Available area to Chosen area.
Remove<<	Click this button to move the selected item in Chosen area to Available area.
Remove All	Click this button to clear all of the selections in Chosen area.
Move Up	Click this button to move the selected item to the upper place.
Move Down	Click this button to move the selected item to the lower place.

Dray Tek

5.12.4.3 Voice Mail Configuration

This page allows users to set actions for voices mails.

IP PBX >> PBX System

Voice Mail Configuration		
Extension for checking message	s 888 (20 ~ 65535)	
Send Voice Message by Ema	il	
Delete Voice Message a	iter Sending Mail	
Day for keeping voice mail	3 (1~7)	
Maximum messages time	30 Sec 💌	
Mail Voice-Mail Setup		
SMTP Server		
Authentication		
User Name		
Password		
	OK Cancel	
xtension for checking	The number specified here is used for the user to	listen

Extension for checking messages	The number specified here is used for the user to listen personal voice mail from IP PBX device.
Send Voice Message by Email	IP PBX can send the voice mail to the specified e-mail address for the incoming call if you check this box. Delete Voice Message after Sending Mail - IP PBX can send the voice mail to the specified e-mail address for the incoming call directly and delete the temporary file in IP PBX if you check this box.
Days for keeping voice mail	Type the days for keeping each voice mail.
Maximum message time	Type the recording length for each voice mail.
SMTP Server	Type IP address or domain name for the server specified for receiving voice messages.
Authentication	Check this box to authenticate the mail server.
User Name	Type a name for IP PBX to authenticate the mail server automatically while connecting.
Password	Type a password for IP PBX to authenticate the mail server automatically while connecting.

5.12.4.4 Office Hours

You can set ten groups of office hours including starting point, ending point on duty day(s).

IP PBX >> PBX System

Office H	lours			
Index	Enable	Office Hour Start (HHMM)	Office Hour End (HHMM)	Weekdays
1	✓	02 💌 25 💌	04 💌 25 💌	🗹 Sun 🗌 Mon 🗌 Tue 🗹 Wed 🗌 Thu 🗌 Fri 🗌 Sat
2		00 🕶 00 💌	00 🕶 00 🛩	Sun Mon Tue Wed Thu Fri Sat
З		00 🕶 00 🛩	00 🕶 00 🛩	🗌 Sun 🗌 Mon 📄 Tue 🗌 Wed 📄 Thu 📄 Fri 🗌 Sat
4		00 🕶 00 💌	00 🕶 00 🛩	Sun Mon Tue Wed Thu Fri Sat
5		00 🕶 00 🛩	00 🕶 00 🛩	🗌 Sun 🗌 Mon 📄 Tue 🗌 Wed 📄 Thu 📄 Fri 🗌 Sat
6		00 🕶 00 💌	00 🕶 00 🛩	Sun Mon Tue Wed Thu Fri Sat
7		00 🕶 00 🛩	00 🕶 00 🕶	🗌 Sun 🗌 Mon 📄 Tue 🗌 Wed 📄 Thu 📄 Fri 🗌 Sat
8		00 🗸 00 🔽	00 🔽 00 🔽	🗌 Sun 🗌 Mon 📄 Tue 🗌 Wed 📄 Thu 📄 Fri 🗌 Sat
9		00 🗸 00 🗸	00 🕶 00 🛩	🗌 Sun 🗌 Mon 📄 Tue 🗌 Wed 📄 Thu 📄 Fri 🗌 Sat
10		00 🖌 00 🔽	00 🗸 00 🗸	Sun Mon Tue Wed Thu Fri Sat

Holiday Setting

Month	Date
1	
2	
3	
4	
5	
6	
7	
8	
9	
10	
11	
12	

Office Hour Start	Use the drop down menu to choose the time as the starting point.
Office Hour End	Use the drop down menu to choose the time as the ending point.
Weekdays	Check the day(s) to apply the office hour for that index.
Date	Specify date(s) for applying the office hour settings in holiday, for example, type 2,4 6 & 7 in the field of Date for Month 1. It means January 2,4,6 & 7 will apply the office hour settings configured in this page.

Clear

Cancel



ΟK

5.12.4.5 Auto Attendant Wizard

The first page is configured for phone calls in office hours.

IP PBX >> PBX System

				Кеу	Action
				0	Ring Extension 1 💌
				1	Plays Prompt : Prompt 7
				2	Ring Extension 💙 1 💙
		Auto Attendant answers the		3	Ring Extension 💙 1 💌
Caller calls Auto	_	call,plays office hours greeting	_	4	Ring Extension 💙 1 💙
Attendant	_	(prompt 5),and	_	5	Ring Extension 👻 1 💌
		waits for caller input		6	Ring Extension 💙 1 💌
	·			7	Ring Extension 💌 1 💌
				8	Ring Extension 👻 1 💌
				9	Ring Extension 👻 1 👻
		ſ	Next >		Cancel

Auto Attendant Wizard - Office Hours

Click Next. The second page is configured for phone calls in non-office hours.

			Кеу	Action
			0	Ring Extension 1 💌
			1	Plays Prompt : Prompt 7
			2	Ring Extension 💙 1 💙
		Auto Attendant answers the call,plays non- office hours greeting (prompt 6),and	3	Ring Extension 💌 1 💌
ller calls	_		4	Ring Extension 💙 1 💙
Auto tendant			5	Ring Extension 💙 1 💙
waits fo	waits for caller	6	Ring Extension 💙 1 💙	
	input	7	Ring Extension 💙 1 💙	
			8	Ring Extension 💙 1 💙
			9	Ring Extension 💙 1 💙

IP PBX >> PBX System

Dray Tek

Ring Extension	Only the extension number selected here will ring. Ring Extension Plays Prompt Ring Hunt Group
Plays Prompt	Audio file will be played automatically.
2-9	Drop down menu 1 contains Ring Receptionist /Plays Prompt/Ring Hunt Group. Drop down menu 2 contains extension name (ex. Tom, Mike)] or prompt [Prompt 1~ Prompt 10, audio files] or Hunt Group Name [(ex. Sales, RD2)]. It will be changed according to drop down menu 1.

Finally, the following window will appear.

IP PBX >> PBX System

Auto Attendant Wizard - Record Prompts
Please enter **** and to XXXX access IVR and auto-attendant message menu.
You can record the office hours and non-office hour greetings or other prompts. Prompt 5 is used as office hours greeting. Prompt 6 is used as non-office hours greeting. Prompt 7 is used as specific purposes.
< Back OK Cancel

5.12.4.6 Prompt Maintenance

The IP PBX system provides several audio files for users to choose for playing. Moreover, users can upload other audio files from USB storage or hard disk or others to make the IP PBX system playing. Users can record audio files and upload to router or download to PC. However, the file format of the audio file must follow the rule stated on the web page. Users can record the audio files through a phone set connected to the router or use audio record program on PC.

IP PBX >> PBX System

Prompt Maintenance

Download Prompt G711 01	▼ Back Up		
Upload			
		Browse Restore	

Note: The file name follows a pre-defined rule:

System Prompt File: v2820pbx_sysprompt.ivr ;

User Prompt File: v2820pbx_g711_userpromptXX.wav; XX: 01~10 ; If g711 Prompt File is upload, we will generate related G729 Prompt File automatically. But we can not generate G711 Prompt file based on G729 Prompt file;

Codec	Channels	Sample rate	Bits
Linear PCM	Stereo, Mono	8k, 11.025k, 12k, 16k, 22.05k, 24k, 32k, 44.1k, 48k	16
A-law g711	Stereo, Mono	8k, 11.025k, 12k, 16k, 22.05k, 24k, 32k, 44.1k, 48k	8
u-law g711	Stereo, Mono	8k, 11.025k, 12k, 16k, 22.05k, 24k, 32k, 44.1k, 48k	8

Download

Download

The audio file can be saved with IVR file format or WAV file format. In general, it will be saved in the router's memory after you record it. To back up the audio file(s) (saved in FLASH of the router) to your computer, please choose the one you want from the drop-down menu and click **Back Up**.

Download	
Prompt G711 01	~
Prompt G711 01	
Prompt G711 02	
Prompt G711 03	
Prompt G711 04	
Prompt G711 05	
Prompt G711 06	
Prompt G711 07	٥V
Prompt G711 08	ile
Prompt G711 09	∇
Prompt G711 10	le
Prompt G729 01	rai
Prompt G729 02	
Prompt G729 03	at
Prompt G729 04	
Prompt G729 05	
Prompt G729 06	
Prompt G729 07	
Prompt G729 09	
Prompt G729 09	-
Prompt G729 10	
System Prompt G711	
System Prompt G729	

Prompt 1 to prompt 10 will be used for user-defined audio files (file format must be .WAV). System Prompt file is provided by router firmware.

Upload	System Prompt file is provided by router firmware. To use such audio file, you have to upload it to flash memory of the router after finishing firmware update. Click this Browse button to browse and choose other audio files.
Restore	Click this button to save the file to the router. Next time, the audio file will be played in IP PBX system.

Upload prompts to your router

You can modify and customize the default system prompt by using the following steps.

Please follow the steps below to upload System Prompt to your router:

- 1. Please use *DOS-BOX FTP client* (Windows built-in FTP client utility) to login VigorIPPBX FTP server.
- 2. Press Enter to pass authentication.
- 3. Type **put v2820_sysprompt.ivr**.
- 4. Wait for a while. The message of **226 System prompts file has been uploaded successfully** will appear
- 5. Type put v2820_g729_sysprompt.ivr.
- 6. Wait for a while. The message of **226 System prompts G729 file has been uploaded successfully** will appear
- 7. Type **quit** to close FTP client. **221 Goodbye! Router will be reboot now** will appear and the router will reboot.

Please follow the steps below to upload G.729 user Prompts to your router:

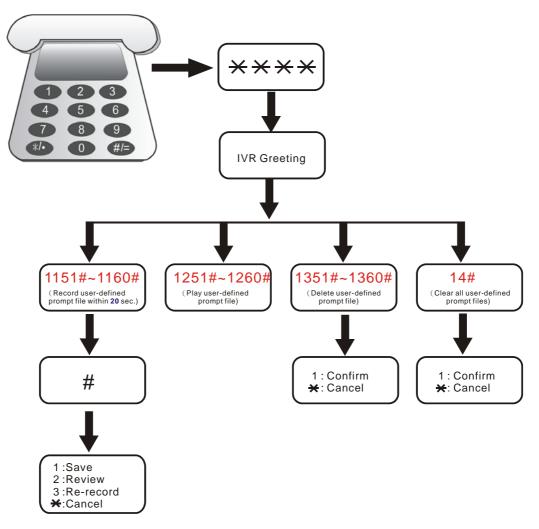
- 1. Please use *DOS-BOX FTP client* (Windows built-in FTP client utility) to login VigorIPPBX FTP server.
- 2. Press Enter to pass authentication.
- 3. Type put v2820_g729_userprompt.ivr.
- 4. Wait for a while. The message of 226 user prompts G729 file has been uploaded successfully will appear.
- 5. Type **quit** to close FTP client. **221 Goodbye! Router will be reboot now** will appear and the router will reboot.

Please follow the steps below to download G729 user Prompts to your computer:

- 1. Please use *DOS-BOX FTP client* (Windows built-in FTP client utility) to login VigorIPPBX FTP server.
- 2. Press Enter to pass authentication.
- 3. Type get v2820_g729_userprompt.ivr.
- 4. Wait for a while. The message of **226 File sent OK** will appear.
- 5. Type **quit** to close FTP client.

Record audio file

Below shows a flow chart for using a phone set to record audio file.



Dray Tek

5.12.4.7 Phone Setting

This page allows user to set phone settings.

IP PBX	>>	PBX	S	∕stem
--------	----	-----	---	-------

Index	Port	Call Feature	Codec	Tone	Gain (Mic/Speaker)	Extension Number	DTMF Relay
1	Phone	CW,CT,	G.729A/B	User Defined	5/5	901	OutBand
<u>2</u>	ISDN1-S0 💌		G.729A/B	User Defined	5/5	903	OutBand
<u>3</u>	ISDN2-TE 🔽		G.729A/B	User Defined	5/5	904	OutBand
RTP	Symme	etric RTP					
	,	TP Port Sta	rt	10050			
	,		1	15000			
	Dvnamic R	TP Port End		110000 1			
	Dynamic R RTP TOS	TP Port End	I	IP preceder	nce 5 💌 101	100000	
	RTP TOS	TP Port End ction Timer	I		nce 5 💌 101 sec	00000	

Phone List

Port – There are three phone ports provided here for you to configure. One (Index 1) is fixed and two (Index 2 & 3) are configurable. **Phone** port allows you to set general settings for analog phones. **ISDN** port allows you to set common settings for ISDN network connection. ISDN1 and ISDN2 port are configurable. Please use the drop down list to choose **ISDN1/2-TE** for Internet connection or choose **ISDN1/2-S0** (ISDN intern) for ISDN phone. In addition, you can connect six phones to this router in certain case. Please refer to **Section 4-1** for detailed information of ISDN phone/network connection.

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.

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

RTP



(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.

Manual	
IP precedence 1	
IP precedence 2	
IP precedence 3	
IP precedence 4	
IP precedence 5	
IP precedence 6	
IP precedence 7	
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)	
AF Class4 (High Drop)	
EF Class	
Manual	~

RTP TOS

VoIP Collection Timer – Not available. **VoIP Collection Timer Length** - Not available.

Detailed Settings for Phone Port

Click the number link of Phone port, you can access into the following page for configuring Phone settings. Below is the sample page for Phone port.

Phone						
Call Feature		Codecs				
🔲 Hotline		Prefer Codec	G.729A/B (8Kbps) 🔽			
Session Timer 90	sec		Single Codec			
DND(Do Not Disturb) Mode		Packet Size	20ms 💌			
Index(1-15) in <u>Schedule</u> 9	Setup:	Voice Active Detector Off 🖌				
	, <u> </u>	Extension	901			
Note: Action and Idle Tin	neout settings will	Number E-mail Address				
be ignored. CLIR (hide caller ID)		E-mail Address				
Call Waiting			Send a test e-mail			
Call Transfer		Voice mail Password				
		MWI				
		💿 Notify User wh	no Subscribed			
		🔘 Force Notify U	ser			
		Expiry Time	1 hour 💌 3600 sec			
		Outgoing Call Us	e			
		SIP1 SIP2	SIP3 SIP4 SIP5 SIP6			
		Answer Mode				
		No answer after	0 sec then			
		Keep Ring	×			
		Busy then				
		Do Nothing	×			
otline	Check the bo] Type in the SIP URL in the fie			
	for dialing a	utomatically wh	en you pick up the phone set.			
ession Timer	you set in th		function. In the limited time t is no response, the connecting.			
ND (Do Not Disturb) Mo	call. During	the period, the o	ithout disturbing by VoIP pho one who dial in will listen bus not listen any ring tone.			
	profiles to co preconfigure detailed cont Index (1-60)	ontrol the DND ed schedules. Re figuration.) in Phone Bool For to section 3.1	Enter the index of schedule mode according to the fer to section 5.8.2 Schedule k - Enter the index of phone b 0.1 DialPlan – Phone Book t			
LIR (hide caller ID)	Check this b phone set.	ox to hide the ca	aller ID on the display panel o			

IP PBX >> PBX System

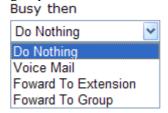


Call Waiting	appear to tell the user new p	s function. A notice sound will hone call is waiting for your o pick up the waiting phone call.		
Call Transfer		is function. Click hook flash to When the phone call connection e. The other two sides can		
Prefer Codec	The codec used for each call party before each session, ar choice. The default codec is bandwidth while maintainin. If your upstream speed is on	g good voice quality. Ily 64Kbps, do not use G.711 have at least 256Kbps upstream if		
	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 will be applied.	s checked, only the selected Codec		
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	not. If not, the router will do	he voice on both sides is active or o something to save the bandwidth invoke this function; click off to Off Con		
Extension Number	Type for specifying an exter	nsion number for such phone set.		
E-mail Address	incoming calls.	eceive media (voice) file sent by is button to send a test e-mail to		
Voice Mail Password	Type a password here. When mail, he/she muse use such j	n the user want to listen the voice password to open it.		
MWI (Message Waiting Indicator)	Check this box and the IP PI are voice mails in the IP pho	BX will notify the user that there one.		

Dray Tek

	Notify User who Subscribed - The user needs to send out SUBSCRIBE message first. When IPPBX detects new voice message from some extension number or the condition of the voice message is changed, it will transfer "NOTIFY" message to the users within the valid time subscribed.
	Force Notify User- The user does not send out SUBSCRIBE message automatically. The IPPBX will deliver "NOTIFY" message to the users if there is a new message or the user registers on IPPBX again.
Outgoing Call Use	There are six outside lines and one ISDN line for you to specify for such extension. Please check the one(s) you want.
Answer Mode	Specify the way to process incoming phone calls. No answer after – When the incoming phone call is not picked up, it will be processed by keeping, forwarding to certain extension or group. Please specify the waiting time and determine the way you want to process.
	No answer after
	Keep Ring
	Keep Ring Voice Mail Foward To Extension

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



Foward To Group

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.

IP PBX >> Phone Settings

Advance Settings >> Phone

Tone Setting	S							
Region Use	r Defined	*						
		Low Fre (Hz)		jh Freq (Hz)	T on 1 (msec)	T off 1 (msec)	T on 2 (msec)	T off 2 (msec)
Dial to	ne	350	440		0	0	0	0
Ringing t	one	400	450		400	200	400	2000
Busy to	ne	400	0		375	375	0	0
Congestion	n tone	0	0		0	0	0	0
Volume Gain	1				DTMF			
Mic Gain(1-10))		5		DTMF Mo	de	OutBand (F	RFC2833)
Speaker Gain	(1-10)		5		Payload 1	Type(RFC2833) 101	
MISC								
Dial Tone Pov	ver Level	(1 - 35)	27					
Ring Frequence	cy (10 -	50HZ)	25					

Region

Select the proper region which you are located. The common settings of **Caller ID Type**, **Dial tone**, **Ringing tone**, **Busy tone** and **Congestion tone** will be shown automatically on the page. If you cannot find out a suitable one, please choose **User Defined** and fill out the corresponding values for dial tone, ringing tone, busy tone, congestion tone by yourself for VoIP phone.

	_ 1
	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.
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 Mode – There are four DTMF modes for you to choose.

InBand - Choose this one then the Vigor will send the DTMF tone as audio directly when you press the keypad on the phone **OutBand** - Choose this one then the Vigor will capture the keypad number you pressed and transform it to digital form then send to the other side; the receiver will generate the tone according to the digital form it receive. This function is very useful when the network traffic congestion occurs and it still can remain the accuracy of DTMF tone.

SIP INFO- Choose this one then the Vigor will capture the DTMF tone and transfer it into SIP form. Then it will be sent to the remote end with SIP message.

DTMF mode

InBand	~
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.

DTMF

Detailed Settings for ISDN1/2-S0 Port

Click the number link of Index 2 or Index 3 (ISDN1-S0 or ISDN2-S0), you can access into the following page for configuring Phone settings.

ISDN1-S0		
Call Feature	Codecs	
Hotline	Prefer Codec	G.729A/B (8Kbps) 🖌
Session Timer 90 sec		Single Codec
DND(Do Not Disturb) Mode	Packet Size	20ms 💌
Index(1-15) in <u>Schedule</u> Setup:	Voice Active Detector	Off 🛩
Note: Action and Idle Timeout settings will	Extension Number 903	
be ignored.	E-mail Address	
CLIR (hide caller ID)	5	Send a test e-mail
Call Waiting Call Transfer	Voice mail Password	
	MWI	
	Notify User who Subs	scribed
	Force Notify User	
	Expiry Time 1 ho	ur 🖌 3600 sec
	Outgoing Call Use	
	✓ SIP1 □ SIP2 □ SIP3 □ ISDN2-TE	SIP4 SIP5 SIP6
	Answer Mode	
	No answer after 0	sec then
	Keep Ring 🖌 🖌	
	Busy then	
	Do Nothing 👻	
1	1	

IP PBX >> PBX System

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.	
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 5.8.2 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.	

Cancel

Advanced

OK

Call Waiting	appear to tell the user new p	is function. A notice sound will hone call is waiting for your o pick up the waiting phone call.	
Call Transfer		is function. Click hook flash to When the phone call connection e. The other two sides can	
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 Cod 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 wi contain 20 ms voice information. 		
	Packet Size	20ms 💙 10ms 20ms 30ms 40ms 50ms 60ms	
	on both sides is active or no	his function can detect if the voice t. If not, the router will do width for other using. Click On to	
Extension Number	Tune for anotifuing on outor	On	
Extension Number E-mail Address		nsion number for such phone set. eceive media (voice) file sent by	
	incoming calls.	is button to send a test e-mail to	
Voice Mail Password	Type a password here. When mail, he/she muse use such	n the user want to listen the voice password to open it.	
MWI (Message Waiting Indicator)		BX will notify the user that there	

Notify User who Subscribed - The user needs to send out

	SUBSCRIBE message first. When IPPBX detects new voice message from some extension number or the condition of the voice message is changed, it will transfer "NOTIFY" message to the users within the valid time subscribed.			
	Force Notify User- The user does not send out SUBSCRIBE message automatically. The IPPBX will deliver "NOTIFY" message to the users if there is a new message or the user registers on IPPBX again.			
Expiry Time It is the time duration that your SIP Registrar server your registration record. Before the time expires, the will send another register request to SIP Registrar and expired another register request to SIP Registrar and 				
Outgoing Call Use	There are six outside lines and one ISDN line for you to specify for such extension. Please check the one(s) you want.			
Answer Mode	Specify the way to process incoming phone calls. No answer after – When the incoming phone call is not picked up, it will be processed by keeping, forwarding to certain extension or group. Please specify the waiting time and determine the way you want to process.			
	No answer after			
	Keep Ring Keep Ring Voice Mail Foward To Extension Foward To Group			
	Busy then – When this extension number is busy, you can forward the incoming phone call to other extension number or group.			

Busy then
Do Nothing
Do Nothing
Voice Mail
Foward To Extension
Foward To Group

In addition, you can press the **Advanced** button to configure tone settings, volume gain, MISC, DTMF mode and MSN number. **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.

IP PBX >> Phone Settings

Advance Settings >> ISDN1-S0

Tone Set	ttings						
Region	User Defined	*					
		Low Freq (Hz)	High Freq (Hz)	T on 1 (msec)	T off 1 (msec)	T on 2 (msec)	T off 2 (msec)
Dia	al tone	350	440	0	0	0	0
Ring	ing tone	400	450	400	200	400	2000
Bus	sy tone	400	0	375	375	0	0
Conge	stion tone	0	0	0	0	0	0
Volume	Gain			DTMF			
Mic Gain((1-10)	5	DTMF Mode OutBand (R			RFC2833)	
Speaker Gain(1-10)		5	Payload Type(RFC2833) 101				
MISC							
Dial Tone Power Level (1 - 35)		(1 - 35) 2	7				
Ring Frequency (10 - 50HZ)		50HZ) 2	5				

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.

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.

Volume GainMic 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.MISCDial 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 Mode – There are four DTMF modes for you to choose.

InBand - Choose this one then the Vigor will send the DTMF tone as audio directly when you press the keypad on the phone **OutBand** - Choose this one then the Vigor will capture the keypad number you pressed and transform it to digital form then send to the other side; the receiver will generate the tone according to the digital form it receive. This function is very useful when the network traffic congestion occurs and it still can remain the accuracy of DTMF tone.

SIP INFO- Choose this one then the Vigor will capture the DTMF tone and transfer it into SIP form. Then it will be sent to the remote end with SIP message.

DTMF mode

InBand	¥
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.

Detailed Settings for ISDN1/2-TE Port

The vigor router allows users to switch the function of ISDN1/ISDN2 port between TE or S0 mode. Please use the drop down list to choose the one you want.



Choose ISDN-TE and click the number link for that port, you will see the following page.

IP PBX >> PBX System

ISDN2-TE Call Feature			Codecs		
Session Timer	90 s	sec	Prefer Codec	G.729A/B (8Kbps) 💌	
DND(Do Not Disturb) Mode				Single Codec	
Index(1-15) in <u>Schedule</u> Setup:			Packet Size	20ms 💌	
, , , , ,			Voice Active Detector	Off 🖌	
Note: Action and Idle Timeout settings will be ignored.			Extension Number 904		
CLIR (hide caller ID)					
OK Cancel Advanced					



Session Timer		e the function. In the limited time that here is no response, the connecting call cally.		
DND (Do Not Disturb) mode	call. During the period,	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.		
	profiles to control the E preconfigured schedule Application>>Schedul Index (1-60) in Phone	 ale - Enter the index of schedule DND mode according to the s. Refer to section le for detailed configuration. Book - Enter the index of phone book m DialPlan >> Phone Book for 		
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 The codec used for each call will be negotiated with the party before each session, and so may not be your defa choice. The default codec is G.729A/B; it occupies litt bandwidth while maintaining good voice quality. If your upstream speed is only 64Kbps, do not use G.7 codec. It is better for you to have at least 256Kbps ups 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 b will be applied.	box is checked, only the selected Codec		
	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	

Extension Number

Type for specifying an extension number for such phone set.



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.

Tone Se	ttings							
Region	User Defined	*						
		Low Freq (Hz)	High Freq (Hz)	T on 1 (msec)	T off 1 (msec)	T on 2 (msec)	T off 2 (msec)	
Dia	al tone	350	440	0	0	0	0	
Ring	ing tone	400	450	400	200	400	2000	
Bus	Busy tone 400		0	375	375	0	0	
Conge	stion tone	0	0	0	0	0	0	
Volume	Gain			DTMF				
Mic Gain	(1-10)	5		DTMF Mode		OutBand (F	OutBand (RFC2833)	
Speaker	Gain(1-10)	5		Payload Type(RFC2833) 101				
MISC								
Dial Tone	e Power Level	(1 - 35) 2	7					
Authent	ication PIN (Code						
Chec	k for ISDN to	VoIP Calls	000					
Chec	k for VoIP to	ISDN Calls	000					

IP PBX >> Phone Settings

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, and congestion tone by yourself for VoIP phone.



ΟK

Cancel

Also, you can specify each field for your necessity. It is

	recommended for you to use communication.	e the default settings for VoIP	
Volume Gain		Gain (1-10) - Adjust the volume of entering number from 1- 10. The ader 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 DTM tone as audio directly when you press the keypad on the phe 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 to according to the digital form it receive. This function is ver useful when the network traffic congestion occurs and it sti 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 set 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.

5.12.5 PBX Status

IP PBX >> PBX Status		
PBX Status		
	Call Detail Records	
	Extension Monitor	

5.12.5.1 Call Detail Records

This page displays call records of IP PBX such as failed call, successful call, no-answer call, date of the call and the duration of each call, and so on.

all Detail Rec	cords		Refresh S	Geconds: 10 💌	<u>Refresh</u>
Index	Date 🗸	<u>From</u>	To	<u>Result</u>	Duration
1					
2					
3					
4					
5					
6					
7					
8					
9					
10					
11					
10					
38					
39					
40					
41					
42					
43					
44					
45					
46					
47					
48					
49					
50					

IP PBX >> PBX Status

 $<\frac{1.50}{501.550}$ | $\frac{51.600}{551.600}$ | $\frac{601.650}{651.700}$ | $\frac{701.750}{701.750}$ | $\frac{751.800}{51.800}$ | $\frac{801.850}{851.900}$ | $\frac{901.950}{901.950}$ | $\frac{951.1000}{951.1000}$ >>

5.12.5.2 Extension Monitor

This page displays owner's name, IP address, status and peer ID for each extension number.

xtension M	onitor		Refresh	n Seconds: 🛛 10 💌	Refres
Index	Name	Extension	IP	Status	Peer ID
1				Offline	
2				Offline	
3				Offline	
4				Offline	
5				Offline	
6				Offline	
7				Offline	
8				Offline	
9				Offline	
10				Offline	

IP PBX >> PBX Status

5.13 Wireless LAN

This function is used for "n" models only.

5.13.1 Basic Concepts

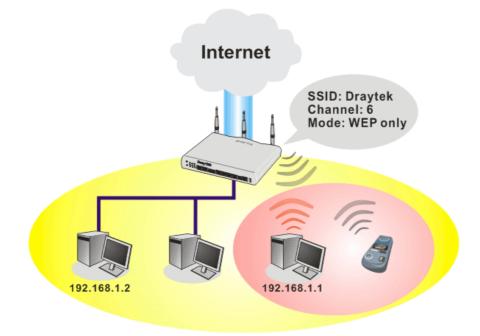
Over recent years, the market for wireless communications has enjoyed tremendous growth. Wireless technology now reaches or is capable of reaching virtually every location on the surface of the earth. Hundreds of millions of people exchange information every day via wireless communication products. The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

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

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

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





Security Overview

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

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

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

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

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

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

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

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

Below shows the menu items for Wireless LAN.



Wireless LAN
General Setup
Security
Access Control
▶ WPS
▶ WDS
Advanced Setting
AP Discovery
Station List
Station List

Wireless LAN >> General Setup

5.13.2 General Setup

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

ble Wireless	5 LAN		
Mode :		Mixed(11b+11g+1	1n) 🔽
Only schedu) in <u>Schedule</u> Se ule profiles that ns are ignored.	etup:, have the action "Force Down" ar	,, e applied to the WLAN, all
	Hide SSID	SSID	Isolate LAN Member
1		default	
2			
3			
4			
Hide SSID:	Prevent SSID f	from being scanned.	
Wireless cli	N: ents (stations)	with the same SSID cannot acce with the same SSID cannot acce	
Channel: C Long Pream	N: ents (stations) hannel 6, 2437MH ble: necessary f	with the same SSID cannot acce	ss wired PCs on LAN.
Wireless cli Channel: C Long Pream Packet-OVE	N: ents (stations) hannel 6, 2437MH ble: necessary f	with the same SSID cannot acce	ss wired PCs on LAN.
Wireless cli Channel: C Long Pream Packet-OVE	N: ents (stations) hannel 6, 2437MH ble: necessary f	with the same SSID cannot acce	ss wired PCs on LAN.
Wireless cli Channel: C Long Pream Packet-OVE Tx Burst Note:	N: ents (stations) hannel 6, 2437MH ble: necessary f RDRIVE TM t	with the same SSID cannot acce	ss wired PCs on LAN.
Wireless cli Channel: C Long Pream Packet-OVE Tx Burst Note: The same to	N: ents (stations) hannel 6, 2437MH ble: necessary f RDRIVE TM t echnology must	with the same SSID cannot acce Iz Long Preamble: for some old 802.11 b devices on	ss wired PCs on LAN.
Wireless cli Channel: C Long Pream Packet-OVE Tx Burst Note:	N: ents (stations) hannel 6, 2437MH ble: necessary f RDRIVE TM t echnology must	with the same SSID cannot acce Iz Long Preamble: for some old 802.11 b devices on	ss wired PCs on LAN.
Wireless cli Channel: C Long Pream Packet-OVE Tx Burst Note: The same to	N: ents (stations) hannel 6, 2437MH ble: necessary f RDRIVE TM t echnology must	with the same SSID cannot acce Long Preamble: for some old 802.11 b devices on also be supported in clients to b	ss wired PCs on LAN.
Wireless cli Channel: C Long Pream Packet-OVE Tx Burst Note: The same to Rate Contro	N: ents (stations) hannel 6, 2437MH ble: necessary f RDRIVE TM t echnology must bl Enable	with the same SSID cannot acce Long Preamble: for some old 802.11 b devices on also be supported in clients to be Upload	ss wired PCs on LAN. y(lower performance) oost WLAN performance. Download
Wireless cli Channel: C Long Pream Packet-OVE Tx Burst Note: The same to Rate Contro SSID 1	N: ents (stations) hannel 6, 2437MH ble: necessary f RDRIVE TM t echnology must bl Enable	with the same SSID cannot acce Long Preamble: for some old 802.11 b devices on also be supported in clients to b Upload 30000 kbps	ss wired PCs on LAN. y(lower performance) oost WLAN performance. Download 30000 kbps
Wireless cli Channel: C Cong Pream Packet-OVE Tx Burst Note: The same to Rate Contro SSID 1 SSID 2	N: ents (stations) hannel 6, 2437MH ble: necessary f RDRIVE TM t echnology must bl Enable	with the same SSID cannot acce Iz V Long Preamble: for some old 802.11 b devices on also be supported in clients to b Upload 30000 kbps 30000 kbps	ss wired PCs on LAN. y(lower performance) oost WLAN performance. Download 30000 kbps 30000 kbps

Enable Wireless LAN Mode Check the box to enable wireless function.

At present, the router can connect to 11b Only, 11g Only, 11n Only, Mixed(11b+11g), Mixed(11g+11n) and Mixed

	Mixed(11b+11g+11n) 11b Only 11g Only 11n Only Mixed(11b+11g) Mixed(11g+11n) Mixed(11b+11g+11n)
Index(1-15)	Set the wireless LAN to work at certain time interval only. You may choose up to 4 schedules out of the 15 schedules pre-defined in Applications >> Schedule setup. The default setting of this filed is blank and the function will always work.
Hide SSID	Check it to prevent from wireless sniffing and make it harder for unauthorized clients or STAs to join your wireless LAN. Depending on the wireless utility, the user may only see the information except SSID or just cannot see any thing about Vigor wireless router while site surveying. The system allows you to set four sets of SSID for different usage. In default, the first set of SSID will be enabled. You can hide it for your necessity.
SSID	Means the identification of the wireless LAN. SSID can be any text numbers or various special characters. The default SSID is "default". We suggest you to change it.
Isolate	 Member –Check this box to make the wireless clients (stations) with the same SSID not accessing for each other. LAN –Check this box to make the wireless clients (stations) with the same SSID not accessing wired PC on LAN.
Channel	Means the channel of frequency of the wireless LAN. The default channel is 6. You may switch channel if the selected channel is under serious interference. If you have no idea of choosing the frequency, please select Auto to let system determine for you.

(11b+11g+11n) stations simultaneously. Simply choose Mix (11b+11g+11n) mode.

Channel:	Channel 6, 2437MHz 🛛 💌
	Auto
	Channel 1, 2412MHz Channel 2, 2417MHz Channel 3, 2422MHz Channel 4, 2427MHz Channel 5, 2432MHz Channel 6, 2437MHz Channel 7, 2442MHz Channel 8, 2447MHz
	Channel 9, 2452MHz
	Channel 10, 2457MHz Channel 11, 2462MHz
	Channel 12, 2467MHz
	Channel 13, 2472MHz

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

Packet-OVERDRIVEThis feature can enhance the performance in data
transmission about 40% for 11g (5% for 11n) by
checking **Tx Burst**. It is active only when both sides of
Access Point and Station (in wireless client) invoke this
function at the same time. That is, the wireless client
must support this feature and invoke the function, too.

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

nfiguration Status Option About		
Ceneral Setting Auto launch when Windows start up Remember mini status position Auto hide mini status Set mini status always on top Enable IP Setting and Proxy Setting in Profile Comp. Remember 200	Advance Setting Disable Radio Eragmentation Threshold : RTS Threshold : Frequency : Ad-hoc Channel:	2346 2347 802.11b/g/n - 2.4GH ¥ 1
<u>G</u> roup Koaming Ad-hoc	Po <u>w</u> er Save Mode: T× <u>B</u> urst :	Disable 💙 Disable 💙
WLAN type to connect Infrastructure and Ad-hoc network Infrastructure network only Ad-hoc network only		
Automatically connect to non-preferred networks		

Rate Control

It controls the data transmission rate through wireless connection.

Upload – Check Enable and type the transmitting rate for data upload. Default value is 30,000 kbps.



Download – Type the transmitting rate for data download. Default value is 30,000 kbps.

5.13.3 Security

This page allows you to set security with different modes for SSID 1, 2, 3 and 4 respectively. After configuring the correct settings, please click **OK** to save and invoke it.

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

Wireless LA	N >> Securit	y Settings
-------------	--------------	------------

SSID 1	SSID 2	SSID 3	SSID 4
	Mode:	[WPA/PSK
WPA:	Set up <u>RADIUS S</u>	<u>erver</u> if 802.1:	1× is enabled.
Encry	ption Mode:		ТКІР
	Pre-Shared Key(I	PSK):	******
	Type 8~63 ASCI "cfgs01a2" or '		or 64 Hexadecimal digits leading by "Ox", for example ".
WEP:			
	Encryption Mode		64-Bit 💙
	◉Key 1 :	[*****
	○Key 2 :	[*****
	○Кеу 3 :	[*****
	○Key 4 :	[******
Type "0x414 For 1 3 Type	42333132". 28 bit WEP key 13 ASCII characte	er or 26 Hexad	decimal digits leading by "Ox", for example "AB312" or adecimal digits leading by "Ox", for example 3536373839414243".

OK Cancel

Mode

There are several modes provided for you to choose.

WPA/PSK	*
Disable	
WEP	
WEP/802.1x Only	
WPA/802.1x Only	
WPA2/802.1x Only	
Mixed(WPA+WPA2/802.1x only)	
WPA/PSK	
WPA2/PSK	
Mixed(WPA+WPA2)/PSK	

Disable - Turn off the encryption mechanism.

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

WEP/802.1x Only - Accepts only WEP clients and the encryption key is obtained dynamically from RADIUS server with 802.1X protocol.

WPA/802.1x Only- Accepts only WPA clients and the encryption key is obtained dynamically from RADIUS server with 802.1X protocol.

	 WPA2/802.1x Only- Accepts only WPA2 clients and the encryption key is obtained dynamically from RADIUS server with 802.1X protocol. Mixed (WPA+WPA2/802.1x only) - Accepts WPA and WPA2 clients simultaneously and the encryption key is obtained dynamically from RADIUS server with 802.1X protocol. WPA/PSK-Accepts only WPA clients and the encryption key should be entered in PSK. WPA2/PSK-Accepts only WPA2 clients and the encryption key should be entered in PSK. Mixed (WPA+ WPA2)/PSK - Accepts WPA and WPA2 clients simultaneously and the encryption key should be entered in PSK.
	Note: You should also set RADIUS Server simultaneously if WEP/802.1x Only, WPA/802.1x Only, WPA2/802.1x Only or Mixed (WPA+WPA2/802.1x only) is selected.
WPA	The WPA encrypts each frame transmitted from the radio using the key, which either PSK (Pre-Shared Key) entered manually in this field below or automatically negotiated via 802.1x authentication. Either 8~63 ASCII characters, such as 012345678(or 64 Hexadecimal digits leading by 0x, such as "0x321253abcde"). Type - Select from Mixed (WPA+WPA2) or WPA2 only. Pre-Shared Key (PSK) - Either 8~63 ASCII characters, such as 012345678(or 64 Hexadecimal digits leading by 0x, such as "0x321253abcde").
WEP	 64-Bit - For 64 bits WEP key, either 5 ASCII characters, such as 12345 (or 10 hexadecimal digitals leading by 0x, such as 0x4142434445.) 128-Bit - For 128 bits WEP key, either 13 ASCII characters, such as ABCDEFGHIJKLM (or 26 hexadecimal digits leading by 0x, such as 0x4142434445464748494A4B4C4D).
	Encryption Mode: 64-Bit 64-Bit 128-Bit
	All wireless devices must support the same WEP

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

Dray Tek

5.13.4 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.

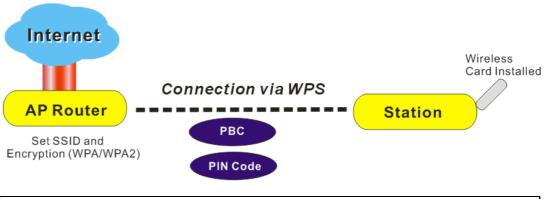
Access Control					Set to Factory Default
Ena	ble Mac Addres:	s Filter			
	SSID 1	🔲 SSID 2	🔲 SSID 3	🔲 SSIC) 4
		MAC Add	ress Filter		
	Index Attribu	ute MAC Add	iress		
	Client's MAC	CAddress :	:::	::	
		Attril	oute :		
		📃 s: Isolate tl	ne station from L	AN	
	Add	Delete	Edit	Cancel	
		ОК	Clear All		

Wireless	LAN>>	Access	Control
11101033		ACCC33	CONTROL

Enable Max Access Filter	Select to enable the MAC Address filter for wireless LAN identified with SSID 1 to 4 respectively. All the clients (expressed by MAC addresses) listed in the box can be grouped under different wireless LAN. For example, they can be grouped under SSID 1 and SSID 2 at the same time if you check SSID 1 and SSID 2.
MAC Address Filter	Display all MAC addresses that are edited before.
Client's MAC Address	Manually enter the MAC address of wireless client.
Attribute	s: Isolate the station from LAN - select to isolate the wireless connection of the wireless client of the MAC address from LAN.
Add	Add a new MAC address into the list.
Delete	Delete the selected MAC address in the list.
Edit	Edit the selected MAC address in the list.
Cancel	Give up the access control set up.
ОК	Click it to save the access control list.
Clear All	Clean all entries in the MAC address list.
Clear All	Clean all entries in the MAC address list.

5.13.5 WPS

WPS (Wi-Fi Protected Setup) provides easy procedure to make network connection between wireless station and wireless access point (vigor router) with the encryption of WPA and WPA2.

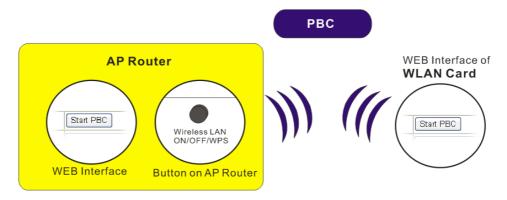


Note: Such function is available for the wireless station with WPS supported.

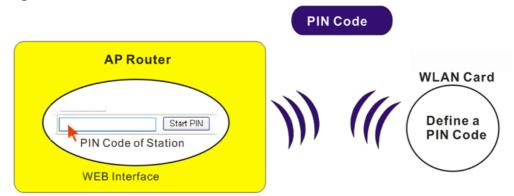
It is the simplest way to build connection between wireless network clients and vigor router. Users do not need to select any encryption mode and type any long encryption passphrase to setup a wireless client every time. He/she only needs to press the **WPS** button on AP and selects that AP on the utility of wireless station. Then WPS will connect for client and router automatically.

There are two methods to do network connection through WPS between AP and Stations: pressing the *Start PBC* button or using *PIN Code*.

• On the side of VigorIPPBX 2820 series which served as an AP, press **Wireless LAN ON/OFF/WPS** button for 2 seconds to wait for client device making network connection through WPS or click **Start PBC** on web configuration interface. On the side of a station with network card installed, press **Start PBC** button of network card.



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



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

Microsof	t Internet Explorer 🛛 🔀
1	WPS only supports in WPA/WPA2-PSK Mode.
	ОК

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

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

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

🗹 Enable WPS 🗘

Wi-Fi Protected Setup Information

WPS Status	Configured
SSID	DrayTek
Authentication Mode	Disable

Device Configure

Configure via Push Button	Start PBC
Configure via Client PinCode	Start PIN

Status: The Authentication Mode is NOT WPA/WPA2 PSK!!

Note: WPS can help your wireless client automatically connect to the Access

- point. ⁽¹⁾: WPS is Disabled.
- Q: WPS is Enabled.
- ②: Waiting for WPS requests from wireless clients.

Enable WPS	Check this box to enable WPS setting.
WPS Status	Display related system information for WPS.
SSID	Display the SSID1 of the router. WPS is supported by SSID1 only.

Dray Tek

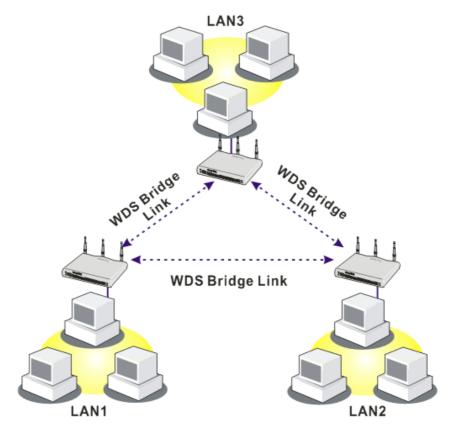
Authentication Mode	Display current authentication mode of the router. Only WPA2/PSK and WPA/PSK support WPS.
Configure via Push Button	Click Start PBC to invoke Push-Button style WPS setup procedure. The router will wait for WPS requests from wireless clients about two minutes. The WPS LED on the router will blink fast when WPS is in progress. It will return to normal condition after two minutes. (You need to setup WPS within two minutes)
Configure via Client PinCode	Please input the PIN code specified in wireless client you wish to connect, and click Start PIN button. The WLAN LED on the router will blink fast when WPS is in progress. It will return to normal condition after two minutes. (You need to setup WPS within two minutes)

5.13.6 WDS

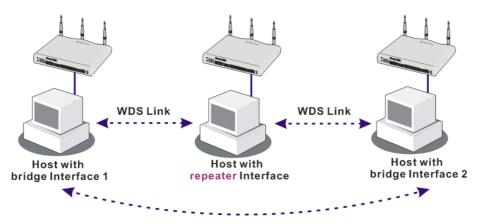
WDS means Wireless Distribution System. It is a protocol for connecting two access points (AP) wirelessly. Usually, it can be used for the following application:

- Provide bridge traffic between two LANs through the air.
- Extend the coverage range of a WLAN.

To meet the above requirement, two WDS modes are implemented in Vigor router. One is **Bridge**, the other is **Repeater**. Below shows the function of WDS-bridge interface:

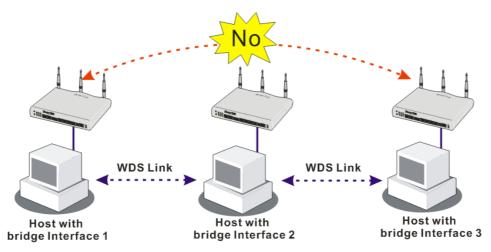


The application for the WDS-Repeater mode is depicted as below:



The major difference between these two modes is that: while in **Repeater** mode, the packets received from one peer AP can be repeated to another peer AP through WDS links. Yet in **Bridge** mode, packets received from a WDS link will only be forwarded to local wired or wireless hosts. In other words, only Repeater mode can do WDS-to-WDS packet forwarding.

In the following examples, hosts connected to Bridge 1 or 3 can communicate with hosts connected to Bridge 2 through WDS links. However, hosts connected to Bridge 1 CANNOT communicate with hosts connected to Bridge 3 through Bridge 2.



Click WDS from Wireless LAN menu. The following page will be shown.

Wireless LAN >> WDS Settings

Mode:		Deidao
	Repeater 🛩	Bridge Enable Peer MAC Address
Security:	_	
🔘 Disable 🛛 V	NEP 💿 Pre-shared Key	
W/FD.		
WEP:	key set in <u>Security Settings</u> .	
	key see in <u>seeding searings</u> .	Note: Disable unused links to get better performance.
Pre-shared Key:		
Туре:		Repeater
⊙ DrayTek WPA	○WPA ○WPA2	Enable Peer MAC Addess
Кеу	*********	
	haracters or 64 hexadecimal x", for example "cfgs01a2" or	
"0x655abcd".	x, for example crysoraz or	
		Access Point Function:
		Enable Disable
		Status:
		Send "Hello" message to peers.
		Link Status
		Note: The status is valid only when the peer also
		supports this function.
	invoke anv	mode for WDS setting. Disable mode will not WDS setting. Bridge mode is designed to fulfi
	the first type one. Disable Disable	WDS setting. Bridge mode is designed to fulfi e of application. Repeater mode is for the seco
	the first type one. Disable	WDS setting. Bridge mode is designed to fulfi
curity	the first type one. Disable Disable Bridge Repeater There are th Pre-shared following W	WDS setting. Bridge mode is designed to fulfi
curity EP	the first type one. Disable Disable Bridge Repeater There are th Pre-shared following W one of the ty Check this b page. If you	WDS setting. Bridge mode is designed to fulfi- e of application. Repeater mode is for the seco recet types for security, Disable , WEP and key . The setting you choose here will make the VEP or Pre-shared key field valid or not. Choose



	Key - Type 8 ~ 63 ASCII characters or 64 hexadecimal digits leading by " $0x$ ".
Bridge	If you choose Bridge as the connecting mode, please type in the peer MAC address in these fields. Four peer MAC addresses are allowed to be entered in this page at one time. Yet please disable the unused link to get better performance. If you want to invoke the peer MAC address, remember to check Enable box in the front of the MAC address after typing.
Repeater	If you choose Repeater as the connecting mode, please type in the peer MAC address in these fields. Four peer MAC addresses are allowed to be entered in this page at one time. Similarly, if you want to invoke the peer MAC address, remember to check Enable box in the front of the MAC address after typing.
Access Point Function	Click Enable to make this router serving as an access point; click Disable to cancel this function.
Status	It allows user to send "hello" message to peers. Yet, it is valid only when the peer also supports this function.

5.13.7 Advanced Setting

This page allows users to set advanced settings such as operation mode, channel bandwidth, guard interval, and aggregation MSDU for wireless data transmission.

Wireless LAN >> Advanced Setting

Operation Mode	💿 Mixed Mode 🔘 Green Field
Channel Bandwidth	○ 20 ④ 20/40
Guard Interval	🔘 long 💿 auto
Aggregation MSDU(A-MSDU)	🔘 Disable 💿 Enable

Operation Mode	 Mixed Mode – the router can transmit data with the ways supported in both 802.11a/b/g and 802.11n standards. However, the entire wireless transmission will be slowed down if 802.11g or 802.11b wireless client is connected. Green Field – to get the highest throughput, please choose such mode. Such mode can make the data transmission happening between 11n systems only. In addition, it does not have protection mechanism to avoid the conflict with neighboring devices of 802.11a/b/g.
Channel Bandwidth	 20- the router will use 20Mhz for data transmission and receiving between the AP and the stations. 20/40 – the router will use 20Mhz or 40Mhz for data transmission and receiving according to the station capability. Such channel can increase the performance for data transit.
Guard Interval	It is to assure the safety of propagation delays and reflections for the sensitive digital data. If you choose auto as guard interval, the AP router will choose short guard interval

	(increasing the wireless performance) or long guard interval for data transmit based on the station capability.
Aggregation MSDU	Aggregation MSDU can combine frames with different sizes. It is used for improving MAC layer's performance for some brand's clients. The default setting is Enable.

5.13.8 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	
		Scan]	
See <u>St</u>	atistics.			
	During the scanning proce t with the router.	ess (~5 secor	nds), no station is allowed to	
Add to	WDS Settings :			
AP's MA	AC address	: :::::		
Add	to	💿 Bridge	🔘 Repeater	

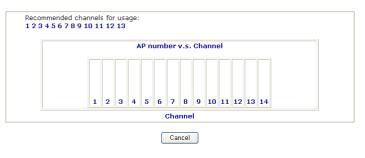
Wireless LAN >> Access Point Discovery

Scan

Statistics

It is used to discover all the connected AP. The results will be shown on the box above this button.

It displays the statistics for the channels used by APs. Wireless LAN >> Site Survey Statistics



If you want the found AP applying the WDS settings, please type in the AP's MAC address on the bottom of the page or choose the AP MAC address from the Scan result field, 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.

5.13.9 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.

Status	MAC Address	Associated with
	Refresh	
Status Codes :	la aparuntian	
C: Connected, M E: Connected, V		
P: Connected, V		
A: Connected, N B: Blocked by A		
N: Connecting.		
F: Fail to pass 8	302.1X or WPA/PSK authen	tication.
Note: After a st	tation connects to the rout	er successfully, it may be
turned off witho connection expir		will still be on the list until the
Add to <u>Access (</u>	Control :	
 Client's MAC add	dress ::::	: : : : : : : : : : : : : : : : : : : :
	Add	

Add

Click this button to add current selected MAC address into Access Control.

5.14 System Maintenance

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

Below shows the menu items for System Maintenance.

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

5.14.1 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.

_		
C ₁ /	etom	Status
Οy	Stelli	Juanas

Model Name Firmware Version Build Date/Time ADSL Firmware Vers	: Vigor2820 PBX : 3.5.3 : Sep 8 2009 18:07:3 sion : 211801_A Annex A		
	LAN		WAN 1
MAC Address	: 00-50-7F-94-E7-80	Link Status	: Disconnected
1st IP Address	: 192.168.1.1	MAC Address	: 00-50-7F-94-E7-81
1st Subnet Mas	k : 255.255.255.0	Connection	:
DHCP Server	: Yes	IP Address	:
DNS	: 168.95.1.1	Default Gateway	:
	SIP Trunk		WAN 2
Index P	rofile Status	Link Status	: Connected
1		MAC Address	: 00-50-7F-94-E7-82
2		Connection	: DHCP Client
3		IP Address	: 192.168.5.27
4		Default Gateway	: 192.168.5.1
5			
6		Wi	reless LAN
		MAC Address	: 00-50-7F-94-E7-80
		Frequency Domain	: Europe
		Firmware Version	: 1.8.1.0
		SSID	: default

Model Name	Display the model name of the router.
Firmware Version	Display the firmware version of the router.
Build Date/Time	Display the date and time of the current firmware build.
ADSL Firmware Version	Display the ADSL firmware version.
LAN	
MAC Address	Display the MAC address of the LAN Interface.



1 st IP Address	Display the IP address of the LAN interface.
I II Auuress	Display the IF address of the LAN interface.
1 st Subnet Mask	Display the subnet mask address of the LAN interface.
DHCP Server	Display the current status of DHCP server of the LAN interface.
DNS	Display the assigned IP address of the primary DNS.
WAN	
Link Status	Display current connection status.
MAC Address	Display the MAC address of the WAN Interface.
Connection	Display the connection type.
IP Address	Display the IP address of the WAN interface.
Default Gateway	Display the assigned IP address of the default gateway.
SIP Trunk	
Index/Profile/Status	Display current status for SIP profiles.

5.14.2 TR-069

This device supports TR-069 standard. It is very convenient for an administrator to manage a TR-069 device through an Auto Configuration Server, e.g., VigorACS.

```
System Maintenance >> TR-069 Setting
```

ACS Server On	Internet 💌
ACS Server	
URL	
Username	
Password	
CPE Client 〇 Enable ④ Disable	3
URL	http://172.16.3.229:8069/cwm/CRN.html
Port	8069
Username	vigor
Password	•••••
dic Inform Settings	
🔘 Disable	
💿 Enable	
Interval Time	900 second(s)
	ОК
Server On	Choose the interface for the router connecting

ACS Server On



ACS Server	URL/Username/Password – Such data must be typed according to the ACS (Auto Configuration Server) you want to link. Please refer to Auto Configuration Server user's manual for detailed information.
CPE Client	It is not necessary for you to type them. Such information is useful for Auto Configuration Server. Enable/Disable – Sometimes, port conflict might be occurred. To solve such problem, you might want to change port number for CPE. Please click Enable and change the port number.
Periodic Inform Settings	The default setting is Enable . Please set interval time or schedule time for the router to send notification to CPE. Or click Disable to close the mechanism of notification.

5.14.3 Administrator Password

This page allows you to set new password.

System Maintenance >> Administrator Password Setup

Administrator Password	
Old Password	
New Password	
Confirm Password	
·	

OK

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

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

5.14.4 Configuration Backup

Backup the Configuration

Follow the steps below to backup your configuration.

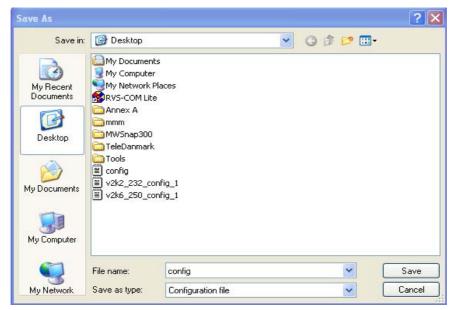
1. Go to **System Maintenance** >> **Configuration Backup**. The following windows will be popped-up, as shown below.

System Maint	enance >> Configuration Backup
Configuration	Backup / Restoration
Restoration	
	Select a configuration file. Browse Click Restore to upload the file. Restore
Backup	Click Backup to download current running configurations as a file.

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

File Dov	vnload 🗙
?	You are downloading the file: config.cfg from 192.168.1.1
	Would you like to open the file or save it to your computer?
	Open Save Cancel More Info
	Always ask before opening this type of file

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



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

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

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

Restore Configuration

System Maintenance >> Configuration Backup

System Maintenance >> SysLog / Mail Alert Setup

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

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

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

5.14.5 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 Access Setup		Mail Alert Setup	
🗹 Enable		🗹 Enable	Send a test e-mail
Server IP Address		SMTP Server	
Destination Port	514	Mail To	
Enable syslog message:		Return-Path	
🗹 Firewall Log		Authentication	
🗹 VPN Log		User Name	
🗹 User Access Log		Password	
🗹 Call Log		Enable E-Mail Alert:	
🗹 WAN Log		🔲 DoS Attack	
☑ Router/DSL inform	ation	IM-P2P	
	ОК	Clear Cancel	
nable (Syslog Acce	ess) Check '	Enable " to activate f	unction of syslog.

The IP address of the Syslog server.

Syslog Server IP

Destination Port	Assign a port for the Syslog protocol.
Enable syslog message	Check the box listed on this web page to send the corresponding message of firewall, VPN, User Access, Call, WAN, Router/DSL information to Syslog.
Enable (Alert Setup)	Check "Enable" to activate function of mail alert.
Send a test e-mail	Make a simple test for the e-mail address specified in this page. Please assign the mail address first and click this button to execute a test for verify the mail address is available or not.
SMTP Server	The IP address of the SMTP server.
Mail To	Assign a mail address for sending mails out.
Return-Path	Assign an e-mail address of another mailbox to accept all returned messages if fatal problems occur at the recipient mailbox. The e-mail address typed here also acts as the Sender address while Vigor sends out the alert e-mails.
Authentication	Check this box to activate this function while using e-mail application.
User Name	Type the user name for authentication.
Password	Type the password for authentication.
Enable E-mail Alert	Check the box to send alert message to the e-mail box while the modem detecting the item(s) you specify here.

Click **OK** to save these settings.

For viewing the Syslog, please do the following:

- 1. Just set your monitor PC's IP address in the field of Server IP Address
- 2. Install the Router Tools in the **Utility** within provided CD. After installation, click on the **Router Tools>>Syslog** from program menu.

🛅 Router Tools V3.5.1	🔹 🔊 About Router Tools	
	🐏 Firmware Upgrade Utility	
	🔟 Syslog	
	🔂 Uninstall Router Tools V3.5.1	
	🕘 Visit DrayTek Web Site	

3. From the Syslog screen, select the router you want to monitor. Be reminded that in **Network Information**, select the network adapter used to connect to the router. Otherwise, you won't succeed in retrieving information from the router.

ntrols		192.168.1.1 Vigor series	G	us ateway IP (Fixed) 	TX Packets	TX Rate
N Status TX Pac		RX Packets 1470		WAN IP (Fixed)	RX Packets	RX Rate
ewall Log VPN On Line Routers		ess Log Call Log	WAN Log Others Host Name:	Network Information Ne	t State	
IP Address	Mask	MAC	NIC Description:	SiS 900-Based F	CI Fast Ethernet Adapt	er - Packet St 🔽
192.168.1.1	255.255.2	00-50-7F-54-6	MAC Address:	00-11-D8-E4-58-CE	Default Geteway:	192.168.1.1
			IP Address: Subnet Mask:	192.168.1.10 ¥ 255.255.255.0	DHCP Server: Lease Obtained:	192.168.1.1 Mon Jan 22 01:28:23 2007
	Refresh		DNS Servers:	168.95.1.1	Lease Expires:	Thu Jan 25 01:28:23 2007
OSL Status						

5.14.6 Time and Date

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

```
System Maintenance >> Time and Date
```

Current System Time 2007 Jun	28 Thu 5 : 53 : 42
Time Setup	
🔘 Use Browser Time	
💿 Use Internet Time Client	
Time Protocol	NTP (RFC-1305) 💌
Server IP Address	pool.ntp.org
Time Zone	(GMT) Greenwich Mean Time : Dublin
Enable Daylight Saving	
Automatically Update Interval	30 min 💌
Current System Time	Click Inquire Time to get the current time.
Jse Browser Time	Select this option to use the browser time from the
	remote administrator PC host as router's system time
	remote administrator PC host as router's system time.
Jse Internet Time	remote administrator PC host as router's system time. Select to inquire time information from Time Server of the Internet using assigned protocol.
	Select to inquire time information from Time Server
'ime Protocol	Select to inquire time information from Time Server of the Internet using assigned protocol.
`ime Protocol erver IP Address	Select to inquire time information from Time Server of the Internet using assigned protocol. Select a time protocol.
Jse Internet Time Fime Protocol Server IP Address Fime Zone Automatically Update Interval	Select to inquire time information from Time Server of the Internet using assigned protocol. Select a time protocol. Type the IP address of the time server.



5.14.7 Management

This page allows you to manage the settings for access control, access list, port setup, and SMP setup. For example, as to management access control, the port number is used to send/receive SIP message for building a session. The default value is 5060 and this must match with the peer Registrar when making VoIP calls.

Management Setup				
Management Access	Control	Management Port Setup		
📃 Allow management f	rom the Internet	💿 User Define Ports	🔘 Default Ports	
FTP Server		Telnet Port	23 (Default: 23)	
🗹 HTTP Server		HTTP Port	80 (Default: 80)	
🗹 HTTPS Server		HTTPS Port	443 (Default: 443)	
🗹 Telnet Server		FTP Port		
SSH Server				
☑ Disable PING from th	e Internet	SSH Port	22 (Default: 22)	
Access List		SNMP Setup		
List IP	Subnet Mask	Enable SNMP Ager	it	
1	~	Get Community	public	
2	~	Set Community	private	
3	~	Manager Host IP		
		Trap Community	public	
		Notification Host IP		
		Trap Timeout	10 seconds	

System Maintenance >> Management

Allow management from the Internet	Enable the checkbox to allow system administrators to login from the Internet. There are several servers provided by the system to allow you managing the router from Internet. Check the box(es) to specify.
Disable PING from the Internet	Check the checkbox to reject all PING packets from the Internet. For security issue, this function is enabled by default.
Access List	You could specify that the system administrator can only login from a specific host or network defined in the list. A maximum of three IPs/subnet masks is allowed. List IP - Indicate an IP address allowed to login to the router. Subnet Mask - Represent a subnet mask allowed to login to the router.
Default Ports	Check to use standard port numbers for the Telnet and HTTP servers.
User Defined Ports	Check to specify user-defined port numbers for the Telnet, HTTP and FTP servers.
Enable SNMP Agent	Check it to enable this function.
Get Community	Set the name for getting community by typing a proper character. The default setting is public.

Set Community	Set community by typing a proper name. The default setting is private.
Manager Host IP	Set one host as the manager to execute SNMP function. Please type in IP address to specify certain host.
Trap Community	Set trap community by typing a proper name. The default setting is public.
Notification Host IP	Set the IP address of the host that will receive the trap community.
Trap Timeout	The default setting is 10 seconds.

5.14.8 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 			
	O Using factory default configuration			
	ОК			

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

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

5.14.9 Firmware Upgrade

Before upgrading your router firmware, you need to install the Router Tools. The **Firmware Upgrade Utility** is included in the tools. The following web page will guide you to upgrade firmware by using an example. Note that this example is running over Windows OS (Operating System).

Download the newest firmware from DrayTek's web site or FTP site. The DrayTek web site is www.draytek.com (or local DrayTek's web site) and FTP site is ftp.draytek.com.

Click System Maintenance>> Firmware Upgrade to launch the Firmware Upgrade Utility.

System Maintenance >> Firmware Upgrade

Web Firmware Upgrade	
----------------------	--

Click Upgrade to upload the file. Upgrade	Select a firmware file.				
Click Upgrade to upload the file. Upgrade			Browse		
	Click Upgrade to upload the file.	Upgrade			

TFTP Firmware Upgrade from LAN

Current Firmware Version: 3.5.3				
Firmware Upgrade Procedures:				
 Click "OK" to start the TFTP server. Open the Firmware Upgrade Utility or other 3-party TFTP client software. Check that the firmware filename is correct. Click "Upgrade" on the Firmware Upgrade Utility to start the upgrade. After the upgrade is compelete, the TFTP server will automatically stop running. 				
Do you want to upgrade firmware ? OK				

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

System Maintenance >> Firmware Upgrade



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

5.15 Diagnostics

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

Below shows the menu items for Diagnostics.

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

5.15.1 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

HEX Format:	
00 50 7F 00 00 00-00 0E A6 2A D5 A1-08 00	
45 00 00 30 89 C9 40 00-7F 06 80 01 C0 A8 01 0A	
41 36 EF 14 08 A4 07 47-33 20 94 D1 00 00 00 00	
70 02 FF FF B9 45 00 00-02 04 05 B4 01 01 04 02	
BE 9C 80 C9 9F A8 80 5B-3D D9 80 19 84 68 00 00	
00 00 00 00 00 00 00 00 00 00 00 00 00	
Decoded Format:	_
192.168.1.10,2212 -> 65.54.239.20,1863 Pr tcp HLen 20 TLen 48 -S Seq 857773265 Ack 0 Win 65535	

Decoded Format

It shows the source IP address (local), destination IP (remote) address, the protocol and length of the package.

Refresh

Click it to reload the page.

5.15.2 Routing Table

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

```
Diagnostics >> View Routing Table
Current Running Routing Table
Key: C - connected, S - static, R - RIP, * - default, ~ - private
* 0.0.0.0/ 0.0.0.0 via 172.16.3.4, WAN2
C~ 192.166.1.0/ 255.255.255.0.0 is directly connected, LAN
C 172.16.0.0/ 255.255.0.0 is directly connected, WAN2
```

Refresh

Click it to reload the page.

5.15.3 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.

Ethernet ARP Cache	Table	<u>Clear</u> <u>Refresh</u>
IP Address	MAC Address	2
192.168.1.10	00-0E-A6-2A-D5-A1	
172.16.2.240	00-05-5D-04-D2-C0	
172.16.2.194	00-50-7F-33-31-E9	
172.16.3.237	00-0C-6E-D0-CA-63	
172.16.3.222	00-50-7F-1A-59-11	
172.16.2.209	00-07-40-82-13-77	
172.16.3.181	00-50-7F-1A-58-CF	
172.16.2.238	00-50-7F-C0-29-1D	
172.16.2.62	00-50-7F-28-6E-21	
172.16.3.201	00-50-7F-1C-49-E5	
220.130.52.220	00-50-7F-C1-06-4D	
172.16.3.115	00-1A-92-92-E8-1D	
172.16.2.114	00-50-7F-C0-25-BD	
172.16.3.134	00-50-7F-33-31-E3	
172.16.2.229	00-50-7F-F0-00-5E	

Refresh

Click it to reload the page.

Clear

Click it to clear the whole table.

5.15.4 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

HCP se	erver: Running				^
Index	IP Address	MAC Address	Leased Time	HOST ID	
L	192.168.1.10	00-0E-16-21-D5-11	0:00:06.820	ok-lccgjyiy075u	
					~

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

5.15.5 NAT Sessions Table

Click **Diagnostics** and click **NAT Sessions Table** to open the setup page.

Diagnostics >> NAT Sessions Table

NAT Active Sessions Tabl	ions rable
--------------------------	------------

Private IP	:Port	#Pseudo Port	Peer IP	:Port	Interface	
92.168.1.10	2473	52059	207.46.106.51	1863		
92.168.1.10	2476	52062	207.46.26.253	7001	WAN2	
92.168.1.10	2477	52063	207.46.26.254	7001	WAN2	
92.168.1.10	2477	52063	207.46.26.254	9	WAN2	
92.168.1.10	2477	52063	207.46.26.253	7001	WAN2	
92.168.1.10	2478	52064	207.68.178.16	80	WAN2	
92.168.1.10	2479	52065	207.68.178.16	80	WAN2	

Private IP:Port

It indicates the source IP address and port of local PC.

#Pseudo Port

It indicates the temporary port of the router used for NAT.



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

5.15.6 Ping Diagnosis

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

which W		a LAN PC or you don't want n, please select "Unspecified ied 💙	
Ping Result	to: Host / IP Host / IP Gateway 1 Gateway 2 DNS	IP Address:	<u>Clear</u>

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: Unspecified Unspecified WAN1 WAN2			
Ping to	Use the drop down list to choose the destination that you want to ping.			
IP Address	Type in the IP address of the Host/IP that you want to ping.			
Run	Click this button to start the ping work. The result will be displayed on the screen.			
Clear	Click this link to remove the result on the window.			

5.15.7 Data Flow Monitor

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

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

Enable Data Flow Monitor Refresh Seconds: 10 Y Page: 1 Y Refresh Index IP Address TX rate(Kbps) RX rate(Kbps) v Action Sessions Current / Peak / Speed Current / Peak / Speed Current / Peak WAN1 0 / 0 / Auto 0 / 0 / Auto WAN2 192.168.5.27 1 / 0 / Auto 1 / 0 / Auto ---Total 1 / 0 / Auto 1 / 0 / Auto 2 / 19 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 + : residual bandwidth used Current/Peak are average. **Enable Data Flow** Check this box to enable this function. Monitor **Refresh Seconds** Use the drop down list to choose the time interval of refreshing data flow that will be done by the system automatically. 10 🕚 Refresh Seconds: RX 10 (Kbps) 15 30 Refresh Click this link to refresh this page manually. Index Display the number of the data flow. **IP Address** Display the IP address of the monitored device. TX rate (kbps) Display the transmission speed of the monitored device. RX rate (kbps) Display the receiving speed of the monitored device.

Diagnostics >> Data Flow Monitor

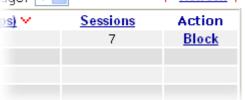
 Sessions
 Display the session number that you specified in Limit Session web page.

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

 age:
 1 v
 | Refresh |

 age:
 1 v
 | Refresh |

 age:
 1 v
 | Action



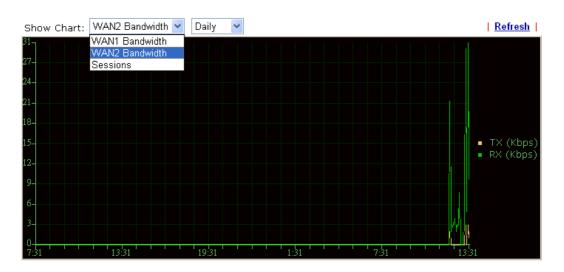
Unblock – the device with the IP address will be blocked in five minutes. The remaining time will be shown on the session column.

age:	1 🛩	<u>Refresh</u>
	Sessions	Action
	blocked / 298	<u>Unblock</u>

5.15.8 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.

Diagnostics >> Traffic Graph



5.15.9 Trace Route

Diagnostics >> 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: Unspecified Protocol: ICMP Host / IP Address: Result Clear
Trace through	Use the drop down list to choose the WAN interface that you wa to ping through or choose Unspecified to be determined by the router automatically. Unspecified WAN1 WAN2
Protocol Host/IP Addre Run Clear	Choose a protocol (ICMP or UDP) for such route.

VigorIPPBX 2820 Series User's Guide

This page is left blank.

Chapter 6: Trouble Shooting

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

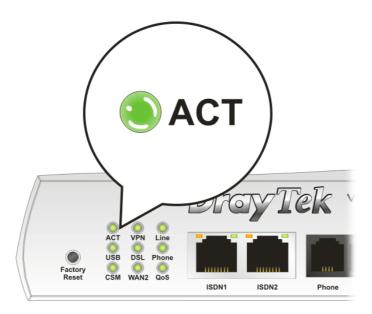
- Checking if the hardware status is OK or not.
- Checking if the network connection settings on your computer are OK or not.
- Pinging the router from your computer.
- Checking if the ISP settings are OK or not.
- Backing to factory default setting if necessary.

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

6.1 Checking If the Hardware Status Is OK or Not

Follow the steps below to verify the hardware status.

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



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

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

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

For Windows



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

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



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



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

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

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

Internet Protocol (TCP/IP) Properties							
General	Alternate Configuration						
this cap	n get IP settings assigned automatically if your network supports ability. Otherwise, you need to ask your network administrator for ropriate IP settings.						
⊙ <u>O</u> btain an IP address automatically							
	e the following IP address:						
IP ad	Idress:						
Subr	net mask:						
<u>D</u> efa	ult gateway:						
00	atain DNS server address automatically						
-OU:	e the following DNS server addresses:						
Prefe	arred DNS server:						
Alter	nate DNS server:						
	Ad <u>v</u> anced						
	OK Cancel						

For MacOs

- 1. Double click on the current used MacOs on the desktop.
- 2. Open the **Application** folder and get into **Network**.
- 3. On the **Network** screen, select **Using DHCP** from the drop down list of Configure IPv4.

			Netwo	ork			
ow All Disp	olays Sound	Network Sta	artup Disk				
	Loca	ition: Auto	matic			•	
	S	how: Built-	-in Ether	net		;	
_	TCP/IP	PPPoE	AppleTa	lk Proxie	es Eth	nernet	
Configu	ure IPv4: 🕕	Jsing DHCP			;		
IP A	Address: 1	92.168.1.10			(Renew DH	ICP Lease
Subne	et Mask: 2	55.255.255.	0	DHCP Clie	nt ID:		
	Router: 1	92.168.1.1				(If required	i)
DNS	Servers:						(Optional)
Search D	omains:						(Optional)
IPv6 A	Address: fe	80:0000:000	00:000:00	020a:95ff:f	e8d:72e	4	
	C	Configure IPv	/6)				?

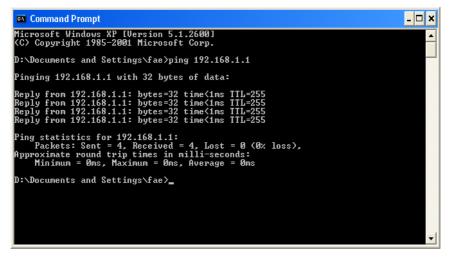
6.3 Pinging the Router from Your Computer

The default gateway IP address of the router is 192.168.1.1. For some reason, you might need to use "ping" command to check the link status of the router. **The most important thing is that the computer will receive a reply from 192.168.1.1.** If not, please check the IP address of your computer. We suggest you setting the network connection as **get IP automatically**. (Please refer to the section 6.2)

Please follow the steps below to ping the router correctly.

For Windows

- 1. Open the **Command** Prompt window (from **Start menu> Run**).
- 2. Type **command** (for Windows 95/98/ME) or **cmd** (for Windows NT/ 2000/XP/Vista). The DOS command dialog will appear.



- 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 302:24:18 on ttyp1 Welcome to Darwin!	8
Vigor10:~ draytek\$ ping 192.168.1.1	
PING 192.168.1.1 (192.168.1.1): 56 data bytes	
64 bytes from 192.168.1.1: icmp_seq=0 ttl=255 time=0.755 ms	
64 bytes from 192.168.1.1: icmp_seq=1 ttl=255 time=0.697 ms	
64 bytes from 192.168.1.1: icmp_seq=2 ttl=255 time=0.716 ms	
64 bytes from 192.168.1.1: icmp_seq=3 ttl=255 time=0.731 ms	
64 bytes from 192.168.1.1: icmp_seq=4 ttl=255 time=0.72 ms ^C	
192.168.1.1 ping statistics	
5 packets transmitted, 5 packets received, 0% packet loss round-trip min/avg/max = 0.697/0.723/0.755 ms Vigor10:~ draytek\$	

6.4 Checking If the ISP Settings are OK or Not

Click **WAN>> Internet Access** and then check whether the ISP settings are set correctly. Click WAN1 or WAN2 link to review the settings that you configured previously.

WAN >> Internet Access

Internet Access								
Index	Display Name	Physical Mode	Config Information					
WAN1		ADSL	Channel: 1, VPI: 0, VCI: 33, Protocol: PPPoE/LLC/SNAP, Modulation: Multimode, Dynamic IP					
WAN2		Ethernet	IP Address:172.16.3.229, Subnet Mask:255.255.0.0, Gateway IP:172.16.3.4					

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

PPPoE / PPPoA	MPoA (RFC1	483/2684)
🔘 Enable 🛛 💿 Dis	able	ISP Access Setup
		Username
DSL Modem Settings Multi-PVC channel	Channel 1	Password
VPI	8	PPP Authentication PAP or CHAP v Idle Timeout -1 second(s)
VCI Encapsulating Type	35	IP Address From ISP WAN IP Alias
Protocol Modulation	PPPoA V Multimode	Fixed IP O Yes No (Dynamic IP) Fixed IP Address
PPPoE Pass-through For Wired LAN For Wireless LAN		 Default MAC Address Specify a MAC Address MAC Address: 00 .50 .7F .94 .E7 .81
ISDN Dial Backup Setu Dial Backup Mode	P None	Index(1-15) in <u>Schedule</u> Setup: =>,,,,
WAN Connection Dete Mode	ction ARP Detect 💌	-
Ping IP TTL:		

For MPoA Users

1. Check if the **Enable** option is selected.

PPPoE / PPPoA	MPoA (RFC)	1483/2684)	
💿 Enable 🔘 Dis	able	WAN IP Network Settin	gs WAN IP Alias
		Obtain an IP address	s automatically
DSL Modem Settings	a	Router Name	
Multi-PVC channel	Channel 2	Domain Name	
Encapsulation			
148	3 Bridged IP LLC		
VPI	8	Specify an IP address	
VCI	88	IP Address	172.16.3.229
Modulation	Multimode 🗸	Subnet Mask	255.255.0.0
	Multimode	Gateway IP Address	172.16.3.4
ISDN Dial Backup Setu	ıp		
Dial Backup Mode	None 😽	Oefault MAC Address	
		Specify a MAC Addrese	SS
WAN Connection Dete	ection	MAC Address: 00 .50	.7F 94 .E7 .81
Mode	ARP Detect 🛩	MAC Address. 00 1.00	
Ping IP		DNS Server IP Address	
TTL:		Primary IP Address	
		Secondary IP Address	
RIP Protocol			
Enable RIP		_	
Bridge Mode			
📃 Enable Bridge Mode			

2. Check if **DSL Modem Settings** is set appropriately.

Check if **IP Address, Subnet Mask** and **Gateway** are set correctly (must identify with the values from your ISP) if you choose **Specify an IP address**.

For 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 2					
PPPoE	Stati	ic or Dynamic IP	PPTP/L2TP		
Inable O Disable		WAN IP Network Se	ttings WAN IP Alias		
		O Obtain an IP address automatically			
	ackup Setup		Router Name	*	
Dial Backup Mode N		None	Domain Name	*	
Keep WAN	Connection		* : Required for son	ne ISPs	
📃 Enable P	ING to keep a	alive	Specify an IP ad	dress	
PING to the	IP		IP Address	172.16.3.229	
PING Interva	al	0 minute(s)	Subnet Mask	255.255.0.0	
WAN Conne	ection Detec	tion	Gateway IP Address	172.16.3.4	
Mode		ARP Detect 🛩	Default MAC Addr		
Ping IP			 Specify a MAC Add 		
TTL:				.50 .7F 94 .E7 .82	
RIP Protoco	bl				
Enable RIP			DNS Server IP Addr	ess	
			Primary IP Address		
			Secondary IP Address	5	
		OK	Cancel		
		SIL	Janoor		

WAN >> Internet Access

For PPTP Users

1. Check if the **Enable** option for **PPTP** Link is selected.

WAN >> Internet Access

PPPoE	Stati	c <mark>or Dyna</mark> r	nic IP	PPTP/L2TP	
🔿 Enabl	e PPTP 🔘 En	able L2TP	Oisable	PPP Setup	
Server Addre	ess			PPP Authentication	PAP or CHAP
Specify Gateway IP Address				Idle Timeout	-1 second(s)
				IP Address Assign WAN IP Alias	ment Method (IPCP)
ISP Access	Setup			Fixed IP: O Yes	No (Dynamic IP)
Username				Fixed IP Address	
Password				WAN IP Network Se	ettings
Index(1-15)	in <u>Schedule</u>	Setup:		💿 Obtain an IP add	dress automatically
=>	, ,	,		Specify an IP ad	ldress
ISDN Dial B	ackup Setup			IP Address	
Dial Backup	Mode	None	~	Subnet Mask	

2. Check if **PPTP Server, Username, Password** and **WAN IP address** are set correctly (must identify with the values from your ISP).

6.5 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 Vigor2820. 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 Vigor2820.

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.

🕼 DrayTek Syslog					
Controls	I92.168.1.1 DrayTek Vig RX Packets 3807	or 2820	V Status etway IP (Static) WAN IP (Static)	TX Packets 0 RX Packets 0	RX Rate 0 TX Rate 0
Fire Wall Log VPN Log	User Access Log Call Lo	WAN Log Ne	twork Infomation	Net State	
Time Apr 12 09:17:49 Apr 12 09:17:49	Vigor [3G]Modem Vigor WAN2 PPPc Vigor WAN2 PPPc Vigor [3G]Modem Vigor [3G]Modem Vigor [3G]Modem Vigor [3G]Modem Vigor WAN2 PPPc Vigor WAN2 PPPc Vigor [3G]Modem Vigor [3G]Modem	status:a1 20 00 00 0	10 00 02 00 03 00 (c021) ConfReq Id. S ID-0 S ID-0 0 00 02 00 02 00 10 00 02 00 02 00 R ID:0 O ID:0 '1X1&D2&C1\$0=0	entifier:0x03 ACCM: 0 entifier:0x00 MRU: 150	
ADSL Status Mode	State L	Ip Speed	Down Speed	SNR Margin	Loop Att

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 VigorIPPBX 2820. 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.

6.6 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

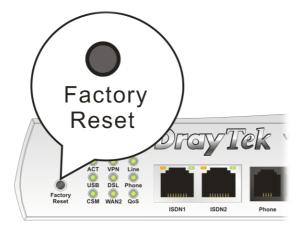
You can reset the router to factory default via Web page.

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.

System Maintenance >> Reboot System			
Reboot System			
	Do you want to reboot your router ?		
	Osing current configuration		
	O Using factory default configuration		
	OK		

Hardware Reset

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



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

6.7 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.

Appendix: Hardware Specifications

Temperature	Operating : 0°C ~ 45°C
	Storage : $-25^{\circ}C \sim 70^{\circ}C$
Humidity	10% ~ 90% (non-condensing)
Max. Power Consumption	10 Watt
Dimension	L241 * W165 * H44 (mm)
Power	DC 12V ~ 15V