

Vigor3100 Series G.SHDSL Security Router



Your reliable networking solutions partner

User's Guide

Vigor 3100 Series G.SHDSL Security Router User's Guide

Version: 2.01 Date: 23/12/2009



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 and Explorer are trademarks of Microsoft Corp. Apple and Mac OS are registered trademarks of Apple Computer Inc. Other products may be trademarks or registered trademarks of their respective manufacturers. 	
Safety Instruction	s 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.

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

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

http://www.draytek.com

Warranty

European Community Declarations

Manufacturer: DrayTek Corp.

Address:No. 26, Fu Shing Road, HuKou Township, HsinChu Industrial Park, Hsin-Chu, Taiwan 303Product:Vigor3100 Series G.SHDSL Routers

DrayTek Corp. declares that Vigor3100 series of routers are in compliance with the following essential requirements and other relevant provisions of R&TTE Directive 1999/5/EEC.

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

The product conforms to the requirements of Low Voltage (LVD) Directive 73/23/EEC by complying with the requirements set forth in EN60950-1.

The *Vigor3100G* is designed for the WLAN 2.4GHz network throughout EC region, Switzerland, and the restrictions of France.

Regulatory Information

Federal Communication Commission Interference Statement

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the 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 POTS and 2.4GHz WLAN network throughout the EC region and Switzerland with restrictions in France. Please see the user manual for the applicable networks on your product.



Table of Contents



Preface	1
1.1 Panel Description	2
1.1.1 Vigor3100	
1.1.2 Vigor3100G 1.1.3 Vigor3100i	
1.1.1 Vigor3100 1.1.2 Vigor3100G 1.1.3 Vigor3100i 1.1.4 Vigor3100V 1.1.5 Vigor3120	5 6
1.2 Hardware Installation	
1.2.1 For Vigor3100/Vigor3100G/Vigor3100V/Vigor3100i 1.2.2 Hardware Installation for Vigor3120 1.2.3 Pin Definition for Flat Module Cable	
1.3 Rack Mount Instruction	10
1.4 Printer Installation	11



Configuring Basic Settings	17
2.1 Changing Password	17
2.2 Quick Start Wizard	19
2.2.1 Adjusting Protocol/Encapsulation	19
2.2.1 Adjusting Protocol/Encapsulation 2.2.2 PPPoE/PPPoA	20
2.2.3 Bridged IP 2.2.4 Routed IP	21
2.2.4 Routed IP	22
2.3 Selecting Correct Annex Type	23
2.4 Online Status	24
2.5 Saving Configuration	25



Advanced Web Configuration	27
3.1 Internet Access	27
3.1.1 Basics of Internet Protocol (IP) Network 3.1.2 PPPoE/PPPoA	
3.1.3 MPoA 3.1.4 Multi-PVCs 3.1.5 DSL Settings	35
3.2 LAN	38
 3.2.1 Basics of LAN 3.2.2 General Setup 3.2.3 Static Route	40 42 45
3.3 NAT	

3.3.1 Port Redirection 3.3.2 DMZ Host 3.3.3 Open Ports	50
3.4 Firewall	
3.4.1 Basics for Firewall 3.4.2 General Setup 3.4.3 Filter Setup 3.4.4 IM Blocking	57 58
3.4.5 P2P Blocking 3.4.6 DoS Defense 3.4.7 URL Content Filter 3.4.8 Web Content Filter	62 63 66
3.5 Bandwidth Management	69
3.5.1 Sessions Limit 3.5.2 Bandwidth Limit 3.5.3 Quality of Service	70
3.6 Applications	76
3.6.1 Dynamic DNS 3.6.2 Schedule 3.6.3 RADIUS	77
3.6.4 UPnP 3.6.5 Wake on LAN	
3.7 VPN and Remote Access	
3.7.1 Remote Access Control	83
3.7.2 PPP General Setup 3.7.3 IPSec General Setup 3.7.4 IPSec Peer Identity	85 86
3.7.5 Remote Dial-In User 3.7.6 LAN to LAN 3.7.7 Connection Management	90
3.8 Certificate Management	98
3.8.1 Local Certificate 3.8.2 Trusted CA Certificate	
3.9 VoIP (for V model only)	
3.9.1 DialPlan 3.9.2 SIP Accounts 3.9.3 Phone Settings	. 104
3.9.4 Status	
3.10 ISDN (for <i>i</i> model only)	
3.10.1 General Setup 3.10.2 Dialing to a Single ISP	. 115
3.10.3 Dialing to Dual ISPs 3.10.4 Virtual TA 3.10.5 Call Control	. 116
3.11 Wireless LAN (for G model only)	
 3.11.1 Basic Concepts 3.11.2 General Setup 3.11.3 Security 3.11.4 Access Control 3.11.5 WDS 	. 124 . 126 . 128
3.11.6 AP Discovery 3.11.7 Station List	



3.11.8 Station Rate Control	134
3.12 VLAN	134
3.12.1 Wired VLAN 3.12.2 Wireless VLAN 3.12.3 VLAN Cross Setup	135 138
3.12.4 Wireless Rate Control	-
3.13 System Maintenance	140
 3.13.1 System Status. 3.13.2 Administrator Password. 3.13.3 Configuration Backup	141 142 144
 3.13.5 Time and Date 3.13.6 Management 3.13.7 Reboot System	146 147
3.14 Diagnostics	148
3.14.1 WAN Connection 3.14.2 Dial-out Trigger 3.14.3 Routing Table	148 149
3.14.4 ARP Cache Table 3.14.5 DHCP Table 3.14.6 NAT Sessions Table	150 150
3.14.7 Wireless VLAN Online Station Table 3.14.8 Data Flow Monitor 3.14.9 Traffic Graph	151
3.14.10 Ping Diagnosis 3.14.11 Trace Route	154



Application and Examples	.155
4.1 Create a LAN-to-LAN connection between remote office and headquarter	155
4.2 Create a remote dial-in user connection between the teleworker and headquarter	162
4.3 QoS Setting Example	166
4.4 LAN – Created by Using NAT	168
4.5 Calling Scenario for VoIP function	170
4.5.1 Calling via SIP Sever 4.5.2 Peer-to-Peer Calling	170 172
4.6 Upgrade Firmware for Your Router	173
4.7 Request a certificate from a CA server on Windows CA Server	176
4.8 Request a CA Certificate and Set as Trusted on Windows CA Server	179



Trouble Shooting	183
5.1 Checking If the Hardware Status Is OK or Not	. 183
5.2 Checking If the Network Connection Settings on Your Computer Is OK or Not	. 184
5.3 Pinging the Router from Your Computer	. 186

5.4 Checking If the ISP Settings are OK or Not	187
5.5 Problems for 3G Network Connection	188
5.6 Backing to Factory Default Setting If Necessary	189
5.7 Contacting Your Dealer	190



Targeting requirement for residential, SOHO (Small Office and Home Office) and business users, the Vigor3100 series are G.SHDSL enabled integrated access device. G.SHDSL is going to be a prevailing standard for business and residential SDSL (Symmetrical DSL) in the rapidly growing worldwide marketplace. Vigor3100/G provides data upto 2.3Mbps through one single pair; Vigor3120 offers data upto 4.6Mbps through two pairs.

The Vigor3100G models are embedded 802.11g compliant wireless module which provides wireless LAN access with line rate as much as 108Mbps with Super GTM. The Vigor3100G models feature WPA2 (802.11i), wireless LAN isolation, and WDS (Wireless Distribution System).

A Virtual Private Network (VPN) is an extension of a private network that encompasses links across shared or public networks like an Intranet. A VPN enables you to send data between two computers across a shared public Internet network in a manner that emulates the properties of a point-to-point private link. The DrayTek Vigor3100 series VPN router supports Internet-industry standards technology to provide customers with open, interoperable VPN solutions such as X.509, DHCP over Internet Protocol Security (IPSec) up to 32 tunnels, and Point-to-Point Tunneling Protocol (PPTP).

1.1 Panel Description

1.1.1 Vigor3100

Front Panel

Dray Vigor3 G.SHDSL Se	/	QoS	LINK © © © © 0 100 © © © 0 FDX © © © 0 1 2 3 4 RST DSL 0 LAN PRN
LED		Status	Explanation
ACT (A	ctivity)	Blinking	The router is powered on and running properly.
VPN		On	The VPN tunnel is launched.
QoS		On	The QoS function is active.
PRN		On	The USB interface printer is ready.
DSL		On	The G.SHDSL line is connected
LAN	LNK	Blinking	It means that Ethernet packets are transmitting.
(1, 2, 3, 4)	100	On	It means that a normal 100Mbps connection is through its corresponding port.
		Off	It means that a normal 10Mbps connection is through its corresponding port.
	FDX	On	It means a full duplex connection.
		Off	It means a half duplex connection.
		Blinking	It means that a packet collision happens.
Interfac	e	Description	
RST (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.	
DSL Connect the G.SHDSL line to access the Inter		HDSL line to access the Internet.	
LAN (1,2,3,4) Connect to the local networked devices.		cal networked devices.	
PRN Connect to the USB printer.		SB printer.	

Rear Panel



Interface	Description		
-	Connecter for a power cord with 100-240 VAC (inlet).		
 0	Power Switch. "1" is ON; "0" is OFF.		

1.1.2 Vigor3100G

Front Panel

Dray Vigor3 G.SHDSL Se	/	Gact Gvpn Ggos Oprn Gwlan	DSL LNK © © © © © 100 © © © © © 1 FDX © © © © © 1 1 2 3 4 RST DSL 1 LAN PRN	
LED		Status	Explanation	
ACT (Activity	y)	Blinking	The router is powered on and running properly.	
VPN		On	The VPN tunnel is launched.	
QoS		On	The QoS function is active.	
PRN		On	The USB interface printer is ready.	
WLAN		On	The wireless LAN function is enabled.	
		Blinking	Wireless traffic goes through.	
DSL On		On	The G.SHDSL line is connected.	
	LNK	Blinking	It means that Ethernet packets are transmitting.	
LAN (1, 2, 3,	100	On	It means that a normal 100Mbps connection is through its corresponding port.	
4)		Off	It means that a normal 10Mbps connection is through its corresponding port.	
	FDX	On	It means a full duplex connection.	
		Off	It means a half duplex connection.	
		Blinking	It means that a packet collision happens.	
Interfac	e	Description		
RST (Factory Reset)		Usage: Turn o keep for more blink rapidly	efault settings. on the router (ACT LED is blinking). Press the hole and e than 5 seconds. When you see the ACT LED begins to than usual, release the button. Then the router will restart ory default configuration.	
DSL		Connect the C	G.SHDSL line to access the Internet.	
LAN (1,	2,3,4)	Connect to th	e local networked devices.	
PRN		Connect to th	e USB printer.	

Rear Panel

Interface	Description
-	Connecter for a power cord with 100-240 VAC (inlet).
 0	Power Switch. "1" is ON; "0" is OFF.

1.1.3 Vigor3100i

Front Panel

Dray Te	<u>k</u>				
Vigor3100i G.SHDSL Security R	louter	SACT OVPN DSL LIK L SQ05 SISDN 100 S S OPRN FDX S S 1 2			
LED		Status	Explanation		
ACT (Activ	ity)	Blinking	The router is powered on and running properly.		
VPN		On	The VPN tunnel is launched.		
QoS		On	The QoS function is active.		
PRN		On	The USB interface printer is ready.		
ISDN		On	The ISDN service function is active.		
		Blinking	It means that data is transmitting.		
DSL		On	The G.SHDSL line is connected		
LAN	LNK	Blinking	It means that Ethernet packets are transmitting.		
(1, 2, 3, 4)	100	On	It means that a normal 100Mbps connection is through its corresponding port.		
		Off	It means that a normal 10Mbps connection is through its corresponding port.		
	FDX	On	It means a full duplex connection.		
		Off	It means a half duplex connection.		
		Blinking	It means that a packet collision happens.		
Interface		Description			
RST (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.			
ISDN		Connect the ISDN c	able.		
DSL		Connect the G.SHD	SL line to access the Internet.		
LAN (1,2,3,	(4)	Connect to the local	networked devices.		
PRN		Connect to the USB	printer.		

Rear Panel

Interface	Description
8	Connecter for a power cord with 100-240 VAC (inlet).
 0	Power Switch. "1" is ON; "0" is OFF.

1.1.4 Vigor3100V

Front Panel

Dray Tek				
Vigor3100V G.SHDSL Security Router			VoiP DSL LAN 0 0 © 2 100 © 0 © 0 © 1 © FDX © 0 © 0 NoIP DSL 1 LAN 9 VoiP DSL LAN PRN 1	
LED		Status	Explanation	
ACT B (Activity)		Blinking	The router is powered on and running properly.	
VPN		On	The VPN tunnel is launched.	
QoS		On	The QoS function is active.	
PRN		On	The USB interface printer is ready.	
VoIP (2,1)	On	The phone is off hook (the handset of phone is hanging).	
		Blinking	A phone call is incoming or on-line.	
DSL C		On	The G.SHDSL line is connected	
LAN	LNK	Blinking	It means that Ethernet packets are transmitting.	
(1, 2, 3, 4)	100	On	It means that a normal 100Mbps connection is through its corresponding port.	
		Off	It means that a normal 10Mbps connection is through its corresponding port.	
	FDX	On	It means a full duplex connection.	
		Off	It means a half duplex connection.	
		Blinking	It means that a packet collision happens.	
Interfa	ce	Description		
RST (Factory Reset)		Usage: Turn of for more than	efault settings. on the router (ACT LED is blinking). Press the hole and keep 5 seconds. When you see the ACT LED begins to blink rapidly lease the button. Then the router will restart with the factory guration.	
VoIP Connecters for		Connecters for	telephone set and analog phone with VoIP communication.	
DSL		Connect the C	G.SHDSL line to access the Internet.	
LAN (1,2,3,4)	Connect to the local networked devices.		
PRN		Connect to th	e USB printer.	

Rear Panel



Interface	Description
-	Connecter for a power cord with 100-240 VAC (inlet).
I 0	Power Switch. "1" is ON; "0" is OFF.

1.1.5 Vigor3120

Front Panel

Dray Vigor31	20	©act ©vpn ©Gds ©PRN	DS. LNK O O O O 100 O O O O FDX O O O FDX O O O O FDX O O FDX O O FDX O O FDX O O FDX O	
LED		Status	Explanation	
ACT (Activity	y)	Blinking	The router is powered on and running properly.	
VPN		On	The VPN tunnel is launched.	
QoS		On	The QoS function is active.	
PRN		On	The USB interface printer is ready.	
DSL		On	The G.SHDSL line is connected.	
	LNK	Blinking	It means that Ethernet packets are transmitting.	
LAN (1, 2, 3,	100	On	It means that a normal 100Mbps connection is through its corresponding port.	
4)		Off	It means that a normal 10Mbps connection is through its corresponding port.	
	FDX	On	It means a full duplex connection.	
		Off	It means a half duplex connection.	
		Blinking	It means that a packet collision happens.	
Interfac	е	Description		
RST (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.		
DSL		Connect the (G.SHDSL line to access the Internet.	
LAN (1-	-4)	Connecter for	r local networked devices.	
PRN		USB interfac	e for printer.	

Rear Panel



Interface	Description
	Connecter for a power cord with 100-240 VAC (inlet).
 0	Power Switch. "1" is ON; "0" is OFF.

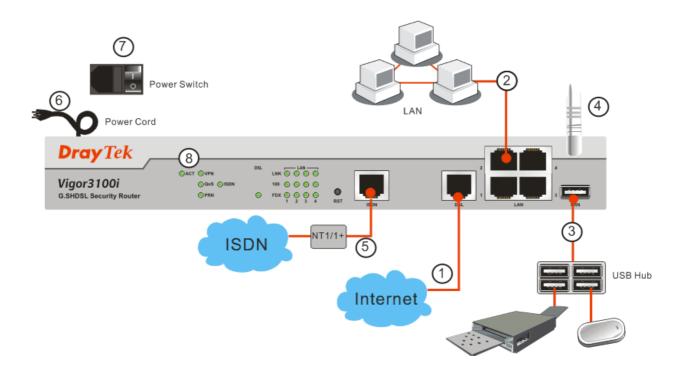
1.2 Hardware Installation

1.2.1 For Vigor3100/Vigor3100G/Vigor3100V/Vigor3100i

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

- 1. Connect the DSL port of the router to the wall outlet with a RJ-11 to RJ-45 (or RJ-45 to RJ-45) cable. For Vigor3120, please refer to 1.2.2.
- 2. Connect one port of 4-port switch to your computer with a RJ-45 cable.
- 3. Connect the printer/3G USB Modem to the router with the USB cable and connect the power cord. If you do not have a printer/3G USB Modem for using, skip this step.
- 4. Connect detachable antennas to the router for Vigor3100G.
- 5. Connect ISDN cable for Vigor3100i.
- 6. Connect one end of the power cord to the power port of the router. Connect the other end to the wall outlet of electricity.
- 7. Power on the router.
- 8. Check the ACT and DSL, LAN LEDs to assure network connections.

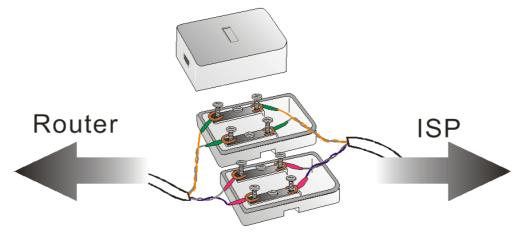
(For the detailed information of LED status, please refer to section 1.1.)



1.2.2 Hardware Installation for Vigor3120

Vigor3120 provides Flat Module Cable (RJ-45, 4x4) for bonding bandwidth for data transmission. Please apply two-pair of circuit from your ISP first for hardware connection.

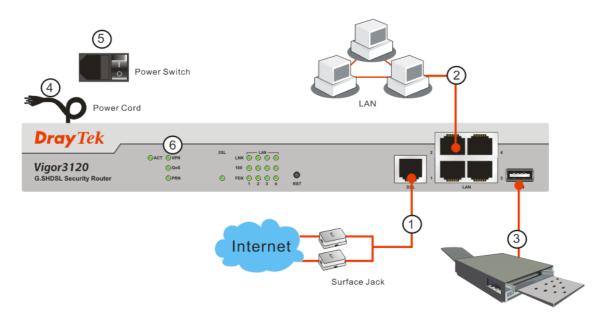
Then, open the cover of surface jack and use a screw driver to loosen the screws inside the surface jack. Notice that lines wrapped with same color tape mean one pair. Please connect them to one surface jack (that will be used to connect to DSL connector of the router). Use the same way to connect another pair of lines to another surface jack (that will be used to connect to ISP).



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

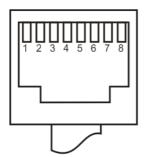
- 1. Connect the DSL port of the router to the wall outlet with a Flat Module Cable (RJ-45, 4x4).
- 2. Connect one port of 4-port switch to your computer with a RJ-45 cable.
- 3. Connect the printer to the router with the USB cable and connect the power cord. If you do not have a printer for using, skip this step.
- 4. Connect one end of the power cord to the power port of the router. Connect the other end to the wall outlet of electricity.
- 5. Power on the router.
- 6. Check the ACT and DSL, LAN LEDs to assure network connections.

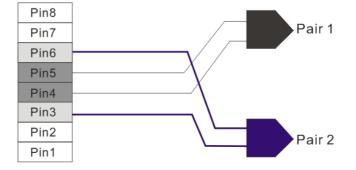
(For the detailed information of LED status, please refer to section 1.1.)



1.2.3 Pin Definition for Flat Module Cable

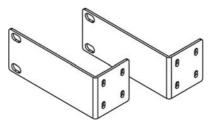
Below shows the pin definition of flat module cable. One pair is composed by Pin4 and Pin5. The other pair is composed by Pin3 and Pin6.



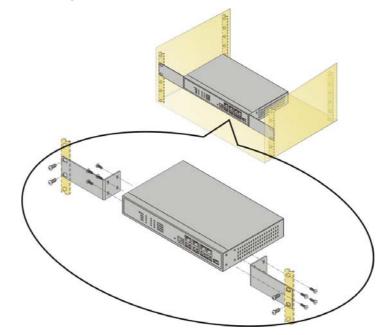


1.3 Rack Mount Instruction

The Vigor3100 series can be mounted on a rack by using standard brackets in a 19-inch rack or optional larger brackets on 23-inch rack (not included). The bracket for the racks are shown below.



Use brackets to set the Vigor router on the rack as shown below.

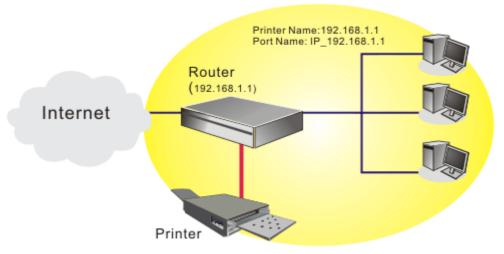


After the bracket installation, the Vigor router chassis can be installed in a rack by using four screws for each side of the rack.



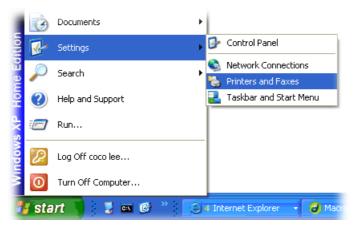
1.4 Printer Installation

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



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

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



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



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



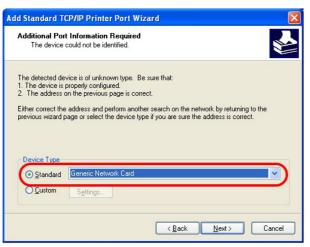
5. In this dialog, choose **Create a new port Type of port** and use the drop down list to select **Standard TCP/IP Port**. Click **Next**.

Add Printer Wizard		
Select a Printer Port Computers communicate w	with printers through ports.	Ś
Select the port you want yo new port.	our printer to use. If the port is not listed, you can creat	ea
OUse the following port:	LPT1: (Recommended Printer Port)	~
Note: Most computers The connector for this	use the LPT1. port to communicate with a local printer. port should look something like this:	
© <u>C</u> reate a new port: Type of port:	Standard TCP/IP Port	
	< <u>B</u> ack Next >	Cancel

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 P	Port Wizard
Add Port For which device do you want	to add a port?
Enter the Printer Name or IP ad	dress, 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.



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 Soft The manufacturer	are and model determine which printer software to	use.
	ufacturer and model of your printer. If your printe Disk. If your printer is not listed, consult your p er software.	
Manufacturer AST AT&T Brother	Printers Brother HL-1060 BR-Script2 Brother HL-1070 BR-Script2	
Buil Canon	Brother HL-1070	

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.

eneral Sha	ring Ports Advance	d Device Settings	
S Br	other HL-1070		
			_
Print to the for checked por		nts will print to the first free	
Port	Description	Printer	^
3.250	Standard TCP/IP Port	Epson Stylus COLOR 1160	
□ IP_1	Standard TCP/IP Port		
□ IP_1	Standard TCP/IP Port	HP LaserJet 1300	
	Standard TCP/IP Port		
	Standard TCP/IP Port		
	Standard TCP/IP Port		
LI PDF	Local Port	PDF995	~
Add P	or <u>t D</u> elet	e Port <u>C</u> onfigure Port.	
-			_
	directional support		
Enable pr	inter pooling		

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.

Port Settings	
Port 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>⊙</u> <u>L</u> PR
Raw Settings	
Port <u>N</u> umber: 91	100
LPR Settings	
Queue Name:	1
LPR Byte Counting Ena	bled
SNMP Status Enabled	
Community Name: pu	ublic
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.

About DrayTek Products Support Partn	ers Contact Us
ome > Support > FAQ	
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)	VoIP
07. Ways for firmware upgrade.	QoS
08. Why is SNMP removed in firmware 2.3.6 and above for Vigor2200 Series routers?	ISDN
09. I failed to upgrade Vigor Router's firmware from my Mac machine constantly, what should	Firewall / IP Filter
uos, maned to upgrade vigor Router's inmware rom my mac machine constantly, what should I do?	Printer Server
10. How to upgrade firmware of Vigor Router remotely ?	USB ISDN TA
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,	USB

FAQ - Printer Server

01. How do I configure LPR printing on Windows2000/XP ?

02. How do I configure LPR printing on Windows98/Me ?

03. How do I configure LPR printing on Linux boxes ?

04. Why there are some strange print-out when I try to print my documents through Vigor210 4P / 2300's print server?

05. What types of printers are compatible with Vigor router?

06. What are the limitations in the USB Printer Port of Vigor Router ?

07. What is the printing buffer size of Vigor Router ?

08. How do I configure LPR printing on Mac OSX ?

09. How do I configure LPR printing on My Windows Vista ?

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

This page is left blank.

Vigor3100 Series User's Guide

2 Configuring Basic Settings

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

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

2.1 Changing Password

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

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



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

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



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

Quick Start Wizard	System Status				
nternet Access	Model Name Firmware Version Build Date/Time	irmware Version		: Vigor3100 series : v2.8.1_RC2 : Wed Oct 24 14:40:3.50 2007	
AT irewall	DSL Firmware Ver	rsion	: R308_1 Annex A		
irewall andwidth Management					
pplications	LAN			WAN	
PN and Remote Access	MAC Address	: 00-50-7F-89-92-10		Link Status	: Disconnected
ertificate Management	1st IP Address			MAC Address	: 00-50-7F-89-92-11
oIP		: 255.255.255.0		Connection	: PPPoE
ystem Maintenance	DHCP Server	: Yes		IP Address	:
agnostics				Default Gateway DNS	: : 194.109.6.66
	VoIP				
	Port	: 1	2		
	SIP registrar				
	Account ID	: change me	e change_me		
All Disks Deserved	Register	:			
	Codec	1			
	In Calls	: 0	0		

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

Administrator Password Old Password	
New Password	
Retype New Password	
)K

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



Connect to 192.	168.1.1 🛛 🛛 🔀
	G.
Login to the Router	Web Configurator
User name:	2
Password:	••••
	Remember my password
	OK Cancel

2.2 Quick Start Wizard

If your Vigor router can be under an environment with high speed NAT, the configuration provide here can help you to deploy and use the router quickly. There are two phases of quick setup, one is protocol/encapsulation configuration; and the other is LAN configuration.

2.2.1 Adjusting Protocol/Encapsulation

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

Annex Type	A 🕶
VPI	0 Auto detect
VCI	33
Protocol / Encapsulation	PPPoe LLC/SNAP
Fixed IP IP Address Subnet Mask	PPPoE LLC/SNAP PPPoE VC MUX PPPoA LLC/SNAP PPPoA VC MUX 1483 Bridged IP LLC 1483 Routed IP LLC 1483 Bridged IP VC-Mux
Default Gateway Primary DNS Second DNS	1483 Routed IP VC-Mux (IPoA) 1483 Bridged IP (IPoE)

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

Annex Type	Choose \mathbf{A} or \mathbf{B} based on the model of the router you have.		
VPI	Stands for Virtual Path Identifier . It is an 8-bit header inside each ATM cell that indicates where the cell should be routed. The ATM, is a method of sending data in small packets of fixed sizes. It is used for transferring data to client computers.		
VCI	Stands for Virtual Channel Identifier. It is a 16-bit field inside ATM cell's header that indicates the cell's next destination as it		

	travels through the network. A virtual channel is a logical connection between two end devices on the network.
Protocol/Encapsulation	Select an IP mode for this WAN interface. There are several available modes for Internet access such as PPPoE , PPPoA , Bridged IP and Routed IP .
Fixed IP	Click Yes to specify a fixed IP for the router. Otherwise, click No (Dynamic IP) to allow the router choosing a dynamic IP. If you choose No , the following IP Address, Subnet Mask and Default Gateway will not be changed.
IP Address	Assign a private IP address for the protocol that you select.
Subnet Mask	Assign a subnet mask value for the protocol of Routed IP and Bridged IP .
Default Gateway	Assign a private IP address to the gateway for the protocol of Routed IP and Bridged IP .
Primary DNS	Assign a private IP address to the primary DNS.
Second DNS	Assign a private IP address to the secondary DNS.

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

PPPoE or PPPoA is used for most of DSL modem users. All local users can share one PPPoE or PPPoA 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** or **PPPoA** connection, please select **PPPoE** or **PPPoA** for this router. The following page will be shown: 3. Set PPPoE / PPPoA

ISP Name	
User Name	
Password	
Confirm Password	
🔲 Always On	
Idle Timeout	180 Seconds
	< Back Next > Finish Cancel

ISP Name	Assign a specific name for ISP requirement.
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.
Always On	Check this box to allow the router connecting to Internet forever.



Idle Timeout

Type in the value (unit is second) as the idle timeout of the connection.

Click Next for viewing summary of such connection.

4. Please confirm your settings:	
Annex Type	: A
VPI	: 0
VCI	: 33
Protocol / Encapsulation	: PPPoE / LLC
Fixed IP	: No
Primary DNS	:
Secondary DNS	:
Always On	: No
Idle Timeout	: 180 Seconds
	< Back Next > Finish Cancel

Click **Finish.** The online status of this protocol will be shown as below.

System Statu	5					Syst	em Uptime:1:52:54
LAN Status		Prima	ry DNS: 194	.109.6.66	S	econdary	DNS: 194.98.0.1
IP Address		TX Packets	RX F	Packets			
192.168.1.1		920	842				
WAN Status		I	GW IP Addr:				Dial PPPoA
Mode	IP Addres	ss TX	Packets	TX Rate	RX Packe	ts RX Ra	ate Up Time
		0		0	0	0	00:00:00
ADSL Informa	tion (ADSL Firmwar	e Version: P	R3.0.1)			
ATM Statisti	cs TX Blo	ocks	RX Blocks		Corrected	Blocks U	ncorrected Blocks
	0		0	(0	0	
ADSL Status	Mode	State	Up Spee	d Dov	vn Speed	SNR Marg	in Loop Att.
	G.991.2	HANDSHAKE	0	0		0.0	0.0

2.2.3 Bridged IP

Online Status

Click **1483 Bridged IP** as the protocol. Type in all the information that your ISP provides for this protocol. 2. Connect to Internet

Annex Type VPI VCI	A V D Auto detect
Protocol / Encapsulation	1483 Bridged IP LLC
Fixed IP	◯Yes ⊙No(Dynamic IP)
IP Address	
Subnet Mask	
Default Gateway	
Primary DNS	
Second DNS	
Second DNS	< Back Next > Finish

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

4. Please confirm your settings:	
Annex Type	: A
VPI	: 0
VCI	: 34
Protocol / Encapsulation	: 1483 Bridge LLC
Fixed IP	: Yes
IP Address	: 192.168.1.16
Subnet Mask	: 255.255.0.0
Default Gateway	: 192.168.1.1
Primary DNS	:
Secondary DNS	:
	Course Martin Course
	< Back Next > Finish Cancel

Click **Finish.** The online status of this protocol will be shown as below.

System Statu	s						Systen	n Uptime:0:0:5
LAN Status		Prim	ary DNS: 194	4.109.6.66	8	Seconda	ary DNS	: 194.98.0.1
IP Address		TX Packet	s RX I	Packets				
192.168.1.1		416	352					
WAN Status			GW IP Addr	:				
Mode	IP Addre	ess	TX Packets	TX Rate	RX Packe	ets R	X Rate	Up Time
		I	D	0	0	0		00:00:00
ADSL Informa	tion	(ADSL Firmw	are Version: P	R3.0.1)				
ATM Statisti	cs TX Bl	ocks	RX Blocks		Corrected	Blocks	Uncor	rected Blocks
	0		0	C)		0	
ADSL Status	Mode	State	Up Spee	d Dov	vn Speed	SNR M	argin	Loop Att.
	G.991.2	HANDSHAK	E 0	0		0.0		0.0

2.2.4 Routed IP

Online Status

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

Annex Type	A 💌
VPI	0 Auto detect
VCI	34
Protocol / Encapsulation	1483 Routed IP LLC
Fixed IP	⊙ Yes 🔘 No(Dynamic IP)
IP Address	192.168.1.16
Subnet Mask	255.255.0.0
Default Gateway	192.168.1.1
Primary DNS	
Second DNS	

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

I. Please confirm your settings:					
Annex Type	: A				
VPI	: 0				
VCI	: 34				
Protocol / Encapsulation	: 1483 Route LLC				
Fixed IP	: Yes				
IP Address	: 192.168.1.16				
Subnet Mask	: 255.255.0.0				
Default Gateway	: 192.168.1.1				
Primary DNS	:				
Secondary DNS	:				
	<pre>< Back Next > Finish Cancel</pre>				

Click **Finish.** The online status of this protocol will be shown as below.

System Status	5					Sy	stem	Uptime:0:0:1
LAN Status		Prim	ary DNS: 19	4.109.6.66	S	econdary	DNS:	: 194.98.0.1
IP Address		TX Packet	s RX	Packets				
192.168.1.1		109	88					
WAN Status			GW IP Add	r:				
Mode	IP Addre	ss	TX Packets	TX Rate	RX Packe	ets RX F	Rate	Up Time
		1	D	0	0	0		00:00:00
ADSL Informa	tion (ADSL Firmw	are Version:	R3.0.1)				
ATM Statistic	s TX Bl	ocks	RX Blocks	5 (Corrected	Blocks L	Incor	rected Blocks
	0		0	C)	0)	
ADSL Status	Mode	State	Up Spe	ed Dov	vn Speed	SNR Mar	gin	Loop Att.
	G.991.2	HANDSHAK	E 0	0		0.0		0.0

2.3 Selecting Correct Annex Type

Internet Access >> DSL Setting

Online Status

After finishing **Quick Start Wizard**, please go to **Internet Access** and choose **DSL Settings** for making sure you have chosen correct annex type for your router.

 AdaptiveRate 	MaxRate : 2312 💌 MinRate : 72 💌
○ FixedRate	2312 💌
Terminal Type	CPE 🗸
AnnexType	A 🗸

Use the drop down list of **Annex Type** for choosing A or B according to the annex type of your router. If you do not choose the correct one, you will not access into Internet. This is very important.



2.4 Online Status

Now, check the online status for your router. 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** or **PPPoA** as the protocol, you will find out a button of **Dial PPPoE** or **Dial PPPoE** in the Online Status web page.

Online Status

LAN Status	Primary DNS: 194.10			94.109.6.66	.66 Secondary DNS: 19			: 194.98.0.1
IP Address		TX Packet	s RX	RX Packets				
192,168,1,1		4012	16	426				
WAN Status			GW IP Add	r:				Dial PPPoE
Mode	IP Addre	ss 1	X Packets	TX Rate	RX Packe	ts RX R	late	Up Time
PPPoE		0)	0	0	0		00:00:00
SDSL Informa	tion (SDSL Firmw	are Version:	R308_1)				
ATM Statisti	cs TX Bl	ocks	RX Block	5	Corrected	Blocks L	Incor	rected Blocks
	0		0		0	C)	
SDSL Status	Mode	State	Up Spe	ed Do	wn Speed	SNR Mar	gin	Loop Att.
	G.991.2	HANDSHAK	FΩ	n		0.0		0.0

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

Secondary DNS	Displays the assigned IP address of the secondary DNS.
LAN Status	
IP Address	Displays the IP address of the LAN interface.
TX Packets	Displays the total transmitted packets at the LAN interface.
RX Packets	Displays the total number of received packets at the LAN interface.
WAN Status	
Mode	Displays the connection mode.
GW IP Addr	Displays the assigned IP address of the default gateway.
IP Address	Displays the IP address of the WAN interface.
TX Packets	Displays the total transmitted packets at the WAN interface.
TX Rate	Displays the speed of transmitted packets at the WAN interface.
RX Packets	Displays the total number of received packets at the WAN interface.
RX Rate	Displays the speed of received packets at the WAN interface.
Up Time	Displays the total system uptime of the interface.
SDSL Information	Displays the firmware version of this router.

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.



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.

Vigor3100 Series User's Guide

3Advanced Web Configuration

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

3.1 Internet Access

3.1.1 Basics of Internet Protocol (IP) Network

IP means Internet Protocol. Every device in an IP-based Network including routers, print server, and host PCs, needs an IP address to identify its location on the network. To avoid address conflicts, IP addresses are publicly registered with the Network Information Centre (NIC). Having a unique IP address is mandatory for those devices participated in the public network but not in the private TCP/IP local area networks (LANs), such as host PCs under the management of a router since they do not need to be accessed by the public. Hence, the NIC has reserved certain addresses that will never be registered publicly. These are known as *private* IP addresses, and are listed in the following ranges: 18

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

What are Public IP Address and Private IP Address

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

Get Your Public IP Address from ISP

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

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



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

Network Connection by 3G USB Modem

For 3G mobile communication through Access Point is popular more and more, Vigor3100 series adds the function of 3G network connection for such purpose. By connecting 3G USB Modem to the USB port of Vigor3100, it can support HSDPA/UMTS/EDGE/GPRS/GSM and the future 3G standard (HSUPA, etc). Vigor3100 with 3G USB Modem allows you to receive 3G signals at any place such as your car or certain location holding outdoor activity and share the bandwidth for using by more people. Users can use four LAN ports on the router to access Internet. Also, they can access Internet via SuperG wireless function of Vigor3100, and enjoy the powerful firewall, bandwidth management, VPN, VoIP features of Vigor3100 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.

3.1.2 PPPoE/PPPoA

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

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

Vigor3100 Series User's Guide



PPPoE/PPPoA Client 💿 Enable 🔘 Disable	ISP Access Setup	
	- ISP Name	
DSL Modem Settings	Username	
Multi-PVC channel Channel 1 🛛 👻	Password	
VPI O		
VCI 33	PPP Authentication PAP or CHAP 💌	
Encapsulating Type LLC/SNAP V	Always On	
	Idle Timeout 180 second(s)	
Protocol PPPoE 💙	IP Address From ISP WAN IP Alias	
PPPoE Pass-through	Fixed IP 🛛 🔘 Yes 💿 No (Dynamic IP)	
For Wired LAN	Fixed IP Address	
WAN Backup Setup	* : Required for some ISPs	
3G USB Modem	Oefault MAC Address	
Dial Backup Mode 🛛 Always On 🛛 👻	Specify a MAC Address	
Go to <u>3G USB Modem Backup</u> Setup	MAC Address :	
ISDN	00 · 50 · 7F :81 · 83 · 09	
Dial Backup Mode 🛛 None 🛛 👻		
	Index(1-15) in <u>Schedule</u> Setup:	

PPPoE/PPPoA Client Click Enable for activating this function. If you click Disable, this function will be closed and all the settings that you adjusted in this page will be invalid. **DSL Modem Settings** Set up the DSL parameters required by your ISP. These are vital for building DSL connection to your ISP. Multi-PVC channel – The selections displayed here are determined by the page of Internet Access – Multi PVCs. Select M-PVCs Channel means no selection will be chosen. **VPI** - Type in the value provided by ISP. VCI - Type in the value provided by ISP. Encapsulating Type - Drop down the list to choose the type provided by ISP. **Protocol** - Drop down the list to choose the one provided by ISP. If you have already used Quick Start Wizard to set the protocol, then it is not necessary for you to change any settings in this group. **PPPoE Pass-through** The router offers PPPoE dial-up connection. Besides, you also can establish the PPPoE connection directly from local clients to your ISP via the Vigor router. 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. WAN Backup Setup **3G USB Modem** – Access Internet with 3G network connection through 3G USB Modem. Always On Dial Backup Mode Go to 3G USB Mode None Packet Trigger

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.

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

Dial Backup Mode

None	*
None	
Packet Trigger	
Always On	

Due to the absence of the ISDN interface in some models, the ISDN dial backup feature and its associated setup options are not available to them. Please refer to the previous part for further information. **None** - Disable the backup function.

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

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

Detail for 3G USB Modem Backup -

Internet Access >> 3G USB Modem Backup

PPP Client Mode	💿 Enable i 🔘 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	draytek	(Optional)
PPP Password	•••••	(Optional)
Index(1-15) in <u>Schee</u>	<u>lule</u> Setup:	
=> ,	,,	

PPP Client Mode - Click **Enable** to activate this mode for backup. **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.

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.

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

ISP Name – Type in the ISP Name provided by ISP in this field. Username – Type in the username provided by ISP in this field. Password – Type in the password provided by ISP in this field. PPP Authentication – Select PAP only or PAP or CHAP for PPP. Always On – Check this box if you want the router keeping connecting to Internet forever.

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

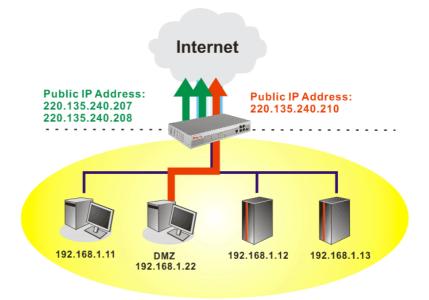
IP Address From ISP Usually ISP dynamically assigns IP address to you each time you connect to it and request. In some case, your ISP provides service to always assign you the same IP address whenever you request. In this case, you can fill in this IP address in the Fixed IP field. Please contact your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

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

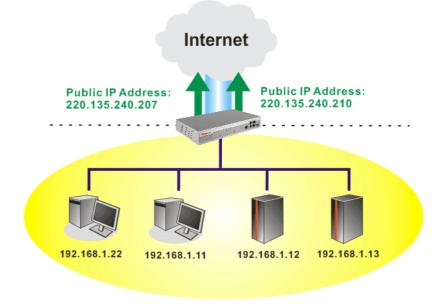
WAN IP Alias - If you have multiple public IP addresses and would like to utilize them on the WAN interface, please use WAN IP Alias. You can set up to 8 public IP addresses other than the current one you are using.

🗃 WAN IP Alias - Microsoft Internet Explorer			
WAN IF	P Alias (M	lulti-NAT)	
Index	Enable	Aux. WAN IP	Join NAT IP Pool
1.	V		v
2.			
з.			
4.			
5,			
6.			
7.			
8.			
		OK Clear All	Close

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



If you do not check **Join NAT IP Pool**, you can still use these public IP addresses for other purpose, such as DMZ host, Open Ports.



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.
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.

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

3.1.3 MPoA

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

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



Internet Access >> MPoA (RFC1483/2684)

MPoA (RFC1483/26	i84) 💿 Enable 🔘 Disable	WAN IP Network Set	ttings
		— 💿 Obtain an IP addı	ress automatically
DSL Modem Setting		Router Name	*
Multi-PVC channel	Channel 2	🔟 Domain Name 📃	*
Encapsulation 148	3 Bridged IP LLC	Specify an IP add	
VPI	0	IP Address	0.0.0.0
	34	Subnet Mask	0.0.0.0
VCI	54	Gateway IP Address	
WAN Backup Setup			
3G USB Modem		* : Required for som	ne ISPs
Dial Backup Mode 🛛 Always On 🛛 🔽		O Default MAC Ad	ldress
Go to 3G USB Modem Backup Setup		O Specify a MAC.	Address
ISDN		MAC Address :	
Dial Backup M	1ode None 🔽	00 · 50 · 7F	:81 . 83 . 09
RIP Protocol		DNS Server IP Addr	ess
Enable RIP		Primary IP Address	
		- Secondary IP Addre	
Bridge Mode		Secondary IF Addre	
Enable Bridge Mo	de		

ΟK

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

DSL Modem Settings	 Set up the DSL parameters required by your ISP. These are vital for building DSL connection to your ISP. Multi-PVC channel - The selections displayed here are determined by the page of Internet Access – Multi PVCs. Select M-PVCs Channel means no selection will be chosen. Encapsulating Type - Drop down the list to choose the type provided by ISP. VPI - Type in the value provided by ISP.
WAN Backup Setup	VCI - Type in the value provided by ISP.3G USB Modem – Access Internet with 3G network connection
	through 3G USB Modem.

Dial Backup Mode	Always On 🛛 💙	۲
Go to <u>3G USB Mode</u>	None	
	Packet Trigger	
	Always On	

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

Dial Backup Mode

None	*
None	
Packet Trigger	
Always On	

Due to the absence of the ISDN interface in some models, the ISDN dial backup feature and its associated setup options are not available to them. Please refer to the previous part for further information. **None** - Disable the backup function.

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

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

Detail for 3G USB Modem Backup -

Internet Access >> 3G USB Modem Backup

3G USB Modem		
PPP Client Mode	⊙ Enable 🔘 Disable	
SIM PIN code		
Modem Initial String	AT&FE0V1X1&D2&C1S0=0 (Default:A	T&FE0V1X1&D2&C1S0=0)
APN Name	Apply	
Modem Dial String	ATDT*99# (Default:A	TDT*99#)
PPP Username	draytek (Optional)	
PPP Password	•••••• (Optional)	
Index(1-15) in Sched	<u>ule</u> Setup:	
=>,],,	
	OK Cancel Default	

PPP Client Mode - Click **Enable** to activate this mode for backup. **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.

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.

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

RIP Protocol

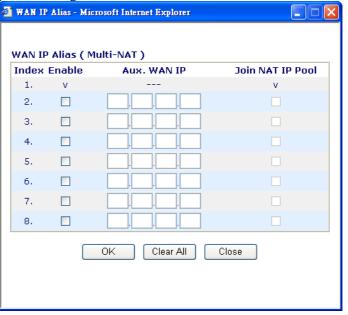
Vigor3100 Series User's Guide



Bridge Mode	If you choose Bridged IP as the protocol, you can check this box to invoke the function.	
WAN IP Network Settings	This group allows you to obtain an IP address automatically and allows you type in IP address manually.	

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

Router Name – Type in the router name provided by ISP.
Domain Name – Type in the domain name that you have assigned.
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.



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.

Default MAC Address	Type in MAC address for the router. You can use Default MAC
	Address or specify another MAC address for your necessity.
	MAC Address – Type in the MAC address for the router manually.
DNS Server IP	Type in the primary IP address for the router. If necessary, type in

Addresssecondary IP address for necessity in the future.

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

3.1.4 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.

Internet Access >> Multi-PVCs Setup

Channel	Enable	VPI	VCI	QoS Type	Protocol	Encapsulation
1.		8	36	UBR 🔽	PPPoE 🔽	VC MUX 🔽
2.	~	8	36	UBR 💌	MPoA 💌	1483 Route IP LLC
з.		8	37	UBR 🔽	PPPoA 🔽	VC MUX 🕑
4.		8	38	UBR 🔽	PPPoA 🔽	VC MUX 🔽
5.		8	39	UBR 🔽	PPPoA 🔽	VC MUX
6.		8	40	UBR 🔽	PPPoA 🔽	VC MUX 🔽
7.		8	41	UBR 🔽	PPPoA 🔽	VC MUX
8.		8	42	UBR 🔽	PPPoA 🔽	VC MUX 🕑

Enable	Type in the primary IP address for the router. If necessary, type				
VPI	Type in the value provided by your ISP.				
VCI	Type in the value provided by your ISP.				
QoS Type	Select a proper QoS type for the channel. QoS Type UBR V UBR CBR ABR nrtVBR rtVBR				
Protocol	Select a proper protocol for this channel. Protocol PPPoE 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				
	Encapsulation1483 Bridged IP LLCVC MUX1483 Bridged IP VC-MuxVC MUX1483 Routed IP VC-Mux(IPoA)LLC/SNAP1483 Bridged IP(IPoE)				

3.1.5 DSL Settings

DSL is one technology that dramatically increases the digital capacity of ordinary telephone lines (the local loops) into the home or office. The speed of DSL is based on the distance between the customer and telco central office.



Below shows settings for Vigor3100/Vigor3100G/Vigor3100i.

Internet Access >> DSL Setting

💿 AdaptiveRate	MaxRate : 2312 🌱 MinRate : 72 💌
○ FixedRate	2312 💌
Terminal Type	
AnnexType	Α 🗸

AdaptiveRate	Set the connection rate for the network.
MaxRate	Select the maximum rate for this setting. Use the drop down list to select the one that suits your router. The default value is 2312.
MinRate	Select the minimum rate for this setting. Use the drop down list to select the one that suits your router. The default value is 72.
FixedRate	If you select this one, only the fixed value is useful.
Terminal Type	Determine the role of this device as a CPE or CO.
Annex Type	Choose the correct annex type (A or B) for your router.

Vigor3120 offers different DSL settings with Vigor 3100/Vigor3100G/Vigor3100V due to its feature of 4-wire bundle mode.

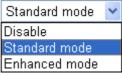
4-wire bundle mode	Standard mode 💌
O AdaptiveRate	MaxRate : 2312 🗹 MinRate : 72 🔽
• FixedRate	2312/4624 V(2-wire / 4-wire)
Terminal Type	CPE 💌
AnnexType	AV

ОK

Internet Access >> DSL Setting

4-wire bundle mode

To have wider bandwidth in network transmission, please choose proper mode in this field. Basically, you can just select the proper one according to the mode that your ISP provides. And you can set FixedRate setting only if you select **Standard mode** or **Enhanced mode** here.



Enhanced mode allows network connection via 2-wire instead if connection via 4-wire fails.

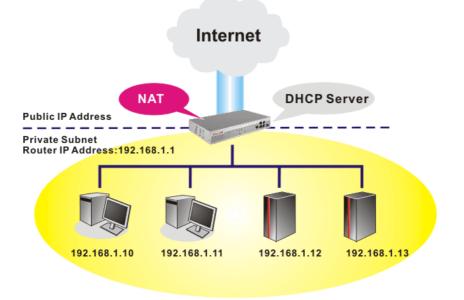
FixedRate	If you select Standard mode or Enhanced mode on 4-wire bundle mode, only the fixed rate is available for line speed. Please use the drop down list to choose the one that you subscribe.
Terminal Type	Determine the role of this device as a CPE or CO.
Annex Type	Choose the correct annex type (A or B) for your router.

3.2 LAN

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

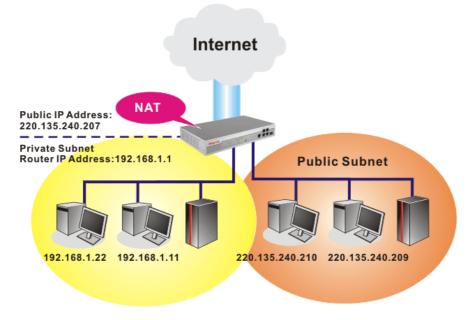
3.2.1 Basics of LAN

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



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





What is Routing Information Protocol (RIP)

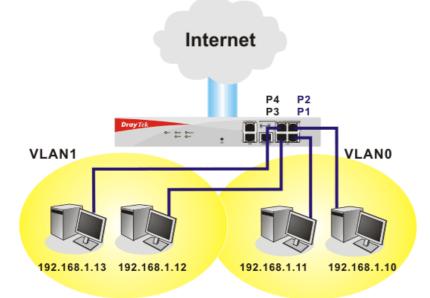
Vigor router will exchange routing information with neighboring routers using the RIP to accomplish IP routing. This allows users to change the information of the router such as IP address and the routers will automatically inform for each other.

What is Static Route

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

What are Virtual LANs and Rate Control

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



Dray Tek

3.2.2 General Setup

This page provides you the general settings for LAN.

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

LAN >> General Setup

Ethernet TCP / IP and I	OHCP Setup				
LAN IP Network Config	uration	DHCP Server Configuration			
For NAT Usage		Senable Server ○ Disable	⊙Enable Server ◯Disable Server		
1st IP Address 192.168.1.1		Relay Agent: 🔘 1st Subne	t 🔾 2nd Subnet		
1st Subnet Mask	255.255.255.0	Start IP Address	92.168.1.10		
For IP Routing Usage 🔘	Enable 💿 Disable	IP Pool Counts	50		
2nd IP Address	192.168.2.1	Gateway IP Address	92.168.1.1		
2nd Subnet Mask	255.255.255.0	DHCP Server IP Address			
	2nd Subnet DHCP Server	for Relay Agent L			
		DNS Server IP Address			
RIP Protocol Control Disable 💌		📃 Force DNS manual sett	ing		
		Primary IP Address			
		Secondary IP Address			
Natas Catting ID MAC IS	and the second second second second	USB IB			

Note: Setting IP MAC binding can perform fixed DHCP IP assignment.

OK

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

Router Web Configurator - Microsoft Internet Explorer	
2nd DHCP Server	
Start IP Address	
IP Pool Counts 0 (max. 10)	
Index Matched MAC Address given IP Address	_
MAC Address : :::::::::::::::::::::::::::::::::	
Add Remove Edit Cancel	
OK Clear All Close	

Vigor3100 Series User's Guide

Dray Tek

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

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

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

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

RIP Protocol Control

Disable	*
Disable	
1st Subnet	
2nd Subnet	

1st Subnet - Select the router to change the RIP information of the 1st subnet with neighboring routers.2nd Subnet - Select the router to change the RIP information of the

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

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

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

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

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

Relay Agent – $(1^{st} subnet/2^{nd} subnet)$ 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 ServerDNS 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 -

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:

LAN Status	Primary DNS	194.109.6.66	Secondary DNS	194.98.0.1
IP Address	TX Packets	RX Packets		
192.168.1.1	2792	2674		

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

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

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

3.2.3 Static Route

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

LAN >> Static Route Setup

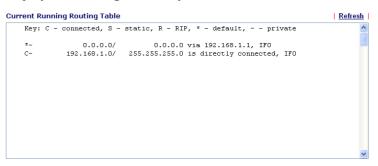
tatic Route Configuration						
Index	Destination Address	Status	Index	Destination Address	Status	
<u>1.</u>	???	?	<u>6.</u>	???	?	
<u>2.</u>	???	?	<u>7.</u>	???	?	
<u>3.</u>	???	?	<u>8.</u>	???	?	
<u>4.</u>	???	?	<u>9.</u>	???	?	
<u>5.</u>	???	?	<u>10.</u>	???	?	

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

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

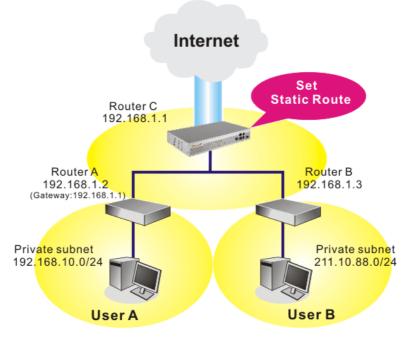


Add Static Routers to Private and Public Networks

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. 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 M	No. 1	
	Status/Action	Active/Add 🗸
	Destination IP Address	192.168.10.0
	Subnet Mask	255.255.255.0
	Gateway IP Address	192.168.1.2
	Network Interface	LAN 🗸

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

2	2		
	Status/Action	Active/Add 🛛 🐱	
	Destination IP Address	211.100.88.0	
	Subnet Mask	255.255.255.0	
	Gateway IP Address	192.168.1.3	
	Network Interface	LAN 🔽	

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

Diagnostics >> View Routing Table

LAN >> Static Route Setup

Ver. C	- connected S -	static, R - RIP, * - default, ~ - private	
Key. C	- conneccea, s -	Static, K = Kir, * = default, * = private	
*~	0.0.0/	0.0.0.0 via 192.168.1.1, IFO	
S~	192.168.10.0/	255.255.255.0 via 192.168.1.2, IFO	
С~	192.168.1.0/	255.255.255.0 is directly connected, IFO	
S~	211.100.88.0/	255.255.255.0 via 192.168.1.3, IFO	

Disable Static Route

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

LAN >> Static Route Setup					
Index No. 2					
Status/Action	Active/Add 💌				
Destination IP Address	Empty/Clear Active/Add				
Subnet Mask	Inactive/Disable				
Gateway IP Address	192.168.1.3				
Network Interface	LAN 💌				
	DK Cancel				

3.2.4 VLAN

Note: This menu is available for **Vigor3100**, **Vigor3100i**, **Vigor3100V** and **Vigor3120** model. For Vigor3100G, please refer to 3.10.

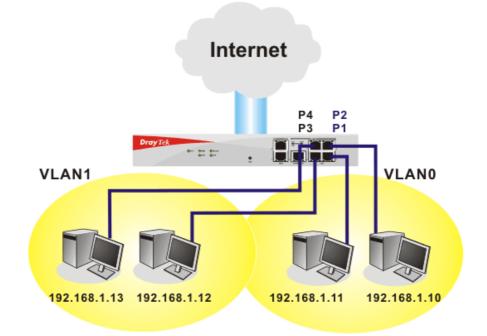
Virtual LAN function provides you a very convenient way to manage hosts by grouping them based on the physical port. You can also manage the in/out rate of each port. Go to LAN page and select VLAN. The following page will appear. Click **Enable** to invoke VLAN function.

Enable				
	P1	P2	P3	P4
VLANO				
VLAN1				
VLAN2				
VLAN3				
	OK	Clear	Cancel	

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.

'LAN Configuration				
🗸 Enable				
	P1	P2	P3	P4
VLANO	v			
VLAN1				v
VLAN2				
VLAN3				

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

3.2.5 Bind IP to MAC

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

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

LAN >> Bind IP to MAC

Bind IP to MAC Note: IP-MAC binding presets DHCP Allocat	ions	
If you select Strict Bind, unspecified		he Internet.
⊙ Enable ○ Disable ○ Strict Bind		
ARP Table <u>Select All</u> <u>Sort</u> <u>Refresh</u>	IP Bind List	Select All Sort
IP Address Mac Address 192.168.1.10 00-0E-A6-2A-D5-A1	Index IP Address	Mac Address
Add and Edit IP Address		
Add	Edit Remove	
	OK	

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.

3.3 NAT

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

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

The benefit of the NAT includes:

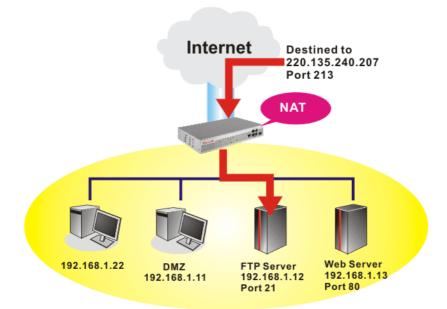
- Save cost on applying public IP address and apply efficient usage of IP address. NAT allows the internal IP addresses of local hosts to be translated into one public IP address, thus you can have only one IP address on behalf of the entire internal hosts.
- Enhance security of the internal network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

Note: 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.

3.3.1 Port Redirection

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





The port redirection can only apply to incoming traffic. The server users inside the LAN can not access public IP address of the server. The correct route is to access the server using the local private IP address of the server, or you should set up an alias in a Windows hosts file. Please only redirect the ports you know you have to forward rather than forward all ports. Otherwise, you will compromise the firewall-type security initially deployed by the NAT facility.

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

Index	Service Name	Prote	ocol	WAN IP		Public Port	Private IP	Private Port	Active
1			*	3.WAN IP Alias[2]	~	0		0	
2			*	3.WAN IP Alias[2]	~	0		0	
3			~	3.WAN IP Alias[2]	~	0		0	
4			*	3.WAN IP Alias[2]	~	0		0	
5			~	1.All 2.WAN IP Alias[1]		0		0	
6			*	3.WAN IP Alias[2] 4.WAN IP Alias[3]		0		0	
7			*	5.WAN IP Alias[4]		0		0	
8			*	6.WAN IP Alias[5] 7.WAN IP Alias[6]		0		0	
9			~	8.WAN IP Alias[7] 9.WAN IP Alias[8]		0		0	
10			~		~	0		0	

NAT >> Configure Port Redirection Table



Service Name	Enter the description of the specific network service.
Protocol	Select the transport layer protocol (TCP or UDP).
WAN IP	Select one of the WAN IP selections for port redirection. Only the selected WAN IP with incoming data will be redirected to the specified IP. If you choose All , all incoming traffic through any

Dray Tek

	WAN IP will be transferred to the IP address specified in this web page.
Public Port	Specify which port can be redirected to the specified Private IP and Port of the internal host.
Private IP	Specify the private IP address of the internal host providing the service.
Private Port	Specify the private port number of the service offered by the internal host.
Active	Check this box to activate the port-mapping entry you have defined.

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

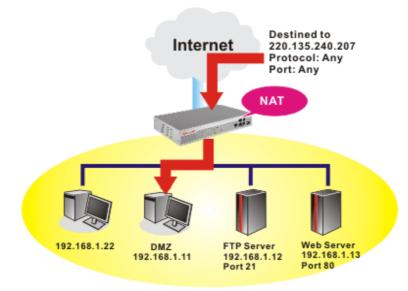
For example, the built-in web configurator in the router is with default port 80, which may conflict with the web server in the local network, http://192.168.1.13:80. Therefore, you need to **change the router's http port to any one other than the default port 80** to avoid conflict, such as 8080. This can be set in the **System Maintenance** >>**Management**. You then will access the admin screen of by suffixing the IP address with 8080, e.g., http://192.168.1.1:8080 instead of port 80.

Management Setup)					
Management Acce	ss Control	Management Port Set	up			
Enable remote firmware upgrade(FTP)		 Default Ports (Telnet 443, FTP: 21) 	 Default Ports (Telnet: 23, HTTP: 80, HTTPS: 443, FTP: 21) 			
Allow management from the Internet		💿 User Define Ports	⊙ User Define Ports			
Disable PING from	the Internet	Telnet Port 23				
		HTTP Port	8080			
Access List List IP	Subnet Mask	HTTPS Port	443			
1	×	FTP Port	21			
2	~					
3	~	SNMP Setup				
		Enable SNMP Agent				
		Get Community	public			
		Set Community	private			
		Manager Host IP				
		Trap Community	public			
		Notification Host IP				
		Trap Timeout	10 seconds			

3.3.2 DMZ Host

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





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

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

NAT >> DMZ Host Setup

DMZ Host Setup		
Enable	Private IP	
		Choose PC

OK

Enable	Check to enable the DMZ Host function.
Private IP	Enter the private IP address of the DMZ host, or click Choose PC to select one.
Choose PC	Click this button and then a window will automatically pop up, as depicted below. The window consists of a list of private IP addresses of all hosts in your LAN network. Select one private IP address in the list to be the DMZ host.

@))	1ttp://19 🔳 🗖 🔀
	192.168.1.11

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



NAT >>	DMZ Host \$	Setup		
DMZ Ho	st Setup			
Index	Enable	Aux. WAN IP	Private IP	
1.		220.135.240.247		Choose PC
		ОК	Clear	

3.3.3 Open Ports

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

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

NAT >> Open Ports Setup

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

Clear All

Index	Indicate the relative number for the particular entry that you want to offer service in a local host. You should click the appropriate index number to edit or clear the corresponding entry.
Comment	Specify the name for the defined network service.
Aux. WAN IP	Display the private IP address of the local host that you specify in WAN Alias.
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 Setup >> Edit Open Ports Setup

Enable Open P	orts				
	Comment	P2P-Emule			
	Local Computer	192 168 1	, 11 Choose PC]	
Protocol	Start Port	End Port	Protocol	Start Port	End Port
1. TCP 🚩	4500	4700	6. 🕶	0	0
2. UDP 💌	4500	4700	7. 🖳 🛩	0	0
3. 🔜 💌	0	0	8 🖌	0	0
4. 🛶 💙	0	0	9 💙	0	0
5 🗸	0	0	10. 🔜 💙	0	0

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

NAT >> Open Ports Setup >> Edit Open Ports Setup

Index No. 1						
🗹 Enable Open I	Ports					
	Comment	P2P-Emule	WAN IP	220.135.240.	247 🔽	
	Local Computer	192 168 1	.11 Choo	ise PC		
Protoco	l Start Port	End Port	Prot	ocol Star	t Port End Port	
1. TCP 🛩	4500	4700	6	✓ 0	0	
2. UDP 🛩	4500	4700	7	✓	0	
3 🛩	0	0	8	✓	0	
4. 🕶 💙	0	0	9	✓	0	
5 💙	0	0	10	▼	0	
OK Clear Cancel						

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

3.4 Firewall

3.4.1 Basics for Firewall

Quick Start Wizard

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

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

1. Enter login password						
Please enter an alpha-numeric strin	ig as your	Passwo	ord (Ma:	< 23 charac	ters).	
New Password						
Confirm Password						
]			
		<	Back	Next >	Finish	Cancel

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

System Maintenance >> Administrator Password Setup

Old Password	
New Password	
Retype New Password	

Firewall Facilities

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

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

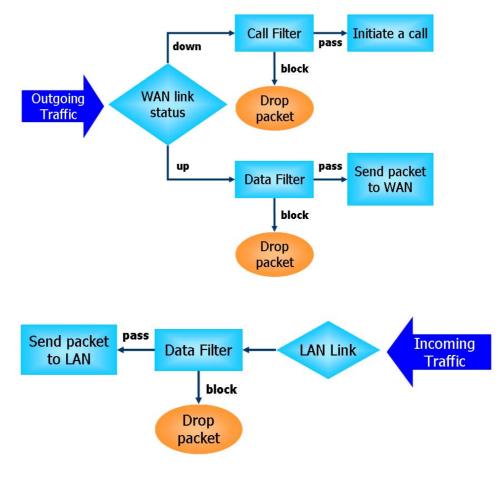


IP Filters

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

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

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



Stateful Packet Inspection (SPI)

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



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

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

Denial of Service (DoS) Defense

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

The **DoS Defense** function enables the Vigor router to inspect every 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. TCP Flag scan
- 5. Trace route
- 6. IP options
- 7. Unknown protocol
- 8. Land attack

9. Smurf attack
10. SYN fragment
11. ICMP fragment
12. Tear drop attack
13. Fraggle attack
14. Ping of Death attack
15. TCP/UDP port scan

URL Content Filtering

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 Filtering

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

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

3.4.2 General Setup

Firewall >> General Setup

General Setup allows you to adjust settings of IP Filter and common options. Here you can enable or disable the **Call Filter** or **Data Filter**. Under some circumstance, your filter set can be linked to work in a serial manner. So here you assign the **Start Filter Set** only. Also you can configure the **Log Flag** settings, **Enable Stateful packet inspection**, **Apply IP filter to VPN incoming packets**, **Drop non-http connection on TCP port 80**, and **Accept incoming fragmented UDP packets**.

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

al Setup		
Call Filter	💽 Enable	Start Filter Set 🛛 Set#1 💌
	🔘 Disable	
Data Filter	💿 Enable	Start Filter Set 🛛 Set#2 💌
	○ Disable	
Log Flag	None 💙	
🗌 Enable statefu	Il packet inspection	
🗌 Apply IP filter	to VPN incoming pack	ets
🗌 Drop non-http	connection on TCP p	ort 80
🗹 Accept incomi	ng fragmented UDP pa	ckets (for some games, ex. CS)

Call Filter	Check Enable to activate the Call Filter function. Assign a start filter set for the Call Filter.
Data Filter	Check Enable to activate the Data Filter function. Assign a start filter set for the Data Filter.
Log Flag	For troubleshooting needs you can specify the filter log here. None - The log function is not activated.

Dray Tek

Block - All blocked packets will be logged.
Pass - All passed packets will be logged.
No Match - The log function will record all packets that are not matched.
Note that the filter log will be displayed on the Telnet terminal when you type the *log -f* command.

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

3.4.3 Filter Setup

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

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

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

```
Filter Set 1
  Comments : Default Call Filter
    Filter Rule
                   Active
                                                       Comments
        1
                     ~
                                                      Block NetBios
        2
                     3
                     4
                     5
                     6
                     7
                     Next Filter Set None
                                  ΟK
                                            Clear
                                                       Cancel
Filter Rule
                          Click a button numbered (1 \sim 7) to edit the filter rule. Click the button
                          will open Edit Filter Rule web page. For the detailed information,
                          refer to the following page.
Active
                          Enable or disable the filter rule.
```

Firewall >> Filter Setup

Firewall >> Filter Setup >> Edit Filter Set



Comment	Enter filter set comments/description. Maximum length is 23-character long
Next Filter Set	Set the link to the next filter set to be executed after the current filter set. Do not make many filter sets a loop.

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

Filter Set 1 Rule 1		
Comments : Block NetBios	Check to enable the Filter Rule	
Pass or Block Block Immediately	Branch to Other Filter Set	
Direction IN 💌	Protocol TCP/UDP 💌	
IP / Source any	Address Subnet Mask Operator Start Port End Port 255.255.255.255 (/32) 137 139	
Destination any	255.255.255 (/32) 💙 😑 💌	
□Keep State	Fragments Don't Care 💌	
	OK Clear Cancel	
Comments	Enter filter set comments/description. Maximum length is 14-character long.	
Check to enable the Filter Rule	Check this box to enable the filter rule.	
Pass or Block	 Specifies the action to be taken when packets match the rule. Block Immediately - Packets matching the rule will be dropped immediately. Pass Immediately - Packets matching the rule will be passed immediately. Block If No Further Match - A packet matching the rule, and that does not match further rules, will be dropped. Pass If No Further Match - A packet matching the rule, and that does not match further rules, will be passed through. 	
Branch to other Filter Set	If the packet matches the filter rule, the next filter rule will branch to the specified filter set. Select next filter rule to branch from the drop-down menu.	
Log	Check this box to enable the log function. Use the Telnet command <i>log-f</i> to view the logs.	
Direction	Set the direction of packet flow. It is for Data Filter only. For the Call Filter , this setting is not available since Call Filter is only applied to outgoing traffic.	
Protocol	Specify the protocol(s) which this filter rule will apply to.	
IP Address	Specify a source and destination IP address for this filter rule to apply to. Place the symbol "!" before a specific IP Address will prevent this rule from being applied to that IP address. To apply the rule to all IP address, enter any or leave the field blank.	

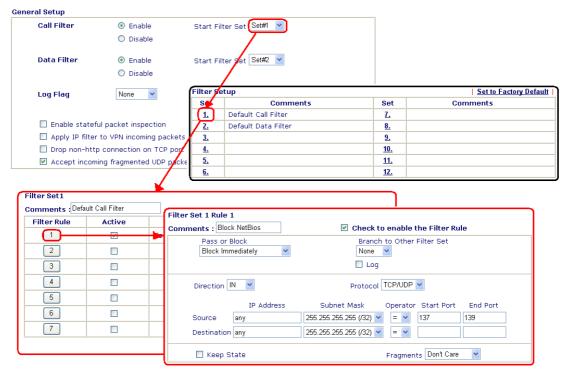
Firewall >> Edit Filter Rule >> Edit Filter Rule

Subnet Mask	Select the Subnet Mask for the IP Address column for this filter rule to apply from the drop-down menu.
Operator, Start Port and End Port	 The operator column specifies the port number settings. If the Start Port is empty, the Start Port and the End Port column will be ignored. The filter rule will filter out any port number. (=) If the End Port is empty, the filter rule will set the port number to be the value of the Start Port. Otherwise, the port number ranges between the Start Port and the End Port (including the Start Port and the End Port). (!=)If the End Port is empty, the port number is not equal to the value of the Start Port. Otherwise, this port number is not between the Start Port and the End Port (including the Start Port and the End Port (including the Start Port and the End Port (including the Start Port and End Port). (>) Specify the port number is larger than the Start Port (includes the Start Port). (<) Specify the port number is less than the Start Port (includes the Start Port).
Keep State	This function should work along with Direction, Protocol, IP address, Subnet Mask, Operator, Start Port and End Port settings. It is used for Data Filter only.
	Keep State is in the same nature of modern term Stateful Packet Inspection. It tracks packets, and accept the packets with appropriate characteristics showing its state is legal as the protocol defines. It will deny unsolicited incoming data. You may select protocols from any, TCP, UDP, TCP/UDP, ICMP and IGMP.
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.

DrayTek

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.



3.4.4 IM Blocking

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

-irewaii >> ii	M Blocking Setup
Instant Mess	enger Applications Blocking Setup
Etiaple IM	Block MSN Messenger
	Block Yahoo Messenger
	Block ICQ/AOL
	Block QQ
Time Schedu	le
Index(1-	-15) in <u>Schedule</u> Setup:,,,,
Note: A	ction and Idle Timeout settings will be ignored.

Dray Tek

3.4.5 P2P Blocking

P2P is the short name of peer to peer. Click **Firewall** and click **P2P Blocking** to open the setup page. You will see a list of common P2P applications. Check **Enable P2P Blocking** and select the one(s) to block. To block selected P2P applications during specific periods, enter the number of the scheduler predefined in **Applications>>Call Schedule**.

Enable P2P B	locking	
Protocol	Applications	Action
eDonkey	eDonkey, eMule, Shareaza, MLDonkey	 Allow Disallow Disallow upload
FastTrack	KazaA, iMesh, MLDonkey	 Allow Disallow
Gnutella	BearShare, Gnucleus, Limewire, Phex, Swapper, XoloX, Shareaza, MLDonkey	 Allow Disallow
BitTorrent	BitTorrent	 Allow Disallow

Firewall >> P2P Blocking Setup

Action

Specify the action for each protocol.

Note: Action and Idle Timeout settings will be ignored.

Allow – Allow the client to access into the application through the specified protocol.

Disallow – Forbid the client to access into the application through the specified protocol.

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

3.4.6 DoS Defense

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

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

Firewall >> DoS defense Setup

🗹 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 fla	ag scan	
Block Land	🗌 Block Tear D	rop	
Block Smurf	🗌 Block Ping of	f Death	
Block trace route	Block ICMP f	ragment	
Block SYN fragment	Block Unknow	wnProtocol	
Block Fraggle Attack			
Defend Tear Drop attack to ma	ake the cerver alive		~
serena rear stop accash oo a	and one berier drifer		
			~

OK	Clear All	Car	106
----	-----------	-----	-----

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. (Refer to Chapter 13 System Maintenance Syslog Access Setup for detail information.)

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

SysLog Access Setup

🗹 Enable		
	Server IP Address	192.168.1.115
	Destination Port	514

ontrols	g	192,168,1.1	~ WAN Status		ی رق
		Vigor 3100 series Dmt.Bis	Getway IP (Fixed)	TX Packets	RX Rate
LAN Status		Vigor 3100 Series Diriciois		0	0
TX Pa	ickets	RX Packets	WAN IP (Fixed)	RX Packets	TX Rate
93	31	1182		0	0
Time Jan 1 00:00:42 Jan 1 00:00:34	Host Vigor Vigor	Message DoS syn_flood Block(10s) 192.168 DoS icmp_flood Block(10s) 192.166			
<		The second se			>

3.4.7 URL Content Filter

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

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

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

Click Firewall and click URL Content Filter to open the setup page.

Firewall >> URL Content Filter

Black List (block those matching keywo	rd)		
○ White List (pass those matching keywo	rd)		
No ACT Keyword	No	ACT	Keyword
1	5		
2	6		
3	7		
4	8		
Note that multiple keywords are allowed	to specify in	the blan	k. For example: hotmail yahoo msn
Prevent web access from IP address	1 7 7		, ,
Enable Excepting Subnets			
No Act IP Address			Subnet Mask
1		~	
2		~	
3		~	
4		~	
ne Schedule		1	7
ndex(1-15) in <u>Schedule</u> Setup:,,	, [be ignored.		
	,, _,, _		J

Enable URL Access Control	Check the box to activate URL Access Control.
Black List (block those matching keyword)	Click this button to restrict accessing into the corresponding webpage with the keywords listed on the box below.
White List (pass those matching keyword)	Click this button to allow accessing into the corresponding webpage with the keywords listed on the box below.
Keyword	The Vigor router provides 8 frames for users to define keywords and each frame supports multiple keywords. The keyword could be a noun, a partial noun, or a complete URL string. Multiple keywords within a frame are separated by space, comma, or semicolon. In



	addition, the maximal length of each frame is 32-character long. After specifying keywords, the Vigor router will decline the connection request to the website whose URL string matched to any user-defined keyword. It should be noticed that the more simplified the blocking keyword list, the more efficiently the Vigor router perform.
Prevent web access from IP address	Check the box to deny any web surfing activity using IP address, such as http://202.6.3.2. The reason for this is to prevent someone dodges the URL Access Control.
	You must clear your browser cache first so that the URL content filtering facility operates properly on a web page that you visited before.
Enable Restrict Web Feature	Check the box to activate the function. <i>Java</i> - Check the checkbox to activate the Block Java object function. The Vigor router will discard the Java objects from the Internet.
	<i>ActiveX</i> - Check the box to activate the Block ActiveX object function. Any ActiveX object from the Internet will be refused. <i>Compressed file</i> - Check the box to activate the Block Compressed file function to prevent someone from downloading any compressed file. The following list shows the types of compressed files that can be blocked by the Vigor router
	 zip, rar, .arj, .ace, .cab, .sit <i>Executable file</i> - Check the box to reject any downloading behavior of the executable file from the Internet. .exe, .com, .scr, .pif, .bas, .bat, .inf, .reg <i>Cookie</i> - Check the box to filter out the cookie transmission from inside to outside world to protect the local user's privacy. <i>Proxy</i> - Check the box to reject any proxy transmission. To control efficiently the limited-bandwidth usage, it will be of great value to provide the blocking mechanism that filters out the multimedia files downloading from web pages. Accordingly, files with the following extensions will be blocked by the Vigor router. .mov .mp3 .rm .ra .au .wmv .wav .asf .mpg .mpeg .avi .ram
Enable Excepting Subnets	Four entries are available for users to specify some specific IP addresses or subnets so that they can be free from the <i>URL Access Control</i> . To enable an entry, click on the empty checkbox, named as ACT , in front of the appropriate entry.
Time Schedule	Specify what time should perform the URL content filtering facility.

3.4.8 Web Content Filter

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

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

CPA(Content Portal Authority) Web Content Filter Setup Select a CPA server: asia.sufcpa.com Activate Free Trial and Purchase Subscription Test a site to verify whether it is categorized SurfControl						
Enable Web Cont						
Groups Child Protection Select All Clear All	Categories (Tick categ	ories to block. Untick to Criminal Hacking Violence	unblock) Drugs/Alcohol Hate speech Weapons			
Leisure Select All Clear All	Advertisements Games Hobbies Personals Sports	Entertainment Glamour Lifestyle Photo Searches Streaming Media	Food Health Motor Vehicles Shopping Travel			
Business Select All Clear All	Computing/Internet	□ Finance □ Real Estate □ Search Engine	☐ Job Search/Career ☐ Reference ☐ Web Mail			
Others Select All Clear All	□Education □News □Usenet news	☐ Hosting sites ☐ Religion ☐ Block all uncategori	☐ Kid Sites ☐ Sex Education sed sites			
F ime Schedule Index(1-15) in <u>Sch</u> Note: Action and Idle	<u>redule</u> Setup:,,,],, pred.				

Dray Tek

3.5 Bandwidth Management

3.5.1 Sessions Limit

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

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

Sessions Limi	t
0	Enable 💿 Disable
Defa	ault Max Sessions: 100
Lim	itation List
Inc	lex Start IP End IP Max Sessions
Spe	cific Limitation
Star	t IP: End IP:
Max	imum Sessions: Add Edit Remove
Time Schedul	e
Index(1-1	.5) in <u>Schedule</u> Setup:,,,,,
Note: Ac	tion and Idle Timeout settings will be ignored.

Bandwidth Management >> Sessions Limit

OK

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 Max session	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 Session	Defines the available session number for specific range of IP addresses. If you do not set the session number in this field, the system will use the default session limit for the specific limitation you set for each index.
Add	Adds the specific session limitation onto the list above.
Edit	Allows you to edit the settings for the selected limitation.



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

3.5.2 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.

🔘 En	able	۲	Disable	_					
Defaul	tтXI	_imit:	200	Kbps	Default	RX Limit:	800	Kbps	
Limita	tion	List							
Index	: S	tart	IP	End	IP		TXlimit	RXlimit	
Specif	ic Lir	nitati	on						
Start I	P:				End IP:				
TX Lim	i+.		Kbps	RX Limi	+ · [Кыра			
17 60							_		
				Add	Edit	Remove			
Schedule									
ndex(1-15)	in S	chedu	ile Setup:			7.			
Note: Actio					, vill be iou	ored		1	
vote, Actio	n anc	Tule	nineout s	secongs «	nii be igi	iorea.			

Bandwidth Management >> Bandwidth Limit

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.
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.

3.5.3 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.



Private Network DS domain 1

DS domain 2

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.

Quality of S	ervice		Set to Factory Default
🗹 Enable ti	he QoS Control		
Direction [OUT 🔽		
Index	Class Name	Reserved_bandwidth Ratio	Setup
1.		25 %	Basic Advanced
2.		25 %	Basic Advanced
з.		25 %	Basic Advanced
4.	Others	25 %	
	IDP Bandwidth Control	Limited_band	width Ratio 25 %
U Outboun	d TCP ACK Prioritize		Online Statistics

OK

Bandwidth Management >> Quality of Service

Enable the QoS Control	The factory default for this setting is checked.
Direction	Define which traffic the QoS Control settings apply to. IN- apply to incoming traffic only. OUT-apply to outgoing traffic only. BOTH- apply to both incoming and outgoing traffic.
Index	The group index number of QoS Control settings. There are total 4 groups.
Class Name	Define the name for the group index.
Reserved Bandwidth Ratio	It is reserved for the group index in the form of ratio of reserved bandwidth to upstream speed and reserved bandwidth to downstream speed .

Clear All



Setup	Basic - s service t Advanc	setup type. e - cu ource	Reserv We pro ustom s addres	ovide a list of co etting of Reserv	Ratio according to the traff mmon service types. ed Bandwidth Ratio based ldress, DiffServ CodePoin	1
Enable UDP Bandwidth Control	field. Th	iis is plica	a prote tion tra	ction of TCP app	vidth ratio on the right plication traffic since aming video will exhaust	
Limited_bandwidth Ratio	The rational The rational The rational Contract	• •	ed here	is reserved for l	imited bandwidth of UDP	•
On Line Statistics	referenc	e. Manage		atistics for quali	ty of service for your	
	Index (Direction	Class Name	Reserved-bandwidth Ratio	Outbound Throughput (Bytes/sec)	
	1	OUT	Class Name	25%		
	2	OUT		25%	0	
	3	OUT		25%	0	
	4	OUT	Others	25%	0	
		1	Refresh Inter	val : 30 🚩 seconds	Reload	
			Ou	tbound Status		

Others

(Bos)

Basic Settings for QoS

Click the **Basic** button to open basic configuration screen for each index number.

ANY AUTH(TCP:113) BGP(TCP:179) BOOTPCLIENT(UDP:68) BOOTPSERVER(UDP:67) CU-SEEME-HI(TCP/UDP:24032) CU-SEEME-LO(TCP/UDP:7648) DNS(TCP/UDP:53)	ADD »	
	onfiguration, we only care address will be replaced wi	about the service type. th any when you press "OK".

Bandwidth Management >> Quality of Service

Choose one of the items from the left box and click **ADD**>>. The selected one will be shown



on the right box. To remove the selected on from the right box, simply choose the one again and click <<**Remove.**

Advanced Settings for QoS

Click this button to open advanced configuration for each index number. You can insert, move, edit or delete select rule in this page.

Bandwidth Management >> Quality of Service

Class Inc	lex #1				
NO	Status	Local Address	Remote Address	DiffServ CodePoint	Service Type
1. 💿	Empty	-	-	-	-
Move Edit	selected selected	Rule (select an Inde Rule	ex Number) to 1	(Rule Number).	

For inserting a rule, click **Insert** to open the following page. Bandwidth Management >> Quality of Service

Qual	ity of Service			
ACT	Local Address	Remote Address	DiffServ CodePoint	Service Type
•	Edit	Edit	ANY	ANY Add Edit Delete
Note	: Please choose/se	tup the Service Ty	/pe first.	
SrcE	dit/DestEdit	It allo	OK Cancel ws you to edit source ad	ldress information.
		🙆 http://1	192.168.1.1/doc/QosIpEdt.htm - Microsoft	Internet Explorer
			Address Type	Any Address 💌
			Start IP Address	Any Address Single Address
			End IP Address	Range Address Subnet Address
			Subnet Mask	0.0.0.0
			ОК	Close

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

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

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



DiffServ CodePoint

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

Service Type

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

ANY	^	C
AUTH(TCP:113)		
BGP(TCP:179)		
BOOTPCLIENT(UDP:68)		
BOOTPSERVER(UDP:67)		
CU-SEEME-LO(TCP/UDP:7648)		
CU-SEEME-HI(TCP/UDP:24032)		連
DNS(TCP/UDP:53) FINGER(TCP:79)		
FTP(TCP:20~21)		1
H.323(TCP:1720)		1
HTTP(TCP:80)		0
HTTPS(TCP:443)		
IKE(UDP:500)		
IPSEC-AH(IP:51)		
IPSEC-ESP(IP:50)		
IRC(TCP/UDP:6667)		1
L2TP(UDP:1701)		
NEWS(TCP:144) NFS(UDP:2049)		
NNTP(TCP:119)		
PING(IP:1)	-	
POP3(TCP:110)		
PPTP(TCP:1723)		
RCMD(TCP:512)	-	
REAL-AUDIO(TCP:7070)		
RTSP(TCP/UDP:554)		
SFTP(TCP:115)		
SMTP(TCP:25) SNMP(TCP/UDP:161)		
LOWINE (ICE/UDE: 161)	¥	

In addition, you can add a new service for your necessity by simply clicking **Add** button to access into the following page.

Bandwidth Management >> Quality of Service

Service Name	
Service Type	TCP
Port Configuration	
Туре	💿 Single i 🔘 Range
Port Number	0 - 0

Service Name – Type in a new service for your request. **Service Type** – Choose the type (TCP, UDP or TCP/UDP) for the new service.

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

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

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

3.6 Applications

3.6.1 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 Setu	ιp	View Log	Force Update
Accounts :			
Index	Domain Name		Active
<u>1.</u>			×
<u>2.</u>			×
<u>3.</u>			x

Dray Tek

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

Enable Dynamic DNS A	ccount
Service Provider	dyndns.org (www.dyndns.org)
Service Type	Dynamic 💌
Domain Name	chronoD1 dyndns.org
Login Name	chrono6853 (max. 23 characters)
Password	(max. 23 characters)
🗌 Wildcards	
🗌 Backup MX	
Mail Extender	
	OK Clear Cancel
ervice Provider	Select the service provider for the DDNS account.
ervice Type	Select a service type (Dynamic, Custom, Static).
omain Name	Type in a domain name that you applied previously.
ogin Name	Type in the login name that you set for applying domain.

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

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

🗹 Enat	ole Dynamic DNS Setup	View Log Fo	rce Update Clea	ar All
	Accounts			
	Index	Domain Name	Active	
	<u>1.</u>	chrono01.dyndns.org	V	
	<u>2.</u>		X	
	3		X	

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

Disable the Function and Clear all Dynamic DNS Accounts

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

Delete a Dynamic DNS Account

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

3.6.2 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.

Index	Status	Index	Status
<u>1.</u>	х	<u>9.</u>	×
<u>2.</u>	х	<u>10.</u>	х
<u>3.</u>	х	<u>11.</u>	×
<u>4.</u>	х	<u>12.</u>	×
<u>5.</u>	х	<u>13.</u>	×
<u>6.</u>	х	<u>14.</u>	×
<u>7.</u>	х	<u>15.</u>	×
8.	×		

Applications >> Schedule

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

Clear All

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

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

Index No. 1			
Enable Schedule Setup			
Start Date (уууу-mn	n-dd) 2004 🕶 - 12 🕶 - 21 💌		
Start Time (hh:mm)			
Duration Time (hh:m	m) 0 💙 : 0 💌		
Action	Force On		
Idle Timeout	Force On Force Down		
	Enable Dial-On-Demand		
How Often	Disable Dial-On-Demand		
O Once			
● Weekdays	에 Mon 에 Tue 에 Wed 에 Thu 에 Fri 이 Sat		
	🗹 Mon 🕑 Tue 🕑 Wed 🖤 Thu 🕑 Fri 🗌 Sat		
Г	OK Clear Cancel		
Enable Schedule Setup	Check to enable the schedule.		
Start Date (yyyy-mm-dd)	Specify the starting date of the schedule.		
Start Time (hh:mm)Specify the starting time of the schedule.			
Duration Time (hh:mm) Specify the duration (or period) for the schedule.			
Action Specify which action Call Schedule should apply during t 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 (office hour). Other time the Internet access connection should be disconnected (Force Down).



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

3.6.3 RADIUS

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

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

Applications >> RADIUS

RADIUS Setup	
Server IP Address	
Destination Port	1812
Shared Secret	
Re-type Shared Secret	
ОК	Clear Cancel

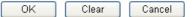
Enable	Check to enable RADIUS client feature	
Server IP Address	Enter the IP address of RADIUS server	
Destination Port	The UDP port number that the RADIUS server is using. The default value is 1812, based on RFC 2138.	
Shared Secret	The RADIUS server and client share a secret that is used to authenticate the messages sent between them. Both sides must be configured to use the same shared secret.	
Re-type Shared Secret	Re-type the Shared Secret for confirmation.	

3.6.4 UPnP

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

Applications >> UPnP

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



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.



	Broadband		onnection on Rou	and the second dealers and the
etwork Tasks Image: Constraint of the second seco	hinet Disconnected WAN Minipart (PPPOE)	General Internet Gateway Status:		Connected
	Dial-up	Duration:		00:19:06
ee Also	test Disconnected DrayTek ISDN PPP	Speed:		100.0 Mbps
ther Places	Internet Gateway IP Broadband Connection on Router Penabled	Packets: Sent:	Internet Gateway	My Computer
My Computer	LAN or High-Speed Internet	Received:	1,115	666
etails 🛞	Local Area Connection	Properties	Disable	
etwork Connections	Realtek RTL8139/810x Family			

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.
1 PBroadband Connection on Router	Services
his 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

The reminder as regards concern about Firewall and UPnP

Can't work with Firewall Software

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

Security Considerations

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

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



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

3.6.5 Wake on LAN

A PC client on LAN can wake up specified PC through the router. Yet the specified PC must have installed a network card supporting WOL function. By the way, WOL function must be set as "Enable" on the BIOS setting of the specified PC.

Application >> Wake on LAN

	Note: Wake on LA can wake up throu		P to MAC function, only binded PCs	
	Wake by: IP Address: MAC Address: Result	MAC Address	Wake Up!	
Wake by		choose Wake by MAC address of Wake by IP Addr The IP address sh	Two types provide for you to wake up the binded IP. If you choose Wake by MAC Address, you have to type the correct MAC address of the host in MAC Address boxes. If you choose Wake by IP Address, you have to choose the correct IP address. The IP address should be binded with MAC address configured in Bind IP to MAC page.	
		Wake by:	MAC Address MAC Address IP Address	
IP Addres	5S	IP to MAC will	that have been configured in Firewall>>Bind be shown in this drop down list. Choose the IP drop down list that you want to wake up.	
MAC Add	lress	Type any one of	the MAC address of the binded PCs.	
Wake Up	!		Click this button to wake up the selected IP. See the following figure. The result will be shown on the box.	



Application >> Wake on LAN

Note: Wake on can wake up th	LAN integrates with <u>Bind IP to MAC</u> function, only binded PCs rough IP.
Wake by:	MAC Address 😪
IP Address:	😒
MAC Address:	Wake Up!
Result	
Send command	to client done.

3.7 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.

3.7.1 Remote Access Control

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

VPN and Remote Access >> Remote Access Control Setup

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

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

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

3.7.2 PPP General Setup

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

VPN and F	Remote /	Access >>	PPP	General	Setup
-----------	----------	-----------	-----	---------	-------

PPP/MP Protocol		IP Address Assignmer	nt for Dial-In Users
Dial-In PPP Authentication		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 will be optionally employed in the router for the remote dial-in user. If the remote dial-in user does not support the MPPE encryption algorithm, the router will transmit "no MPPE encrypted packets". Otherwise, the MPPE encryption scheme will be used to encrypt the data. **Require MPPE (40/128bits)** Selecting this option will force the router to encrypt packets by using the MPPE encryption algorithm. In addition, the remote dial-in user will use 40-bit to perform encryption prior to using 128-bit for encryption. In other words, if 40-bit MPPE

Maximum MPPE This option indicates that the router will use the MPPE encryption scheme with maximum bits (128 bits) to encrypt the data.

scheme will be applied to encrypt the data.

encryption method is not available, then 128-bit encryption

- 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 AddressEnter 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 192.168.1.202 to
be the Start IP Address.



3.7.3 IPSec General Setup

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

There are two phases of IKE/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) and/or Encapsulating Security Payload (ESP) for the following IKE exchange and mutual examination of the secure tunnel establishment.

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. Vigor supports IPSec used ESP to encrypt the data payload. There are two encryption methods in IPSec: Transport and Tunnel. Transport mode encrypts only the data portion, a.k.a. payload, of each packet, but not the header. Transport mode is used in L2TP over IP Sec. The more secure Tunnel mode encrypts both the header and the payload. Tunnel mode is used in IPSec. ESP can be used alone or in conjunction with AH.

VPN and Remote Access >> I	PSec General Setup
VPN IKE/IPSec General Setup	
	users and Dynamic IP Client (LAN to LAN).
IKE Authentication Met	hod
Pre-Shared Key	
Re-type Pre-Shared Key	
IPSec Security Method	
Medium (AH)	
Data will be authentic	, but will not be encrypted.
High (ESP)	
XE Authentication Method	 OK Cancel I This usually applies to those are remote dial-in user or node (LAN-to-LAN) which uses dynamic IP address and
	IPSec-related VPN connections such as L2TP over IPSec an
	IPSec tunnel.
	Pre-Shared Key - Currently only support Pre-Shared Key authentication. Pre-Shared Key- Specify a key for IKE authentication
	Re-type Pre-Shared Key- Confirm the pre-shared key.
PSec Security Method	Medium - Authentication Header (AH) means data will be authenticated, but not be encrypted. By default, this option i

High - Encapsulating Security Payload (ESP) means payload (data) will be encrypted and authenticated. You may select encryption algorithm from Data Encryption Standard (DES), Triple DES (3DES), and AES.

3.7.4 IPSec Peer Identity

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

VPN and Remote Access >> IPSec Peer Identity

Index		Name	Index		Name	
<u>1.</u>	???		<u>9.</u>	???		
<u>2.</u>	???		<u>10.</u>	???		
<u>3.</u>	???		<u>11.</u>	???		
<u>4.</u>	???		<u>12.</u>	???		
<u>5.</u>	???		<u>13.</u>	???		
<u>6.</u>	???		<u>14.</u>	???		
<u>7.</u>	???		<u>15.</u>	???		
<u>8.</u>	???		<u>16.</u>	???		

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

VPN and Remote Access >> IPSec Peer Identity

Profile Name draytek_user2				
O Accept Any Peer ID				
O Accept Subject Alternative Name				
Туре	IP Address 🛛 👻			
IP				
Accept Subject Name				
Country (C)	TW			
State (ST)				
Location (L)	HsinChu			
Orginization (O)	Draytek			
Orginization Unit (OU)	Marketing			
Common Name (CN)				
Email (E)	service@draytek.com			

Profile NameTyAccept Any Peer IDC

Type in a name in this file.

Click to accept any peer regardless of its identity.



Accept Subject Alternative Name	Click to check one specific field of digital signature to accept the peer with matching value. The field can be IP Address , Domain , or E-mail Address . The box under the Type will appear according to the type you select and ask you to fill in corresponding setting.
Accept Subject Name	Click to check the specific fields of digital signature to accept the peer with matching value. The field includes Country (C), State (ST), Location (L), Organization (O), Organization Unit (OU), Common Name (CN), and Email (E).

3.7.5 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 or build the VPN connection. You may set parameters including specified connection peer ID, connection type (ISDN, VPN including PPTP, IPSec Tunnel, and L2TP by itself or over IPSec) and corresponding security methods, etc.

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

VPN and Remote Access >> Remote Dial-in User

Index	User	Status	Index		User	Status
<u>1.</u>	???	×	<u>9.</u>	???		×
<u>2.</u>	???	×	<u>10.</u>	???		х
<u>3.</u>	???	×	<u>11.</u>	???		×
<u>4.</u>	???	×	<u>12.</u>	???		×
<u>5.</u>	???	×	<u>13.</u>	???		х
<u>6.</u>	???	×	<u>14.</u>	???		×
<u>7.</u>	???	×	<u>15.</u>	???		х
<u>8.</u>	???	×	<u>16.</u>	???		×

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

Set to Factory Default	Click to clear all indexes.
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

Iser account and Authentication	
Enable this account	Username ???
Idle Timeout 300 second(s)	Password
Allowed Dial-In Type	IKE Authentication Method
▼ ISDN	Pre-Shared Key
▶ РРТР	IKE Pre-Shared Key
☑ IPSec Tunnel	Digital Signature (X.509)
🗹 L2TP with IPSec Policy None 🛛 👻	??? 🔽
Specify Remote Node Remote Client IP or Peer ISDN Number or Peer ID	IPSec Security Method Medium (AH) High (ESP) DES Ø3DES ØAES Local ID (optional)
	Callback Function
	Check to enable Callback function
	Specify the callback number
	Callback Number
	Check to enable Callback Budget Control
	Callback Budget 30 minute(s)

OK Clear Cancel

Enable this account	Check the box to enable this function. Idle Timeout- If the dial-in user is idle over the limitation of the timer, the router will drop this connection. By default, the Idle Timeout is set to 300 seconds.
ISDN	Allow the remote ISDN dial-in connection. You can further set up Callback function below. You should set the User Name and Password of remote dial-in user below
PPTP	Allow the remote dial-in user to make a PPTP VPN connection through the Internet. You should set the User Name and Password of remote dial-in user below
IPSec Tunnel	Allow the remote dial-in user to trigger a IPSec VPN connection through Internet.
L2TP	 Allow the remote dial-in user to make a L2TP VPN connection through the Internet. You can select to use L2TP alone or with IPSec. Select from below: None - Do not apply the IPSec policy. Accordingly, the VPN connection employed the L2TP without IPSec policy can be viewed as one pure L2TP connection. Nice to Have - Apply the IPSec policy first, if it is applicable during negotiation. Otherwise, the dial-in VPN connection becomes one pure L2TP connection. Must -Specify the IPSec policy to be definitely applied on the L2TP connection.
Specify Remote Node	Check the checkbox- You can specify the IP address of the remote dial-in user or peer ID (should be the same as the ID you set in the Local ID of IKE advanced settings window). Enter Peer ISDN number if you select ISDN above. Also, you should



	further specify the corresponding security methods on the right side. Uncheck the checkbox- This means the connection type you select above will apply the authentication methods and security methods in the general settings .
User Name	This field is applicable when you select PPTP or L2TP w/ or w/out IPSec policy above. This field is also applicable if you select ISDN.
Password	This field is applicable when you select PPTP or L2TP w/ or w/out IPSec policy above. This field is also applicable if you select ISDN.
IKE Authentication Method	 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 w/ or w/o specify the IP address of the remote node. Pre-Shared Key - Input 1-63 characters as pre-shared key. Digital Signature (X.509) - Select one predefined in the X.509 Peer ID Profiles.
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. Local ID - Specify a local ID to be used for Dial-in setting in the LAN-to-LAN Profile setup. This item is optional.
Callback Function	 The callback function provides a callback service only for the ISDN dial-in user. The router owner will be charged the connection fee by the telecom. Check to enable Callback function-Enables the callback function. Specify the callback number-The option is for extra security. Once enabled, the router will ONLY call back to the specified Callback Number. Check to enable callback budget control-By default, the callback function has a time restriction. Once the callback budget has been exhausted, the callback mechanism will be disabled automatically. Callback Budget (Unit: minutes)- Specify the time budget for the dial-in user. The budget will be decreased automatically per callback connection.

3.7.6 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 (ISDN, VPN including PPTP, IPSec Tunnel, and L2TP by itself or over IPSec) and corresponding security methods, etc.

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

Index	Name	Status	Index	Name	Status
<u>1.</u>	???	×	<u>9.</u>	???	×
<u>2.</u>	???	×	<u>10.</u>	???	х
<u>3.</u>	???	×	<u>11.</u>	???	×
<u>4.</u>	???	×	<u>12.</u>	???	×
<u>5.</u>	???	×	<u>13.</u>	???	×
<u>6.</u>	???	×	<u>14.</u>	???	×
<u>7.</u>	???	×	<u>15.</u>	???	×
<u>8.</u>	???	×	<u>16.</u>	???	×

<< <u>1-16 | 17-32</u> >>

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

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.

VPN and Remote Access >> LAN to LAN

Profile Name	???		Call Direction 💿 Bo	oth 🔿 Dial-Out 🔿 Dial-In
Enable this profile		Always on		
			Idle Timeout 300	second(s)
			Enable PING to keep	
			PING to the IP	
2. Dial-Out Settings				
Type of Server I a	m calling		Link Type	64k bps 😽
ISDN			Username	???
O PPTP			Password	
🔘 IPSec Tunnel			PPP Authentication	
O L2TP with IPSec	Policy None	*	VJ Compression	💿 On 🔘 Off
Dial Number for ISD Server IP/Host Nam (such as 5551234, ı	e for VPN.	123.45.67.89)	IKE Authentication M Pre-Shared Key IKE Pre-Shared Key Digital Signature(X.S Pre-Shared Key Digital Signature(X.S Pre-Shared Key IPSec Security Method Medium(AH) High(ESP) DES with Advanced Index(1-15) in Scheduli Callback Function (C Require Remote to	bod thout Authentication
			Require Remote to	Callback
			📃 Provide ISDN Numb	er to Remote

Profile Name	Specify a name for the profile of the LAN-to-LAN connection.
Enable this profile	Check here to activate this profile.
Call Direction	Specify the allowed call direction of this LAN-to-LAN profile. Both :-initiator/responder Dial-Out - initiator only Dial-In - responder only.
Always On or Idle Timeout	Always On-Check to enable router always keep VPN connection.Idle Timeout: The default value is 300 seconds. If the connection has been idled over the value, the router will drop the connection.
Enable PING to keep alive	This function is to help the router to determine the status of IPSec VPN connection, especially useful in the case of abnormal VPN IPSec tunnel disruption. For details, please refer to the note below. Check to enable the transmission of PING packets to a specified IP address.
PING to the IP	Enter the IP address of the remote host that located at the other-end of the VPN tunnel.
	Enable PING to Keep Alive is used to handle abnormal IPSec VPN connection disruption. It will help to provide the state of a VPN connection for router's judgment of redial. Normally, if any one of VPN peers wants to disconnect the connection, it should follow a serial of packet exchange

	procedure to inform each other. However, if the remote peer disconnect without notice, Vigor router will by no where to know this situation. To resolve this dilemma, by continuously sending PING packets to the remote host, the Vigor router can know the true existence of this VPN connection and react accordingly.
ISDN	Build ISDN dial-out connection to the server. You should set up Link Type and identity like User Name and Password for the authentication of remote server. You can further set up Callback (CBCP) function below.
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 IPsec	 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.
Server IP/Host Name for	You can specify the IP address of the remote dial-out user.
User Name	This field is applicable when you select PPTP or L2TP with or without IPSec policy above. This field is also applicable if you select ISDN.
Password	This field is applicable when you select PPTP or L2TP with or without IPSec policy above. This field is also applicable if you select ISDN.
PPP Authentication	This field is applicable when you select PPTP or L2TP with or without IPSec policy above. This field is also applicable if you select ISDN. PAP/CHAP is the most common selection due to wild compatibility.
VJ compression	This field is applicable when you select PPTP or L2TP with or without IPSec policy above. This field is also applicable if you select ISDN. 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 Encapsulating Security Payload (ESP)- means payload (data) will be encrypted and authenticated. Select from below: **DES without Authentication** -Use DES encryption algorithm and not apply any authentication scheme.

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

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

3DES with Authentication-Use triple DES encryption algorithm and apply MD5 or SHA-1 authentication algorithm. **AES without Authentication-**Use AES encryption algorithm and not apply any authentication scheme.

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

Advanced

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

The window of Advance setup is as show below:

KE phase 1 mode	💿 Main mode	O Aggressive mode
KE phase 1 proposal	DES_MD5_G1/DES	_SHA1_G1/3DES_MD5_G1/3DES_MD5_G2 🔽
KE phase 2 proposal	HMAC_SHA1/HMAC	_MD5 🗸
KE phase 1 key lifetime	28800	(900 ~ 86400)
KE phase 2 key lifetime	3600	(600 ~ 86400)
Perfect Forward Secret	 Disable 	🔿 Enable
ocal ID		

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

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

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

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

reused to avoid the computation complexity in phase 2. The default value is inactive this function.
 Local ID-In Aggressive mode, Local ID is on behalf of the IP address while identity authenticating with remote VPN server. For Main mode, the length of the ID is limited to 47 characters.
 Callback Function (for *i* models only)
 The callback function provides a callback service as a part of PPP suite only for the ISDN dial-in user. The router owner will be charged the connection fee by the telecom.
 Require Remote to Callback-Enable this to let the router to require the remote peer to callback for the connection afterwards.
 Provide ISDN Number to Remote-In the case that the remote

peer requires the Vigor router to callback, the local ISDN number will be provided to the remote peer. Check here to allow the Vigor router to send the ISDN number to the remote router. This feature is useful for i model only.

Allowed Dial-In Type			
ISDN		Username	???
PPTP		Password	
☑ IPSec Tunnel		VJ Compression	💿 On 🔘 Off
IPSec Tunnel IDSec Tunnel IDSec Tunnel IDSec Tunnel Specify ISDN CLID or Remote VPN Gateway Peer ISDN Number or Peer VPN Server IP ID Or Peer ID		IKE Authentication M ✓ Pre-Shared Key IKE Pre-Shared Key Digital Signature(X.S) ??? IPSec Security Methentication ✓ Medium (AH) High (ESP) ✓ DES ✓ 3DE Callback Function (C) □ Use the Following Callback Number	od ES V AES BCP) Inction Number to Callback
		Callback Budget	0 minute(s)
4. TCP/IP Network Sett	ings		
My WAN IP	0.0.0.0	RIP Direction	TX/RX Both 💌
Remote Gateway IP	0.0.0.0	For NAT operation, tre	at remote sub-net as
Remote Network IP	0.0.0.0		Private IP 💌
Remote Network Mask	255.255.255.0 More	Change default rou	te to this VPN tunnel
	ок с	Cancel	

Allowed Dial-In Type	Determine the dial-in connection with different types.
ISDN:	Allow the remote ISDN dial-in connection. You can further set up Callback function below. You should set the User Name and Password of remote dial-in user below.
РРТР	Allow the remote dial-in user to make a PPTP VPN connection through the Internet. You should set the User Name and Password of remote dial-in user below.
IPSec Tunnel	Allow the remote dial-in user to trigger a IPSec VPN connection through Internet.

2 Dial-In Sottings



L2TP	Allow the remote dial-in user to make a L2TP VPN connection through the Internet. You can select to use L2TP alone or with IPSec. Select from below: None- Do not apply the IPSec policy. Accordingly, the VPN connection employed the L2TP without IPSec policy can be viewed as one pure L2TP connection. Nice to Have- Apply the IPSec policy first, if it is applicable during negotiation. Otherwise, the dial-in VPN connection becomes one pure L2TP connection. Must- Specify the IPSec policy to be definitely applied on the L2TP connection.
Specify Remote VPN Gateway	You can specify the IP address of the remote dial-in user or peer ID (should be the same with the ID setting in dial-in type) by checking the box. Enter Peer ISDN number if you select ISDN above (This feature is useful for <i>i</i> model only.). Also, you should further specify the corresponding security methods on the right side.
	If you uncheck the checkbox, the connection type you select above will apply the authentication methods and security methods in the general settings.
User Name	This field is applicable when you select PPTP or L2TP with or without IPSec policy above. This field is also applicable if you select ISDN.
Password	This field is applicable when you select PPTP or L2TP with or without IPSec policy above. This field is also applicable if you select ISDN.
VJ Compression	VJ Compression is used for TCP/IP protocol header compression. This field is applicable when you select PPTP or L2TP with or without IPSec policy above. This field is also applicable if you select ISDN.
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 dial-in user. The router owner will be charged the connection fee by the telecom. Check to enable Callback function-Enables the callback function. Callback number-The option is for extra security. Once enabled, the router will ONLY call back to the specified Callback Number. Callback budget- By default, the callback function has limitation of callback period. Once the callback budget is exhausted, the function will be disabled automatically. Callback Budget (Unit: minutes)- Specify the time budget for the dial-in user. The budget will be decreased automatically per callback connection. The default value 0 means no limitation of callback period.
My WAN IP	This field is only applicable when you select PPTP or L2TP with or without IPSec policy above. The default value is 0.0.0.0, which means the Vigor router will get a WAN IP address from the remote router during the IPCP negotiation phase. If the WAN IP address is fixed by remote side, specify the fixed IP address here.
Remote Gateway IP	This field is only applicable when you select PPTP or L2TP with or without IPSec policy above. The default value is 0.0.0.0, which means the Vigor router will get a remote Gateway IP address from the remote router during the IPCP negotiation phase. If the WAN IP address is fixed by remote side, specify the fixed IP address here.
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 router to direct all traffic destined to more Remote Network IP Addresses/ Remote Network Mask through the VPN connection. This is usually used when you find there are several subnets behind the remote VPN router. Profile Index :1 Remote Network 192.168.3.0 / 08 Add Remove Modify
RIP Direction	The option specifies the direction of RIP (Routing Information Protocol) packets. You can enable/disable one of direction here. Herein, we provide four options: TX/RX Both, TX Only, RX Only, and Disable.
RIP Version	Select the RIP protocol version. Specify Ver. 2 for greatest compatibility.
For NAT operation, treat remote sub-net as	While communicating with remote subnet, the router can treat it as private subnet by sending packets with the router's private IP address, or treat it as public subnet by sending



	packets with the router's public IP address.
Change default route to this VPN tunnel	Check this box to change the default route with this VPN tunnel. Be aware that this setting is available only for one WAN interface is enabled. It is not available when both WAN interfaces are enabled.

3.7.7 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.

Dial-out Tool	Refresh S	econds : 10 🖌 Refresh
	(test2)220.135.240.210	
VPN Connection Status Current Page: 2		Back
VPN Type Remote IP	Virtual Network Tx Pkts Tx Rate Rx Pkts Rx	Rate UpTime
	xxxxxxxx : Data i: xxxxxxxx : Data i:	
Dial	Click this button to execute dial out fund	ction.
Refresh Seconds	Choose the time for refresh the dial info and 30.	ormation among 5, 10,
Refresh	Click this button to refresh the whole co	onnection status.
VPN and Remote Access:	> VPN Connection Management	

VPN and Remote Access >> VPN Connection Management

VPN and Remote Access >> Connection Management

Dial-o	ut Tool					Refrest	n Seconds	; : 10 💌	Refresh
					•	Dial			
VPN Connection Status						_			
Curren	t Page: 1								Next
VPN	Туре	Remote IP	Virtual Network	Tx Pkts	Tx Rate	Rx Pkts	Rx Rate	UpTime	
1 (22)	IPSec Tunnel AH-MD5 Auth	192.168.2.24	192.168.22.0/24	7	165	4	3	0:1:2	Drop
2 (23)	IPSec Tunnel AH-MD5 Auth	192.168.2.25	192.168.23.0/24	1	з	1	з	0:1:2	Drop
3 (24)	IPSec Tunnel AH-MD5 Auth	192.168.2.26	192.168.24.0/24	1	3	1	3	0:1:2	Drop
4 (25)	IPSec Tunnel AH-MD5 Auth	192.168.2.27	192.168.25.0/24	1	з	1	з	0:0:57	Drop

xxxxxxxx : Data is encrypted. xxxxxxxx : Data isn't encrypted.

3.8 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.

3.8.1 Local Certificate

ertificate Management >> Local Certificate				
509 Local Certificate Configuration				
Name	Subject	Status	Modify	
Local			View Delete	
GENERATE	IMPORT REFRESH			
X509 Local C	ertificate			
			<u>~</u>	

Generate

Click this button to open Generate Certificate Request window.

Subject Alternative Name	
Туре	Domain Name 💙
Domain Name	
Subject Name	
Country (C)	
State (ST)	
Location (L)	
Orginization (O)	
Orginization Unit (OU)	
Common Name (CN)	
Email (E)	
Кеу Туре	RSA V
Key Size	1024 Bit 🗸

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

Click this button to import a saved file as the certification information.

Import



Click this button to refresh the information listed below.

Refresh 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: x509 Local Certificate Configuration

Name	Subject	Status	Modify
Local	/C=TW/O=DrayTek/emailAddress	Requesting	View Remove
GENERATE	IMPORT REFRESH		
X509 Lo	ocal Certificate Request		
MIIBqj(Bgkqhk: A4GNAD(hX4Dp85 x/G0A7(oCkwJw hkiG9w(Yo6xQg) vvVXnhl	EGIN CERTIFICATE REQUEST CCARMCAQAwQTELMAkGA1UEBhMCVFcxEDAO iG9w0BCQEWEXByZXNzQGRyYX10ZWsuY29t CBiQKBgQDQYB7wmZFfFhN9/IeQnG03Xk++ 9cUF9dloACGGiM/tcBOckdcZdPFFvIXcP3 CTvO/fQzpxroCw1JTjLSjS0/Bn9v50951G YJKoZIhvcNAQkOMRowGDAWBgNVHREEDZAN DBAQUFAAOBgQBuIWx4Mf18xeLQN7nz30cK hiXfnaRX4rdLj6ywBQ9aVdNHr+t11LgVq0 WUx2gq/QIQ6tYs+Stws+51pU+UNGSnj6je ND CERTIFICATE REQUEST	MIGfMAOGCSqGS hqFb297aPJ6+g s3uxa2Fj8aeTj: ve3aGly1cEcmU ggtkcmF5dGVrL; VC4h574hhm/ME CxxcNj1LfLm9t	Ib3DQEBAQUA ksBer1wa5w0 9W+ELxwhI1o 7jqeQIDAQAB mNvbTANBgkq kgemB/eWrIN JFWi4iw30ci
			~

3.8.2 Trusted CA Certificate

Trusted CA certificate lists three sets of trusted CA certificate.

```
Certificate Management >> Trusted CA Certificate
```

X509 Trusted CA Certificate Configuration

Name	Subject	Status	Modify
Trusted CA-1			View Delete
Trusted CA-2			View Delete
Trusted CA-3			View Delete

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

Certificate Management >> Trusted CA Certificate

imported will be listed on the Trusted CA Certificate window.

nport 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.



rtificate Information - Microsoft Inte	ernet Explorer	
Contifi	cate Detail Information	
		1
Certificate Name:	Trusted CA-1	
Issuer:		
Subject:		
Subject Alternative Name:		
Valid From:		
Valid To:		
	Close	_

3.9 VoIP (for V model only)

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

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

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

sip: user:password @ host: port

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

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

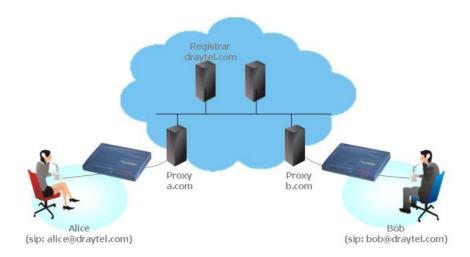
Usually there will be two types of calling scenario, as illustrated below:

• Calling via SIP Servers

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

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





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

• Peer-to-Peer

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



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

3.9.1 DialPlan

This page allows you to set phone book and digit map for the VoIP function. Click the **Phone Book** and **Digit Map** links on the page to access into next pages for dialplan settings.

```
VoIP >> DialPlan Setup
```

```
DialPlan Configuration

        Phone Book

        Digit Map
```

Phone Book

In this section, you can set your VoIP contacts in the "phonebook", called DialPlan. It can help you to make calls quickly and easily by using "speed-dial" **Phone Number**. There are



total 60 index entries in the DialPlan for you to store all your friends and family members' SIP addresses.

VoIP >> DialPlan Setup

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

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

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

VoIP >> DialPlan Setup

Phone Book Index No. 1				
🗹 Enable				
Phone Number	1			
Display Name	Polly			
SIP URL	1112 @ fwd.pulver.com			
Enable	OK Clear Cancel Click this to enable this entry.			
Phone Number	The speed-dial number of this index. This can be any number you choose, using digits $0-9$ and $*$.			
Display Name	The Caller-ID that you want to be displayed on your friend's screen. This let your friend can easily know who's calling without memorizing lots of SIP URL Address.			
SIP URL	Enter your friend's SIP Address			

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.

Enable	Prefix Number	Mode	OP Number	Min Len	Max Len	Interface
~	03	Replace 🛩	8863	7	9	VolP1 🔽
✓	886	Strip 🔽	886	7	9	VoIP4 💌
		None 🔽		0	0	VoIP1 🔽
		None 🗸		0	0	VoIP1 🔽
		None 🗸 🗸		0	0	VoIP1 🔽
		None 🗸 🗸		0	0	VoIP1 🔽
		None 🗸 🗸		0	0	VoIP1 🔽
		None 🔽		0	0	VolP1 🔽
		None 🔽		0	0	VoIP1 🔽
		None 🔽		0	0	VoIP1 🔽
		None 🔽		0	0	VoIP1 🔽
		None 🔽		0	0	VoIP1 🔽
		None 🔽		0	0	VoIP1 🔽
		None 🔽		0	0	VoIP1 🔽
		None 🔽		0	0	VoIP1 🔽
		None 🔽		0	0	VoIP1 🔽
		None 💌		0	0	VoIP1 💌
		None 💌		0	0	VoIP1 💌
		None 💌		0	0	VolP1 💌
		None 🔽		0	0	VoIP1 🔽
nable		Check this	K Cancel box to invoke thi	s setting.		
refix Nu	ımber	The phone OP numbe	number set here : r.	is used to a	dd, strip, o	or replace t
Iode		added with specific Vo Strip - Wh deleted by VoIP inter page) as an	action. en you choose thi in the prefix number oIP interface. nen you choose th the prefix number face. Take the about n example, the OF y for the prefix nu	er for callir is mode, th r for callin ove picture number of	ng out thro ne OP num g out throu (Prefix Ta f 886 will	ugh the ber will be ugh the spe uble Setup

VoIP >> DialPlan Setup

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" and sent to SIP server.



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 six pre-saved SIP accounts.

3.9.2 SIP Accounts

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

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

Index	Profile	Domain/Realm	Proxy	Account Name	Ring	Port	Status
1				change_me	VoIP1		-
2				change_me	VoIP1	VoIP2	-
<u>3</u>				change_me	VoIP1	VoIP2	-
4				change_me	📃 VoIP1	VoIP2	-
<u>5</u>				change_me	VoIP1	VoIP2	-
<u>6</u>				change_me	VoIP1	VoIP2	-
NAT Tra	iversal Se	tting			R: success reg -: fail to regist		
	STUN s	erver:					
	Externa	I IP:					
	SIP PIN	G interval:	150	sec			

VoIP >> SIP Accounts

Index	Click this link to access into next page for setting SIP account.
Profile	Display the profile name of the account.
Domain/Realm	Display the domain name or IP address of the SIP registrar server.
Proxy	Display the domain name or IP address of the SIP proxy server.
Account Name	Display the account name of SIP address before @.
Ring Port	Specify which port will ring when receiving a phone call.
STUN Server	Type in the IP address of the STUN server.
External IP	Type in the gateway IP address.
SIP PING interval	The default value is 150 (sec). It is useful for a Nortel server NAT Traversal Support.
Status	Show the status for the corresponding SIP account. R means such account is registered on SIP server successfully. – means the account is failed to register on SIP server.

Click number under index field to open the following page:

VoIP >> SIP Accounts

Profile Name	(11 char m	ax.)
Register via	None 💌 📃 Call without Re	gistration
SIP Port	5060	
Domain/Realm		(63 char max.)
Proxy		(63 char max.)
🗌 Act as outbound p	roxy	
Display Name	(23 char m	ax.)
Account Number/Name	change_me	(63 char max.)
Authentication ID		(63 char max.)
Password		(63 char max.)
Expiry Time	1 hour 🔽 3600 sec	
NAT Traversal Support	None 💌	
Ring Port	VoIP1 VoIP2	
Ring Pattern	1 💌	

Profile NameAssign a name for this profile for identifying. You can type
similar name with the domain. For example, if the domain name
is *draytel.org*, then you might set *draytel-1* in this field.Register viaIf you do not want to register for VoIP phone, please choose
None. In addition, some SIP server allows users to use VoIP
function without registering. For such server, please check the
box of make call without register. Choosing Auto is
recommended. The system will select a proper way for your

VoIP call.	
Register via	

None 🛛 🐱
None
Auto
WAN
LANAVPN

SIP Port Set the port number for sending/receiving SIP message for building a session. The default value is **5060.** Your peer must set the same value in his/her Registrar. **Domain/Realm** Set the domain name or IP address of the SIP Registrar server. Proxy Set domain name or IP address of SIP proxy server. By the time you can type:port number after the domain name to specify that port as the destination of data transmission (e.g., nat.draytel.org:5065) Act as Outbound Proxy Check this box to make the proxy acting as outbound proxy. The caller-ID that you want to be displayed on your friend's **Display Name** screen. Account Number/Name Enter your account name of SIP Address, e.g. every text before @. **Authentication ID** Check the box to invoke this function and enter the name or number used for SIP Authorization with SIP Registrar. If this setting value is the same as Account Name, it is not necessary for you to check the box and set any value in this field. Password The password provided to you when you registered with a SIP service. **Expiry Time** The time duration that your SIP Registrar server keeps your registration record. Before the time expires, the router will send another register request to SIP Registrar again. NAT Traversal Support If the router (e.g., broadband router) you use connects to internet by other device, you have to set this function for your necessity. NAT Traversal Support None None Stun manual nortel None – Disable this function. Stun – Choose this option if there is Stun server provided for vour router. Manual - Choose this option if you want to specify an external IP address as the NAT transversal support. Nortel – If the soft-switch that you use supports Nortel solution, you can choose this option. **Ring Port** Set VoIP 1 or VoIP 2 as the default ring port.



Ring Pattern

Choose a ring tone type for the VoIP phone call.

Ring Pattern



Below shows successful SIP accounts for your reference.

VoIP >> SIP Accounts

SIP Ac	counts List				٦	Refresh
Index	Profile	Domain/Realm	Proxy	Account Name	Ring Port	Status
1	draytel_1	draytel.org	draytel.org	813177	VoIP1 VoIP2	-
2	draytel_2	draytel.org	draytel.org	812862	🗌 VoIP1 🛛 VoIP2	R
<u>3</u>	draytel_3	draytel.org	draytel.org	811997	VoIP1 VoIP2	-
<u>4</u>	IPTEL	iptel.org	iptel.org	kevin	🗌 VoIP1 🛛 VoIP2	-
<u>5</u>	FWD	fwd.pulver.com	fwd.pulver.com	56894	VoIP1 VoIP2	-
<u>6</u>	SeedNet	seed.net.tw	139,175,232,13	070901002	🗹 VoIP1 🛛 VoIP2	R

R: success registered on SIP server -: fail to register on SIP server

3.9.3 Phone Settings

This page allows user to set phone settings for VoIP 1 and VoIP 2 respectively.

VoIP >> Phone Settings

Phone	List						
Index	Port	Call feature	Codec	Tone	Gain (Mic/Speaker)	Default SIP Account	DTMF Relay
1	VoIP1		G.729A/B	User Defined	5/5	draytel_1	InBand
2	VoIP2		G.729A/B	User Defined	5/5	draytel_1	InBand

RTP

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

RTP

Symmetric RTP – Check this box to invoke the function. To make the data transmission going through on both ends of local router and remote router not misleading due to IP lost (for example, sending data from the public IP of remote router to the private IP of local router), you can check this box to solve this problem.

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

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

e 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 Class3 (Medium Drop) AF Class3 (Medium Drop) AF Class4 (Low Drop) AF Class4 (Medium Drop) AF Class4 (Medium Drop) AF Class4 (High Drop) AF Class4 (High Drop) AF Class4 (High Drop) AF Class4	
	IP precedence 5	×
	· ·	1

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

Click the number 1 or 2 link under Index column, you can access into the following page for configuring Phone settings.

RTP TOS

VoIP >> Phone Settings

Call feature			Codecs	
🔲 Hotline			Prefer Codec	G.729A/B (8Kbps) 🔽
Session Timer	3600	sec		🔲 Single Codec
T.38 Fax Function			Packet Size	20ms 💌
			Voice Active Detector	Off 💌
Call Forwarding	disable 🔽			
SIP URL			Default SIP Account	1-draytel_1 🔽
Time Out	30 sec		Play dial tone only whether the second se	nen account registered
DND(Do Not Disturb) M Index(1-15) in Sci Note: Action and be ignored.	<u>nedule</u> Setup:), tings will		
CLIR (hide caller ID)				
Call Waiting				
📃 Call Transfer				

Hotline	Check the box to enable it. Type in the SIP URL in the field for dialing automatically when you pick up the phone set.
Session Timer	Check the box to enable the function. In the limited time that you set in this field, if there is no response, the connecting call will be closed automatically.
T.38 Fax function	If the remote end also supports FAX function, you can check this box to enable this function.
Call Forwarding	There are four options for you to choose. Disable is to close call forwarding function. Always means all the incoming calls will be forwarded into SIP URL without any reason. Busy means

the incoming calls will be forwarded into SIP URL only when the local system is busy. **No answer** means if the incoming calls do not receive any response, they will be forwarded to the SIP URL by the time out.

Call Forwarding

disable	*
disable	
always	
busy	
no answer	

	abc@iptel.org) as the site f	no answer P URL (e.g., aaa@draytel.org or for call forwarded. ut for the call forwarding. The				
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.					
		of schedule profiles to control the preconfigured schedules. Refer to detailed configuration.				
CLIR (hide caller ID)	Check this box to hide the phone set for the remote side	caller ID on the display panel of the de.				
Call Waiting	appear to tell the user new	his function. A notice sound will phone call is waiting for your to pick up the waiting phone call.				
Call Transfer		his function. Click hook flash to When the phone call connection ne. The other two sides can				
Prefer Codec	codec used for each call wi before each session, and so The default codec is G.729 while maintaining good vo If your upstream speed is o	s the default for your VoIP calls. The ill be negotiated with the peer party o many not be your default choice. OA/B; it occupies little bandwidth ice quality. only 64Kbps, do not use G.711 codec. at least 256Kbps upstream if you				
	Prefer Codec	G.729A/B (8Kbps) G.711MU (64Kbps) G.711A (64Kbps) G.729A/B (8Kbps) G.723 (6.4kbps) G.726 32 (32kbps)				

Single Codec – If the box is checked, only the selected Codec will be applied.

Packet Size-The amount of data contained in a single packet. The default value is 20 ms, which means the data packet will contain 20 ms voice information.

20ms 🔽	
10ms	
20ms	
30ms	
40ms	
50ms	
60ms	

Voice Active Detector - This function can detect if the voice on both sides is active or not. If not, the router will do something to save the bandwidth for other using. Click On to invoke this function; click off to close the function.

Voice Active Detector

Off	*
Off	
On	

Default SIP Account There are six groups of SIP accounts that you can set. Use the drop down list to choose the profile name of the account as the default one.

Default SIP Account	1-draytel_1 💌
Play dial tone only whether the second se	1-draytel 1 2-draytel_2 3-draytel_3 4-IPTEL 5-FVVD 6-SeedNet

Play dial tone only when account registered - Check this box to invoke the function.

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

VoIP >> Phone Settings

Tone Sett	ings							
Region [FSK_ETSI	•						
		Low Freq (Hz)	High Freq (Hz)	T on 1 (msec)	T off 1 (msec)	T on 2 (msec)	T off 2 (msec)	
Dial tone		350	440	0	0	0	0	
Ringing tone		400	450	400	200	400	2000	
Busy tone		400	0	375	375	0	0	
Congestion tone		0	0	0	0	0	0	
Volume G	Gain			DTMF				
Mic Gain(1	L-10)	5	5		le	InBand 🔽		
Speaker G	iain(1-10)	5		Payload Type(rfc2833)		101		
MISC								
Dial Tone	Power Level	27	7					
Ring Frequ	lency	25	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.

Advance Settings >> Phone



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.

DTMF mode – There are four selections provided here: InBand:Choose this one then the Vigor will send the DTMF tone as audio directly when you press the keypad on the phone OutBand: Choose this one then the Vigor will capture the keypad number you pressed and transform it to digital form then send to the other side; the receiver will generate the tone according to the digital form it receive. This function is very useful when the network traffic congestion occurs and it still can remain the accuracy of DTMF tone. SIP INFO: Choose this one then the Vigor will capture the

DTMF tone and transfer it into SIP form. Then it will be sent to the remote end with SIP message.

DTMF mode

InBand	Y
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.

3.9.4 Status

VoIP >> Status

DTMP

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

Status Refresh Seconds: 10 💌 Refresh									Refresh		
Port §	Status	Codec	PeerID	Elapse (hh:mm:ss)	Tx Pkts	Rx Pkts	Rx Losts	Rx Jitter (ms)	In Calls	Out Calls	Speaker Gain
VoIP1	IDLE			00:00:00	0	0	0	0	0	0	5
VoIP2	IDLE			00:00:00	0	0	0	0	0	0	5

Date		Time	Duration	In/Out	Peer ID
(mm-dd-y	ууу)	(hh:mm:ss)	(hh:mm:ss)		
00-00-	0	00:00:00	00:00:00	-	
00-00-	0	00:00:00	00:00:00	-	
00-00-	0	00:00:00	00:00:00	-	
00-00-	0	00:00:00	00:00:00	-	
00-00-	0	00:00:00	00:00:00	-	
00-00-	0	00:00:00	00:00:00	-	
00-00-	0	00:00:00	00:00:00	-	
00-00-	0	00:00:00	00:00:00	-	
00-00-	0	00:00:00	00:00:00	-	
00-00-	0	00:00:00	00:00:00	-	

Refresh Seconds

Specify the interval of refresh time to obtain the latest VoIP calling information. The information will update immediately

when the Refresh button is clicked.

Refresh Seconds	:	10	*
		5	
		10	
		30	

Port	It shows current connection status for the port of VoIP1, VoIP2, ISDN1 and ISDN2. Status of ISDN is available for VGi model only.				
Status	It shows the VoIP connection status. IDLE - Indicates that the VoIP function is idle. HANG_UP - Indicates that the connection is not established (busy tone). CONNECTING - Indicates that the user is calling out. WAIT_ANS - Indicates that a connection is launched and waiting for remote user's answer. ALERTING - Indicates that a call is coming. ACTIVE-Indicates that the VoIP connection is launched.				
Codec	Indicates the voice codec employed by present channel.				
PeerID	The present in-call or out-call peer ID (the format may be IP or Domain).				
Elapse	The format is represented as seconds.				
Tx Pkts	Total number of transmitted voice packets during this connection session.				
Rx Pkts	Total number of received voice packets during this connection session.				
Rx Losts	Total number of lost packets during this connection session.				
Rx Jitter	The jitter of received voice packets.				
In Calls	The accumulating times of in-call.				
Out Calls	The accumulating times of out-call.				
Speaker Gain	The volume of present call.				
Log	Display logs of VoIP calls.				

3.10 ISDN (for *i* model only)

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.

3.10.1 General Setup

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

ISDN >> General Setup

ISDN Setup

ISDN Port	💿 Enable 🔘 Disable	Blocked MSN numbers for the router
Country Code	International 🔽	1.
Own Number		2.
"Own Number" means that remote end the ISDN num		з.
outgoing call.	ioor whom it's placing an	4.
MSN numbers for the rout	er	5.
	1.	
	2.	
	3.	
"MSN Numbers" means that accept number-matched addition, MSN service sho local ISDN network provid	incoming calls. In ould be supported by the	
	0	К

ISDN Port	Click Enable to open the ISDN port and Disable to close it.
Country Code	For proper operation on your local ISDN network, you should choose the correct country code.
Own Number	Enter your ISDN number. Every outgoing call will carry the number to the receiver.
Blocked MSN Numbers for the router	Enter the specified MSN number into the fields to prevent the router from dialing the specific MSN number.
MSN Numbers for the Router	MSN Numbers mean that the router is able to accept only number-matched incoming calls. In addition, MSN services should be supported by local ISDN network provider. The router provides three fields for MSN numbers. Note that MSN services must be acquired from your local telecommunication operators. By default, MSN function is disabled. If you leave the fields blank, all incoming calls will be accepted without number matching. 1,2,3 fields – Fill in the portion that is different with the own number. For example, the own number is 1234567 and three MSN numbers are 1234550 , 1234517 and 1234582 respectively. You can type in 1234567 in the filed of own number. Fill in 50 , 17 and 67 on the fields of 1,2 and 3 one by one without typing 12345.
Mapping to VoIP Ports	Check to specify ringing from FXS1 and/or FXS2 when the router accepts the incoming calls by identifying MSN number(s). If you do not specify any port in this field, the ISDN loop through ring port will be determined by the configuration in ISDN port in VoIP>>Phone Settings .



3.10.2 Dialing to a Single ISP

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

ISDN >>	Dialing	to a	Single	ISP
5011	Diamig	ιυa	Single	

ISP Access Setup		PPP/MP Setup	PPP/MP Setup		
SP Name	prima	Link Type	Dialup BOD 🛛 👻		
Dial Number	9834737	PPP Authentication	PAP or CHAP 🔽		
Username	amor	Idle Timeout	180 second(s) nent Method (IPCP)		
Password	••••	Fixed IP	○ Yes ⊙ No (Dynamic IP)		
Require ISP callback (CBCP)		Fixed IP Address			
Index(1-15) in <u>Sc</u>	:hedule Setup:				
=>, [,,				

OK

ISP Name	Enter your ISP name.			
Dial Number	Enter the ISDN access number provided by your ISP.			
Username	Enter the username provided by your ISP.			
Password	Enter the password provided by your ISP.			
Require ISP Callback (CBCP)	If your ISP supports the callback function, check this box to activate the Callback Control Protocol during the PPP negotiation.			
Scheduler (1-15)	Enter the index of schedule profiles to control the Internet access according to the preconfigured schedules.			
Link Type	There are four link types: Link Disable, Dialup 64 Kbps, Dialup 128 Kbps, and Dialup BOD. Link Disable - Disable the ISDN dial-out function. Dialup 64Kbps - Use one ISDN B channel for Internet access. Dialup 128Kbps - Use both ISDN B channels for Internet access. Dialup BOD - BOD stands for bandwidth-on-demand. The router will use only one B channel in low traffic situations. Once the single B channel bandwidth is fully used, the other B channel will be activated automatically through the dialup. For more detailed BOD parameter settings, please refer to the Advanced Setup field > Call Control and PPP/MP Setup.			
PPP Authentication	PAP Only - Configure the PPP session to use the PAP protocol to negotiate the username and password with the ISP.PAP or CHAP - Configure the PPP session to use the PAP or CHAP protocols to negotiate the username and password with the ISP.			
Idle Timeout	Idle timeout means the router will be disconnect after being idle for a preset amount of time. The default is 180 seconds. If you set the time to 0, the ISDN connection to the ISP will always remain on.			
Fixed IP	In most environments, you should not change these settings as most ISPs provide a dynamic IP address for the router when it connects to the ISP. If your ISP provides a fixed IP address, check Yes t o invoke			

this function and enter the IP address in the field of **Fixed IP** Address.

Fixed IP Address Type the IP address.

3.10.3 Dialing to Dual ISPs

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

ISDN >> Dialing to Dual ISPs

Dual ISP					
Common Settings	;	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 Setu	3	Secondary ISP Setup			
ISP Name	prima	ISP Name	dingo		
Dial Number	9834737	Dial Number	8849343		
Username	amor	Username	amor		
Password	••••	Password	••••		
IP Address Assign	nment 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			
ОК					

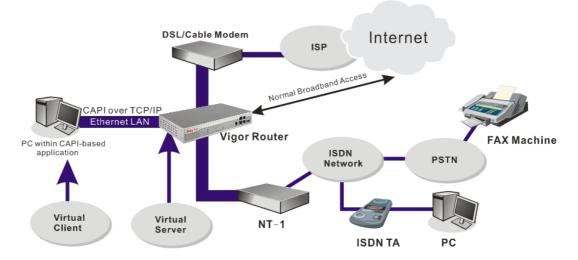
Most configuration parameters are the same as those of the previous part. This screen provides a checkbox to enable the Dual ISPs function and adds the secondary ISP Setup section field. Check the corresponding box and enter the second ISP information. About the details please refer to the descriptions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

3.10.4 Virtual TA

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

- The Virtual TA client only supports MicrosoftTM Windows 98/SE/2000/XP platforms.
- The Virtual TA client only supports the CAPI 2.0 protocol and has no built-in FAX engine.
- One ISDN BRI interface has two B channels. The maximum number of active clients is also two.
- Before you configure the Virtual TA, you must set the correct country code.





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

Before describing the configuration of Virtual TA in the Vigor routers, please heed the following limitations.

- The Virtual TA client only supports MicrosoftTM Windows 98/SE/2000/XP platforms.
- The Virtual TA client only supports the CAPI 2.0 protocol and has no built-in FAX engine.
- One ISDN BRI interface has two B channels. The maximum number of active clients is also 2.
- Before you configure the Virtual TA, you must set the correct country code in **ISDN Setup**.

Virtual TA Setup Virtual TA Server 💿 Enable 🔘 Disable Virtual TA Users Profiles Active Username Password MSN1 MSN2 MSN3 1. 2. з. 4. 5. ΟK Virtual TA Server **Enable:** Select it to activate the server. **Disable:** Select it to deactivate the server. All Virtual TA applications will be terminated. Virtual TA User Profiles

applications will be terminated.ual TA User ProfilesUsername - Enter the username of a specific client.
Password - Enter the password of a specific client.
MSN 1/2/3 - MSN stands for Multiple Subscriber Number. It
means you can apply to more than one ISDN lines number over a
single subscribed line. Note that the service must be acquired

DrayTek

ISDN >> Virtual TA

from your telecom. Specify the MSN numbers for a specific client. If you have no MSN services, leave this field blank. **Active -** Check it to enable the client to access the server.

Install a Virtual TA Client

- 1. Insert the CD-ROM bundled with your Vigor router. Find **VTA Client** tool in the Utility menu and click on the Install button.
- 2. Follow the on-screen instructions of the installer. The last step will ask you to restart your computer. Click **OK** to restart your computer.
- 3. After the computer restarts, you will see a VT icon in the taskbar (usually in the bottom-right of the screen, near the clock) as shown below.

When the icon text is GREEN, the Virtual TA client is connected to the Virtual TA server and you can launch your CAPI-based software to use the client to access the router. If the icon text is RED, it means the client has lost the connection to the server. This time, please check the physical Ethernet connection.

Configure a Virtual TA Client/ Server

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

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

User Profile

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

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

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



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





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

Virtual TA Login	
User Name :	alan
Password :	XXXX
OK	Cancel

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

MSN Configuration

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

Suppose that you could assign the MSN number 123 to the client "alan".

Virtual TA Setup						
Virtual TA Server : Enable Disable						
Virtual TA Users Pro	files					
Username	Password	MSN1	MSN2	MSN3	Active	
1. alan	••••	123			\checkmark	
2.						

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

3.10.5 Call Control

Some applications require that the router (only for the ISDN models) be remotely activated, or be able to dial up to the ISP via the ISDN interface. Vigor routers provide this feature by allowing user to make a phone call to the router and then ask it to dial up to the ISP. Accordingly, a teleworker can access the remote network to retrieve resources. Of course, a fixed IP address is required for WAN connection and some internal network resource has to be exposed for remote users, such as FTP, WWW.Please set **Dialing to a Single ISP** first before configuring this web page.

ISDN >> Call Control

Call Control Setup			
Dial Retry	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)
7		-	

ΟK

Dial Retry	It specifies the dial retry counts per triggered packet is the packet who local network. The default setting each triggered packet, the router w connected to the ISP or remote act	be destination is outside the is no dial retry. If set to 5, for vill dial 5 times until it is
Dial Delay Interval	It specifies the interval between dialup retries. By default, the interval is 0 second.	
Remote Activation	It specifies a phone number in the Remote Activation field to enable the remote activation function. If the router accepts a call from the number 12345678, it will terminate the incoming call immediately and dial to the ISP.	
Link Type	Because ISDN has two B channels (64Kbps/per channel), you can specify whether you would like to have single B channel, two B channels or BOD (Bandwidth on Demand). Four options are available: Link Disable, Dialup 64Kbps, Dialup 128Kbps, Dialup BOD.	
	Link Type	Dialup BOD Link Disable Dialup 64Kbps Dialup 128Kbps Dialup BOD
PPP Authentication	It specifies the PPP authentication method for PPP/MP connections. Normally you can set it to PAP/CHAP for better compatibility.	
TCP Header Compression	VJ Compression - It is used for TCP/IP protocol header compression. Normally it is set to None to improve bandwidth	



	utilization. TCP Header Compression None None VJ COMP
Idle Timeout	Because our ISDN link type is "Dial On Demand", the connection will be initiated only when needed.
High Water Mark and High Water Time	BOD stands for bandwidth-on-demand for Multiple-Link PPP (ML-PPP or MP). High Water Mark/ High Water Time/ Low Water Mark/Low Water Time parameters are applied when you set the Link Type to Dialup BOD . The ISDN usually uses one B channel to access the Internet or remote network when you choose the Dialup BOD link type. The router will use the parameters here to decide on when you activate/drop the additional B channel. Note that cps (characters-per-second) measures the total link utilization.
	These parameters specify the situation in which the second channel will be activated. With the first connected channel, if its utilization exceeds the High Water Mark and such a channel is being used over the High Water Time, the additional channel will be activated. Thus, the total link speed will be 128kbps (two B channels).
Low Water Mark and Low Water Time	These parameters specify the situation in which the second channel will be dropped. In terms of the two B channels, if their utilization is under the Low Water Mark and these two channels are being used over the High Water Time, the additional channel will be dropped. As a result, the total link speed will be 64kbps (one B channel).

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

3.11 Wireless LAN (for G model only)

This function is used for G models only.

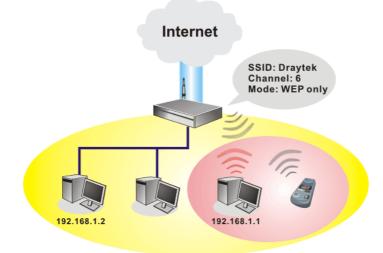
3.11.1 Basic Concepts

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

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

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

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



Security Overview

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

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

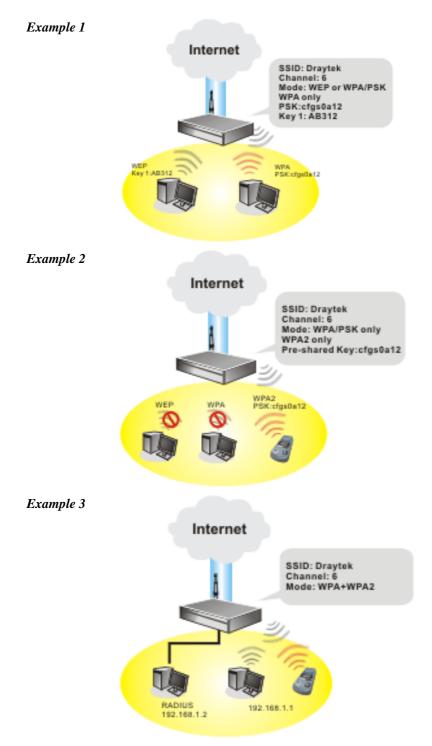
WEP (Wired Equivalent Privacy) is a legacy method to encrypt each frame transmitted via radio using either a 64-bit or 128-bit key. Usually access point will preset a set of four keys and it will communicate with each station using only one out of the four keys.

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

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

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





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.

3.11.2 General Setup

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

Wireless LAN >> General S	etup
General Setting (IEEE 802.	11)
Enable Wireless LAN	
Mode :	Mixed(11b+11g)
SuperG Overdrive:	◉ Off ◯ On
Note : The overdrive e down other parts of th	nhances the WLAN-to-LAN throughput; however, it may slow ne router.
Index(1-15) in <u>Schedule</u> Setup:	
SSID :	default
Channel :	Channel 6, 2437MHz 💌
Note: If SuperG mode	is enabled, channel is fixed at 6.
Hide SSID	
Hide SSID : prevent S	SSID from being scanned.
Long Preamble : nec	essary for some older 802.11b devices only (lowers performance).
	OK Cancel
Enable Wireless LAN	Check the box to enable wireless function.
Mode	Select an appropriate wireless mode. Mixed (11b+11g+SuperG) - The radio can support IEEE802.11b, IEEE802.11g and SuperG protocols
	simultaneously. Mixed (11b+11g) - The radio can support both IEEE802.11b and IEEE802.11g protocols simultaneously
	SuperG - The radio only supports SuperG. 11g only - The radio only supports IEEE802.11g.
	11b only - The radio only supports IEEE802.11b.
	Mode : Mixed(11b+11g)
	Mixed(11b+11g+SuperG)
	Mixed(11b+11g) SuperG Only
	11g Only
	11b Only
SuperG Overdrive	Enhance the transmission rate up to 108Mbps between the
	host and the clients. Generally, the maximum transmission
	rate is 54Mbps without such feature. Notice that the network card in client must also support SuperG. If not, the
	rate would be 54Mbps even if you enable this function.
ndex(1-15)	Set the wireless LAN to work at certain time interval only
	You may choose up to 4 schedules out of the 15 schedules
	pre-defined in Applications >> Schedule setup. The
	default setting of this filed is blank and the function will



always work.

SSID	The default SSID is "default". We suggest you change it to a particular name. It is the identification of the wireless LAN. SSID can be any text numbers or various special characters.	
Channel	The channel of frequency of the wireless LAN. The default channel is 6. You may switch channel if the selected channel is under serious interference.	
	Channel :	Channel 6, 2437MHz Channel 1, 2412MHz Channel 2, 2417MHz Channel 3, 2422MHz Channel 4, 2427MHz Channel 5, 2432MHz Channel 5, 2432MHz Channel 8, 2447MHz Channel 8, 2447MHz Channel 9, 2452MHz Channel 10, 2457MHz Channel 11, 2462MHz Channel 12, 2467MHz Channel 13, 2472MHz
Hide SSID	Check it to prevent from wireless sniffing and make it harder for unauthorized clients or STAs to join your wireless LAN. Depending on the wireless utility, the user may only see the information except SSID or just cannot see any thing about Vigor wireless router while site surveying.	
Long Preamble	This option is to define the length of the sync field in an 802.11 packet. Most modern wireless network uses short preamble with 56 bit sync filed instead of long preamble with 128 bit sync field. However, some original 11b wireless network devices only support long preamble. Check it to use Long Preamble if needed to communicate with this kind of devices.	

3.11.3 Security

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

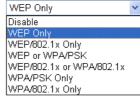
Wireless LAN >>	Security	Settings
-----------------	----------	----------

Mode :	Disable 💌
Set up RADIUS Se	rver if 802.1× is enabled.
WPA:	
Туре:	Mixed(WPA+WPA2) OWPA2 Only
Pre-Shared Key(PSK)	*****
Type 8~63 ASCII "cfgs01a2" or "0	character or 64 Hexadecimal digits leading by "Ox", for example x655abcd".
WEP:	
Encryption Mode:	64-Bit 👻
Use	WEP Key
⊙ Key 1 :	*****
○Key 2 :	******
○кеу 3:	****
○Key 4 :	****
"Óx4142333132". For 128 bit WEP key Type 13 ASCII character	or 10 Hexadecimal digits leading by "0x", for example "AB312" or or 26 Hexadecimal digits leading by "0x", for example 10313233343536373839414243".

Mode :

Mode

There are several modes provided for you to choose.



Disable - Turn off the encryption mechanism.

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

WEP/802.1x Only - Accept WEP clients with 802.1x authentication. Since the key will be auto-negotiated during authentication, the field of key setting below will be not available for input.

WEP or WPA/PSK - Accept WEP and WPA clients with legal key accordingly. Only Mixed (WPA+WPA2) is applicable if you select WPA/PSK.

WEP/802.1x or WPA/802.1x - Accept WEP or WPA clients with 802.1x authentication. Only Mixed(WPA+WPA2) is applicable if you select WPA/PSK. Since the key will be auto-negotiated during authentication, the field of key setting below will be not available for input.

WPA/PSK Only - Accept WPA clients and the encryption key should be entered in PSK. Remember to select WPA type to define either Mixed or WPA2 only in the field below.

WPA/802.1x Only - Accept WPA clients with 802.1x authentication. Remember to select WPA type to define either Mixed or WPA2 only in the field below. Since the key will be



	auto-negotiated during authentication, the field of key setting below will be not available for input.	
WPA	The WPA encrypts each frame transmitted from the radio usin the key, which either PSK entered manually in this field below automatically negotiated via 802.1x authentication. Type - Select from Mixed (WPA+WPA2) or WPA2 only. Pre-Shared Key (PSK) - Either 8~63 ASCII characters, such 012345678(or 64 Hexadecimal digits leading by 0x, such as "0x321253abcde").	wor
WEP	 64-Bit - For 64 bits WEP key, either 5 ASCII characters, such 12345 (or 10 hexadecimal digitals leading by 0x, such as 0x4142434445.) 128-Bit - For 128 bits WEP key, either 13 ASCII characters, s as ABCDEFGHIJKLM (or 26 hexadecimal digits leading by 0 such as 0x4142434445464748494A4B4C4D). 	such
	Encryption Mode: 64-Bit 64-Bit 128-Bit	
	All wireless devices must support the same WEP encryption b	oit

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

3.11.4 Access Control

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

ccess Control	
🗹 Enable Acces	s Control
	Policy : Activate MAC address filter 💌
	MAC Address Filter
	Index Attribute MAC Address
	Client's MAC Address :::::::
	s: Isolate the station from LAN
	Note: Two attributes cannot coexist with each other.
	Add Remove Edit Cancel

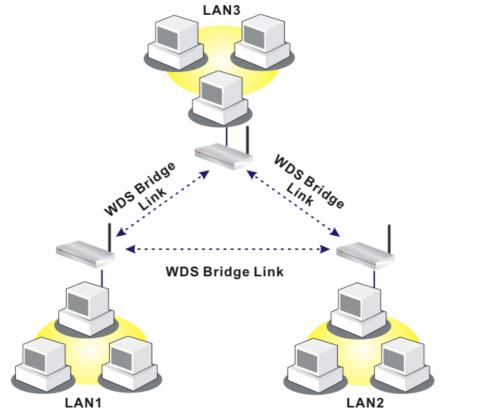
Enable Access Control	Select to enable the MAC Address access control feature.
Policy	Select to enable any one of the following policy. Choose Activate MAC address filter to type in the MAC addresses for other clients in the network manually. Choose Isolate WLAN from LAN will separate all the WLAN stations from LAN based on the MAC Address list. Policy : Activate MAC address filter Activate MAC address filter Isolate WLAN from LAN
MAC Address Filter	Display all MAC addresses that are edited before. Four buttons (Add, Remove, Client's MAC Address - Manually enter the MAC address of wireless client.
Attribute	s – select it 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.

3.11.5 WDS

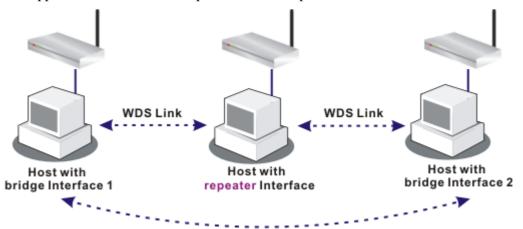
WDS means Wireless Distribution System. It is a protocol for connecting two access points (AP) wirelessly. Usually, it can be used for the following application:

- Provide bridge traffic between two LANs through the air.
- Extend the coverage range of a WLAN.

To meet the above requirement, two WDS modes are implemented in Vigor router. One is **Bridge**, the other is **Repeater**. Below shows the function of WDS-bridge interface:



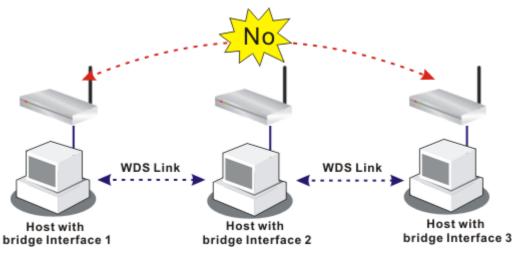
The application for the WDS-Repeater mode is depicted as below:



The major difference between these two modes is that: while in **Repeater** mode, the packets received from one peer AP can be repeated to another peer AP through WDS links. Yet in **Bridge** mode, packets received from a WDS link will only be forwarded to local wired or wireless hosts. In other words, only Repeater mode can do WDS-to-WDS packet forwarding.



In the following examples, hosts connected to Bridge 1 or 3 can communicate with hosts connected to Bridge 2 through WDS links. However, hosts connected to Bridge 1 CANNOT communicate with hosts connected to Bridge 3 through Bridge 2.



Click **WDS** from **Wireless LAN** menu. The following page will be shown.

WDS Settings	Set to Factory Default
	Bridge
Mode: Bridge 🎽	Enable Peer MAC Address
Security:	
💿 Disable 🔘 WEP 🔘 Pre-shar	d Key
WEP:	
Use the same WEP key set in Sec.	
Settings.	
Encryption Mode 🔡 64-bit 💟	Note: Disable unused links to get better
Key index 🛛 : 1 🔽	performance.
The key index is fixed if the security	node is not Repeater
"WEP Only".	Enable Peer MAC Addess
Key :	
The key format is the same as the or Security Settings.	e used in
	Access Point Function:
	💿 Enable 🔹 🔿 Disable
Pre-shared Key:	
Type : TKIP	Status:
Кеу :	Send "Hello" message to peers.
Type 8~63 ASCII characters or 64 he digits leading by "Ox", for example "cf "Ox655abcd".	
	OK Cancel
Aode	Choose the mode for WDS setting. Disable mode will not
loue	invoke any WDS setting. Bridge mode is designed to fulfill th
	first type of application. Repeater mode is for the second one
	Mode: Disable 🗸
	Disable
	Bridge
	Repeater
ecurity	There are three types for security, Disable , WEP and
v	

Wireless LAN >> WDS Settings

Pre-shared key. The setting you choose here will make the



	following WEP or Pre-shared key field valid or not. Choose one of the types for the router.
WEP	Check this box to use the same key set in Security Settings page. If you did not set any key in Security Settings page, this check box will be dimmed.
	 Encryption Mode - If you checked the box of Use the same WEP key, you do not need to choose 64-bit or 128-bit as the Encryption Mode. If you do not check that box, you can set the WEP key now in this page. Key Index - Choose the key that you want to use after selecting the proper encryption mode. Key - Type the content for the key.
Pre-shared Key	Type 8 ~ 63 ASCII characters or 64 hexadecimal digits leading by " $0x$ ".
Bridge	If you choose Bridge as the connecting mode, please type in the peer MAC address in these fields. Six peer MAC addresses are allowed to be entered in this page at one time. Yet please disable the unused link to get better performance. If you want to invoke the peer MAC address, remember to check Enable box in the front of the MAC address after typing.
Repeater	If you choose Repeater as the connecting mode, please type in the peer MAC address in these fields. Two peer MAC addresses are allowed to be entered in this page at one time. Similarly, if you want to invoke the peer MAC address, remember to check Enable box in the front of the MAC address after typing.
Access Point Function	Click Enable to make this router serving as an access point; click Disable to cancel this function.
Status	It allows user to send "hello" message to peers. Yet, it is valid only when the peer also supports this function.

3.11.6 AP Discovery

Wireless LAN >> Access Point 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.

		-			
cess Point List					
	BSSID	Channel	SSID		
		Scan			
See <u>St</u>	atistics.				
	During the scanning t with the router.	process (~5 secc	inds), no statio	n is allowed to	
Add to	WDS Settings :				
AP's MA	C address		:::	Add	

If you want the found AP applying the WDS settings, please type in the AP's MAC address on the bottom of the page and click **Add**. Later, the MAC address of the AP will be added to the page of WDS setting.



3.11.7 Station List

Wireless LAN >> Station List

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

Station List		
	Status	MAC Address
	1	Refresh
	tus Codes :	
	Connected, No en Connected, WEP.	cryption.
	Connected, WPA. Connected, WPA2	
B:	Blocked by Acces:	
	Connecting. Fail to pass 802.1	× or WPA/PSK authentication.
		i connects to the router successfully, it may be itice. In that case, it will still be on the list until the
	nection expires.	
Ad	d to <u>Access Contro</u>	<u>1</u> :
Clie	ent's MAC address	
		Add

Refresh

Add

Click this button to refresh the status of station list.

Click this button to add current selected MAC address into Access Control.

3.11.8 Station Rate Control

This page allows you to control the upload and download rate of each wireless client (station). Please check the box of **Enable** to invoke this setting. The range for the rate is between $100 \sim 30,000$ kbps.

Wireles	s LAN >> Station Rate Co	ontrol			
Station	Rate Control				
🗹 Enab	le				
	Upload Rate :		300	00 Kbps	
	Download Rate :		300	00 Kbps	
	Note: 1. Range: 100~30,000 Kb 2. The specified rates are				
		ОК	Cance		

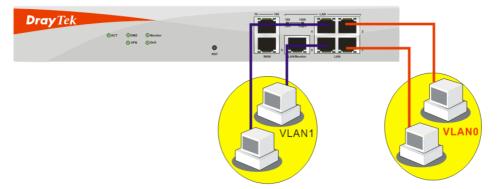
3.12 VLAN

Note: This menu is available for **Vigor3100G** model only. For Vigor3100 and Vigor3120, please refer to 3.2.4.

Virtual LAN function provides you a very convenient way to manage hosts by grouping them based on the physical port.

3.12.1 Wired VLAN

PCs connected to Ethernet ports of the router can be divided into different groups and formed VLAN. PCs under the same groups can share each other information through the router and will not be peeked by other groups.



The VLAN >> Wired VALN allows you to configure VLAN settings through wired connection to achieve the above intention. Simply check P1 and P2 boxes on the line of VLAN0; and check P3 and P4 boxes on the line of VLAN1.

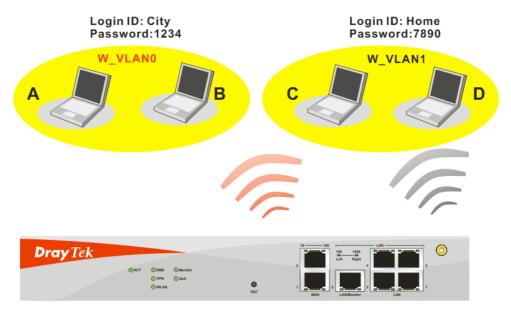
VLAN >> Wired VLAN Configuration

Wired VLAN Configura	ition			
🗹 Enable				
	P1	P2	P3	P4
VLANO		✓		
VLAN1			\checkmark	
VLAN2				
VLAN3				
Enable		eck this box to enantiguration).	ble this function	n (for VLAN
P1 – P4	bei be che VL	ng grouped in spec grouped in differe ock the box. For ex	cified VLAN. B nt VLAN at the ample, if you cl N1-P1, you can	make P1 to be grouped
VLAN0-3	Thi	s router allows yo	u to set 4 group	s of virtual LAN.

3.12.2 Wireless VLAN

PCs (equipped with wireless network cards) connected to the router through wireless interface can be divided into different groups and formed W_VLAN. PCs under the same groups can share each other information through the router and will not be peeked by other groups.

PCs under the same groups can use same Login ID and password to access into Internet. For example, see the following graphic. Both A and B use the same login ID (City) and password (1234). Therefore, they are grouped in the same W_VLAN.



The VLAN >> Wireless VALN allows you to configure Wireless VLAN settings through wireless connection to achieve the above intention. Simply type Login ID and password with City and 1234 in the boxes of W_VLAN0. And type Login ID and password with Home and

7890 in the boxes of W_VLAN1. Users can configure fifteen groups of wireless VLAN in this page.

VLAN >> Wireless VLAN Setup

🗹 Enable						View <u>Online</u>	Station Table
W_VLAN	Login ID	Password	Attributes	W_VLAN	Login ID	Password	Attributes
0			Details	8			Details
1			Details	9			Details
2			Details	10			Details
з			Details	11			Details
4			Details	12			Details
5			Details	13			Details
6			Details	14			Details
7			Details	15			Details
1. Login ID: 2. Disable b hroughput 3. Login UR	proadcast and will be reduc & for wireless		ffic to maximi	ze wireless '			e WLAN
1. Login ID 2. Disable k throughput 3. Login UR http://ww	proadcast and will be reduc & for wireless	l multicast tra ed. clients: lan/login.htr	ffic to maximi n or http://	ze wireless ' /(Vigor IP A Cancel	ddress) /logi i	n.htm	
1. Login ID 2. Disable b throughput 3. Login UR http://ww	proadcast and will be reduc & for wireless	l multicast tra ed. clients: lan/login.htr C	ffic to maximi n or http:// OK heck this b	ze wireless /(Vigor IP A Cancel pox to invo	ddress) /logi] oke wireles	n.htm ss VLAN fu	unction.
 Disable t throughput Login UR 	proadcast and will be reduc & for wireless	l multicast tra ed. clients: lan/login.htr C T	ffic to maximi n or http:// OK heck this b	ze wireless /(Vigor IP A Cancel pox to invo	ddress) /logi] oke wireles	n.htm	unction.
1. Login ID 2. Disable b throughput 3. Login UR http://ww	proadcast and will be reduc L for wireless ww.draytek.v	I multicast trai ed. clients: lan/login.htr C T ch	ffic to maximi n or http:// OK heck this b ype Login haracters.	ze wireless /(Vigor IP A Cancel Dox to invo ID for dif	ddress)/logi] oke wirele: ?ferent grou	n.htm ss VLAN fu	unction. LAN with
1. Login ID 2. Disable b throughput 3. Login UR http://ww cnable cogin ID	proadcast and will be reduc L for wireless ww.draytek.v	I multicast tra ed. clients: lan/login.htr C T ch T ch C	ffic to maximi n or http:// OK heck this b ype Login haracters. ype passwo haracters.	ze wireless /(Vigor IP A Cancel Dox to invo ID for dif	ddress)/logi] oke wireles fferent grou	n.htm ss VLAN fu 1ps of W_V	unction. 'LAN with 'LAN with
1. Login ID 2. Disable b throughput 3. Login UR http://ww Cnable ogin ID	proadcast and will be reduc L for wireless ww.draytek.v	I multicast tra ed. clients: lan/login.htr C T ch T ch C W	ffic to maximi n or http:// OK heck this b ype Login haracters. ype passwo haracters. lick this bu /_VLAN.	ze wireless ' /(Vigor IP A Cancel Dox to invo ID for dif Ord for dif utton to se	ddress)/logi] oke wireles fferent grou	n.htm ss VLAN fu ups of W_V ups of W_V ll attributes	unction. 'LAN with 'LAN with
1. Login ID 2. Disable b throughput 3. Login UR http://ww Cnable ogin ID	proadcast and will be reduc L for wireless ww.draytek.v	I multicast tra ed. clients: lan/login.htr C T ch T ch C W	ffic to maximi n or http:// OK heck this b ype Login haracters. ype passwo haracters. lick this bu /_VLAN.	ze wireless ' /(Vigor IP A Cancel Doox to invo ID for dif ID for dif ord for dif atton to se	ddress)/logi] oke wireles fferent grou	n.htm ss VLAN fu 1ps of W_V ups of W_V	unction. 'LAN with 'LAN with
1. Login ID 2. Disable b throughput 3. Login UR http://ww Cnable ogin ID	proadcast and will be reduc L for wireless ww.draytek.v	I multicast tra ed. clients: lan/login.htr C T ch T ch C W	ffic to maximi n or http:// OK heck this b ype Login haracters. ype passwo haracters. lick this bu /_VLAN. Activate Expired t Com	ze wireless ' /(Vigor IP A Cancel Doox to invo ID for dif ord for dif atton to see	ddress)/logi] oke wireles fferent grou	n.htm ss VLAN fu ups of W_V ups of W_V ll attributes $2006 \times -1 \times -1$ $2010 \times -1 \times -1$ group.	unction. 'LAN with 'LAN with

Activated Date – Use the drop down lists to set the activated date for the wireless VLAN. The wireless VLAN function will be available when the time is arrival.

Expired Date – Use the drop down lists to set the expired date for the wireless VALN. This function will be invalid when the time is arrival.

Connect all WDS links with this VALN group – Check this box to activate this connection.

Isolate each member in this VLAN group – Check this box to isolate all the members in this VLAN group and not allow the information sharing among them.



Disable broadcast and	Check this box to prevent broadcast and multicast traffic
multicast traffic	forwarding to all W_VLAN.

How can you (wireless client) access into Internet?

After finishing the configuration of wireless VLAN, the wireless clients connecting to this router must do the following steps to access into Internet.

- 1. Open a browser and type http://www.draytek.vlan/login.htm or http://(vigor router's IP address)/login.htm on the address line.
- 2. The following screen will appear.

Login ID	City
Password	
	OK

DrayTek Wireless VLAN

- 3. Type in Login ID and Password that was configured in Wireless VLAN Setup page. In this case, we choose the configuration set in first group of W_VLAN (City and 1234).
- 4. When the accessing is successful, the following screen will appear.

http://192.168.1.1 - DrayTek Wireless		
	DrayTek Wireless VLAN	
Link Status:Active 創 完成 创 创 叙述叙述	User login succeeds !!!	
	Copyright © 2005, DrayTek Corp. All Rights Reserved.	~

Note: The floating window with connection time will be shown on the screen till you logout.

^

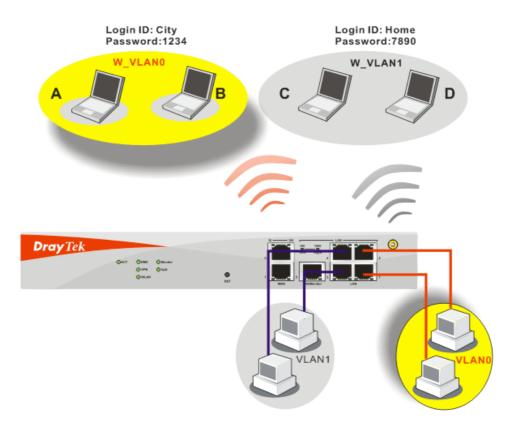
5. You can go to **Diagnostics>>Wireless VLAN Online Station** for viewing the connection status whenever you want.

	nline Station Table		Refre
IP Address	MAC Address	Login ID	
192.168.1.15	00-14-85-26-00-8C	City	
192.168.1.16	00-0E-35-A8-A4-E7	Home	

Diagnostics >> Wireless VLAN Online Station

3.12.3 VLAN Cross Setup

This function allows the router to integrate VLAN and W_VLAN for managing different computers (notebooks). See the following picture for an example. With VLAN Cross Setup, notebook A/B and PCs on VLAN0 can share resources without difficulty.



The VLAN >> VALN Cross Setup allows you to set a communication bridge between computers in Wireless VLAN and wired VLAN. To achieve the intention of the above illustration, simply check the box under VLAN0 on the line of W_VLAN0.



VLAN >> VLAN Cross Setup

nable				
	VLANO	VLAN1	VLAN2	VLAN3
W_VLAN0				
W_VLAN1				
W_VLAN2				
W_VLAN3				
W_VLAN4				
W_VLAN5				
W_VLAN6				
W_VLAN7				
W_VLAN8				
W_VLAN9				
W_VLAN10				
W_VLAN11				
W_VLAN12				
W_VLAN13				
W_VLAN14				
W_VLAN15				
WDS				
VDS links belong Ni: wired VLAN i	to the same VLAN , see Wired VLAN	Setup for details.	etails. ross settings to be ef	fective.
ole	ок С	Clear heck this box to	Cancel	Cross Setup fur
				•
AN0-3		represents the g terface.	roups of virtual	LAN connecte
VLAN0-15		represents the g	roups of wireles	s VLAN comn

3.12.4 Wireless Rate Control

Rate Control manages the transmission rate of data in and out through the router. You can also manage the in/out rate of each wireless VLAN. Go to **VLAN** menu and select **Wireless Rate Control**. The following page will appear. Click **Enable** to invoke VLAN function.

For the rate control of wireless connection, please open VLAN menu and choose **Wireless Rate Control**. The following page will be shown for you to adjust.

Enable			Range : 1	00~30,000 Kbps, I	ncrement : 100 Kbps
V_VLAN	Upload Rate (Kbps)	Download Rate (Kbps)	W_VLAN	Upload Rate (Kbps)	Download Rate (Kbps)
0	300 00	300 00	8	300 00	300 00
1	300 00	300 00	9	300 00	300 00
2	300 00	300 00	10	300 00	300 00
3	300 00	300 00	11	300 00	300 00
4	300 00	300 00	12	300 00	300 00
5	300 00	300 00	13	300 00	300 00
6	300 00	300 00	14	300 00	300 00
7	300 00	300 00	15	300 00	300 00
ote: Spe able	cified rate is an a <u>c</u>	rate contro	Cancel box to en		ion (for Rate Con sion rate for uploa
load R	ate	download. It decides t	the rate of	data transmiss	sion for output. T

VLAN >> Wireless VLAN Rate Control

20,000kbps. Adjust the values according to your necessity.

3.13 System Maintenance

Download Rate

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.

It decides the rate of data transmission for input. The default setting is 300. The range must be between 100 kbps to

3.13.1 System Status

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



System Status

Model Name Firmware Version Build Date/Time DSL Firmware Ver		: Vigor3100 series : v2.8.1_RC2 : Wed Oct 24 14:40:: : R308_1 Annex A	3.50 2007	
LAN MAC Address 1st IP Address 1st Subnet Mask DHCP Server	: 192.168.	1.1	WAN Link Status MAC Address Connection IP Address Default Gateway DNS	: Disconnected : 00-50-7F-89-92-11 : PPPoE : : : 194.109.6.66
VoIP				
Port	: 1	2		
SIP registrar	1			
Account ID	: change_me	change_me		
Register	1			
Codec	1			
In Calls	: 0	0		
Out Calls	: 0	0		
Model Name	Т	Displays the mo	del name of the ro	uter

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

3.13.2 Administrator Password

This page allows you to set new password.

System Maintenance >> Administrator Password Setup

Administrator Password			
Old Password			
New Password			
Retype New Password			

OK

Old PasswordType in the old password. The factory default setting for password is
blank.New PasswordType in new password in this filed.



Retype New Password Type in the new password again.

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

3.13.3 Configuration Backup

Backup the Configuration

Follow the steps below to backup your configuration.

System Maintenance >> Configuration Backup

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

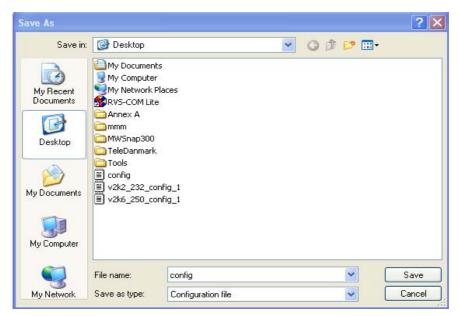
Configuration	Backup / Restoration
Restoration	
	Select a configuration file.
Backup	Click Backup to download current running configurations as a file. Backup Cancel

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

File Dov	vnload 🛛 🔀
?	You are downloading the file: config.cfg from 192.168.1.1
	Would you like to open the file or save it to your computer?
	Open Save Cancel More Info
	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.

Dray Tek



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

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

Restore Configuration

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

System Maintenance >> Configuration Backup		
Configuratior	n 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.	
	Backup Cancel	

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

3.13.4 Syslog/Mail Alert

SysLog function is provided to help 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
Server IP Address	SMTP Server
Destination Port 514	Mail To
Enable syslog message:	Return-Path
 Firewall Log VPN Log User Access Log Call Log WAN Log Router/DSL information 	Authentication User Name Password

Enable	Click "Enable" to activate this function.
Server IP Address	The IP address of the Syslog server.
Destination Port	Assign a port for the Syslog protocol.
Enable syslog message	Check the box to display the specified log.
SMTP Server	The IP address of the SMTP server.
Mail To	Assign a mail address for sending mails out.
Return-Path	Assign a path for receiving the mail from outside.

Click **OK** to save these settings.

For viewing the Syslog, please do the following:

System Maintenance >> SysLog / Mail Alert Setup

- 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 V2.5.4 🔹 🕨	🕥 About Router Tools
	🏘 Ez Configurator Vigor2100 Series
	🐴 Firmware Upgrade Utility
	🔟 Syslog
	🥑 Uninstall Router Tools V2.5.4
	🍯 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.

		Vigor serie	s Dmt.Bis	Gateway IP (Fixed	i) TX Packet	s RX Rate
AN Status TX Pa	ickets	RX Pack	ets	WAN IP (Fixed)	, RX Packet	s TX Rate
96	51	759			0	0
wall Log VPN	User Acces	s Log Ca	ll Log WAN Lo	g Network Infomation	n Net State	
n Line Routers			Host Name:	niki-pc	_	
IP Address 92.168.1.1	Mask 255.255.255.0	MAC 00-50-	NIC Descriptio	Keenek K 115015	9 Family PCI Fast E	Ethernet NIC - : 🔽
			MAC Address:	00-0E-A6-2A-D5-A1	Default Geteway:	192.168.1.1
			IP Address:	192.168.1.10	DHCP Server:	192.168.1.1
			Subnet Mask:	255.255.255.0	Lease Obtained:	Wed Apr 06 16:59:40 2005
	R	> efresh	DNS Servers:	168.95.1.1 192.168.1.1	Lease Expires:	Sat Apr 09 16:59:40 2005
			· · · · · · · · · · · · · · · · · · ·			

3.13.5 Time and Date

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

```
System Maintenance >> Time and Date
```

Time Information	
Current System Time	2000 Jan 3 Mon 18 : 11 : 22 Inquire Time
Time Setup	
🔘 Use Browser Time	
💿 Use Internet Time	Client
Time Protocol	NTP (RFC-1305) 💌
Server IP Address	
Time Zone	(GMT) Greenwich Mean Time : Dublin 🛛 👻
Enable Daylight Sav	
Automatically Upda	e Interval 30 sec 💌
Current System Time	OK Cancel Click Inquire Time to get the current time.
Use Browser Time	Select this option to use the browser time from the remote administrator PC host as router's system time.
Use Internet Time	Select to inquire time information from Time Server on the using assigned protocol.
Fime Protocol	Select a time protocol.

Time ZoneSelect the time zone where the router is located.

Enable Daylight Saving This function is valid for some area.



Internet

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

Click **OK** to save these settings.

3.13.6 Management

The port number used to send/receive SIP message for building a session. The default value is 5060 and this must match with the peer Registrar when making VoIP calls.

Management Setup		
Management Access Control	Management Port S	etup
Enable remote firmware upgrade(FTP)	ODefault Ports (Telr 443, FTP: 21)	net: 23, HTTP: 80, HTTPS:
Allow management from the Internet	💿 User Define Ports	
☑ Disable PING from the Internet	Telnet Port	23
Access List	HTTP Port	80
List IP Subnet Mask	HTTPS Port	443
1	FTP Port	21
2	SNMP Setup	
3	Enable SNMP Age	nt
	Get Community	public
	Set Community	private
	Manager Host IP	
	Trap Community	public
	Notification Host IP	
	Trap Timeout	10 seconds

Г	OK	

Enable remote firmware upgrade	Chick the checkbox to allow remote firmware upgrade through FTP (File Transfer Protocol).
Allow management from the Internet	Enable the checkbox to allow system administrators to login from the Internet. By default, it is not allowed.
Disable PING from the Internet	Check the checkbox to reject all PING packets from the Internet. For security issue, this function is enabled by default.
Access List	You could specify that the system administrator can only login from a specific host or network defined in the list. A maximum of three IPs/subnet masks is allowed. List IP - Indicate an IP address allowed to login to the router. Subnet Mask - Represent a subnet mask allowed to login to the router.
Default Ports	Check to use standard port numbers for the Telnet and HTTP servers.
User Defined Ports	Check to specify user-defined port numbers for the Telnet and HTTP servers.
Enable SNMP Agent	Check it to enable this function.
Get Community	Set the name for getting community by typing a proper character. The default setting is public.

System Maintenance >> Management



Set Community	Set community by typing a proper name. The default setting is private.
Manager Host IP	Set one host as the manager to execute SNMP function. Please type in IP address to specify certain host.
Trap Community	Set trap community by typing a proper name. The default setting is public.
Notification Host IP	Set the IP address of the host that will receive the trap community.
Trap Timeout	The default setting is 10 seconds.

3.13.7 Reboot System

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

System Mainte	nance >> Reboot System
Reboot System	
	Do You want to reboot your router ?
	Outling current configuration
	OUsing factory default configuration
1	OK

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

3.13.8 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 steps will guide you to upgrade firmware. In the following, we use an example to explain the firmware upgrade. 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

Current Firmware Version :	v2.8.1_RC2
Firmware Upgrade Procedu	ires:
• 1. Click "OK" to start the T	
• 2. Open the Firmware Upgr	ade Utility or other 3-party TFTP client software.
3. Check that the firmware	
• 4. Click "Ungrade" on the F	irmware Ungrade Utility to start the ungrade.
 3. Check that the firmware 4. Click "Upgrade" on the F 5. After the upgrade is cor 	e filename is correct. irmware Upgrade Utility to start the upgrade. npelete, the TFTP server will automatically stop running
Do you want to upgrade fir	muuaro 2

ΟK



3.14 Diagnostics

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

3.14.1 WAN Connection

Diagnostics >> WAN Connection

Click **Diagnostics** and click **WAN Connection** to open the web page. Such page will be different slightly based on the model of your router.

ISDN Link Status	DOWN	
Internet Access	>> <u>Dial ISDN</u>	
B Channel	B1	B2
Activity	Idle	Idle
Drop Connection	>> <u>Drop B1</u>	>> <u>Drop B2</u>
Broadband Access Mode/Status		
Internet Access	>> <u>Dial PPPoE/P</u>	PPoA
WAN IP Address		
Drop Connection	>> Drop PPPoE/	PPPoA

Refresh	To obtain the latest information, click here to reload the page.
Broadband Access Mode/Status	Display the broadband access mode and status. If the broadband connection is active, it will show Internet access mode is enabled. If the connection is idle, it will show "".
WAN IP Address	The WAN IP address for the active connection.
Dial PPPoE or PPPoA	Click it to force the router to establish a PPPoE or PPPoA connection.

3.14.2 Dial-out Trigger

Click **Diagnostics** and click **Dial-out Trigger** to open the web page.

Diagnostics >> Dial-out Trigger

Dial-o	ut Triggered Packet Header	<u>Refresh</u>
	HEX Format:	
	00 00 00 00 00 00 00 00 00 00 00 00 00	
	00 00 00 00 00 00 00-00 00 00 00 00 00 0	
	00 00 00 00 00 00 00-00 00 00 00 00 00 0	
	00 00 00 00 00 00 00-00 00 00 00 00 00 0	
	00 00 00 00 00 00 00-00 00 00 00 00 00 0	
	00 00 00 00 00 00 00 00 00 00 00 00 00	
	Decoded Format:	
	0.0.0.0 -> 0.0.0.0 Pr O len O (O)	

Refresh

Click it to reload the page.

3.14.3 Routing Table

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

```
Diagnostics >> View Routing Table
```

```
Current Running Routing Table
```

```
<u>Refresh</u>
Key: C - connected, S - static, R - RIP, * - default, ~ - private
                        0.0.0.0/
*~
                                                       0.0.0.0 via 192.168.1.1, IFO

      192.168.10.0/
      255.255.0 via 192.168.1.2, IFO

      192.168.1.0/
      255.255.0 via 192.168.1.2, IFO

      211.100.88.0/
      255.255.0 via 192.168.1.3, IFO

S~
С~
S~
```

Refresh

Click it to reload the page.

3.14.4 ARP Cache Table

Click Diagnostics and click ARP Cache Table to view the content of the ARP (Address Resolution Protocol) cache held in the router. The table shows a mapping between an Ethernet hardware address (MAC Address) and an IP address.

```
Diagnostics >> View ARP Cache Table
```

Ethernet ARP Cache 1	laple	<u>Clear</u>	<u>Refresh</u>
IP Address	MAC Address		^
192.168.1.11	00-0E-A6-2A-D5-A1		
			~

Refresh	Click it to reload the page.
Clear	Click it to clear the whole table.

3.14.5 DHCP Table

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

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

Diagnostics >> View DHCP Assigned IP Addresses

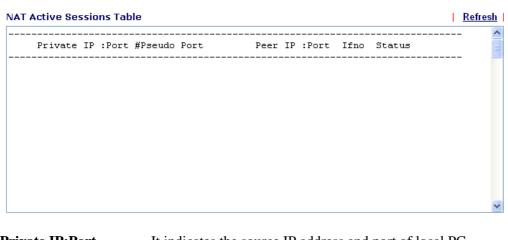
```
DHCP IP Assignment Table Refrest
```

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

3.14.6 NAT Sessions Table

Click Diagnostics and click NAT Sessions Table to open the setup page.

```
Diagnostics >> NAT Sessions Table
```



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.

Ifno	It indicates the interface of the WAN connection.

Refresh Click it to reload the page.

3.14.7 Wireless VLAN Online Station Table

Diagnostics >> Wireless VLAN Online Station

This function is available for **G** model only.

Click **Diagnostics** and click **Wireless VLAN Online Station Table to** open the web page. It will display the IP address, MAC address and Login ID information for all the Wireless VLAN stations.

P Address	MAC Address	Login ID	
92.168.1.15	00-14-85-26-00-8C	City	
92.168.1.16	00-0E-35-18-14-E7	Home	

IP Address	Display the IP address of the wireless station.
MAC Address	Display the MAC address of the wireless station.
Login ID	Display the login ID that the wireless station belongs to.

3.14.8 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.

essions Limit	
Enable O Disable	
Default Max Sessions: 100	
Limitation List	
Index Start IP	End IP

Bandwidth Management >> Sessions Limit

Click Diagnostics and click Data Flow Monitor to open the web page.



Diagnostics >> Data Flow Monitor

🗹 Enable Data Flow Monitor

Order by:	P 🚩 Refre	esh Seconds: 5 💌	F	Page: 1 💌	<u>Refresh</u>
Index		TX rate(Kbps)	RX rate(Kbps)	Sessions	Action

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.

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



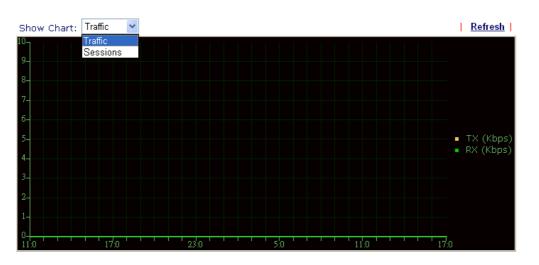
	Page: 1 💌	<u>Refresh</u>
RX rate(Kbps)	Sessions	Action
	21	<u>Block</u>

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

	Page: 1 💌	<u>Refresh</u>
(rate(Kbps)	Sessions	Action
	blocked / 299	<u>Unblock</u>

3.14.9 Traffic Graph

Click **Diagnostics** and click **Traffic Graph** to pen the web page. Choose WAN1 Bandwidth/WAN2 Bandwidth or Sessions for viewing different traffic graph. Click **Refresh** to renew the graph at any time.





The horizontal axis represents time. Yet the vertical axis has different meanings. For WAN1/WAN2 Bandwidth chart, the numbers displayed on vertical axis represent the numbers of the transmitted and received packets in the past.

For Sessions chart, the numbers displayed on vertical axis represent the numbers of the NAT sessions during the past.

3.14.10 Ping Diagnosis

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

Diagnostics >>	Ping Diagnosis
Diagnootioo	i nig biegnooio

Ping Diagnosis	
Ping to: Host / IP 💌	IP Address:
	Run
Result	<u>Clear</u>

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

3.14.11 Trace Route

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

Diagnostics >> Trace Route

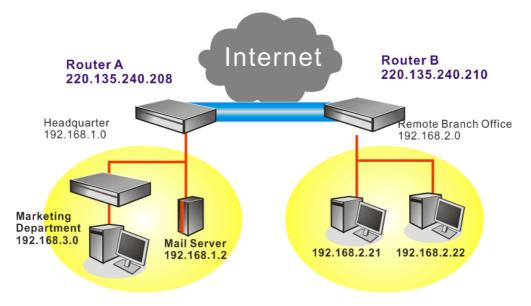
Host / IP Address:	
Result	<u>Clear</u>
traceroute to 172.16.3.229, 30 hops max 1 Request timed out. * 2 Request timed out. * Trace complete.	

Host/IP Address	It indicates the IP address of the host.	
Run	Click this button to start route tracing work.	
Clear	Click this link to remove the result on the window.	

4 Application and Examples

4.1 Create a LAN-to-LAN connection between remote office and headquarter

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



Settings in Router A in headquarter:

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

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

PPP General Setup				
PPP/MP Protocol	IP Address Assignment for Dial-In Users			
Dial-In PPP Authentication	Start IP Address 192.168.1.200			
Dial-In PPP Encryption Optional MPPE				
Mutual Authentication (PAP) OYes • No				
Username				
Password				

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



VPN	IKE/I	PSec	General	Setup
DOM: N	in one			mint in

·····				
Dial-in Set up for Remote Dial-in users and Dynamic IP Client (LAN to LAN).				
IKE Authentication Method				
Pre-Shared Key	••••			
Re-type Pre-Shared Key	•••••			
IPSec Security Method				
Medium (AH)				
Data will be authentic, but will	not be encrypted.			
High (ESP) 🗹 DES 🗹 3DES	AES			
Data will be encrypted and aut	hentic.			

- 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.

1. Common	Settings
-----------	----------

Profile Name	Branch 1	Call Direction 💿 Both 🔿 Dial-Out 🔿 Dial-In
Enable this profile		Always on
		Idle Timeout 300 second(s)
		Enable PING to keep alive
		PING to the IP 192.168.2.21

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.

Type of Server I am calling	Link Type 64k bps 🔛
© ISDN	Username ???
O PPTP	Password
⊙ IPSec Tunnel	PPP Authentication PAP/CHAP
OL2TP with IPSec Policy Nice to Have 💟	VJ Compression On Off
Dial Number for ISDN or Server IP/Host Name for VPN. (such as5551234,draytek.com or 123.45.67.89)	IKE Authentication Method
220.135.240.210	IKE Pre-Shared Key
	O Digital Signature(X.509)
	IPSec Security Method ○ Medium(AH) ⊙ High(ESP) DES without Authentication ♥
	Advanced
	Scheduler (1-15)
	Callback Function (CBCP)
	Require Remote to Callback
	Provide ISDN Number to Remote

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



Username Password PPP Authentication VJ Compression IKE Authentication M Pre-Shared Key IKE Pre-Shared Key Digital Signature(X.50	
IKE Authentication VJ Compression IKE Authentication M Pre-Shared Key IKE Pre-Shared Key Digital Signature(X.50	PAP/CHAP V On Off ethod
VJ Compression IKE Authentication M Pre-Shared Key IKE Pre-Shared Key Digital Signature(X.50	On Off ethod
IKE Authentication M Pre-Shared Key IKE Pre-Shared Key Digital Signature(X.50	On ○ Off
Pre-Shared Key IKE Pre-Shared Key Digital Signature(X.50	
Digital Signature(X.50	
	19)
1,,,	ut Authentication 💌
	Scheduler (1-15)

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.

Allowed Dial-In Type	
ISDN	Username ???
□ PPTP	Password
☑ IPSec Tunnel	VJ Compression On Off
L2TP with IPSec Policy Nice to Have	IKE Authentication Method
SpecifyISDN CLID orRemote VPN Gateway	☑ Pre-Shared Key
Peer ISDN Number orPeer VPN Server IP	IKE Pre-Shared Key
220.135.240.210	Digital Signature(X.509)
or Peer ID	111 🗸
	IPSec Security Method I Medium (AH) High (ESP)
	🗹 DES 🗹 3DES 🗹 AES
	Callback Function (CBCP)
	Enable Callback Function
	Use the Following Number to Callback
	Callback Number
	Callback Budget 0 minute(s)

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

Allowed Dial-In Type	_
ISDN .	Username draytek_br
▶ РРТР	Password ••••••
IPSec Tunnel	VJ Compression 💿 On 🔿 Off
L2TP with IPSec Policy Nice to Have	IKE Authentication Method
SpecifyISDN CLID orRemote VPN Gateway	Pre-Shared Key
Peer ISDN Number orPeer VPN Server IP	IKE Pre-Shared Key
	Digital Signature(X.509)
or Peer ID	
	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 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 TX/RX Both 🕶
Remote Gateway IP	0.0.0.0	RIP Version Ver. 2 💌
Remote Network IP	192.168.2.0	For NAT operation, treat remote sub-net as
Remote Network Mask	255.255.255.0	Private IP 💌
	More	□ Change default route to this VPN tunnel

Settings in Router B in the remote office:

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

PPP General Setup		
PPP/MP Protocol	IP Address Assignment for Dial-In Users	
Dial-In PPP Authentication PAP or CHAP V	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 IKE/IPSec General Setup Dial-in Set up for Remote Dial-in users and	Dynamic IP Client (LAN to LAN).
IKE Authentication Method	
Pre-Shared Key	••••
Re-type Pre-Shared Key	••••
IPSec Security Method	
Medium (AH)	
Data will be authentic, but will r	not be encrypted.
High (ESP) 🛛 DES 🗹 3DES	✓ AES
Data will be encrypted and auth	entic.

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

Profile Name	Branch 1	Call Direction 💿 Both 🔿 Dial-Out 🔿 Dial-In
Enable this pro	file	Always on
		Idle Timeout 300 second(s)
		Enable PING to keep alive
		PING to the IP 192,168,2,21

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.

Type of Server I am calling	Link Type 64k bps
O ISDN	Username ???
○ РРТР	Password
⊙ IPSec Tunnel	PPP Authentication PAP/CHAP
OL2TP with IPSec Policy Nice to Have	VJ Compression On Off
Dial Number for ISDN or Server IP/Host Name for VPN. (such as5551234,draytek.com or 123.45.67.89)	IKE Authentication Method <pre>OPre-Shared Key</pre>
220.135.240.128	IKE Pre-Shared Key
	O Digital Signature(X.509)
	IPSec Security Method Medium(AH) High(ESP) DES without Authentication
	Scheduler (1-15)
	Require Remote to Callback
	Provide ISDN Number to Remote

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

connection.

Type of Server I am calling	Link Type	64k bps 💙
OISDN	Username	draytek_hq
⊙ РРТР	Password	
O IPSec Tunnel	PPP Authentication	
OL2TP with IPSec Policy Nice to Have 💌	VJ Compression	⊙ On ◯ Off
Dial Number for ISDN or Server IP/Host Name for VPN. (such as5551234,draytek.com or 123.45.67.89)	IKE Authentication M Pre-Shared Key 	lethod
220.135.240.128	IKE Pre-Shared Key	•••••
	Oigital Signature(X.50	bd
	Callback Function (C	
	Require Remote to (
	Provide ISDN Numbe	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.

Allowed Dial-In Type	
ISDN	Username ???
РРТР	Password
☑ IPSec Tunnel	VJ Compression On Off
L2TP with IPSec Policy Nice to Have	IKE Authentication Method
SpecifyISDN CLID orRemote VPN Gateway	Pre-Shared Key
Peer ISDN Number orPeer VPN Server IP	IKE Pre-Shared Key
220.135.240.128	Digital Signature(X.509)
or Peer ID	111 💌
	IPSec Security Method ✓ Medium (AH) High (ESP) ✓ DES ♥ 3DES ♥ AES
	Callback Function (CBCP) Enable Callback Function Use the Following Number to Callback Callback Number
	Callback Budget 0 minute(s)

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

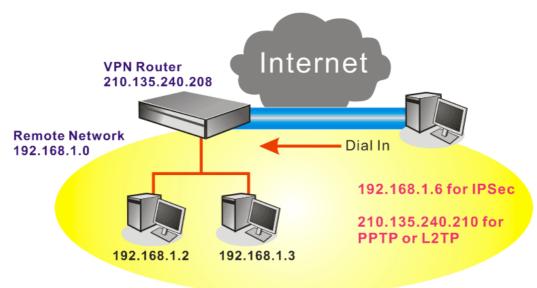
Allowed Dial-In Type	
ISDN .	Username draytek_hq
PPTP	Password •••••
IPSec Tunnel	VJ Compression ⊙ On ○ Off
L2TP with IPSec Policy Nice to Have	IKE Authentication Method
SpecifyISDN CLID orRemote VPN Gateway	✓ Pre-Shared Key
Peer ISDN Number orPeer VPN Server IP	IKE Pre-Shared Key
	Digital Signature(X.509)
or Peer ID	111
	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 Settings

My WAN IP	0.0.0.0	RIP Direction	TX/RX Both 💌
Remote Gateway IP	0.0.0.0	RIP Version	Ver. 2 💌
Remote Network IP	192.168.1.0	For NAT operation, trea	
Remote Network Mask	255.255.255.0		Private IP 🚩
	More	Change default rout	e to this VPN tunnel

4.2 Create a remote dial-in user connection between the teleworker and headquarter

The other common case is that you, as a teleworker, may want to connect to the enterprise network securely. According to the network structure as shown in the below illustration, you may follow the steps to create a Remote User Profile and install Smart VPN Client on the remote host.



Settings in VPN Router in the enterprise office:

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



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



VPN IKE/IPSec General Setup

Dial	Dial-in Set up for Remote Dial-in users and Dynamic IP Client (LAN to LAN).						
	IKE Authenti	cation Met	hod				
	Pre-Shared Ke	ey		••••			
	Re-type Pre-S	Shared Key		•••••			
	IPSec Securi	ty Method					
	🗹 Medium (Ał	H)					
	Data will b	e authentic	, but will n	ot be enci	rypted.		
	High (ESP)	🗹 DES	🗹 3DES	🗹 AES			
	Data will b	e encrypte	d and auth	entic.			

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

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

User account and Authentication	
Enable this account	Username draytek_user1
Idle Timeout 300 second(s)	Password
Allowed Dial-In Type	IKE Authentication Method
ISDN	Pre-Shared Key
PPTP	IKE Pre-Shared Key
PSec Tunnel	Digital Signature (X.509)
L2TP with IPSec Policy None	111 🐱
Specify Remote Node Remote Client IP or Peer ISDN Number 210.135.240.210 or Peer ID	IPSec Security Method Medium (AH) High (ESP) MDES M3DES MAES 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)

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.

Enable this account	Username draytek_user1
Idle Timeout 300 second(s)	Password ••••••
Allowed Dial-In Type	IKE Authentication Method
ISDN	Pre-Shared Key
✓ PPTP	IKE Pre-Shared Key
IPSec Tunnel	Digital Signature (X.509)
L2TP with IPSec Policy None	111 🗸
Specify Remote Node Remote Client IP or Peer ISDN Number 210.135.240.210 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)

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.				
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 :	*****			
Type of VPN				
○ PPTP	◯ L2TP			
 IPSec Tunnel 	L2TP over IPSec			
PPTP Encryption				
No encryption				
Require encryption Maximum strength encryption				
Use default gateway on remote network				
OK Cancel				

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

IPSec Policy Setti	ng	X				
My IP : Type of IPSec	•					
🔘 Standard IPS		0.0.0.0				
Remote Su Remote Su	bnet : bnet Mask :	255 . 255 . 255 . 0				
 Virture IP 	DrayT	ek Virture Interface 🔽				
	n IP address a an IP address	utomatically (DHCP over IPSec)				
IP Addr		192 . 168 . 1 . 201				
Subnet	Mask:	255 , 255 , 255 , 0				
Security Method O Medium(AH) MD5	•)High(ESP) DES				
Authority Method						
Certification	Authority:	Browse				
0	к	Cancel				

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

Dial To YPN	X			
Session Name:	office			
VPN Server IP/HOST	Name(such as 123.45.67.89 or draytek.com)			
192.168.1.1				
	dura hali succed			
User Name :	draytek_user1			
Password :	****			
Type of VPN	OL2TP			
O IPSec Tunne	OL2TP over IPSec			
PPTP Encryption O No encryption Require encryption O Maximum strength encryption				
Use default gateway on remote network OK 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

1.

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

Make sure the QoS Control on the left corner is checked. And select BOTH in Direction. 1.

QoS Cont	QoS Control Setup				
Enable the QoS Control					
Direction BOTH V					
Index	OUT s Name				
1.					

2. Enter the Class Name of Index 1. In this index, she will set reserve bandwidth for Email using protocol POP3 and SMTP. Click Basic button on the right. E-MAIL Advance

96

3. Select POP3 and SMTP on the left column and add to right column. Click OK to exit.

25

ANY AUTH(TCP:113)		POP3(TCP:110) SMTP(TCP:25)
BGP(TCP:179) BOOTPCLIENT(UDP:68) BOOTPSERVER(UDP:67)	ADD >>	
CU-SEEME-HI(TCP/UDP:24032) CU-SEEME-LO(TCP/UDP:7648)	< REMOVE	
DNS(TCP/UDP:53) FINGER(TCP:79)		

4. Enter the Class Name of Index 2. In this index, she will set reserve bandwidth for



Basic

HTTPS. And click Basic button on the right.

		U				
2.	HTTPS	25	%	Basic	Advance	•

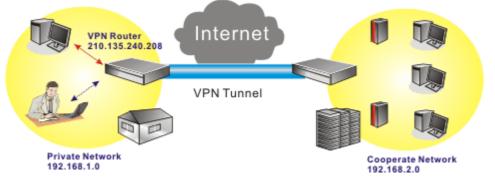
5. Select HTTPS in the list on the left column and click on ADD to add to right column. Click OK to exit.

ANY AUTH(TCP:113) BGP(TCP:179) BOOTPCLIENT(UDP:68) BOOTPSERVER(UDP:67) CU-SEEME-HI(TCP/UDP:24032) CU-SEEME-LO(TCP/UDP:7648) DNS(TCP/UDP:53)	ADD >>	HTTPS(TCP:443)
DNS(TCP/UDP:53) FINGER(TCP:79))	

6. Check the Enable UDP Bandwidth Control on the bottom to prevent enormous UDP traffic of VoIP influent other application.



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



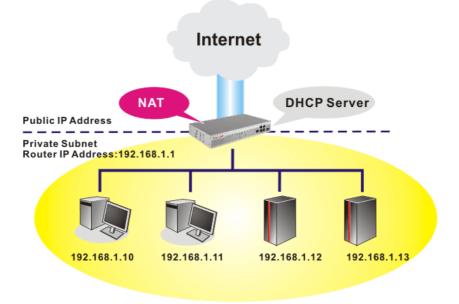
8. Click Edit to open a new window. First, check the ACT box. Then click SrcEdit to set a Jane's subnet address. Click DestEdit to set headquarter's subnet address. Leave other fields and click OK.

QoS	Control Setup			
АСТ	Source Address	Destination Address	DiffServ CodePoint	Service Type
	192.168.1.0(mask:2 SrcEdit	192.168.2.0(mask:2 DestEdit	ANY	ANY Add Edit Delete

Note :Please choose/setup the Service Type first.

4.4 LAN - Created by Using NAT

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



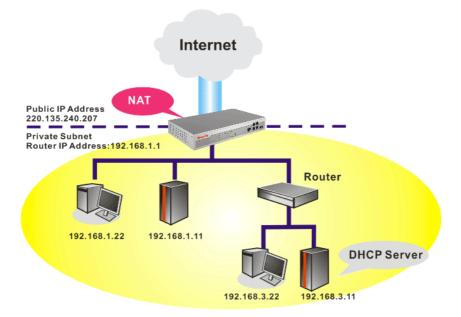
You can just set the settings wrapped inside the red rectangles to fit the request of NAT usage.

AN IP Network Conf	figuration	DHCP Server Configu	ration
For NAT Usage		💿 Enable Server 🔘 Disa	able Server
1st IP Address	192.168.1.1	Relay Agent: 🔘 1st Su	ubnet 🔾 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 Addres	55
	2nd Subnet DHCP Server	for Relay Agent DNS Server IP Addres	ss
		Force DNS manual	l setting
RIP Protocol Control	Disable 💌	Primary IP Address	
		Secondary IP Addres	s

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.

LAN >> General Setup





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

LAN >> General Setup

Ethernet TCP / IP and	d DHCP Setup		
LAN IP Network Conf	iguration	DHCP Server Configura	tion
For NAT Usage		◯ Enable Server ⊙ Disab	le Server
1st IP Address	192.168.1.1	Relay Agent: O 1st Sub	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	192.168.3.11
	2nd Subnet DHCP Server	for Relay Agent DNS Server IP Address	
		Force DNS manual s	
RIP Protocol Control	Disable 🚩	Primary IP Address	
		Secondary IP Address	

4.5 Calling Scenario for VoIP function

4.5.1 Calling via SIP Sever

Example 1: Both John and David have SIP Addresses from different service providers.

VolP >> DialPlan Setur

John's SIP URL: 1234@draytel.org, David's SIP URL: 4321@iptel.org

Settings for John

DialPlan index 1 Phone Number: 1111 Display Name: David SIP URL: 4321@iptel.org

🗹 Enable					
	Phone Number		1111		
	Display Name		David		
	SIP URL		4321	@ iptel.org	
VoIP >> SIF	Accounts	OK	Clear	Cancel	

Call without Registration

(23 char max.)

sec

(63 char max.)

Auto

5060

proxy

John

1234

....

1 🛩

1 hour 💌 3600 None 💌

VoIP1 VoIP2

draytel.org

draytel.org

SIP Accounts Settings ----

Profile Name: draytel1 Register via: Auto SIP Port: 5060 (default) Domain/Realm: draytel.org Proxy: draytel.org Act as outbound proxy: unchecked Display Name: John Account Number/Name: 1234 Authentication ID: unchecked Password: **** Expiry Time: (use default value)

CODEC/RTP/DTMF ----

(Use default value)

Settings for David DialPlan index 1 Phone Number:2222 Display Name: John SIP URL:1234@draytel.org

SIP Accounts Settings ----

Profile Name: iptel 1 Register via: Auto SIP Port: 5060(default) Domain/Realm: iptel.org Proxy: iptel.org Act as outbound proxy: unchecked Display Name: David Account Name: 4321 Authentication ID: unchecked Password: **** Expiry Time: (use default value)

CODEC/RTP/DTMF ----

(Use default value)

John calls David ---

Register via

Domain/Realm

Display Name

Password

Expiry Time

Rina Port

Ring Pattern

Act as outbo

Account Number/Name

Authentication ID

NAT Traversal Support

SIP Port

He picks up the phone and dials 1111#. (DialPlan Phone Number for David)

OK Cancel

Phone Book	Index No. 1			
🗹 Enable				
	Phone Number	2222		
	Display Name	John		
	SIP URL	1234	@ draytel.org	

VoIP >> SIP Accounts

Profile Name	iptel 1 (11 chai	r max.)
Register via	Auto 🔽 🗌 Call without	Registration
SIP Port	5060	
Domain/Realm	iptel.org	(63 char max.)
Ргоху	iptel.org	(63 char max.)
🗌 Act as outbound p	гоху	
Display Name	David (23 cha	r max.)
Account Number/Name	4321	(63 char max.)
Authentication ID		(63 char max.)
Password	••••	(63 char max.)
Expiry Time	1 hour 🕑 3600 sec	
NAT Traversal Support	None 🖌	
Ring Port	VoIP1 VoIP2	
Ring Pattern	1 🗸	

David calls John

He picks up the phone and dials 2222# (DialPlan Phone Number for John)



Example 2: Both John and David have SIP Addresses from the same service provider.

John's SIP URL: 1234@draytel.org, David's SIP URL: 4321@draytel.org

Settings for John

DialPlan index 1 Phone Number: 1111 Display Name: David SIP URL: 4321@draytel.org

SIP Accounts Settings ----

Profile Name: draytel 1 Register via: Auto SIP Port: 5060 (default) Domain/Realm: draytel.org Proxy: draytel.org Act as outbound proxy: unchecked Display Name: John Account Number/Name: 1234 Authentication ID: unchecked Password: **** Expiry Time: (use default value)

CODEC/RTP/DTMF ----

(Use default value)

VoIP >> DialPlan Setup

VoIP >> SIP Accounts

Enable				
	Phone Number	1111		
	Display Name	David		
	SIP URL	4321	@ draytel.org	

Profile Name	draytel 1 (11 cha	r max.)
Register via	Auto 🕑 🗌 Call without	Registration
SIP Port	5060	
Domain/Realm	draytel.org	(63 char max.)
Ргоху	draytel.org	(63 char max.)
🗌 Act as outbound p	roxy	
Display Name	John (23 cha	r max.)
Account Number/Name	1234	(63 char max.)
Authentication ID		(63 char max.)
Password	••••	(63 char max.)
Expiry Time	1 hour 🕑 3600 sec	
NAT Traversal Support	None 🛩	
Ring Port	VoIP1 VoIP2	
Ring Pattern	1 🛩	

John calls David

VoIP >> DialPlan Setup

He picks up the phone and dials 1111#. (DialPlan Phone Number for David) Or, He picks up the phone and dials 4321#. (David's Account Name)

Settings for David

DialPlan index 1 Phone Number:2222 Display Name: John SIP URL:1234@draytel.org

SIP Accounts Settings ----

Profile Name: John Register via: Auto SIP Port: 5060(default) Domain/Realm: draytel.org Proxy: iptel.org Act as outbound proxy: unchecked Display Name: David Account Name: 4321 Authentication ID: unchecked Password: **** Expiry Time: (use default value)

CODEC/RTP/DTMF---

(Use default value)

Phone Book Index No. 1 🗹 Enable 2222 Phone Number John Display Name SIP URL 1234 @ draytel.org OK Clear Cancel VoIP >> SIP Accounts SIP Account Index No. 1 Profile Name (11 char max.) draytel 1 Register via Auto Call without Registration SIP Port 5060 draytel.org Domain/Realm (63 char max.) draytel.org Proxv (63 char max.) Act as outbound roxv David Display Name (23 char max.) Account Number/Name 4321 (63 char max.) Authentication ID (63 char max.) Password (63 char max.) 1 hour 💌 3600 Expiry Time sec NAT Traversal Support None 🗸 VoIP1 VoIP2 **Ring Port** Ring Pattern 1 🛩

OK Cancel

David calls John

He picks up the phone and dials 2222# (DialPlan Phone Number for John) Or, He picks up the phone and dials 1234# (John's Account Name)



4.5.2 Peer-to-Peer Calling

Example 3: Arnor and Paulin have Vigor routers respectively, they can call each other *without* SIP Registrar. First they must have each other's IP address and assign an Account Name for the port used for calling.

Arnor's SIP URL: 1234@214.61.172.53

Settings for Arnor

DialPlan index 1 Phone Number: 1111 Display Name: paulin SIP URL: 4321@ 203.69.175.24

SIP Accounts Settings ---

Profile Name: Paulin Register via: None SIP Port: 5060(default) Domain/Realm: (blank) Proxy: (blank) Act as outbound proxy: unchecked Display Name: Arnor Account Name: 1234 Authentication ID: unchecked Password: (blank) Expiry Time: (use default value)

CODEC/RTP/DTMF---

(Use default value)

Paulin's SIP URL: 4321@ 203.69.175.24

Phone Book Index No. 1		
🗹 Enable		
Phone Number	1111	
Display Name	paulin	
SIP URL	4321	@ 203.69.175.24
ſ	OK Clear	Cancel
L		
oIP >> SIP Accounts		
IP Account Index No. 1		
Profile Name	Paulin (44 - L
	i admir	11 char max.)
Register via		11 char max.) vithout Registration
Register via SIP Port		
-	Auto Call v	
SIP Port	Auto Call v	vithout Registration
SIP Port Domain/Realm	Auto Call v 5060	(63 char max.)
SIP Port Domain/Realm Proxy	Auto Call w 5060	(63 char max.)
SIP Port Domain/Realm Proxy Act as outbound p	Auto Call w 5060	(63 char max.)
SIP Port Domain/Realm Proxy Act as outbound p Display Name	Auto Call w 5060	vithout Registration (63 char max.) (63 char max.) 23 char max.)
SIP Port Domain/Realm Proxy Act as outbound p Display Name Account Number/Name	Auto Call w 5060	rithout Registration (63 char max.) (63 char max.) 23 char max.) (63 char max.)
SIP Port Domain/Realm Proxy Act as outbound p Display Name Account Number/Name	Auto Call v S060 Call v Call v S060 Call v Call	vithout Registration (63 char max.) (63 char max.) 23 char max.) (63 char max.) (63 char max.)
SIP Port Domain/Realm Proxy Display Name Account Number/Name Account Number/Name Password	Auto Call v 5060 Amor (1234	vithout Registration (63 char max.) (63 char max.) (63 char max.) (63 char max.) (63 char max.)
SIP Port Domain/Realm Proxy Act as outbound p Display Name Account Number/Name Authentication ID Password Expiry Time	Auto So60 So60 Auto Call v So60 Amor (1 1234 I hour So00	vithout Registration (63 char max.) (63 char max.) (63 char max.) (63 char max.) (63 char max.)

OK Cancel

Arnor calls Paulin

VoIP >> DialPlan Setup

He picks up the phone and dials **1111#**. (DialPlan Phone Number for Arnor)

Settings for Paulin

DialPlan index 1 Phone Number:2222 Display Name: Arnor SIP URL: 1234@214.61.172.53

SIP Accounts Settings ----

Profile Name: Arnor Register via: None SIP Port: 5060(default) Domain/Realm: (blank) Proxy: (blank) Act as outbound proxy: unchecked Display Name: Paulin Account Name: 4321 Authentication ID: unchecked Password: (blank) Expiry Time: (use default value)

CODEC/RTP/DTMF---

(Use default value)

Phone Book Index No. 1 Final Enable Phone Number Display Name Arnor SIP URL 1234 Q 241.61.172.53 OK Clear Cancel

VoIP >> SIP Accounts

Profile Name	Arnor	(11 char max.)
Register via	Auto 🔽 🗌 Cal	without Registration
SIP Port	5060	
Domain/Realm		(63 char max.
Proxy		(63 char max.
🗌 Act as outbound p	гоху	
Display Name	Paulin	(23 char max.)
Account Number/Name	4321	(63 char max.
Authentication ID		(63 char max.
Password	••••	(63 char max.)
Expiry Time	1 hour 🔽 3600	sec
NAT Traversal Support	None 💌	
Ring Port	VoIP1 VoIP2	
Ring Pattern	1 🛩	

Paulin calls Arnor

He picks up the phone and dials **2222**# (DialPlan Phone Number for John)



4.6 Upgrade Firmware for Your Router

Before upgrading your router firmware, you need to install the Router Tools. The **Firmware Upgrade Utility** is included in the tools.

- 1. Insert CD of the router to your CD ROM.
- 2. From the webpage, please find out Utility menu and click it.
- 3. On the webpage of Utility, click **Install Now!** (under Syslog description) to install the corresponding program.

Please remember to set as follows in your DrayTek Router :

• Server IP Address : IP address of the PC that runs the Syslog

```
• Port Number : Default value 514
```

Install Now!

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

Tools Name	Released Date	Version	OS	Support Model	Download
Router Tools	28/03/2007	3.7	MS-Windows	All Model	Zip
Smart VPN Client	18/08/2006	3.2.6	MS-Windows	All Model	zip
Smart VPN Client	21/06/2007	3.2.6	MS-Vista	All Model	zip
LPR	27/06/2005	1.0	MS-Windows	For Print Function	zip
VTA	15/09/2005	2.8	Windows2000/XP	For ISDN Model	zip
DialPlan	26/01/2006	2.5_lite	MS-Windows	For VoIP Model	zip

- 7. Choose the one that matches with your operating system and click the corresponding link to download correct firmware (zip file).
- 8. Next, decompress the zip file.

9. Double click on the icon of router tool. The setup wizard will appear.



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

៉ Firmware Upgrade	Otility 3.5.2 📃 🗖 🔀
Operation Mode Upgrade Backup Setting	Router IP:
Time Out(Sec.)	Password:
5	
Port	
69	Abort Send

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



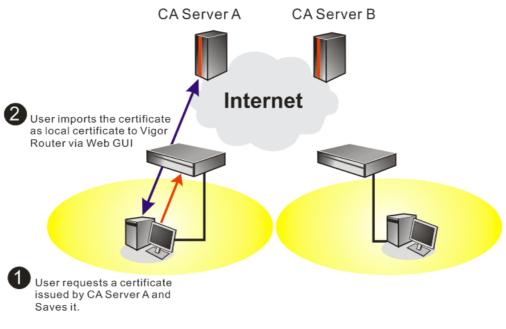
🐴 Firmware Upgrade I	Jtility 3.5.2
Operation Mode Upgrade Backup Setting	Router IP: 192.168.1.1 Firmware file: D:\3100 series\\V3100_tw01
Time Out(Sec.)	Password:
5	
Port 69	Abort Send

14. Click Send.

៉ Firmware Upgrade I	Jtility 3.5.2
Operation Mode	Router IP: 192.168.1.1
Backup Setting	Firmware file: D:\3100 series\V3100_tw01
Time Out(Sec.)	Password:
5	
Port	
69	Abort Send
Sending	

15. Now the firmware update is finished.

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



1. Go to Certificate Management and choose Local Certificate.

Certificate Management >> Local Certificate

X509 Local Certi	ficate Configuration		
Name	Subject	Status	Modify
Local			View Delete
GENERATE	IMPORT REFRESH		
X509 Loc	al Certificate		
			~
			~

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

Generate Certificate Request	
Subject Alternative Name	
Туре	Domain Name 💌
Domain Name	
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 💌

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

Name	Subject	Status	Modify
Local	/C=TW/O=DrayTek/emailAddress	Requesting	View Remove
GENERATE	IMPORT REFRESH		
MIIBqj Bgkqhk A4GNAD hX4bp8 x/GOA7 oCkwJw hkiG9w Yo6xQg vvVXnh	EGIN CERTIFICATE REQUEST CCARMCAQAwQTELMAkGA1UEBhMCVFcxEDAO iG9w0BCQEWEXByZXNzQGRyYX10ZWsuY29t CBiQKBgQDQYB7wnZFfFNN9/IeQnG03Xk++ 9cUF9dloACGGiM/tcBockdcZDFFvIXcP3 CTV0/fQzpxroCw1JTjLSjS0/Bn9v50951G YUK0ZIhvcNAQkOMRowGDAWBgNVHREEDzAN OBAQUFAAOBgQBuIWx4Mf18xeLQN7nz30cK hiXfnaRX4rdLj6ywBQ9aVdNHr+t11LgVq0 WUx2gq/QIQ6tYs+Stws+51pU+UNGSnj6je ND CERTIFICATE REQUEST	MIGfMAOGCSqGS hqFb297aPJ6+g s3uxa2Fj8aeTj ve3aGly1cEcmU ggtkcmF5dGVrL VC4h574hhm/ME CxxcNj1LfLm9t	Ib3DQEBAQUA ksBer1wa5w0 9W+ELxwhIlo 7jqeQIDAQAB mNvbTANBgkq kgemB/eWrIN JFWi4iw30ci

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:
Next >

Select Advanced request.

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

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

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

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

Microsoft Certifica	te Services vigor		<u>Home</u>
Submit A Save	d Request		
		request or PKCS #7 renewal request generated by an external application (such as a w it to the certification authority (CA).	eb
Saved Request:			
Certificate Request (PKCS #10 or #7):	BEGIN CERTIFICATE REQUI MIJEgiCARMCAQAWGTELMAKGAIU BgdghiGHOBCCEWEXPZXNeQQR A4GNADCBICHEGODCBYTMAZFFFNA hX4bp89cUF9dloACGG1M/teBock X/GOA7CTWO/fQepxroCwIJTjL535 <	EBhMCVFcxEDAO yYX102WsuY29t 9/IeQnG03Xk++ dc2APFFvIXcP3	
	Browse for a file to insert.		
Certificate Templa			
	Administrator 👻		
Additional Attribut	Administrator Authenticated Session		
Attributes:	Basic EFS EFS Recovery Agent User	< >	
	IPSEC (Offline request) Router (Offline request)		
	Subordinate Certification Authority Web Server	Subm	it >

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



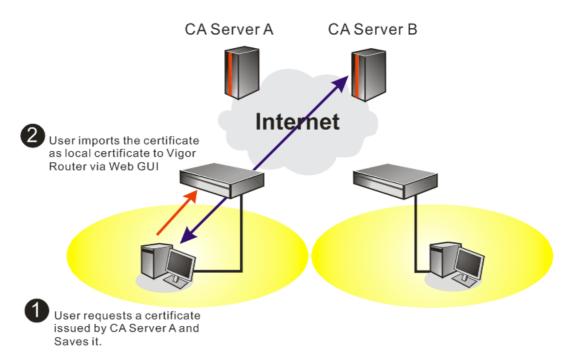
you will find the below window showing "-----BEGINE CERTIFICATE-----"...." X509 Local Certificate Configuration

Name	Subject	Status	Modify
Local	/emailAddress=press@draytek	Not Valid Yet	View Remove
GENERATE	IMPORT REFRESH		
	EGIN CERTIFICATE		····
	CCBECGAWIBAGIKYSRISAABAAABTANBGKQ	• –	
	JVUzEOMAwGA1UEAxMFdmlnb3IwHhcNMDUu		
	UzWjBBMSAwHgYJKoZIhvcNAQkBFhFwcmVz		
A1UEBh	MCVFcxEDAOBgNVBAoTBORyYX1UZWswgZ8u	JDQYJKoZIhvcNAQEH	BQADgYOA
MIGJAO	GBANBgHvCZkV8WE338h5CcbTdeT76GoVvk	3to8nr6CSwF6vXBr	nA6Ffhun
z1xQX1	2WgAIYaIz+1wE5yR1x108UW8hdw/eze7Fr	YWPxp50P1b4QvHCH	ເງພງH8bQD
sJ0879	9DOnGugLCU1OMtKNLT8Gf2/nT3nUa97dos	XLVwRyZTuOp5AgM	BAAGjggL4
MIIC9D	AWBqNVHREEDzANqqtkcmF5dGVrLmNvbTAd	BqNVHQ4EFqQUunRI	VGQYCZWM
	VoFVhyq4swVAYDVROjBEOwS4AUzQjEORhF		-
-	AJBGNVBAYTA1VTMQ4wDAYDVQQDEwV2aWdv		
MBOxCz			

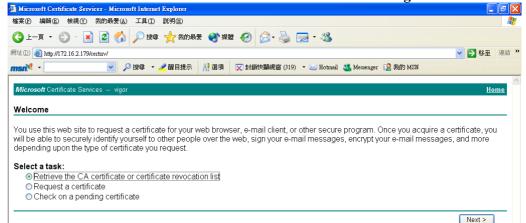
6. You may review the detail information of the certificate by clicking **View** button. **Certificate Information**

Name :	Local
Issuer :	/C=US/CN=vigor
Subject :	/emailAddress=press@draytek.com/C=TW/O=DrayTek
Subject Alternative Name :	DNS:draytek.com
Valid From :	Aug 30 23:16:53 2005 GMT
Valid To :	Aug 30 23:16:53 2007 GMT

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



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



2. In Choose file to download, click CA Certificate Current and Base 64 encoded, and Download CA certificate to save the .cer. file.

🗿 Microsoft Certificate Services - Microsoft Internet Explorer	- B X
檔案(P) 編輯(E) 檢視(Y) 我的最爱(A) 工具(D) 說明(H)	<u></u>
③ 上-頁 • ◎ - ≥ ② ☆ /> 按母 ☆ 我的最爱 ④ 媒體 ❷ ◎ - ≧ □ - 恣	
網址 (1) 🕘 http://172.16.2.179/certsrv/certearc.asp	▶ 移至 連結 ※
man ^N · D 搜尋 · Z 醒目提示 🛛 滋須 🔽 封鎖快顯視窗 (319) · 🖂 Hotmail 🐇 Messenger 🗜 我的 MSN	
<i>Microsoft</i> Certificate Services vigor	Home
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 authorit CA certification path will be installed for you automatically.	y, because the
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. **X509 Trusted CA Certificate Configuration**

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

IMPORT	REFRESH
--------	---------

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

Certificate Name:	Trusted CA-1
Issuer:	/C=US/CN=vigor
Subject:	/C=US/CN=vigor
Subject Alternative Name:	
Valid From:	Aug 30 23:08:43 2005 GMT
Valid To:	Aug 30 23:17:47 2007 GMT

Certificate Detail Information

5 Trouble Shooting

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

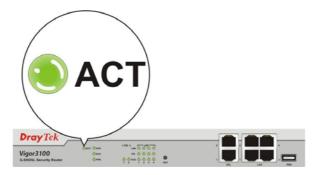
- > Checking if the hardware status is OK or not.
- Checking if the Network Connection Settings on your computer is OK or not.
- > Pinging the Router from your computer.
- Checking if the ISP Settings are OK or not.
- Backing to factory default setting if necessary.

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

5.1 Checking If the Hardware Status Is OK or Not

Follow the steps below to verify the hardware status.

- 1. Check the power line and WLAN/LAN cable connections. Refer to "**1.2 Hardware Installation**" on quick start guide 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 execute the hardware installation again. And then, try again.

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

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

For Windows

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

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



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



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

🕹 eth0 Properties 🔹 🤶 🗙
General Authentication Advanced
Connect using:
B ASUSTeK/Broadcom 440x 10/100 lr
This connection uses the following items:
☑
Gos Packet Scheduler Ser Internet Protocol (TCP/IP)
Install Properties Description Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.
 ✓ Show icon in notification area when connected ✓ Notify me when this connection has limited or no connectivity
OK Cancel

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

Internet Protocol (TCP/IP) Prop	erties 🛛 🛛 🔀
General Alternate Configuration	
You can get IP settings assigned auto this capability. Otherwise, you need to the appropriate IP settings.	
Obtain an IP address automatica	ally
OUse the following IP address: —	
IP address:	
S <u>u</u> bnet mask:	
Default gateway:	
Obtain DNS server address auto	matically
OUse the following DNS server ac	Idresses:
Preferred DNS server:	· · · · ·
Alternate DNS server:	· · · ·
	Advanced
	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.

0 0	Network	0
Show All Displays Sou	Network Startup Disk	
Lo	ocation: Automatic 🛟 Show: Built-in Ethernet 🛟	
TCP/	/IP PPPoE AppleTalk Proxies Ethernet	
Configure IPv4:	Using DHCP	
IP Address:	192.168.1.10 Renew DH0	CP Lease
Subnet Mask: Router:	(If required))
DNS Servers:		(Optional)
Search Domains:		(Optional)
IPv6 Address:	fe80:0000:0000:0000:020a:95ff:fe8d:72e4	
	Configure IPv6	?
Click the lock to p	revent further changes.	Apply Now

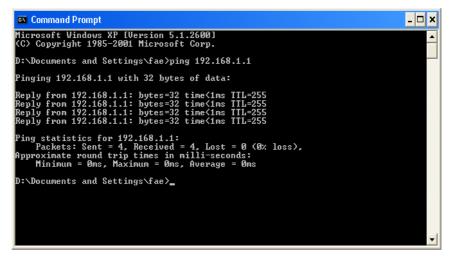
5.3 Pinging the Router from Your Computer

The default gateway IP address of the router is 192.168.1.1. For some reason, you might need to use "ping" command to check the link status of the router. **The most important thing is that the computer will receive a reply from 192.168.1.1.** If not, please check the IP address of your computer. We suggest you setting the network connection as **get IP automatically**. (Please refer to the section 5.2)

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.



$\Theta \Theta \Theta$	Terminal — bash — 80x24	
Welcome to Darwin Vigor10:~ draytek PING 192.168.1.1 64 bytes from 192 64 bytes from 192 64 bytes from 192 64 bytes from 192	an 3 02:24:18 on ttyp1 ! \$ ping 192.168.1.1 (192.168.1.1): 56 data bytes .168.1.1: icmp_seq=0 ttl=255 time=0.755 ms .168.1.1: icmp_seq=1 ttl=255 time=0.697 ms .168.1.1: icmp_seq=2 ttl=255 time=0.716 ms .168.1.1: icmp_seq=4 ttl=255 time=0.721 ms .168.1.1: icmp_seq=4 ttl=255 time=0.722 ms	8
192.168.1.1 p 5 packets transmi	ing statistics tted, 5 packets received, 0% packet loss g/max = 0.697/0.723/0.755 ms \$ ∎	

5.4 Checking If the ISP Settings are OK or Not

Click Internet Access Setup group and then check whether the ISP settings are set correctly.

For PPPoE/PPPoA Users

- 1. Check if the **Enable** option is selected.
- 2. Check if all parameters of **DSL Modem Settings** are entered with correct values that you got from your ISP.
- 3. Check if **Username** and **Password** are entered with correct values that you **got from** your **ISP**.

PPPoE/PPPoA Client 🔷 Enable 💿 Disable	ISP Access Setup		
	ISP Name hinet		
DSL Modem Settings	Username 86623721@hinet.net		
Multi-PVC channel Channel 1 🛛 👻			
VPI O	Password ••••••		
VCI 33	PPP Authentication PAP or CHAP 😪		
	🗖 Always On		
Encapsulating Type LLC/SNAP 💌	Idle Timeout 180 second(s)		
Protocol PPPoE V	IP Address From ISP WAN IP Alias		
PPPoE Pass-through	Fixed IP 🔿 Yes 💿 No (Dynamic IP)		
For Wired LAN	Fixed IP Address		
WAN Backup Setup	* : Required for some ISPs		
3G USB Modem	Oefault MAC Address		
Dial Backup Mode 🛛 Always On 🛛 👻	Specify a MAC Address		
Go to <u>3G USB Modem Backup</u> Setup	MAC Address :		
ISDN	00 · 50 · 7F :81 · 83 · 09		
Dial Backup Mode 🛛 None 🛛 😪			
	Index(1-15) in <u>Schedule</u> Setup:		

Internet Access >> PPPoE / PPPoA

For MPoA (RFC1483/2684) Users

- 1. Check if the **Enable** option is selected.
- 2. Check if all parameters of **DSL Modem Settings** are entered with correct values that you got from your **ISP**.
- 3. Check if **IP** Address, Subnet Mask and Gateway are set correctly, or use DHCP server to obtain IP automatically by clicking Obtain an IP address automatically.

MPoA (RFC148	3/2684)	🔘 Enable 💿 Disable	WAN IP Networ	k Settings	5	
			– 🔘 Obtain an IP	address	automatically	
DSL Modem Settings			Router Name		*	
Multi-PVC channel Channel 2		Domain Name		*		
Encapsulation	1402 D.	idged IP LLC	💿 Specify an Il	P address	WAN IP Alias	
	1403 DI		IP Address	1	172.16.3.229	
VPI VCI		0	Subnet Mask	[1	172.16.3.4	
VCI		54	Gateway IP Ad	dress		
Go to <u>3</u> ISDN Dial Back	em «up Mode	odem Backup Setup	* : Required fo • Default MA • Specify a MAC Address • 00 • 50 • 50 • DNS Server IP	AC Address MAC Addre : . 7F :81	; 255	
RIP Protocol						
🔲 Enable RIP			Primary IP Add			
Bridge Mode	e Mode		 Secondary IP 	Address [

5.5 Problems for 3G Network Connection

When you have trouble in using 3G network transmission, please check the following:

Check if USB LED lights on or off

You have to wait about 15 seconds after inserting 3G USB Modem into your Vigor3100. 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 Vigor3100.

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.



		Vigor3100 series annex A	Getway IP (Static)	TX Packets	RX Rate
AN Status				0	0
TX Packets	;	RX Packets	WAN IP (Static)	RX Packets	TX Rate
6442		3807		0	0
-					
Wall Log VPN Lo	g User Acce	ss Log Call Log WAN I	Log Network Infomation	Net State	
-		1 Maria			
Time	Host	Message			
pr 12 09:17:49	Vigor		ocol:LCP(c021) ConfReq Id	entitier:0x03 ACCM: 0	JXJ Authe:
pr 12 09:17:49	Vigor Vigor		0 00 00 00 00 02 00 03 00 ocol:LCP(c021) ConfReg Id		00 4001
pr 12 09:17:49 pr 12 09:17:49	Vigor	WAN2 PPPoE => Pion WAN2 PPPoE <= V:1		entitier/0x00 PdR0:15	OU ACCK
pr 12 09:17:49	Vigor	[3G]Modem response: C			
pr 12 09:17:49	Vigor		0 00 00 00 00 02 00 02 00		
pr 12 09:17:49	Vigor		0 00 00 00 00 02 00 02 00		
pr 12 09:17:49	Vigor	[3G]Modem dial ATDT			
pr 12 09:17:49	Vigor	WAN2 PPPoE -> V:1			
pr 12 09:17:49	Vigor	WAN2 PPPoE <== V:1	T:1 PADO ID:0		
pr 12 09:17:49	Vigor	[3G]Modem response: C	OK		
pr 12 09:17:49	Vigor		T&FE0V1X1&D2&C1S0=0		-
		$WAN2 PPPoE \implies V:1$	T:1 PADI ID:0		<u>M</u>
or 12 09:17:49	Vigor	TT 2224 20 2 2 2 0 20			
	V 1201				>

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 Vigor3100. In addition, please refer to the manual of 3G USB Modem for LED Status to make sure if the modem connects to Internet via HSDPA mode. If you want to use the modem indoors, please put it on the place near the window to obtain better signal receiving.

5.6 Backing to Factory Default Setting If Necessary

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

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

Software Reset

You can reset router to factory default via Web page.

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

```
System Maintenance >> Reboot System
```

Reboot System

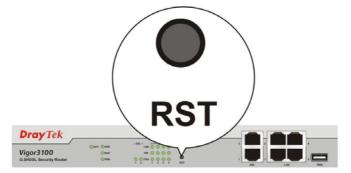
Do You want to reboot your router ?

○ Using current configuration ⊙ Using factory default configuration



Hardware Reset

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



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

5.7 Contacting Your Dealer

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

