



Your reliable networking solutions partner

User's Guide

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

Version: 3.0 Firmware Version: V3.6.3 Date: 12/12/2012

Copyright Information

Copyright Declarations	Copyright 2012 All rights reserved. This publication contains information that is protected by copyright. No part may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language without written permission from the copyright holders.
Trademarks	 The following trademarks are used in this document: Microsoft is a registered trademark of Microsoft Corp. Windows, Windows 95, 98, Me, NT, 2000, XP, Vista and Explorer are trademarks of Microsoft Corp. Apple and Mac OS are registered trademarks of Apple Inc. Other products may be trademarks or registered trademarks of their respective manufacturers.
Safety Instructio	ns 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

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

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

http://www.draytek.com

Warranty



European Community Declarations

Manufacturer: DrayTek Corp.

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

DrayTek Corp. declares that Vigor2710 Series of routers are in compliance with the following essential requirements and other relevant provisions of R&TTE Directive 1999/5/EEC.

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

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

Regulatory Information

Federal Communication Commission Interference Statement

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



This product is designed for the DSL, POTS, DECT 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



Introduction	1
1.1 Web Configuration Buttons Explanation	
1.2 LED Indicators and Connectors	2
1.2.1 For Vigor2710 1.2.2 For Vigor2710n 1.2.3 For Vigor2710Vn 1.2.4 For Vigor2710VDn	
1.3 Hardware Installation	10
1.4 Printer Installation	11



Initial Configuration	17
2.1 Accessing the Web User Interface	17
2.2 Changing Password	19
2.3 Quick Start Wizard	20
2.3.1 Adjusting Protocol/Encapsulation 2.3.2 PPPoE/PPPoA	20 22
2.3.3 1483 Bridged IP 2.3.4 1483 Routed IP	23
2.4 Service Activation Wizard	26
2.5 VoIP Wizard	29
2.6 Online Status	30
2.6.1 Physical Connection 2.6.2 Virtual WAN	30 32
2.7 Saving Configuration	33
2.8 Registering Vigor Router	33



Application and Example	37
3.1 How to configure settings for IPv6 Service	37
3.2 How Can I Use FTP to Get the Files from USB Storage Device Connecting to Vigor Route	
3.3 How to Customize Your Login Page	50
3.4 Create a LAN-to-LAN Connection Between Remote Office and Headquarter	51
3.5 Create a Remote Dial-in User Connection Between the Teleworker and Headquarter	58
3.6 LAN – Created by Using NAT	63
3.7 Calling Scenario for VoIP function	65



3.7.1 Calling via SIP Sever 3.7.2 Peer-to-Peer Calling	65 67
3.8 Request a certificate from a CA server on Windows CA Server	
3.9 Request a CA Certificate and Set as Trusted on Windows CA Server	
3.10 Creating an Account for MyVigor	75
3.10.1 Creating an Account via Vigor Router 3.10.2 Creating an Account via MyVigor Web Site	



Advanced Configuration	83
4.1 Internet Access	83
 4.1.1 Basics of Internet Protocol (IP) Network 4.1.2 PPPoE/PPPoA 4.1.3 MPoA 4.1.4 IPv6 4.1.5 Multi-PVCs 	
4.2 LAN	105
 4.2.1 Basics of LAN 4.2.2 General Setup 4.2.3 Static Route 4.2.4 VLAN 4.2.5 Bind IP to MAC 	107 112 116
4.3 NAT	118
 4.3.1 Port Redirection	123 126
4.4 Firewall	130
4.4.1 Basics for Firewall.4.4.2 General Setup.4.4.3 Filter Setup4.4.4 DoS Defense	132 136
4.5 Objects Settings	148
 4.5.1 IP Object 4.5.2 IP Group 4.5.3 IPv6 Object 4.5.4 IPv6 Group 4.5.5 Service Type Object 4.5.6 Service Type Group 4.5.7 Keyword Object 4.5.8 Keyword Group 4.5.9 File Extension Object 	
4.6 CSM	167
4.6.1 APP Enforcement Profile 4.6.2 URL Content Filter Profile 4.6.3 Web Content Filter Profile	170
4.7 Bandwidth Management	178
4.7.1 Sessions Limit	178



4.7.2 Bandwidth Limit 4.7.3 Quality of Service	. 182
4.7.4 APP QoS	
4.8 Applications	
4.8.1 Dynamic DNS 4.8.2 Schedule	
4.8.3 RADIUS	
4.8.4 UPnP	. 198
4.8.5 IGMP	
4.8.6 Wake on LAN	
4.9 VPN and Remote Access	
4.9.1 Remote Access Control 4.9.2 PPP General Setup	
4.9.3 IPSec General Setup	
4.9.4 IPSec Peer Identity	
4.9.5 Remote Dial-in User	
4.9.6 LAN to LAN 4.9.7 Connection Management	
4.10 Certificate Management	
4.10.1 Local Certificate 4.10.2 Trusted CA Certificate	
4.10.2 Trusted CA Certificate	
4.11 VoIP	
4.11.1 DialPlan	
4.11.2 SIP Accounts	
4.11.3 Phone Settings	. 242
4.11.4 DECT	
4.11.5 Status	
4.12 Wireless LAN	
4.12.1 Basic Concepts	
4.12.2 General Setup 4.12.3 Security	
4.12.4 Access Control.	
4.12.5 WPS	
4.12.6 WDS	
4.12.7 Advanced Setting 4.12.8 WMM Configuration	
4.12.9 AP Discovery	
4.12.10 Station List	. 272
4.13 USB Application	. 273
4.13.1 USB General Settings	. 273
4.13.2 USB User Management	
4.13.3 File Explorer 4.13.4 USB Disk Status	
4.14 System Maintenance.	
4.14.1 System Status 4.14.2 TR-069	
4.14.2 TR-009 4.14.3 Administrator Password	
4.14.4 User Password	. 283
4.14.5 Login Page Greeting	
4.14.6 Configuration Backup 4.14.7 Syslog/Mail Alert	
4.14.8 Time and Date	



4.14.9 Management 4.14.10 Reboot System	292
4.14.10 Reboot System	
4.14.11 Firmware Upgrade	295
4.14.12 Activation	
4.15 Diagnostics	298
4.15.1 Dial-out Triggering	298
4.15.2 Routing Table	
4.15.3 ARP Cache Table	300
4.15.4 IPv6 Neighbour Table	300
4.15.5 DHCP Table	301
4.15.6 NAT Sessions Table	302
4.15.7 Data Flow Monitor	303
4.15.8 Traffic Graph	305
4.15.9 Ping Diagnosis	306
4.15.10 Trace Route	307
4.16 Product Registration	308



1	Trouble Shooting	309
	5.1 Checking If the Hardware Status Is OK or Not	309
	5.2 Checking If the Network Connection Settings on Your Computer Is OK or Not	310
	5.3 Pinging the Router from Your Computer	312
	5.4 Checking If the ISP Settings are OK or Not	313
	5.5 Problems for 3G Network Connection	314
	5.6 Backing to Factory Default Setting If Necessary	314
	5.7 Contacting Your Dealer	315



Vigor2710 series is an ADSL router. It integrates IP layer QoS, NAT session/bandwidth management to help users control works well with large bandwidth.

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

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

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

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

1.1 Web Configuration Buttons Explanation

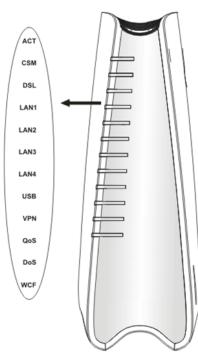
Several main buttons appeared on the web pages are defined as the following:

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

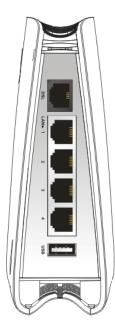
1.2 LED Indicators and Connectors

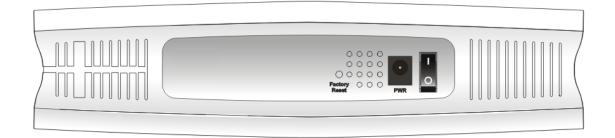
Before you use the Vigor router, please get acquainted with the LED indicators and connectors first.

1.2.1 For Vigor2710



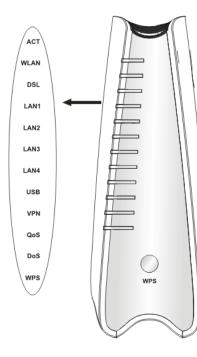
LED	Status	Explanation
ACT	Blinking	The router is powered on and running
(Activity)		normally.
	Off	The router is powered off.
CSM	On	The profile(s) of CSM (Content Security
		Management) for IM/P2P, URL/Web
		Content Filter application can be enabled
		from Firewall >>General Setup. (Such
		profile must be established under CSM menu).
DSL	On	The router is ready to access Internet
DSL	Oli	through DSL link.
	Blinking	Slowly: The modem is ready.
	Diniking	Quickly: The connection is training.
	On	The port is connected.
LAN 1/2/3/4	Off	The port is disconnected.
	Blinking	The data is transmitting.
USB	On	A USB device is connected and active.
COD	Blinking	The data is transmitting.
VPN	On	The VPN tunnel is active.
QoS	On	The QoS function is active.
-		· · ·
DoS	On Di l	The DoS/DDoS function is active.
WCE	Blinking	It will blink while detecting an attack.
WCF	On	The profile(s) of CSM (Content Security Management) for Web Content Filter
		application can be enabled from Firewall
		>>General Setup. (Such profile must be
		established under CSM menu)
Interface	Descripti	on
DSL	Connecter	for accessing the Internet through ADSL2/2+.
LAN (1-4)		s for local networked devices.
USB	Connecter	for USB storage device (Pen Driver/Mobile
	HD) or pri	



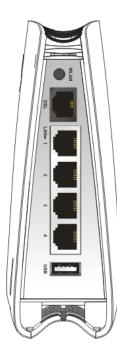


Interface	Description
Factory Reset	Restore the default settings. Usage: Turn on the router (ACT LED is blinking). Press the hole and keep for more than 5 seconds. When you see the ACT LED begins to blink rapidly than usual, release the button. Then the router will restart with the factory default configuration.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

1.2.2 For Vigor2710n



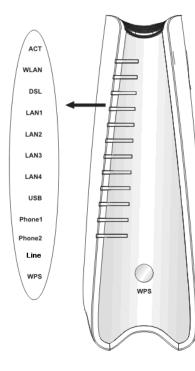
LED	Status	Explanation
ACT	Blinking	The router is powered on and running
(Activity)	Dillikilig	normally.
(neuvity)	Off	The router is powered off.
WLAN	On	Wireless access point is ready.
	Blinking	It will blink while wireless traffic goes
	Diming	through.
DSL	On	The router is ready to access Internet
		through DSL link.
	Blinking	Slowly: The modem is ready.
		Quickly: The connection is training.
T A DT 1/0/0/4	On	The port is connected.
LAN 1/2/3/4	Off	The port is disconnected.
	Blinking	The data is transmitting.
USB	On	A USB device is connected and active.
	Blinking	The data is transmitting.
VPN	On	The VPN tunnel is active.
QoS	On	The QoS function is active.
DoS	On	The DoS/DDoS function is active.
	Blinking	It will blink while detecting an attack.
WPS	On	The WPS is on.
	Off	The WPS is off.
	Blinking	Waiting for wireless client sending requests
	-	for connection about two minutes.
WPS Button	On	Press this button for 2 seconds to wait for
		client device making network connection through WPS. When the LED lights up, the
		WPS will be on.
	Off	The WPS is off.
	Blinking	Waiting for wireless client sending requests
	U	for connection about 2 minutes.
Interface	Descripti	
WLAN		utton once to enable (WLAN LED on) or
	disable (W	LAN LED off) wireless connection.
DSL	Connecter	for accessing the Internet through ADSL2/2+.
LAN (1-4)		for local networked devices.
USB		for USB storage (Pen Driver Mobile/HD) or
	printer.	
	I	



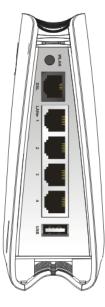


Interface	Description
Factory Reset	Restore the default settings. Usage: Turn on the router (ACT LED is blinking). Press the hole and keep for more than 5 seconds. When you see the ACT LED begins to blink rapidly than usual, release the button. Then the router will restart with the factory default configuration.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

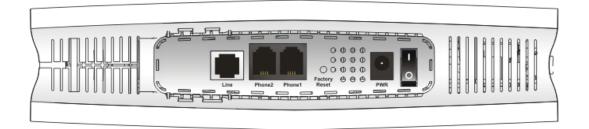
1.2.3 For Vigor2710Vn



LED	Status	Explanation
ACT	Blinking	The router is powered on and running
(Activity)		normally.
	Off	The router is powered off.
WLAN	On	Wireless access point is ready.
	Blinking	It will blink while wireless traffic goes
		through.
DSL	On	The router is ready to access Internet
	D1: 1 ·	through DSL link.
	Blinking	Slowly: The modem is ready. Quickly: The connection is training.
	On	The port is connected.
LAN 1/2/3/4	Off	The port is disconnected.
	Blinking	The data is transmitting.
USB	On	A USB device is connected and active.
USD	Blinking	The data is transmitting.
Phone1/	On	The phone connected to this port is off-hook.
Phone2	Off	The phone connected to this port is on-hook.
-	Blinking	A phone call comes.
Line	On	A PSTN phone call comes (in and out).
2	0.1	However, when the phone call is
		disconnected, the LED will be off about six
		seconds later.
	Off	There is no PSTN phone call.
WPS	On	The WPS is on.
	Off	The WPS is off.
	Blinking	Waiting for wireless client sending requests
WDC D //	0	for connection about two minutes.
WPS Button	On	Press this button for 2 seconds to wait for client device making network connection
		through WPS. When the LED lights up, the
		WPS will be on.
	Off	The WPS is off.
	Blinking	Waiting for wireless client sending requests
		for connection about 2 minutes.
Interface	Descripti	
WLAN		utton once to enable (WLAN LED on) or LAN LED off) wireless connection.
DSL	Connecter	for accessing the Internet through ADSL2/2+.
LAN (1-4)	Connecters	for local networked devices.
USB		for USB storage (Pen Driver Mobile/HD) or
	printer.	

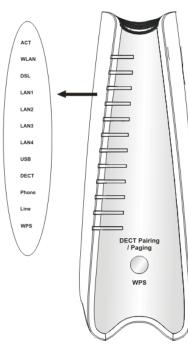






Interface	Description
Line	Connector of analog phone for PSTN life line.
Phone2/Phone1	Connecter of analog phone for VoIP communication.
Factory Reset	Restore the default settings. Usage: Turn on the router (ACT LED is blinking). Press the hole and keep for more than 5 seconds. When you see the ACT LED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

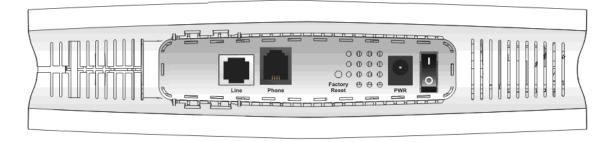
1.2.4 For Vigor2710VDn



LED	Status	Explanation
ACT	Blinking	The router is powered on and running
(Activity)	0.02	normally.
	Off	The router is powered off.
WLAN	On	Wireless access point is ready.
	Blinking	It will blink while wireless traffic goes through.
DSL	On	The router is ready to access Internet through DSL link.
	Blinking	Slowly: The modem is ready. Quickly: The connection is training.
	On	The port is connected.
LAN	Off	The port is disconnected.
1/2/3/4	Blinking	The data is transmitting.
USB	On	A USB device is connected and active.
002	Blinking	The data is transmitting.
DECT	On	DECT phone is in use
	Off	DECT phone is idle or off.
	Blinking	A DECT phone call comes.
Phone	On	The phone connected to this port is
Thome	Oli	off-hook.
	Off	The phone connected to this port is
	011	on-hook.
	Blinking	A phone call comes.
Line	On	A PSTN phone call comes (in and out). However, when the phone call is disconnected, the LED will be off about
	Off	six seconds later.
WDC	Off	There is no PSTN phone call.
WPS	On	The WPS is on.
	Off	The WPS is off.
	Blinking	Waiting for wireless client sending requests for connection or DECT handset about two minutes.
DECT	On	DECT Pairing and WPS: Press and
Pairing/Pag		hold the button for more than 2
ing / WPS		seconds then you could try to register
Button		DECT phone with 2710 within 2
		minutes.
		DECT Paging : Press once. All handsets
		will have beep sound, press the button
		again or press any key on any handset will stop the beep sound.
	Off	The WPS is off.
	Blinking	Waiting for wireless client sending requests for connection about 2 minutes.



Interface	Description
WLAN	Press the button once to enable (WLAN LED on) or disable (WLAN LED off) wireless connection.
DSL	Connector for accessing the Internet through ADSL2/2+.
LAN (1-4)	Connectors for local networked devices.
USB	Connector for USB storage (Pen Driver/Mobile HD) or printer.

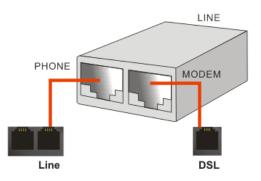


Interface	Description
Line	Connector for PSTN life line.
Phone	Connector of analog phone for VoIP communication.
Factory Reset	Restore the default settings. Usage: Turn on the router (ACT LED is blinking). Press the hole and keep for more than 5 seconds. When you see the ACT LED begins to blink rapidly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

1.3 Hardware Installation

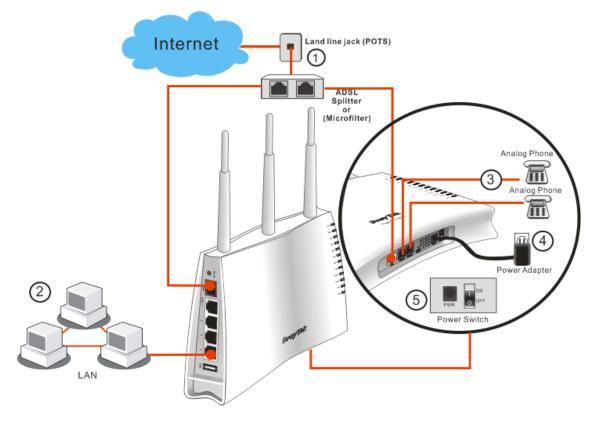
Before starting to configure the router, you have to connect your devices correctly.

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



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

Here, we take Annex A model as an example for describing hardware installation.

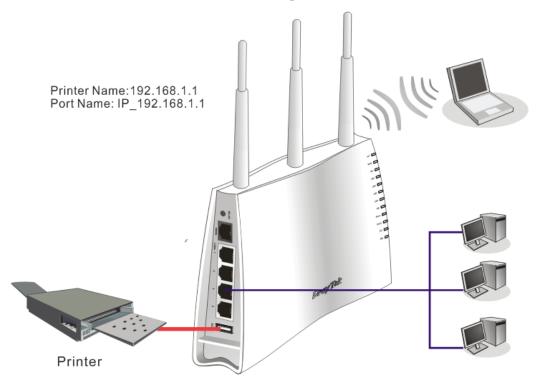


Caution:

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

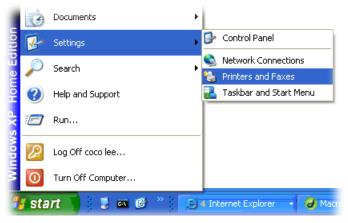
1.4 Printer Installation

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



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

1. Connect the printer with the router through USB/parallel port.



2. Open Start->Settings-> Printer and Faxes.

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





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

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

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

Select the port you want yo new port.	our printer to use. If the port is not listed, you a	can create a
OUse the following port:	LPT1: (Recommended Printer Port)	~
Co Co		

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**.

Standard TCP/IP Printer Add Port For which device do you want	
Enter the Printer Name or IP a	ddress, and a port name for the desired device.
Printer Name or IP <u>A</u> ddress:	192.168.1.1
Port Name:	IP_192.168.1.1
	<back next=""> Cancel</back>

7. Click Standard and choose Generic Network Card.

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

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



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

	and model determine which printer software to use.	2
	facturer and model of your printer. If your printer can Disk. If your printer is not listed, consult your printer	
compatible printe		
Manufacturer	Printers	
AST AT&T	Prother HL-1060 BR-Script2	1
	Brother HL-1070 BR-Script2	
and the second se		
Brother	Brother HL-1070	
Brother	Brother HL-1070 Brother HL-1070 Brother HL-10PS70PS Brother HL-10PS70PS	
Brother Bui Canon This driver is digitally	BIOMER HL-TUPS/DPS	Have Disk

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

Print to the following port(s). Documents will print to the first free shecked port.	
Port Description Printer	1
□ 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	
IP_1 Standard TCP/IP Port	
IP_1 Standard TCP/IP Port	
☑ IP_1 Standard TCP/IP Port Brother HL-1070	
PDF Local Port PDF995	
Add Port. Delete Port Configure Pr	ort
	ort
Enable bidirectional support	

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 LPR name.

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	
Raw Settings	
Port Number:	9100
LPR Settings	-
Queue Name:	51
LPR Byte Counting En	abled
SNMP Status Enabled	
Community Name:	public
SNMP Device Index	

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/Application Notes**; find out the link of **Printer Server** and click it; then click the **What types of printers are compatible with Vigor router?** link.

Dray Tek		ila partes
About DrayTek Products	Supports Solutions Multi-Media Demo Contact Us Q Search	
FAQ / Application	You are here: Home + Supports + FAQ / Application Notes + Printer Server	
Basic		a
Firmware Upgrade	Printer Server	
WAN		
IPv6	1. What types of printers are compatible with Vigor router?	2012/01/12
Triple-Play	2. How do I configure LPR printing on Windows7?	2012/08/20
Dual WAN	3. How do I configure LPR printing on My Windows Vista ?	2009/01/20
LAN	4. How do I configure LPR printing on Linux boxes ?	2009/01/20
DHCP	5. How do I configure LPR printing on Windows2000/XP ?	2010/04/06
NAT	5. How do reoningule EFR printing on windows2000/XF ?	2010/04/00

This page is left blank.



For using 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 accessing into the web configurator of Vigor router and how to adjust settings for accessing Internet successfully..

2.1 Accessing the Web User Interface

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

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

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



3. Please type "admin/admin" as the Username/Password and click Login.

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

4. Now, the **Main Screen** will appear.

Vigor27	2 + Firewall Router	
Auto Logout 👻 🛛 IRG	System Status	
Quick Start Wizard Service Activation Wizard VoIP Wizard Online Status	Model Name : Vigor2710V Firmware Version : 3.6.3 Build Date/Time : Nov 2 2012 16:34:49 ADSL Firmware Version : 211011_A Hardware: Annex A	
Internet Access LAN NAT Firewall Objects Setting	LAN WAN 1 MAC Address : 00-50-7F-92-F5-00 Link Status : Disconnected 1st IP Address : 192.168.1.1 MAC Address : 00-50-7F-92-F5-01 1st Subnet Mask : 255.255.255.0 Connection : PPPOE DHCP Server : Yes IP Address : DNS : 8.8.8.8 Default Gateway :	
SM Jandwidth Management Applications FPN and Remote Access Certificate Management JoIP JSB Application System Maintenance	VoIP Port Profile Reg. In/Out Phone1 No 0/0 Phone2 No 0/0 ONLY Phone 2 can access the PSTN line during power failure.	
iagnostics	Address Scope Internet Access Mode	

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

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

1	AutoLogout 🚩	I
4	Auto Logout	
C	Dff	q
1	. min	
3	3 min	
5	5 min	
1	LO min	

2.2 Changing Password

Please change the password for the original security of the router.

- 1. Open a web browser on your PC and type **http://192.168.1.1.** A pop-up window will open to ask for username and password.
- 2. Please type "admin/admin" as the Username/Password and click Login.
- 3. Go to System Maintenance page and choose Administrator Password/User Password.

System Maintenance >> Administrator Password Setup		
Administrator Password		
Old Password		
New Password		
Confirm Password		
Note:Password can contain only a-z A-Z 0-9 , ;	$: " <> * + = \setminus ? @ # ^ ! ()$	
	ОК	

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

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

2.3 Quick Start Wizard



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

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

Quick Start Wizard

Please enter an alpha-nume	ric string as your Password (Max 23 characters).	
Old Password	•••	
New Password	••••	
Confirm Password	••••	

2.3.1 Adjusting Protocol/Encapsulation

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

Quick Start Wizard

VPI	0 Auto detect
VCI	33
Protocol / Encapsulation	PPPoE LLC/SNAP
Fixed IP	○Yes ④No(Dynamic IP)
IP Address	
Subnet Mask	
Default Gateway	
Primary DNS	
Second DNS	

Available settings are explained as follows:

Item	Description	
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 .		
	Protocol / Encapsulation Fixed IP IP Address Subnet Mask Default Gateway Primary DNS	1483 Bridged IP LLC	
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 an 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 an IP address to a Routed IP and Bridged	the gateway for the protocol of IP .	
Primary DNS	Assign an IP address to	the primary DNS.	
Second DNS	Assign an IP address to	the secondary DNS.	

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

2.3.2 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.

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

1. If your ISP provides you the **PPPoE** connection, please select **PPPoE** for this router.

ect to Internet	
VPI	0 Auto detect
VCI	33
Protocol / Encapsulation	PPP₀E LLC/SNAP ✓
Fixed IP	○Yes ④No(Dynamic IP)
IP Address	
Subnet Mask	
Default Gateway	
Primary DNS	
Second DNS	

2. The following page will be shown:

Quick Start Wizard		
Set PPPoE / PPPoA		
User Name		
Password		
Confirm Password		
	< Back Next > Finish	Cancel

Available settings are explained as follows:

Item	Description
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.
Back	Click it to return to previous setting page.
Next	Click it to get into the next setting page.
Cancel	Click it to give up the quick start wizard.

- 3. Type in all the information that your ISP provides for this protocol.
- 4. Click **Next** for viewing summary of such connection.

Quick Start Wizard

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

- 5. Click **Finish.** Then, the system status of this protocol will be shown.
- 6. Now, you can enjoy surfing on the Internet.

2.3.3 1483 Bridged IP

If your ISP provides you the Bridge connection, click 1483 Bridged IP as the protocol.
 Quick Start Wizard

VPI	0 Auto detect
VCI	33
Protocol / Encapsulation	1483 Bridged IP LLC
Fixed IP	○ Yes ③ No(Dynamic IP)
IP Address	
Subnet Mask	
Default Gateway	
Primary DNS	
Second DNS	

2. Type in all the information that your ISP provides for this protocol. Click **Next** for viewing summary of such connection.

se confirm your settings:	
VPI:	0
VCI:	33
Protocol / Encapsulation:	1483 Bridge LLC
Fixed IP:	No
Primary DNS: Secondary DNS:	
Secondary DNS.	

- 3. Click **Finish.** Then, the system status of this protocol will be shown.
- 4. Now, you can enjoy surfing on the Internet.

2.3.4 1483 Routed IP

1. If your ISP provides you the **1483 Routed IP** connection, click **1483 Routed IP** as the protocol.

ect to Internet	
VPI	0 Auto detect
VCI	33
Protocol / Encapsulation	1483 Routed IP LLC
Fixed IP	◯Yes ⊙No(Dynamic IP)
IP Address	
Subnet Mask	
Default Gateway	
Primary DNS	
Second DNS	

2. Type in all the information that your ISP provides for this protocol. Click **Next** to see the following page.

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

- 3. Click **Finish.** Then, the system status of this protocol will be shown.
- 4. Now, you can enjoy surfing on the Internet.

2.4 Service Activation Wizard

Service Activation Wizard can guide you to activate WCF service (Web Content Filter) with a quick and easy way. For the Service Activation Wizard is only available for admin operation, therefore, please type "admin/admin" on Username/Password while Logging into the web configurator.

Note: Web Content Filter (WCF) is not a built-in service of Vigor router, but a service powered by Commtouch. If you want to use such service (trial or formal edition), you have to perform the procedure of activation first. For the service of formal edition, please contact with your dealer for detailed information.

Service Activation Wizard is a tool which allows you to use trial version or update the license of WCF directly without accessing into the server (**MyVigor**) located on <u>http://myvigor.draytek.com</u>. For using Web Content Filter Profile, please refer to section **Web Content Filter Profile** for detailed information.

Now, please follow the steps listed below to activate WCF feature for your router.

1. Open Service Activation Wizard.



Service Activation Wizard

2. The screen of **Service Activation Wizard** will be shown as follows. Choose the one you need and click **Next**. In this case, we choose to activate free trail edition.

lect the service type that you want to active	ate			
This wizard is used for activating - Web Content Filter Please choose the edition you need.				
Free trial edit	tion			
O Formal edition		key		
		Next >	Finish	Cancel

Free trial edition: it offers a period of trial for you to get acquainted with WCF function.

Formal edition with license key: you can extend the license valid time manually.

Note: If you activate **Formal edition with license key** first, the free trial edition will be invalid.



3. In the following page, you can activate the Web content filter service at the same time or individually. When you finish the selection, please click **Next**.

ect the service type that you want to activate			
This product provides 30 days of free trial, please	e choose the item you want to use.		
WCF service:			
Web Content Filter (BPiM)			
BPjM is the web content filter based on service operated in service. This is a free service without guarantee.	n Germany. We recommend only users live in Germany to try the $\ensuremath{BPjM}\xspace$ WCF		
	Activation Date : 2011-02-11		
	ise Agreement h operated in the worldwide. There is a 30-day trial period. After trial, you can		
purchase Draytek's prepared Commouch Globalview wo	Activation Date : 2011-02-11		
	Activation Date : 2011-02-11		
✓ I have read and accept the above Agreement. (Ple			

Commtouch is the web content filter based on Commtouch operated in the worldwide. There is a 30-day trial period. After trial, you can purchase DrayTek's prepared Commtouch GlobalView WCF package from DrayTek dealer.

4. Setting confirmation page will be displayed as follows, please click **Next**.

Please	confirm your settings	
	Sevice Type : Sevice Activated :	Trial version Web Content Filter (Commtouch)
	Please click <mark>Back</mark> to re-se	elect service type you to activate.
		< Back Next > Finish Cancel

5. Wait for a moment till the following page appears.

Service Activation Wizard

Service Activation Wizard

Connection Succeeded!

Please check the following item(s) to enable services on your router.

Enable Web Content Filter

Next > Finish

When such page appears, you can enable or disable these services for your necessity. Then, click **Finish.**

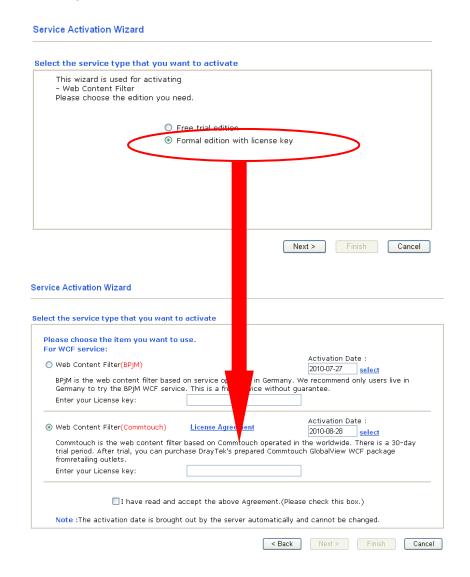


Note: The service will be activated and applied as the default rule configured in **Firewall>>General Setup**.

6. Now, the web page will display the service that you have activated according to your selection(s). The valid time for the free trial of these services is one month.

	DrayTek Service	e Activation	
Service Name	Start Date	Expire Date	Status
Web Content filter	2010-07-27	2010-08-27	Commtouch
Please check if the licen normal operation for you			

Later, if you need to extend the license valid time, you can also use the **Service Activation Wizard** again to reach your goal by clicking the radio button of **Formal edition with license key** and clicking **Next**.





Check the box of **"I have read and accept the above.."** and click **Next.** Follow the on-screen instruction to install the formal edition of WCF license.

2.5 VoIP Wizard

Vigor router offers a quick method to configure settings for VoIP application. Follow the steps listed below.

1. Open VoIP Wizard.



2. The screen of VoIP Wizard will be shown as follows.

VoIP service provide	uumam			
/oIP service provider	draytel.org 🖌 🖌	draytel.org	(63 char max).	
SIP Port	5060			
Account quickly				
Phone 1 (default mappir	ng to Account 1)			
Account Number/Name		(63 char max).		
Password		(63 char max).		
Phone 2 (default mappir	ng to Account 2)			
🗹 use the same Accou	unt as phone1			
Account Number/Name		(63 char max).		
Password		(63 char max).		

Available settings are explained as follows:

Item	Description
Set VoIP service provider domain	 VoIP service provider - Use the drop down list to choose the ISP which offers the VoIP service for your router. If your ISP is not in the list, simply type the name of the ISP in the entry box. SIP Port – Use the default setting (5060).
Set Account quickly	Account Number/Name – Type the account number/name registered to your ISP.
	Password – Type the password for the account registered to your ISP.
	Use the same Account as phone 1 – If you don't need to configure Phone 2 settings, simply check this box.
Next	Click it to get into the next setting page.
Cancel	Click it to give up the quick start wizard.

3. After finished the settings above, click Next for viewing summary of such connection.

VoIP Wizard	
Please confirm your setting	js:
VoIP Service Provider	draytel.org
SIP Port	5060
Phone 1 Account	5633s
Phone 2 Account	5633s
Click Back to modify char	nges if necessary. Otherwise, click Finish to save current settings.
	< Back Next > Finish Cancel

4. Click Finish. A page of VoIP Wizard Setup OK!!! will appear.

VoIP Wizard			

VoIP Wizard Setup OK!

2.6 Online Status



2.6.1 Physical Connection

Such page displays the physical connection status such as LAN connection status, WAN connection status, ADSL information, and so on.

If you select **PPPoE** as the protocol, you will find out a link of **Dial PPPoE** or **Drop PPPoE** in the Online Status web page.

Online Status

Physical Conne					System upt	ime: 2days 22:0
	IPv4			IPv6		
LAN Status Primary		ry DNS: 8.8.8.8	DNS: 8.8.8.8 Second		Secondary DNS: 8.8.4.4	
IP Address		TX Packets	RX Pac	kets		
192.168.1.1		15469	38468			
WAN 1 Status						>> <u>Dial PPPo</u>
Enable	Lin	e	Name	Mode	Up Time	
Yes	ADS	5L		PPPoE	00:00:00	
IP	GW	IP	TX Packets	TX Rate(Bps)	RX Packets	RX Rate(Bps)
			0	0	0	0
Message [PPP 9	Shutdown]				
ADSL Informat	ion (ADSL Firmware	Version: 21101	L1_A)		
ATM Statistic	s TX Co	ells	RX Cells	TX CRC err	s RX (CRC errs
	0		0	0	0	
ADSL Status	Mode	State	Up Speed	Down Speed	SNR Margin	Loop Att.
		READY	0	0	0	0

Detailed explanation is shown below:



Item	Description
LAN Status	Primary DNS- Display the primary DNS server address for WAN interface.
	Secondary DNS - Display the secondary DNS server address for WAN interface.
	IP Address-Display the IP address of the LAN interface.
	TX Packets- Display the total transmitted packets at the LAN interface.
	RX Packets -Display the total received packets at the LAN interface.
WAN Status	Enable – Yes in red means such interface is available but not connected. Yes in green means such interface is connected.
	Line – Display the physical connection of this interface.
	Name – Display the name of the router.
	Mode - Display the type of WAN connection (e.g., PPPoE
	Up Time - Display the total uptime of the interface.
	IP - Display the IP address of the WAN interface.
	GW IP - Display the IP address of the default gateway.
	TX Packets - Display the total transmitted packets at the WAN interface.
	TX Rate - Display the speed of transmitted octets at the WAN interface.
	RX Packets - Display the total number of received packets at the WAN interface.
	RX Rate - Display the speed of received octets at the WAY interface.
ADSL Information	ATM Statistics – Display the ATM layer information.
	TX Cells –Display the total number of ATM transmission cells.
	RX Cells –Display the total number of ATM received cell
	TX CRC errs – Display the total number of transmission CRC errors.
	RX CRC errs –Display the total number of CRC errors received.
	ADSL Status – Display the ADSL layer information.
	Mode – Display the type of ADSL mode, such as T1.413, G.DMT, ADSL2+(G.992.5), and so on.
	State – Display the ADSL connection status, such as Ready, HANDSHAKING, SHOWTIME and so on.
	Up Speed – Display the upstream rate.
	Down Speed – Display the downstream rate.
	SNR Margin – Display number of SRR Margin.
	Loop Att Display the number of Loop Attenuation.

Note: The words in green mean that the WAN connection of that interface (WAN1) is ready for accessing Internet; the words in red mean that the WAN connection of that interface (WAN1) is not ready for accessing Internet.

2.6.2 Virtual WAN

Such page displays the virtual WAN connection information.

Virtual WAN are used by TR-069 management, VoIP service and so on.

The Application field will list the purpose of such WAN connection.

Online Status

Virtual WAN				System	Uptime: 44:36:
WAN 3 Status					
Enable	Line	Name	Mode	Up Time	Application
Yes	ADSL			00:00:00	Management
IP	GW IP	TX Packets	TX Rate(Bps)	RX Packets	RX Rate(Bps)
		0	0	0	0
WAN 4 Status					
Enable	Line	Name	Mode	Up Time	Application
Yes	ADSL			00:00:00	Management
IP	GW IP	TX Packets	TX Rate(Bps)	RX Packets	RX Rate(Bps)
		0	0	0	0
WAN 5 Status					
Enable	Line	Name	Mode	Up Time	Application
Yes	ADSL			00:00:00	Management
IP	GW IP	TX Packets	TX Rate(Bps)	RX Packets	RX Rate(Bps)
		0	0	0	0

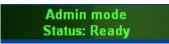
Detailed explanation is shown below:

Item	Description
WAN Status	Enable – Yes in red means such interface is available but not enabled. Yes in green means such interface is enabled.
	Line – Display the physical connection (Ethernet, or USB) of this interface.
	Name – Display the name of the router.
	Mode - Display the type of WAN connection (e.g., PPPoE).
	Up Time - Display the total uptime of the interface.
	IP - Displays the IP address of the WAN interface.
	GW IP - Display the IP address of the default gateway.
	TX Packets - Display the total transmitted packets at the WAN interface.
	TX Rate - Display the speed of transmitted octets at the WAN interface.
	RX Packets - Display the total number of received packets at the WAN interface.
	RX Rate - Display the speed of received octets at the WAN interface.



2.7 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..

2.8 Registering Vigor Router

You have finished the configuration of Quick Start Wizard and you can surf the Internet at any time. Now it is the time to register your Vigor router to MyVigor website for getting more service. Please follow the steps below to finish the router registration.

1 Please login the web configuration interface of Vigor router by typing "**admin/admin**" as User Name / Password.

Username	admin
Password	
	Login
Copyright©, DrayTek Corp. Al	Rights Reserved.

2 Click **Support Area>>Production Registration** from the home page.



3 A Login page will be shown on the screen. Please type the account and password that you created previously. And click Login. If not, please refer to section 4.13 Creating an Account for MyVigor.

	Please take a moment to register. Membership Registration entitles you to upgrade firmwar for your purchased product and receive news about upcoming products and services!	e
LOGIN		
UserName :	james_fae	
Password :	******	
Auth Code :	txxhdd t xxhdd	
	If you cannot read the word, <u>click here</u>	
	Forgotten password? Login	
Don't have a l	MyVigor Account? Create an account now	
(

If you are having difficulty logging in, contact our customer service. Customer Service : (886) 3 597 2727 or

4 The following page will be displayed after you logging in MyVigor. From this page, please click **Add** or **Product Registration**.

Dray Tek				М
E Home				Searc
 About Us Product My Information VigorACS SI Vigor Series Management 	Your Device List	<mark>_fae</mark> 2011-08-24 09:3 123.110.144.22 e : 2011-08-24 2	0 3:01:15 84	Add
Negistration	Serial Number / Host ID 104001703857	Device Name Vigor2110	Model Vigor2110	Note
Customer Survey	<u>200807100001</u>	VigorPro5300	VigorPro5300	-
	200911030001	ryan	VigorPro5300	-

5 When the following page appears, please type in Nickname (for the router) and choose the right registration date from the popup calendar (it appears when you click on the box of Registration Date). After adding the basic information for the router, please click **Submit**.

Dray Tek				My	/igor
i Home				Search	GO
D About Us	My Product		Search for t	his site	GO
My Information	Registration Device				
🦕 VigorACS SI	Serial number :	20110822143203	01		
🗘 Vigor Series	Nickname : *	Vigor2710			
🌣 Management	Registration Date : *	08-24-2011]		
S Product	Usage :	– Select – 🛛 👻			
Registration	Product Rating :	– Select – 🛛 💌	(Your opinion so	far)	
Customer Survey	No. of Employees :	– Select – 🛛 🎽] (In total within yo	ur company)	
	Supplier :		(Where	you bought it from)	
	Date of Purchase :		(mm-de	1-yyyy]	
	Internet Connection : *	t i i i i i i i i i i i i i i i i i i i			
	Cable	ADSL	VDSL	Eiber	
	🗖 3G	WIMAX	🔲 LTE		
Convrictels @DravTek Com				Cancel Sub	mit

6 When the following page appears, your router information has been added to the database.

Your device has been successfully added to the database.

- OK
- 7 Now, you have finished the product registration.
- 8 After clicking **OK**, you will see the following page. Your router has been registered to *myvigor* website successfully.

Dray Tek	4 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1		/	My Vigo	
Home			Se	arch	
D About Us	My Information				
Product	Welcome, draytekfae Last Login Time : 2011-08-24				
My Information	Last Login From : 123.110.14 Current Login Time : 2011-08-				
VigorACS SI	Current Login From : 114.37.1	42.184	. .		
Vigor Series	Your Device List		RowNo : 5 🍟 PageNo : 2 🛩		
🌣 Management					
Customer Survey	Serial Number / Host ID	Device Name	Model	Note	
- customer ourrey	20100707144801	Vigor3300V	Vigor3300		
	20100708105301	Vigor2820	Vigor2820		
	20101005104801	Vigor2700	Vigor2700		
	2010121707335201	Vigor2920	Vigor2920		
	2011082214320301	Vigor2710	Vigor2710		
		Vigor2710	Vigor2710		

This page is left blank.

Vigor2710 Series User's Guide



3.1 How to configure settings for IPv6 Service

Due to the shortage of IPv4 address, more and more countries use IPv6 to solve the problem. However, to continually use the original rich resources of IPv4, both IPv6 and IPv4 networks shall communicate for each other via intercommunication mechanism to complete the shifting job from IPv4 to IPv6 gradually. At present, there are three common types of intercommunication mechanisms:

Dual Stack

The user can use both IPv4 and IPv6 techniques at the same time. That means adding an IPv6 stack on the origin network layer to let the host own the communication capability of IPv4 and IPv6.

• Tunnel

Both IPv6 hosts can be communicated for each other via existing IPv4 network environment. The IPv6 packets will be encapsulated with the header of IPv4 first. Later, the packets will be transformed and adjusted as IPv4 payload. Once the packets arrive the border between IPv4 and IPv6, the header of IPv4 on the packets will be removed. Then, the packets with IPv6 address will be forwarded to the destination of IPv6 network.

Translation

Such feature is active only for the user who uses IPv4 to communicate with other user using IPv4 service.

Before configuring the settings on Vigor2710, you need to know which connection type that your IPv6 service used.

Note: For the IPv6 service, you have to configure WAN/LAN settings before using the service.

I. Configuring the WAN Settings

For the IPv6 WAN settings for Vigor2710, there are five connection types to be chosen: PPP, TSPC, AICCU, DHCPv6 Client and Static IPv6.

1. Access into the web configurator of Vigor2710. Open Internet Access>>IPv6.

Internet Access
PPPoE / PPPoA
MPoA (RFC1483/2684)
▶ IPv6
Multi-PVCs
LAN

2. In the following figure, use the drop down list to choose a proper connection type.

lode		
Internet Access Mode		
Connection Type	PPP	*
Note : IPv4 WAN setting shoul	d be PPPoE client.	

Different connection types will bring out different configuration page. Refer to the following:

• PPP – Dual Stack application, IPv4 and IPv6 services can be utilized at the same time

Choose PPP and type the information for PPPoE of IPv4.

PPoE / PPPoA Client	lioue			
PPPoE/PPPoA Client	⊙ Enable O Disable	ISP Access Setup		
DEL Madam Cattings		ISP Name		
DSL Modem Settings Multi-PVC channel	Channel 1 🐱	Username	73768631@hinet.net	
		Password	•••••	
/PI	8	PPP Authentication	PAP or CHAP 🔽	
/CI	35	🗹 Always On		
Encapsulating Type	LLC/SNAP 🔽	Idle Timeout	-1 second(s)	
Protocol	PPPoE 🐱	IP Address From ISP	WAN IP Alias	
Modulation	Multimode 🔽	Fixed IP O Yes O N	DVNamic IP)	
		Fixed IP Address		
PPPoE Pass-through				
For Wired LAN		O Default MAC Address		
For Wireless LAN		O Specify a MAC Address		
protocol, the router will	ked while using the PPPoA behave like a modem PPoE client on the LAN.	MAC Address: 00 .50		
VLAN Enable		Index(1-15) in Schedule	Setup	
VID	0 (0~4095)	=>		
Priority	0 (0~7)			
WAN Connection Dete	ction			
Mode	ARP Detect 🐱			
Ping IP				
TTL:				
МТИ	1442 (Max:1492)			
Bridge Mode				
🔲 Enable Bridge Mode				

Vigor2710 Series User's Guide



Access into the setting page for IPv6 service, it is not necessary for you to configure anything.

Internet Access >> IPv6	
IPv6 Mode	
Internet Access Mode]
Connection Type	PPP 🔽
Note : IPv4 WAN setting she	ould be PPPoE client.
1	
	OK

Click **OK** and open **Online Status**. If the connection is successful, you will get the IP address for IPv4 and IPv6 at the same time.

Online Status

Physical Conne	ction				System Upt	ime: Oday 0:6:38
	IPv4			IPv6		
LAN Status		Prima	ry DNS: 168.95	5.192.1	Secondary DN	S: 168.95.1.1
IP Address		TX Packets	RX Pac	kets		
192,168,1,1		1794	2884			
WAN 1 Status						>> Drop PPPoE
Enable	Line	2	Name	Mode	Up Time	
Yes	ADS	L		PPPoE	0:02:16	
IP	GW	IP	TX Packets	TX Rate(Bps)	RX Packets	RX Rate(Bps)
114.44.49.209	9 168	.95.98.254	927	765	886	557
ADSL Informat	tion ()	ADSL Firmwar	e Version: 2110	011_A)		
ATM Statistics	5 TX Ce	lls	RX Cells	TX CRC e	rrs RX (CRC errs
	3447		4920	0	210	
ADSL Status	Mode	State	Up Speed	Down Speed	SNR Margin	Loop Att.
	G.992.3 annex L	SHOWTIME	56000	4009196	6	23

Online Status

Physical Connect	tion		System Uptime	: Oday 0:8:14		
	IPv4		IPv6		IPv6	
LAN Status						
IP Address						
	0:201:250:7FFF:FE9 :FE92:F500/64 (Link					
TX Packets	RX Packets	TX Bytes	RX Bytes			
107	122	11951	12030			
WAN1 IPv6 Stat	tus			>> Drop PPP		
Enable	Mode	Up Time				
Yes	PPP	0:03:51				
ID			Gateway IP			
	0:201:250:7FFF:FE9 FE92:F501/128 (Link	2:F501/128 (Global))	FE80::90:1A00:242:AD52			
DNS IP						
2001:B000:168 2001:B000:168						
TX Packets	RX Packets	TX Bytes	RX Bytes			
91	80	8250	9885			

• TSPC – Tunnel application, both IPv6 hosts communicate through IPv4 network

Choose **TSPC** and type the information for TSPC service.

Note: While using such mode, you have to make sure the IPv4 network connection is normal.

(In the following figure, the TSPC information is obtained from <u>http://gogo6.com/</u> after applied for the service.)

ternet Access >> IPv6	
Pv6 Mode	
Internet Access Mode	
Connection Type	TSPC
TSPC Configuration	
Username	88886666
Password	•••••
Confirm Password	••••••
Tunnel Broker	amsterdam.freenet6.net

Click **OK** and open **Online Status**. If the connection is successful, the physical connection will be shows as follows:

Online Status

Physical Connect	tion		System Uptim	ie: Oday 0:1:14		
	IPv4		IPv4 IPv6		IPv6	
LAN Status						
IP Address						
	:D00:250:7FFF:FE92 :FE92:F500/64 (Link					
TX Packets	RX Packets	TX Bytes	RX Bytes			
9	17	766	1342			
WAN1 IPv6 Stat	tus					
Enable	Mode	Up Time				
Yes	TSPC	0:00:30				
IP			Gateway IP			
2001:5C0:1400 FE80::722B:A09	:B::10B9/128 (Globa 97/128 (Link)	al)				
TX Packets	RX Packets	TX Bytes	RX Bytes			
11	8	872	752			

• AICCU – Tunnel application

Choose AICCU and type the information for AICCU of IPv6.

Note: While using such mode, you have to make sure the IPv4 network connection is normal.

(In the following figure, the AICCU information is obtained from <u>https://www.sixxs.net/main/</u> after applied for the service.)

ernet Access >> IPv6	
v6 Mode	
Internet Access Mode Connection Type	AICCU
AICCU Configuration	
Username	AHJ5-SIXXS
Password	•••••
Confirm Password	•••••
Tunnel Broker	tic.sixxs.net
Subnet Prefix	2001:4DD0:FF00:83E4:: / 64

Click **OK** and open **Online Status**. If the connection is successful, the physical connection will be shows as follows:

Online Status				
Physical Connec	tion		System	Uptime: Oday 0:4:2
	IPv4		IPv6	
LAN Status IP Address				
	0:83E4:250:7FFF:FE :FE92:F500/64 (Link	92:F500/64 (Global) :)		
TX Packets	RX Packets	TX Bytes	RX Bytes	
11	33	930	2906	
WAN1 IPv6 Stat	tus			
Enable	Mode	Up Time		
Yes	AICCU	0:03:17		
IP			Gateway IP	
	0:3E4::2/64 (Global) 00:3E4:2/64 (Link))		
TX Packets	RX Packets	TX Bytes	RX Bytes	
8	2	700	2084	

• DHCPv6 Client

Choose DHCPv6 Client. Click one of the identity associations and type the IAID number.

Internet Access >> IPv6	
IPv6 Mode	
Internet Access Mode Connection Type	DHCPv6 Client
DHCPv6 Client Configurat Identity Association IAID (Identity Association	O Prefix Delegation ③ Non-temporary Address

Click **OK** and open **Online Status**. If the connection is successful, the physical connection will be shows as follows:

Online Status

Physical Connec	tion		System Uptime: Oday 0:15:59
IPv4			IPv6
LAN Status			
IP Address FE80::250:7FFF	:FE92:F500/64 (Link)		
TX Packets	RX Packets	TX Bytes	RX Bytes
749	945	102782	86758
WAN1 IPv6 Sta	tus		
Enable	Mode	Up Time	
Yes	DHCPv6 Client	0:15:24	
IP			Gateway IP
2001:1111:222 FE80::200:FF:F	2:3333::1111/64 (Glo E00:0/64 (Link)	obal)	
TX Packets	RX Packets	TX Bytes	RX Bytes
5	24	366	45

• Static IPv6

Choose Static IPv6. Type IPv6 address, Prefix Length and Gateway Address.

rnet Access >> IPv6	
6 Mode	
Internet Access Mode	
Connection Type	Static IPv6
Static IPv6 Address configuration	
IPv6 Address	/ Prefix Length
2001:1111:2222:3333::1111	/ 64 Add Delete
Current IPv6 Address Table	
Index IPv6 Address/Prefix Length	Scope
1 FE80::200:FF:FE00:0/64	Link

Click **OK** and open **Online Status**. If the connection is successful, the physical connection will be shows as follows:

Online Status				
Physical Connec	tion		System Uptime: Oday ():1:0
	IPv4		IPv6	
LAN Status IP Address				
FE80::250:7FFF	:FE92:F500/64 (Link)			
TX Packets	RX Packets	TX Bytes	RX Bytes	
5	49	390	4158	
WAN1 IPv6 Stat	us			
Enable	Mode	Up Time		
Yes	Static IPv6	0:00:26		
тр			Gateway IP	
2001:1111:222 FE80::200:FF:FE	2:3333::1111/64 (Glo 200:0/64 (Link)	obal)		
TX Packets	RX Packets	IX Bytes	RX Bytes	
5	39	366	58	

II. Configuring the LAN Settings

After finished the WAN settings for IPv6, please configure the LAN settings to make the router's client getting the IPv6 address.

1. Access into the web configurator of Vigor2710. Open LAN>> General Setup. Click the IPv6 button.

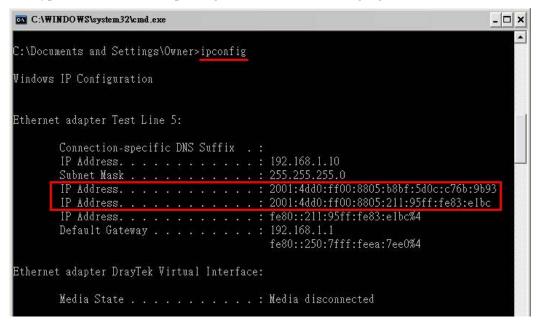
rnet TCP / IP and DHCF	P Setup LAN 1 IPv6 Setup
Thet ICP / IP and Drice	EAN TIPVO Setup
RADVD Configuration	
💿 Enable 🛛 🔘 Disabl	le
Advertisement Lifetim	e 1800 Seconds (Range : 600 - 9000)
DHCPv6 Server Config	-
	🕽 Disable Server
Start IPv6 Address	2001:4DD0:FF00:8805::20
End IPv6 Address	2001:4DD0:FF00:8805::50
DNS Server IPv6 Add	
Primary DNS Server	2001:470:20::2
Secondary DNS Serve	r
Static IPv6 Address co	onfiguration
IPv6 Address	/ Prefix Length
	/ Add Delete
Current IPv6 Addres	s Table
Index IPv6 Address/	-
5 C C C C C C C C C C C C C C C C C C C	FF00:8805:250:7FFF:FEEA:7EE0/64 Global 7FFF:FEEA:7EE0/64 Link
2 12001120017	

- 2. In the field of **RADVD Configuration**, the default setting is **Enable**. The client's PC will ask RADVD service for the Prefix of IPv6 address automatically, and generate an Interface ID by itself to compose a full and unique IPv6 address.
- 3. In the field of **HCPv6 Server Configuration**, when DHCPv6 service is enabled, you can assign available IPv6 address for the client manually.

Note: When both mechanisms are enabled, the client can determine which mechanism to be used (e.g., the default mechanism for Windows7 is RADVD).

III. Confirming IPv6 Service Run Successfully

1. Make sure you have obtained the correct IPv6 IP address. Get into MS-DOS interface and type the command of "ipconfig". Refer to the following figure.



From the above figure we can see IPv6 IP address has been detected by the system.

2. Use the Ping command to ping any IPv6 address indicating an IPv6 website. For example, <u>www.kame.net</u> is a website supporting IPv4 IP and IPv6 IP services. Its IPv6 address is seen with a format of 2001:200:dff:fff1:216:3eff:feb1:44d7.

C:\WINDOWS\system32\cmd.exe	- - ×
C:\Documents and Settings\Owner>ping 2001:200:dff:fff1:216:3eff:feb1:44d7	
Pinging 2001:200:dff:fff1:216:3eff:feb1:44d7 with 32 bytes of data:	
Reply from 2001:200:dff:fff1:216:3eff:feb1:44d7: time=743ms Reply from 2001:200:dff:fff1:216:3eff:feb1:44d7: time=623ms Reply from 2001:200:dff:fff1:216:3eff:feb1:44d7: time=626ms Reply from 2001:200:dff:fff1:216:3eff:feb1:44d7: time=617ms	
Ping statistics for 2001:200:dff:fff1:216:3eff:feb1:44d7: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds: Minimum = 617ms, Maximum = 743ms, Average = 652ms	
C:\Documents and Settings\Owner>	▼

After getting the above message, it means the IPv6 service has been activated successfully.

3. Connect to the website for IPv6. Open a web browser and type an URL of IPv6, e.g., <u>www.kame.net</u>. If your computer accesses into the website by using IPv6 address, you may see a turtle dancing on the screen. If not, only a steady turtle will be seen.



If you can see a turtle dancing on the screen, that means IPv6 service is ready for you to access and utilize.



3.2 How Can I Use FTP to Get the Files from USB Storage Device Connecting to Vigor Router?

There are three methods to get files from USB devices connecting to router.

- File Explorer Under Administration operation, the administer can control the files on USB storage device through USB Application>>File Explorer.
- FTP Use common FTP utility.
- Samba Invoke Samba service and use <u>\\192.168.1.1</u> to access into the USB storage device.

Files on USB storage device can be reviewed by opening **USB Applicaiton>>File Explorer.** Below shows the example of getting files from FTP:

1. Plug the USB device to the USB port on the router. Make sure **Disk Connected** appears on the **Connection Status** as the figure shown below:

USB Application >> USB Disk Status			
USB Mass Sto	orage Device Status		
Connection S	tatus: Disk Connected		Disconnect USB Disk
Write Protect	t Status: No		
Disk Capacity	/: 2009 MB		
USB Disk Us	ers Connected		<u>Refresh</u>
Index	Service	IP Address(Port)	Username

Note: If the write protect switch of USB disk is turned on, the USB disk is in READ-ONLY mode. No data can be written to it.

2. Then, please open **USB Application** >> **USB General Settings** to enable Samba service.

USB General Settings	
General Settings	
Simultaneous FTP Connections	5 (Maximum 6)
Default Charset	English 💌
Samba Service Settings(Network Neigh	borhood)
Disable	
● LAN Only ○ LAN And WAN	
NetBios Name Service	
Workgroup Name	WORKGROUP
Host Name	Vigor

3. Setup a user account for the FTP service by using **USB Application** >>**USB User Management.** Click **Enable** to enable FTP/Samba User account. Here we add a new account "user1" and assign authorities "Read", "Write" and "List" to it.

USB Application >> USB User Management

Profile Index: 1	
FTP/Samba User	🕐 Enable 🔷 Disable
Username	user1
Password	(Maximum 11 Characters)
Confirm Password	
Home Folder	2
Access Rule	
File	Read Write Delete
Directory	🗹 List 🔲 Create 🗖 Remove
Note: The folder name can only contair space.	h the following characters: A-Z a-z 0-9 \$ % ' @ ~ ` ! () / and
space.	
	OK Clear Cancel

- 4. Click **OK** to save the configuration.
- 5. Make sure the FTP service is running properly. Please open a browser and type <u>ftp://192.168.1.1</u>. Use the account "**user1**" to login.

Log On	As 🔀
9	Either the server does not allow anonymous logins or the e-mail address was not accepted.
	FTP server: 192.168.1.1
	User name:
	Password:
	After you log on, you can add this server to your Favorites and return to it easily.
⚠	FTP does not encrypt or encode passwords or data before sending them to the server. To protect the security of your passwords and data, use Web Folders (WebDAV) instead.
	Learn more about <u>using Web Folders</u> .
	Log on anonymously
	Log On Cancel

6. When the following screen appears, it means the FTP service is running properly.

👰 ftp://192.168.1.1/ - Microsoft	Internet Explorer	
<u>File E</u> dit <u>V</u> iew F <u>a</u> vorites <u>T</u> ools	Help	
🕞 Back 🔹 🕥 - 🏂 🔎 Se	earch 😥 Folders 🛄 🕶	
Address 👰 ftp://192.168.1.1/		
Other Places Internet Explorer Internet Explorer My Documents Shared Documents My Network Places	FinalDataEn opkg-install	tempstorage iTunesSetu vlc-1.1.5-wi Air-supply-lost in love.mp3 Crystal Flower.mp3

7. Return to **USB Application** >> **USB Disk Status**. The information for FTP server will be shown as below.



Note: If the write protect switch of USB disk is turned on, the USB disk is in **READ-ONLY** mode.No data can be written to it.

Now, users in LAN of Vigor2710 can access into the USB storage device by typing ftp://192.168.1.1 on any browser. They can add or remove files / directories, depending on the Access Rule for FTP account settings in **USB Application >>USB User Management.**

3.3 How to Customize Your Login Page

Login page can be customized to fit the request of the administrator.

1. Open **System Maintenance>>Login Page Greeting**. Check the box, **Enable** to enable this function. Type a brief description (e.g., *Just for Carrie*) in the field of **Login Page Title** which will be shown on the heading of the login dialog. Type any message or description in the field of **Welcome Message and Bulletin** which will be shown on the bottom of the login dialog. Next, click **OK**.

System	Maintenance	>> L	.ogin	Page	Greeting
--------	-------------	------	-------	------	----------

Enable			
Login Page Title	Just for Carrie	(31 char max.)	
Welcome Message a	nd Bulletin (Max 511 characte	rs) <u>Preview</u>	Set to Factory Default
message is displa with your own mes HTML so lists suc	pr=red>Welcome Messageayed in the Login page of ssage. The we sh as this one can be cre or img can be used<!--</th--><td>the router. Repl lcome message can ated Oth</td><td>ace this text be written in</td>	the router. Repl lcome message can ated Oth	ace this text be written in
	e Message and Bulletin: =red>Welcome Message <td>t></td> <td></td>	t>	

- OK Cancel
- 2. Log out the web user interface.
- 3. Open a new tab in the same browser (for IE 7.0/FireFox and above) or open a new web browser.
- 4. Try to access into the web configurator (e.g., 192.168.1.1) of Vigor router. Please note *"Just for Carrie"* is displayed as a heading on the login dialog box.

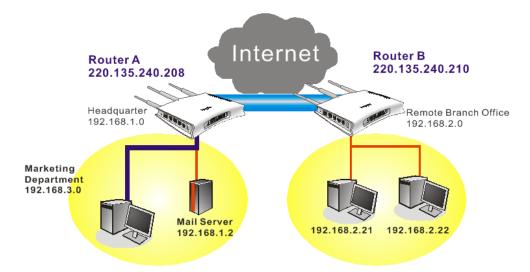
	Just for Carrie
Username Password	admin ••••••] Login
Copyright©, DrayTek Corp. A Welcome Message	
· · · ·	ogin page of the router. Replace this text with your own message. n in HTML so lists such as this one can be created img can be used

5. After typing the username and password (defined in User Management>>User **Profile**), click Login. You can access into Internet or access into the Landing Page if configured in User Management>>General Setup.



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

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



Settings in Router A in headquarter:

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

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

VPN and Remote Access >> PPP General Setup

PPP/MP Protocol		IP Address Assignme	
Dial-In PPP PAP or CHAP	*	(When DHCP Disable	e set)
Authentication		Start IP Address	192.168.1.200
Dial-In PPP Encryption (MPPE) Optional MPPE	*		
Mutual Authentication (PAP) 🛛 🔘 Yes	s 💿 No		
Username			
Password			

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

VPN	and	Remote	Access	>>	IPSec	General	Setup
	our roa	i tonioto	/			00110101	ootap

VPN IKE/IPSec General Setup

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

	by manife in energy (in the in try).
IKE Authentication Method	
Pre-Shared Key	••••
Confirm Pre-Shared Key	••••
IPSec Security Method	
🗹 Medium (AH)	
Data will be authentic, but will r	not be encrypted.
High (ESP) 🛛 🗹 DES 📝 3DES	✓ AES
Data will be encrypted and auth	entic.
	OK Cancel

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

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

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

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

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

If a **PPP-based service** is selected, you should further specify the remote peer IP



Address, Username, Password, PPP Authentication and VJ Compression for this Dial-Out connection.

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

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

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

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

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

3. Dial-In Settings		
Allowed Dial-In Type		
PPTP	Username	draytek
IPSec Tunnel	Password	•••••
L2TP with IPSec Policy None	VJ Compression	💿 On 🔘 Off
Specify Remote VPN Gateway Peer VPN Server IP 220.135.240.210 or Peer ID	IKE Authentication Me Pre-Shared Key IKE Pre-Shared Key Digital Signature(X.509 None IPSec Security Method Medium (AH) High (ESP) DES V 3DES))) 1

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

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

Settings in Router B in the remote office:

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

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

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



VPN and	Remote	Access	>> IPS	ec Genera	I Setup
---------	--------	--------	--------	-----------	---------

VPN IKE/IPSec General Setup

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

 eet ap ter nomete blar in abere ana	
IKE Authentication Method	
Pre-Shared Key	••••
Confirm Pre-Shared Key	••••
IPSec Security Method	
🗹 Medium (AH)	
Data will be authentic, but will r	not be encrypted.
High (ESP) 🗹 DES 🗹 3DES	▼ AES
Data will be encrypted and auth	entic.
	OK Cancel

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

VPN and Remote Access >> LAN to LAN	
Profile Index : 1 1. Common Settings	
Profile Name Branch 1 ✓ Enable this profile Netbios Naming Packet ⊙ Pass ○ Block	Call Direction Both Dial-Out Dial-In Always on Idle Timeout 300 second(s) Enable PING to keep alive PING to the IP

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

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

2. Dial-Out Settings

Type of Server I am calling PPTP IPSec Tunnel L2TP with IPSec Policy	Username ??? Password
Server IP/Host Name for VPN. (such as draytek.com or 123.45.67.89) 220.135.240.208	IKE Authentication Method Pre-Shared Key IKE Pre-Shared Key Digital Signature(X.509) None IPSec Security Method Medium(AH) High(ESP) DES without Authentication Advanced Index(1-15) in Schedule Setup: , , , , , ,

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

Type of Server I am calling	Username	draytek
PPTP	Password	•••••
O IPSec Tunnel	PPP Authentication	
O L2TP with IPSec Policy None	VJ Compression	💿 On 🔘 Off
Server IP/Host Name for VPN. (such as draytek.com or 123.45.67.89) 220.135.240.208	IKE Authentication Me	ethod
	KE Pre-Shared Key	
	O Digital Signature(X.50	J9)
	IPSec Security Metho	d
	Medium(AH)	
	O High(ESP) DES with	out Authentication 💉
	Advanced	
	Index(1-15) in <u>Schedule</u>	Setup:
		,

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

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

3. Dial-In Settings

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

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

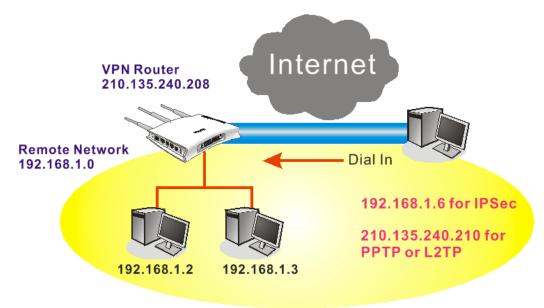
3. Dial-In Settings			
Allowed Dial-In Type			
✓ РРТР	Username	draytek	
🔲 IPSec Tunnel	Password	•••••	
L2TP with IPSec Policy None	VJ Compression	💿 On 🔘 Off	
✓ Specify Remote VPN Gateway	IKE Authentication Me	ethod	
Peer VPN Server IP	✓ Pre-Shared Key		
220.135.240.208	IKE Pre-Shared Key		
or Peer ID	Digital Signature(X.50	9)	
	None 🗸		
	IPSec Security Metho	d	
	🗹 Medium (AH)		
	High (ESP)		
	🗹 DES 🗹 3DES	6 🗹 AES	

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

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

3.5 Create a Remote Dial-in User Connection Between the Teleworker and Headquarter

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



Settings in VPN Router in the enterprise office:

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

eneral S	setu	p	
		IP Address Assignment	for Dial-In Users
1		(When DHCP Disable se	t)
		Start IP Address	192.168.1.200
	*		
💿 No			
	: • No		IP Address Assignment (When DHCP Disable se Start IP Address

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



VPN and Remo	ote Access >> IPSec	General Setup
--------------	---------------------	---------------

VPN and Remote Access >> Remote Dial-in User

VPN IKE/IPSec General Setup

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

 	-,
IKE Authentication Method	
Pre-Shared Key	
Confirm Pre-Shared Key	••••
IPSec Security Method	
🗹 Medium (AH)	
Data will be authentic, but will r	not be encrypted.
High (ESP) 🛛 🗹 DES 📝 3DES	✓ AES
Data will be encrypted and auth	entic.
	OK Cancel

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

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

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

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

VPN and Remote Access >> Remote Dial-in User

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

Settings in the remote host:

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

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

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

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



Dial To VPN	×		
Session Name:	Office		
VPN Server IP/HOST	VPN Server IP/HOST Name(such as 123.45.67.89 or draytek.com)		
192.168.1.1			
User Name :	draytek_user1		
Password :	******		
Type of VPN]		
O PPTP	O L2TP		
 IPSec Tunnel 	CL2TP over IPSec		
PPTP 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 —	172.16.3.100	
Standard IPS	iec Tunnel	
Remote Su		
Remote Subnet Mask : 255 . 255 . 0		
Virture IP Obtain a		iek Virture Interface
	an IP address e	
IP Address: 192 . 168 . 1 . 201		
Subnet Mask: 255 , 255 , 255 , 0		
Security Method Medium(AH) MDS	•	High(ESP) DES
Authority Method Pre-shared Key : *****		
Certification Authority:		
OK Cancel		

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

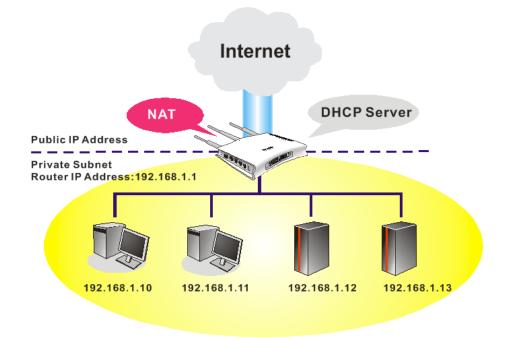


Dial To YPN	X
Session Name:	office
VPN Server IP/HOST Name(such as 123.45.67.89 or draytek.com)	
192.168.1.1	
User Name :	draytek user1
Password :	*****
Fassword .	
Type of VPN	0
• PPTP	OL2TP
O IPSec Tunne	L2TP over IPSec
PPTP Encryption	
O No encryption	
Maximum strength encryption	
Use default gateway 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.

3.6 LAN - Created by Using NAT

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



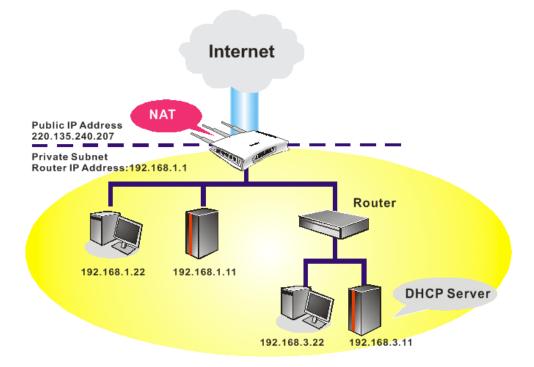
You can just set the settings wrapped inside the red rectangles to fit the request of NAT usage.

LAN >> General Setup

Ethernet TCP / IP and	DHCP Setup					
LAN IP Network Configuration			DHCP Server Configuration			
For NAT Usage		٦ I	🧿 Enable Server 🔘 Disat	ole Server		
1st IP Address	192.168.1.5		Relay Agent: 🔘 1st Subr	net 🔾 2nd Subnet		
1st Subnet Mask	255.255.255.0		Start IP Address	192.168.1.10		
For IP Routing Usage 🤇) Enable 💿 Disable	J	IP Pool Counts	50		
2nd IP Address	192.168.2.1		Gateway IP Address	192.168.1.5		
2nd Subnet Mask	255.255.255.0		DHCP Server IP Address			
	2nd Subnet DHCP Server		for Relay Agent			
			DNS Server IP Address			
RIP Protocol Control	Disable 🚩		📃 Force DNS manual se	tting		
			Primary IP Address			
			Secondary IP Address			
	r		Secondary IP Address			

To use another DHCP server in the network rather than the built-in one of Vigor Router, you have to change the settings as show below.





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

LAN >> General Setup

Ethernet TCP / IP and D	HCP Setup				
LAN IP Network Configuration		DHCP Server Configuration			
For NAT Usage		◯Enable Server ⊙Disable Server			
1st IP Address	192.168.1.5	Relay Agent: 🔘 1st Subr	et 🔾 2nd Subnet		
1st Subnet Mask	255.255.255.0	Start IP Address	192.168.1.10		
For IP Routing Usage 🔘	Enable 💿 Disable	IP Pool Counts	50		
2nd IP Address	192.168.2.1	Gateway IP Address	192.168.1.5		
2nd Subnet Mask	255.255.255.0	DHCP Server IP Address	192.168.3.11		
21	nd Subnet DHCP Server	for Relay Agent			
		DNS Server IP Address			
RIP Protocol Control	Disable 🏼 😽	📃 Force DNS manual set	tting		
		Primary IP Address			
		Secondary IP Address			
		ок			

3.7 Calling Scenario for VoIP function

3.7.1 Calling via SIP Sever

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

VolP >> DialPlan Setup

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

Settings for John

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

SIP Accounts Settings ----

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

CODEC/RTP/DTMF ---

(Use default value)

Enable							
	Phone Number		1111				
	Display Name		David				
	SIP URL		4321	C	p i	ptel.org	
	Dial Out Account		Default 💌				
	Loop through		None 👻				
	Backup Phone Nu	nber					
VoIP >> SIP	Accounts	OK	Clear	Car	nce	1	
SIP Account	Index No. 1						
Pro	ifile Name	draytel 1		(11 c	har	rmax.)	
Rei	gister via	Auto	~	Call witho	ut	Registration	

Profile Name	drayter i (11 char max	.)
Register via	Auto 🔽 🗌 Call without Regis	stration
SIP Port	5060	
Domain/Realm	draytel.org	(63 char max.)
Proxy	draytel.org	(63 char max.)
📃 Act as outbound pro	ху	
Display Name	John (23 char 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 💙	
	✓ Phone	
Ring Port	🗌 ISDN1-S0 Any 💌	
	ISDN2-TE	
Ring Pattern	1 💌	
	OK Cancel	

John calls David ---

VoIP >> DialPlan Setup

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

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)

🗹 Enable		
	Phone Number	2222
	Display Name	John
	SIP URL	1234 @ draytel.org
	Dial Out Account	Default 💌
	Loop through	None 💌
	Backup Phone Number	

Dray Tek

	VoIP >> SIP Accounts		
CODEC/RTP/DTMF	SIP Account Index No. 1		
	Profile Name	iptel 1 (11 char max	<.)
(Use default value)	Register via	Auto 🔄 🗌 Call without Regi	
	SIP Port	5060	
	Domain/Realm	iptel.org	(63 char max.)
	Proxy	iptel.org	(63 char max.)
	Act as outbound pro:	xy	
	Display Name	David (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 🖌	
		✓ Phone	
	Ring Port	🗌 ISDN1-S0 Any 💌	
		ISDN2-TE	
	Ring Pattern	1 🛩	
		OK Cancel	

David calls John

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

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

VolP >> DialPlan Setup

VolP >> SIP Accounts Account Index No. 1 Profile Name

Register via

Act as outbound proxy Display Name

Account Number/Name

Authentication ID

NAT Traversal Support

SIP Port Domain/Realm

Proxy

Password

Expiry Time

Ring Port

Ring Pattern

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

Phone Number	1111			
Display Name	David			
SIP URL	4321	a	draytel.org	
Dial Out Account	Default 😁			
Loop through	None 💌			
Backup Phone Number		_		

(11 char max.)

Call without Registration

(23 char max.)

sec

(63 char max.)

draytel 1

Auto 5060 ٣

draytel

draytel 1

1234

1 hour 💌 None 👻

Phone 🗆 ISDN1-SD 🗛 🎽

1 ~

SON2-TE

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)

John calls David

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

3600

OK Cancel



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)

Phone Book Index No. 1 Enable Phone Number 2222 Display Name John draytel org SIP URL 1234 Default 💌 Dial Out Accoun Loop through None 💌 Backup Phone OK Clear Cancel VolP >> SIP Accounts IP Account Index No. 1 Profile Name (11 char max.) Auto Register via Call without Registration 5060 SIP Port draytel 1 Domain/Realn (63 char max.) Proxy draytel 1 (63 char max.) Act as out **Display Name** David (23 char max.) Account Number/Name 4321 (63 char max.) Authentication ID (63 char max.) Password (63 char max.) Expiry Time M 3600 1 hour SPC NAT Traversal Support None 💌 Phone Ring Port ISON1-SO Any ISDN2-TE

CODEC/RTP/DTMF----

(Use default value)

David calls John

Ring Pattern

VolP >> DialPlan Setup

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)

OK Cancel

1 🛩

3.7.2 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.

VolP >> DialPlan Setup

Arnor's SIP URL: 1234@214.61.172.53

Paulin's SIP URL: 4321@ 203.69.175.24

Settings for Arnor

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

SIP Accounts Settings ----

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

CODEC/RTP/DTMF----

(Use default value)

max.)
max.)
nax.)
nax.) nax.)

lattern 1 💌

Phone

ISDN1-S0 Any W

Arnor calls Paulin

Ring Port

Ring Pattern



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 ----

CODEC/RTP/DTMF---

(Use default value)

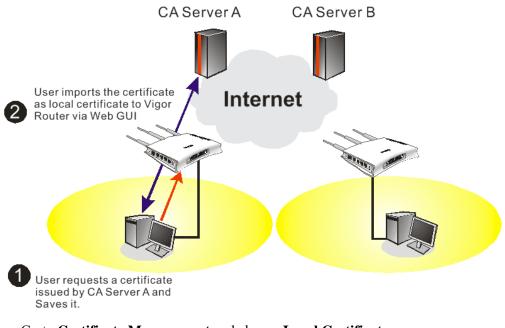
VoIP >> DialPlan Setup Phone Book Index No. 1 Enable Phone Number 2222 Display Name Arnor SIP URL 1234 © 214.61.172.53 Dial Out Account Default 💌 Loop through None 💌 Backup Phone Number OK Clear Cancel VoIP >> SIP Accounts SIP Account Index No. 1 Profile Name (11 char max.) Arnor None ۷ Register via Call without Registration SIP Port 5060 Domain/Realm (63 char max.) Proxy (63 char max.) Display Name Paulio (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 💌 Phone ISDN1-S0 Any Y Ring Port Ring Pattern 1 ~

OK Cancel

Paulin calls Arnor

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

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



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

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

Dray Tek

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

Certificate Management >> Local Certificate

Generate Certificate Request		
Subject Alternative Name		
Туре	IP Address 👻	
IP		
Subject Name		
Country (C)		
State (ST)		
Location (L)		
Orginization (O)		
Orginization Unit (OU)		
Common Name (CN)		
Email (E)		
Кеу Туре	RSA M	_
Key Size	1024 Bit 🔽	
	Generate	

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

X509 Local Cer	tificate Configuration		
Name	Subject	Status	Modify
Local	/C=TW/ST=HC/L=HC/O=Draytek/O	Requesting	View Delete
GENERATE X509 Lo	IMPORT REFRESH		
MIIBqj EwJIQz CQEWE31 AoGBAL a1X/fi m6+0f4: hkiG9w 9yojHp; eorpDa	EGIN CERTIFICATE REQUEST CCARMCAQAwajELMAkGA1UEBhMCVFcxCzAJ EQMA4GA1UEChMHRHJheXR1azELMAkGA1UE NicHBvcnRAZBjheXR1ay5jh2OugZ2wDQY31 MJdTsqfF97FEpYy+1qeJVJGuSRtqG6Etw8 gmEccQA2LPSQ1Q05Qychwq07Bm0EDf10wH x24QQnjXXgc1COBj11Aa6MLSce1synZhkg; DBAQUFAAOBgQCq3sdw7c21t9qn4U6X2Bj3 stNsmWsMRuAwGeKCWc8S/gLtHr6iccMoT 1/rC92wCraOtSXUmPqNojytq8BxStTEAVU N CERTIFICATE REQUEST	CxMCURQxIjAgB KoZIhvcNAQEBB yTU5HQvXpAzcr wCalAZQoGvIiO hQIQN5uFAgMBA Jzu7JHafSSeUn bQFx/LWdaEPU5	gkqhkiG9wOB QADgYOANIGJ gJBGrikTUBX DMC7f5w9xA8 AGgADANBgkq aYD2efCmGfX LqryBKKgC9t
			~

4. Connect to CA server via web browser. Follow the instruction to submit the request. Below we take a Windows 2000 CA server for example. Select **Request a Certificate**.

<i>Microsoft</i> Certificate Services vigor	<u>Hom</u>
<i>Nelcome</i>	
You use this web site to request a certificate for your web browser, e-mail client, or other secure program. Once you acquire a certificate will be able to securely identify yourself to other people over the web, sign your e-mail messages, encrypt your e-mail messages, and mo depending upon the type of certificate you request.	
Select a task:	
Retrieve the CA certificate or certificate revocation list	
Check on a pending certificate	
Next	>

Select Advanced request.

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

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

Microsoft Certifica	ite Services vigor	Ha
Submit A Save	d Request	
oubline A ouve		
		request or PKCS #7 renewal request generated by an external application (such as a web t to the certification authority (CA).
Saved Request:		
Certificate Request (PKCS #10 or #7):	BEGIN CERTIFICATE REQUI MIIBGJCCARMCAQAwQTELMAKGAIU BgkqhkiG9DBCQEWEXBYZXNZQQR A4GNADCBIQKBgQDQYB7wmZfFhM hX4bpB9cUF9dloACGGiM/tcBOck x/GGA7CTvO/fQ2pxroCwIJTJL5J Browse for a file to inset.	EBhMCVFcxEDAO 9/IEQDG03Xk++ dc2dFFv1XcP3
Certificate Templa	ate:	
	Administrator 🗸	
	Administrator Authenticated Session Basic EFS	
	EFS Recovery Agent User IPSEC (Offline request)	
	Router (Offline request) Subordinate Certification Authority Web Server	Submit >

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

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

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

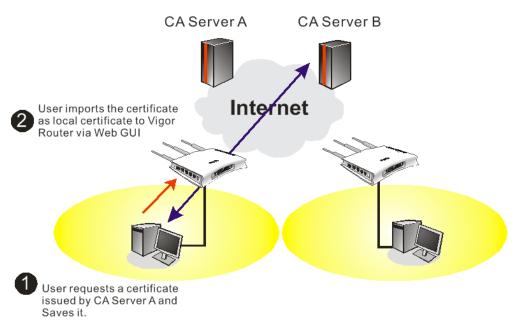
NameSubjectStatusModifyLocal/C=TW/ST=HC/L=HC/O=Draytek/ORequestingViewDeleteGENERATEIMPORTREFRESHStory Certificate RequestStory Certificate RequestBEGIN CERTIFICATE REQUESTMIIBQ;CARMCAQAwa;ELMAKGA1UESTMIIBQ;CCARMCAQAwa;ELMAKGA1UESTMIIBQ;CCARMCAQAwa;ELMAKGA1UESTMIIBQ;CCARMCAQAwa;ELMAKGA1UESTMIIBQ;CCARMCAQAwa;ELMAKGA1UESTMIIBQ;CCARMCAQAwa;ELMAKGA1UESTAGBALMJGA1UECMMCAQAwa;ELMAKGA1UECMCUKQX]AgBgkqhkiG9w0BCQEWEJ3NICHBYCRAZHJneXRIazSib2Oug28wDQYJKOZIhvcNAQEBBQADgYOAMIGJAGBALMJGTSqfP97FEpYy+IqeJVJGuSRtqGEEtw8yTUSHQvXpAzcrgJBGrikTUBXa1X//fgnEccQA2LPSQ1Q8SQychwq07Bm0EDf10wHwCa1AZQoGvIiODMC7f5w9xA8m6+0f4x24QQn;XXgciC0Bj1iAa6MLSce1synZhkgq01QNSUAJAMBAKGADANBgkqhkiG9w0BAQUFAA0BgQCq3sdwVc21t9qn4U6X2BJsVzu7JHafSSeUnaYD2efCMGfXSyojHpstNsmWsMRuAw6eKCWc85/gLtHnf6iccMoToQFx/LWdaEPU5LqryBKKgC9teorpa1/rC92wcra0t8XUmPqNoiytq8BxStTE8vULiIxmwaBvc1hWFSXKVLU7g==END CERTIFICATE REQUEST	i09 Local Cer	tificate Configuration		
GENERATE IMPORT REFRESH X509 Local Certificate Request BEGIN CERTIFICATE REQUEST MIIBqjCCARMCAQAwajELMAkGA1UEbhMCVFcxCzAJBgNVBAgTAkhDMQswCQYDVQQH EwJIQzEQMA4GA1UEChMHRHJheXRlazELMAkGA1UECxMCUkQxIjAgBgkqhkiG9w0B CQEWE3N1cHBvcnRA2HJheXRlaz5jb2Owg28wDQYJKoZIhvcNAQEBBQADgYOAMIGJ AoGBALMJdTsqfF97FEpYy+IqeJVJGuSRtqG6Etw8yTU5HQvXpAzcrgJBGrikTUBX a1X//fgnEccQA2LPSQIQ8SQchwq07Bm0EDf1DwHwCalA2QGvIiODMC7f5w9xA8 m64+0f4x24QQnjXXgciC0Bj1iAa6MLScelsynZhkgnQ1QNSuFAgMBAAGgADANBgkq hkiG9w0BAQUFAA0BgQCq3sdwVc21t9qn4U6X2BJsVzu7JHafSSeUnaYDzefCmGfX 9yojHpstNsmWsMRuAwGeKCWc8S/gLtHnc6iccMoT0QFx/LWdaEPUSLqryBKKgC9t eorpDa1/rC92wCra0t8XUmPqNoiytq8BxStTE8vULiIxmwaBvc1hWFSXKVLU7g==	Name	Subject	Status	Modify
X509 Local Certificate Request BEGIN CERTIFICATE REQUEST MIIBqjCCARMCAQAwajELMAkGA1UEBhMCVFcxC2AJBgNVBAgTAkhDMQswCQYDVQQH EwJIQzEQMA4GA1UEChMHRHJheXRlazELMAkGA1UECxMCUkQxIjAgBgkqhkiG9w0B CQEWE3N1cHBvcnRAZHJheXRlaz5jb20wg28wDQYJK0ZIhvcNAQEBBQADgYOAMIGJ AoGBALMJdTsqfF97FEpYy+IqeJVJGuSRtqG6Etw8yTU5HQvXpAzcrgJBGrikTUBX a1X//fgnEccQA2LPSQ1Q85Qychwq07Bm0EDf10wHwCalA2QoGv1i0DMC7f5w9xA8 m6+0f4x24QQnjXXgciC0BjliAaGMLScelsynZhkgnQ1QNSuFAgMBAAGgADANBgkq hkiG9w0BAQUFAA0BgQCq3sdwVc21t9qn4U6X2BJSVzu7JHafSSeUnaYD2efCmGfX 9yojHpstNsmWsMRuAw6cKCWc88/gLtHnc6iccMoToOFx/LWdaEPU5LqryBKKgC9t eorpDa1/rC92wCra0t8XUmPqNoiytq8BxStTE8vULiIxmwaBvc1hWFSXKVLU7g==	Local	/C=TW/ST=HC/L=HC/O=Draytek/0	Requesting	View Delete
MIIBqjCCARMCAQAwajELMAkGA1UEBhMCVFcxCzAJBgNVBAgTAkhDMQswCQYDVQQH EwJIQzEQMA4GA1UEChMHRHJheXRlazELMAkGA1UECxMCUkQxIjAgBgkqhkiG9wOB CQEWE3N1cHBvcnRAZHJheXRlay5jb2Owg28wDQYJKoZIhvcNAQEBBQADgYOAMIGJ AoGBALMJdTsqfF97FEpYy+IqeJVJGuSRtqG6Etw8yTU5HQvXpAzcrgJBGrikTUBX a1X//fgnEccQA2LPSQIQ8SQychwqO7BmOEDf10wHwCalAZQGVIiODMC7f5w9xA8 m6+0f4xZ4QQnjXXgciCOBj1iAa6MLScelsynZhkgnQ1QN5uFAgMBAAGgADANBgkq hkiG9wOBAQUFAAOBgQCq3sdwVc2lt9qn4U6X2BJsVzu7JHafSSeUnaTDZefCmGfX 9yojHpstNsmWsMRuAwGeKCWc8S/gLtHnr6iccMoToQFx/LWdaEPUSLqryBKKgC9t eorpDa1/rC92wCra0t8XUmPqNoiytq8BxStTE8vULiIxmwaBvc1hWFSXKVLU7g==				
	MIIBqj EwJIQz CQEWE3 AcOBAL a1X//f m6+0f4 hkiG9w 9yojHp eorpDa	CCARMCAQAwajELMAkGAIUEBhMCVFcxCzAJ EQMA4GA1UEChMHRHJheXRlazELMAkGA1UE N1CHBvcnRAZHJheXRlay5jb2Owg28wDQYJ MJdTsqfF97FEyYy+IqeJVJGuSRtqG6Etw8 gnEccQA2LPSQIQ85Qychwq07Bm0EDf10wH x24QQnjXXgciCOBj1iAa6MLScelsynZhkg OBAQUFAAOBgQCq3sdwVc2lt9qn4U6X2BJs ³ stNsmWsMRuAwGeKCWc85/gLtHhr6iccNoT 1/rC9ZwCraOt8XUmPqNoiytq8BxStTE8vU	C×MCURQXIJAgB KoZIhvcNAQEBB yTU5HQvXpAzcr wCalAZQoGvIiO nQ1QN5uFAgMBA Vzu7JHafSSeUn oQFx/LWdaEPU5	gkqhkiG9w0B QADgY0AMIGJ gJBGrikTUBX DMC7f5w9xA8 AGgADANBgkq aqYDzefCmcfX LqryBKKgC9t

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

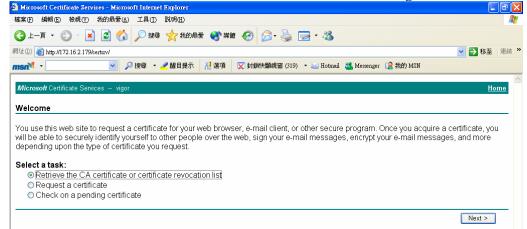
Name :	Local
Issuer :	/C=US/CN=vigor
Subject :	/emailAddress=press@draytek.com/C=TW/O=Draytek
Subject Alternative Name :	DNS:draytek.com
Valid From :	Aug 30 23:08:43 2005 GMT
Valid To :	Aug 30 23:17:47 2007 GMT

Dray Tek

3.9 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**.



Dray Tek

- 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 🌀 上一頁 🔹 💿 · 😰 🟠 🔎 搜尋 🧙 我的最爱 🜒 媒體 🚱 🔗 - 🌺 🔜 • 🆄 網址 (1) 🍓 http://172.16.2.179/certsrv/certcarc.asp ✓ → 移至 連結 msnM -🔻 🔎 搜尋 🝷 🥒 醒目提示 🛛 🕌 選項 🛛 🔀 封鎖快顯視窗 (319) 🝷 🔤 Hotmail 🔉 Messenger [2 我的 MSN Retrieve The CA Certificate Or Certificate Revocation List Install this CA certification path to allow your computer to trust certificates issued from this certification authority It is not necessary to manually install the CA certification path if you request and install a certificate from this certification authority, because the CA certification path will be installed for you automatically Choose file to download: CA Certificate: Current [vigor(1)] Previous [vigor] ○DER encoded or ●Base 64 encoded Download CA certificate Download CA certification path Download latest certificate revocation list
- 3. Back to Vigor router, go to **Trusted CA Certificate**. Click **IMPORT** button and browse the file to import the certificate (.cer file) into Vigor router. When finished, click refresh and you will find the below illustration.

Certificate Management >> Trusted CA Certificate

X509 Trusted CA Certificate Configuration

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

IMPORT REFRESH

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

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

Close

Note: Before setting certificate configuration, please go to System Maintenance >> Time and Date to reset current time of the router first.

3.10 Creating an Account for MyVigor

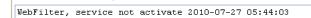
The website of MyVigor (a server located on <u>http://myvigor.draytek.com</u>) provides several useful services (such as Anti-Spam, Web Content Filter, Anti-Intrusion, and etc.) to filtering the web pages for the sake of protecting your system.

To access into MyVigor for getting more information, please create an account for MyVigor.

3.10.1 Creating an Account via Vigor Router

1. Click **CSM>> Web Content Filter Profile**. The following page will appear.

Web-Filter License [Status:Not Activated]]		Activ
Setup Query Server	auto-selected		Find more
Setup Test Server	auto-selected		Find more
Web Content Filter P	rofile Table:		Set to Factory Defa
Profile	Name	Profile	Name
1.	Default	5.	
<u>2.</u>		<u>6.</u>	
)r		-	
	•	. . ,	4 6 11 -
lick System Ma	intenance>>Activ	vation to op	en the following page.
			Activate via interface : auto-select
System Maintenanc	e >> Activation		
System Maintenanc Web-Filter License	e >> Activation		Ac



2. Click the **Activate** link. A login page for MyVigor web site will pop up automatically.

DGIN			
UserName :			
Password :			
Auth Code :		AYi GXZ	
	If you cannot read the w	ord, <u>click here</u>	
	Forget passwor	d? Login	
Don't have a	MyVigor Account ?	<u>Create an ac</u>	count now

- Customer Service : (886) 3 597 2727 or email to :<u>Webmaster@draytek.com</u>
- 3. Click the link of **Create an account now**.
- 4. Check to confirm that you accept the Agreement and click Accept.

Agreement	hts/Surg theorem and
Agreement	=====================================
	1. Agreement
Personal Information	Draytek provides MyVigor(myvigor.draytek.com) service according to this agreement. When you use
r ersonar miormation	MyVigor service, it means that you have read, understand and agree to accept the items listed in this
	agreement. Draytek can modify or change the content of the items without any reasons. It is
Preferences	suggested for you to notice the medications or changes at any time. If you still use MyVigor service
rielelelices	after knowing the modifications and changes of this service, it means you have read, understand and
	agree to accept the modifications and changes. If you do not agree the content of this agreement,
Completion	please stop using My∀igor service.
compretion	
	2. Registration
	To use this service, you have to agree the following conditions:
	(a) Provide your complete and correct information according to the registration steps of this service.
	(b) If you provide any incorrect or fake information here. DravTek has the right to pause or terminate
	I have read and understand the above Agreement. (Use the scroll bar to view the entire agreement)

5. Type your personal information in this page and then click **Continue**.

	Account Informati	ion
BAgreement	UserName:*	Mary Check Account
		(3 ~ 20 characters)
	Password:*	••••
2 Personal		(4~20 characters : Do not set the same as the username.)
Information	Confirm Password:*	••••
	Personal Informat	tion
3 Preferences	First Name:*	Mary
	Last Name:*	Ted
Completion	Company Name:	Tech Ltd.
	Email Address:*	mary_ted@tech.com
		Please note that a valid E-mail address is required to receive the Subscription Code. You will need this code to activate your account.
	Tel:	0
	Country:*	SWITZERLAND
	Career:*	Supervisor

6. Choose proper selection for your computer and click **Continue**.

Register		
Create an account - I	Please enter personal profile.	
Agreement	How did you find out about this website?	Internet 💌
Hyrocinent	What kind of anti-virus do you use?	AntiVir
Personal	I would like to subscribe to the MyVigor e-letter.	
Information	I would like to receive DrayTek product news.	
3 Preferences	Please select the mail server for receiving the verification mail.	Global Server 💌
4 Completion		<< Back Continue >>

7. Now you have created an account successfully. Click START.



8. Check to see the confirmation *email* with the title of **New Account Confirmation** Letter from <u>myvigor.draytek.com</u>.

***** This is an automated message from myvigor draytek.com.*****

Thank you (Mary) for creating an account.

Please click on the activation link below to activate your account

Link : Activate my Account

9. Click the **Activate my Account** link to enable the account that you created. The following screen will be shown to verify the register process is finished. Please click **Login**.

Register	Search for this site	GO
Register Confirm		
	Thank for your register in VigorPro Web Site The Register process is completed	



- 10. When you see the following page, please type in the account and password (that you just created) in the fields of **UserName** and **Password**.
 - This service is available for MyVigor member only. Please login to access MyVigor. If you are not one of the members of MyVigor, please create an account first.

LOGIN		
UserName :	Mary	
Password :	••••	
Auth Code :	T4he1C	T4he1C
	lf you cannot read t	he word, <u>click here</u>
	Forget pass	sword? Login
Don't have a	MyVigor Account	? Create an account now
If you a	Customer Service	ing in, contact our customer service. : (888) 3 597 2727 or aster@draytek.com

11. Now, click **Login**. Your account has been activated. You can access into MyVigor server to activate the service (e.g., WCF) that you want.

3.10.2 Creating an Account via MyVigor Web Site

1. Access into <u>http://myvigor.draytek.com</u>. Find the line of **Not registered yet?**. Then, click the link **Click here!** to access into next page.

Dray Tek	MyVig	or	Customer Survey
ft Home	Search	60	
AL	MyVigor for you	^	Login
About Us Product My Information VigorPro	MyVigor website replaces the VigorPro site as DrayTek's portal site for the latest products and services in network security, including Anti- Virus, Anti-Spam, Web Content Filter etc. The products and functions that are supported in this site include:		UserName Password AuthCode
	VigorPro Unified Security Firewall series:		QbkqVd
	 Activation of CommtouchTM GlobalView Web Content Filter license key Activation of DT Anti-Virus license key Activation of Kaspersky Anti-Virus license key Activation of CommtouchTM Anti-Spam license key and 		If you can't read the AuthCode , <u>click here</u> Login Forget password?
	membership <u>Vigor routers (for models that support Commtouch</u> TM)		Not registered yet ? <u>Click here !</u>
	 Activation of CommtouchTM GlobalView Web Content Filter license key 		
	The MyVigor website contains a trail version of Commtouch TM GlobalView Web Content Filter, which allows the users to set filters to block out undesirable web pages in the Internet jungle.		
Please use IE 5.0 or above (resolution 1024 * 768) for best display. © DrayTek Corp.	More customer-oriented services are planned for MyVigor site for the near future.	~	

Dray Tek

2. Check to confirm that you accept the Agreement and click Accept.



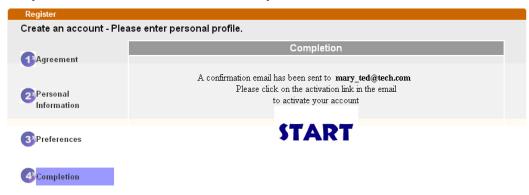
3. Type your personal information in this page and then click Continue.

	Account Informati	ion
Agreement	UserName:*	Mary Check Account
	Password:*	(3 ~ 20 characters)
2 Personal		(4 ~ 20 characters : Do not set the same as the username.)
Information	Confirm Password:*	••••
	Personal Informat	tion
3 Preferences	First Name:*	Mary
	Last Name:*	Ted
Completion	Company Name:	Tech Ltd.
	Email Address:*	mary_ted@tech.com
		Please note that a valid E-mail address is required to receive the Subscription Code. You will need this code to activate your account.
	Tel:	0 -
	Country:*	SWITZERLAND
	Career:*	Supervisor 🗸

4. Choose proper selection for your computer and click Continue.

Register		
Create an account	- Please enter personal profile.	
	How did you find out about this website?	Internet 💌
Ungreement	What kind of anti-virus do you use?	AntiVir
2 Personal	l would like to subscribe to the MyVigor e-letter.	
Information	l would like to receive DrayTek product news.	V
3 Preferences	Please select the mail server for receiving the verification mail.	Global Server 💌
4 Completion		<< Back Continue >>

5. Now you have created an account successfully. Click START.



6. Check to see the confirmation *email* with the title of New Account Confirmation Letter from myvigor.draytek.com.

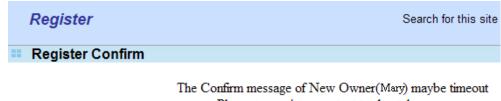
***** This is an automated message from myvigor draytek.com.*****

Thank you (Mary) for creating an account.

Please click on the activation link below to activate your account

Link : Activate my Account

7. Click the Activate my Account link to enable the account that you created. The following screen will be shown to verify the register process is finished. Please click Login.



Please try again or contact to draytek.com

Close Login 8. When you see the following page, please type in the account and password (that you just created) in the fields of **UserName** and **Password**. Then type the code in the box of Auth Code according to the value displayed on the right side of it.

This service is available for MyVigor member only. Please login to access MyVigor. If you are not one of the members of MyVigor, please create an account first.

LOGIN			
UserName :	Mary		
Password :	••••		
Auth Code :	T4he1C	T4he1C	
	lf you cannot read th	e word, <u>click here</u>	
	Forget pass	word? Login	
Don't have a	MyVigor Account	? Create an acc	ount now
If you		ng in, contact our customer servi	ice.

Now, click **Login**. Your account has been activated. You can access into MyVigor server to activate the service (e.g., WCF) that you want.

email to :webmaster@draytek.com





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

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

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

Vigor271 ADSL2/2	0 Series + Firewall Router	Dray Tek
Auto Logout 👻 📭 🗸	System Status	<u><</u>
Quick Start Wizard Service Activation Wizard VoIP Wizard Online Status	Model Name: Vigor2710VFirmware Version: 3.6.3Build Date/Time: Nov 2 2012 16:34:49ADSL Firmware Version: 211011_A Hardware: Annex A	
Internet Access LAN NAT Firewall Objects Setting	LAN MAC Address : 00-50-7F-92-F5-00 1st IP Address : 192.168.1.1 Ist Subnet Mask : 255.255.255.0 DHCP Server : Yes DNS : 8.8.8.8	WAN 1 : Disconnected : 00-50-7F-92-F5-01 : PPPoE : 2 : 2
CSM Bandwidth Management Applications VPN and Remote Access Certificate Management VoIP USB Application System Maintenance	VoIP Port Profile Reg. In/Out Phone1 Wizard1 No 0/0 Phone2 Wizard1 No 0/0 ONLY Phone 2 can access the PSTN line during power failure.	
Diagnostics	Address Scope Internet LAN FE80::250:7FFF:FE92:F500/64 Link	Access Mode

4.1 Internet Access

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

4.1.1 Basics of Internet Protocol (IP) Network

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

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

Dray Tek

What are Public IP Address and Private IP Address

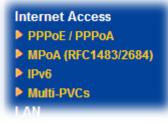
As the router plays a role to manage and further protect its LAN, it interconnects groups of host PCs. Each of them has a private IP address assigned by the built-in DHCP server of the Vigor router. The router itself will also use the default **private IP** address: 192.168.1.1 to communicate with the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

Get Your Public IP Address from ISP

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

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

Below shows the menu items for Internet Access.



4.1.2 PPPoE/PPPoA

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

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



Internet Access >> PPPoE / PPPoA

PPPoE/PPPoA Client	⊙ Enable 🔘 Disable	ISP Access Setup
	Channel 1 v 0 33 LLC/SNAP v PPPoE v Multimode v Kked while using the PPPoA behave like a modem which lient on the LAN. 0 (0~4095)	 ISP Name Username Password PPP Authentication PAP or CHAP ▼ Always On Idle Timeout -1 second(s IP Address From ISP WAN IP Alias Fixed IP ○ Yes ● No (Dynamic IP) Fixed IP Address ● Default MAC Address ● Specify a MAC Address MAC Address: 00 .50 .7F :92 .F5 .01 Index(1-15) in Schedule Setup:
Priority	0 (0~7)	
WAN Connection Dete		-
Mode Ping IP TTL:	ARP Detect	
мти	1442 (Max:1492)	
Bridge Mode		_

Available settings are explained as follows:

Go to 3G USB Modem Setup

Item	Description
Enable/Disable	Click Enable for activating this function. If you click Disable , this function will be closed and all the settings that you adjusted in this page will be invalid.
DSL Modem Settings	Set up the DSL parameters required by your ISP. These are vital for building DSL connection to your ISP.
	Multi-PVC channel - The selections displayed here are determined by the page of Internet Access – Multi PVCs. Select M-PVCs Channel means no selection will be chosen.
	VPI - Type in the value provided by ISP.
	VCI - Type in the value provided by ISP.
	Encapsulating Type - Drop down the list to choose the type provided by ISP.

OK

	Protocol - Drop down the list to choose the one provided by ISP.If you have already used Quick Start Wizard to set the protocol, then it is not necessary for you to change any settings in this group.
	Modulation – Drop down the list to choose a proper modulation for the router.
PPPoE Pass-through	The router offers PPPoE dial-up connection. Besides, you also can establish the PPPoE connection directly from local clients to your ISP via the Vigor router. When PPPoA protocol is selected, the PPPoE package transmitted by PC will be transformed into PPPoA package and sent to WAN server. Thus, the PC can access Internet through such direction.
	For Wired LAN – If you check this box, PCs on the same network can use another set of PPPoE session (different with the Host PC) to access into Internet.
	For Wireless LAN – If you check this box, PCs on the same wireless network can use another set of PPPoE session (different with the Host PC) to access into Internet.
	VLAN Enable - Enable the function of VLAN with tag. The router will add specific VLAN number to all packets while sending them out. Please type the tag value and specify the priority for the packets sending by the router.
	VID – Type the value as the VLAN ID number. The range is form 0 to 4095.
	Priority – Type the packet priority number for such VLAN. The range is from 0 to 7.
WAN Connection Detection	 Such function allows you to verify whether network connection is alive or not through ARP Detect or Ping Detect. Mode – Choose ARP Detect or Ping Detect for the system to execute for WAN detection. Ping IP – If you choose Ping Detect as detection mode, you have to type IP address in this field for pinging. TTL (Time to Live) – Displays value for your reference. TTL value is set by telnet command.
MTU	It means Max Transmit Unit for packet. The default setting is 1442.
Bridge Mode	If you check this box to invoke the function, the router will work as a bridge.
WAN Backup Setup	3G USB Modem ✓ Ie Disable 3G USB Modem
	Dial Backup Mode - If you install a 3G USB modem on the



router, choose the **3G USB Modem** to perform WAN backup via USB device. Then, click the **3G USB Modem Backup** link to access into the following page for configuring detailed settings.

USB Modem Setu)	
PPP Client Mode	🔿 Enable 💿 Disable	
SIM PIN code		
Modem Initial String	AT&FE0V1X1&D2&C1S0=0	(Default:AT&FE0V1X1&D2&C1S0=0)
APN Name		Apply
Modem Initial String2	AT	
Modem Dial String	ATDT*99# SCDMA:ATDT*98*1#)	(Default:ATDT*99#, CDMA:ATDT#777, TD-
PPP Username		(Optional)
PPP Password		(Optional)
PPP Authentication	PAP or CHAP	
Index(1-15) in <u>Sch</u> =>,	edule Setup:	
WAN Connection I	Detection	
Mode	ARP Detect 🛩	
Ping IP		
TTL:		

PPP Client Mode - Click **Enable** to activate this mode for WAN2.

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

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

APN Name – APN (Access Point Name) is provided by your ISP for identifying different access points. Simply click **Apply** to apply such name. Finally, you have to click **OK** to save the setting.

Apply – Activate the function of identification.

Modem Initial String2 - The initial string 1 is shared with APN. In some cases, users may need another initial *AT* command to restrict 3G band or do any special settings.

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.

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

Mode – Choose ARP Detect or Ping Detect for the system

	to execute for WAN detection.
	Ping IP – If you choose Ping Detect as detection mode, you have to type IP address in this field for pinging.
	TTL (Time to Live) – Displays value for your reference. TTL value is set by telnet command.
	Default – Click this button to reset to factory setting.
ISP Access Setup	Enter your allocated username, password and authentication parameters according to the information provided by your ISP. If you want to connect to Internet all the time, you can check Always On .
	Username – Type in the username provided by ISP in this field.
	Password – Type in the password provided by ISP in this field.
	PPP Authentication – Select PAP only or PAP or CHAP for PPP.
	Idle Timeout – Set the timeout for breaking down the Internet after passing through the time without any action. This setting is active only when the Active on demand option for Active Mode is selected in WAN>> General Setup page.

IP Address From ISP	Usually ISP dynamically assigns IP address to you each time you connect to it and request. In some case, your ISP provides service to always assign you the same IP address whenever you request. In this case, you can fill in this IP address in the Fixed IP field. Please contact your ISP before you want to use this function.				
	WAN IP Alias - If you have multiple public IP addresses and would like to utilize them on the WAN interface, please use WAN IP Alias. You can set up to 8 public IP addresses other than the current one you are using. Notice that this setting is available for WAN1 only. Type the additional WAN IP address and check the Enable box. Then click OK to exit the dialog.				
			Multi-NAT)		
		Enable	Aux. WAN IP	Join NAT IP Pool	
	1.				
	2.		192.168.1.56		
	3.		192.168.1.89		
	4.		0.0.0.0		
	5.		0.0.0.0		
	6.		0.0.0.0		
	7.		0.0.0.0		
	8.		0.0.0.0		
			OK Clear All ck Yes to use this ne box of Fixed IP	Close function and type in a fixed Address.	
	Default MAC Address – You can use Default MAC Address or specify another MAC address by typing on the boxes of MAC Address for the router.				
	Specify a MAC Address – Type the MAC address for the router manually.				
	of time set prev	schedu iously	le for your request in Applications –	• You can type in four sets . All the schedules can be Schedule web page and you e set in that web page.	

After finishing all the settings here, please click \mathbf{OK} to activate them.

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

MPoA (RFC1483/2684)	🔘 Enable 💿 Disable	WAN IP Network Setting	
DSL Modem Settings Multi-PVC channel Encapsulation 148 VPI VCI Modulation VLAN Enable VID Priority	Channel 2 3 Bridged IP LLC 0 88 Multimode 0 0 0 0 0 0 0 0 0	 Specify an IP address IP Address Subnet Mask Gateway IP Address Default MAC Address Specify a MAC Address 	Vigor * S WAN IP Alias 0.0.0.0 0.0.0.0 0.0.0.0 S
WAN Connection Detec Mode Ping IP TTL:		MAC Address: 00 .50 DNS Server IP Address Primary IP Address Secondary IP Address	.7F :92 .F5 .01
MTU RIP Protocol Enable RIP Bridge Mode Enable Bridge Mode WAN Backup Setup Dial Backup Mode Go to 3G USB Mode		-	

Internet Access >> MPoA (RFC1483/2684)

Available settings are explained as follows:

Item	Description
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.

OK



	Encapsulating Type - Drop down the list to choose the type
	provided by ISP.
	VPI - Type in the value provided by ISP.
	VCI - Type in the value provided by ISP.
	Modulation – Drop down the list to choose a proper modulation for the router.
	VLAN Enable - Enable the function of VLAN with tag. The router will add specific VLAN number to all packets while sending them out. Please type the tag value and specify the priority for the packets sending by the router.
	VID – Type the value as the VLAN ID number. The range is form 0 to 4095.
	Priority – Type the packet priority number for such VLAN. The range is from 0 to 7.
WAN Connection Detection	Such function allows you to verify whether network connection is alive or not through ARP Detect or Ping Detect.
	Mode – Choose ARP Detect or Ping Detect for the system to execute for WAN detection.
	Ping IP – If you choose Ping Detect as detection mode, you have to type IP address in this field for pinging.
	TTL (Time to Live) – Displays value for your reference. TTL value is set by telnet command.
MTU	It means Max Transmit Unit for packet. The default setting is 1442.
RIP Protocol	Routing Information Protocol is abbreviated as RIP (RFC1058) specifying how routers exchange routing tables information. Click Enable RIP for activating this function.
Bridge Mode	If you check this box to invoke the function, the router will work as a bridge.
WAN Backup Setup	3G USB Modem ♥ Disable 3G USB Modem
	Dial Backup Mode - If you install a 3G USB modem on the router, choose the 3G USB Modem to perform WAN backup via USB device. Then, click the 3G USB Modem Backup link to access into the following page for configuring detailed settings.

3G USB Modem Setu PPP Client Mode	○ Enable ● Disable
SIM PIN code	
Modem Initial String	AT&FE0V1X1&D2&C1S0=0 (Default:AT&FE0V1X1&D2&C1S0=0)
APN Name	Apply
Modem Initial String2	AT
Modem Dial String	ATDT*99# (Default:ATDT*99#, CDMA:ATDT#777, TD- SCDMA:ATDT*98*1#)
PPP Username	(Optional)
PPP Password	(Optional)
PPP Authentication	PAP or CHAP
Index(1-15) in Sc	redule Setup:
=>,	
WAN Connection	Detection
Mode	ARP Detect
Ping IP	
TTL:	
	OK Cancel Default

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

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

APN Name – APN (Access Point Name) is provided by your ISP for identifying different access points. Simply click **Apply** to apply such name. Finally, you have to click **OK** to save the setting.

Apply – Activate the function of identification.

Modem Initial String2 - The initial string 1 is shared with APN. In some cases, users may need another initial *AT* command to restrict 3G band or do any special settings.

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.

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

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

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

TTL (Time to Live) – Displays value for your reference.



	TTL value is set by telnet command.			
	Default – Click this button to reset to factory setting.			
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.			
	-	lress – Click this	radio button to specify	
	WAN IP Alias. Ye than the current or available for WAN	ou can set up to 8 ne you are using. N1 only. Type the	AN interface, please us public IP addresses of Notice that this setting additional WAN IP Then click OK to exit	
	WAN2 IP Alias (Multi	i-NAT)		
	Index Enable	Aux. WAN IP	Join NAT IP Pool	
	1. 🔽			
	2.	192.168.1.56		
	3. 🔽	192.168.1.89		
	4.	0.0.0.0		
	5.	0.0.0.0		
	6.	0.0.0.0		
	7.	0.0.0.0		
	8. C	0.0.0.0	Close	
	IP Address – Typ	a in the private I	D address	
	Subnet Mask – T	•		
	Gateway IP Address – Type in gateway IP address.			
	Default MAC Ad	dress Type in se Default MAC	MAC address for the Address or specify	
	MAC Address – ' manually.	Type in the MAC	C address for the router	
DNS Server IP Addres	71 1		the router. If necessary cessity in the future.	

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



4.1.4 IPv6

During the procedure of IPv4 PPPoE connection, we can get the IPv6 Link Local Address between the gateway and Vigor router through IPv6CP. Later, use DHCPv6 or Accept RA to acquire the IPv6 prefix address (such as: 2001:B010:7300:200::/64) offered by the ISP. In addition, PCs under LAN also can have the public IPv6 address for Internet access by means of the generated prefix.

IPv6 – PPP

No need to type any other information for PPP mode.

nterne	t Access	s >>	Pv6

Internet Access Mode	
Connection Type	PPP 💌
Note : IPv4 WAN setting shou	be PPPoE client.

Note: At present, the **IPv6 prefix** can be acquired via the PPPoE mode connection which is available for the areas such as Taiwan (hinet), the Netherlands, Australia and UK.

IPv6 – TSPC

Internet Access >> IPv6

Tunnel setup protocol client (TSPC) is an application which could help you to connect to IPv6 network easily.

Please make sure your IPv4 WAN connection is OK and apply one free account from hexago (<u>http://gogonet.gogo6.com/page/freenet6-account</u>) before you try to use TSPC for network connection. TSPC would connect to tunnel broker and requests a tunnel according to the specifications inside the configuration file. It gets a public IPv6 IP address and an IPv6 prefix from the tunnel broker and then monitors the state of the tunnel in background.

After getting the IPv6 prefix and starting router advertisement daemon (RADVD), the PC behind this router can directly connect to IPv6 the Internet.

Internet Access Mode	
Connection Type	TSPC
TSPC Configuration	
Username	
Password	
Confirm Password	
Tunnel Broker	

Available settings are explained as follows:



Item	Description
Username	Type the name obtained from the broker.
Password	Type the password assigned with the user name.
Confirm Password	Type the password again to make the confirmation.
Tunnel Broker	Type the address for the tunnel broker IP, FQDN or an optional port number.

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

IPv6 – AICCU

Internet Access >> IPv6

Internet Access Mode		
Connection Type	AICCU	
AICCU Configuration		
Username		
Password		
Confirm Password		
Tunnel Broker	tic.sixxs.net	
Subnet Prefix	/	

OK

Available settings are explained as follows:

Item	Description
UsernameType the name obtained from the broker. Please ap account at http://www.sixxs.net/ . It is suggested for apply another username and password.	
Password	Type the password assigned with the user name.
Confirm Password	Type the password again to make the confirmation.
Tunnel Broker	Type the address for the tunnel broker IP, FQDN or an optional port number.
Subnet Prefix	Type the subnet prefix address getting from service provider

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

IPv6 – DHCPv6

DHCPv6 client mode would use DHCPv6 protocol to obtain IPv6 address from server.

Internet Access >> IPv6

v6 Mode	
Internet Access Mode	
Connection Type	DHCPv6 Client
DHCPv6 Client Configuratio	n
Identity Association	Prefix Delegation O Non-temporary Address
IAID (Identity Association ID	2567106181

ОК

Available settings are explained as follows:

Item	Description
Identify Association	Choose Prefix Delegation or Non-temporary Address as the identify association.
IAID	Type a number as IAID.

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

IPv6 – Static IPv6

This type allows you to setup static IPv6 address for WAN interface.

Internet Access >> IPv6

nternet Access Mode	
Connection Type	Static IPv6
Static IPv6 Address configuration	
IPv6 Address	/ Prefix Length
	/ Add Delete
Current IPv6 Address Table	
Index IPv6 Address/Prefix Length	Scope

Available settings are explained as follows:

Item	Description		
Static IPv6 Address	IPv6 Address – Type the IPv6 Static IP Address.		



configuration	Prefix Length – Type the fixed value for prefix length.
	Add – Click it to add a new entry.
	Delete – Click it to remove an existed entry.
Current IPv6 Address Table	Display current interface IPv6 address.

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

4.1.5 Multi-PVCs

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

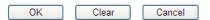
General

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

Internet Access >> Multi-PVCs

Genera	d 👘	ATM Qos	S	Port-based	Bridge	PVC to	PVC Binding/Add Tag
Channel		Enable	VPI	VCI	QoS Type	Protocol	Encapsulation
1.			0	33	UBR 🔽	PPPoE 💌	LLC/SNAP
2.			0	88	UBR 💌	MPoA 💌	1483 Bridged IP LLC
3.	WAN		1	43	UBR 🔽	PPPoA 🗸	VC MUX
4.	<u>WAN</u>		1	44	UBR 🗸	PPPoA 🗸	VC MUX 🗸
5.	WAN		1	45	UBR 🗸	PPPoA 🗸	VC MUX 🗸
6.			1	46	UBR 🗸	PPPoA 🗸	VC MUX
7.			1	47	UBR 🗸	PPPoA 🗸	VC MUX
8.			1	48	UBR 🗸	PPPoA 🗸	VC MUX

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



Available settings are explained as follows:

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

	PPPoE V PPPoA PPPoE MPoA	
Encapsulation		pe for this channel. The types will be to the protocol setting that you choose. Encapsulation
		1483 Bridged IP LLC
	Encapsulation	1483 Bridged IP LLC 1483 Route IP LLC 1483 Bridged IP VC-Mux 1483 Routed IP VC-Mux(IPoA) 1483 Bridged IP(IPoE)

WAN link for Channel 3, 4, 5

WAN link for Channel 3, 4, 5 are provided for router-borne application such as TR-069 and VoIP. The settings must be applied and obtained from your ISP. For your special request, please contact with your ISP and then click WAN link of Channel 3, 4 or 5 to configure your router.

WAN for Router-borne App	plication: Management	*			
O Enable					
DSL Modem Settings					
VPI 1	QoS Type	UBR 🖌	PVC Binding	Disable 👻	
VCI 43	Protocol	PPPoA 🐱	Add Tag 📃	0	
	Encapsulation	VC MUX 🔽			
WAN Connection Detection					
Mode	ARP Dete	ct 🚩			
Ping IP					
TTL:					
PPPoE/PPPoA Client		MPoA (RF	C1483/2684)		
ISP Access Setup		🔿 Obtain	an IP address	automatically	r
ISP Name		Router N	ame	Vigor	*
Username		Domain N	ame		*
Password		*: Requir	ed for some ISF	s	
PPP Authentication	PAP or CHAP	Specify	y an IP address	5	
Always On		IP Addres	s		
Idle Timeout	-1 second(s)	Subnet N	lask		
IP Address From ISP		Gateway	IP Address		
Fixed IP 🛛 🔿 Yes 💿 No	(Dynamic IP)	DNS Serv	er IP Address		
Fixed IP Address		Primary IP	Address		

Dray Tek

Item	Description
WAN for Router-borne Application	 Choose the router service for channel 3, 4 or 5. Management - It can be specified for general management (Web configuration/telnet/TR069). If you choose Management, the configuration for this PVC will be effective for Web configuration/telnet/TR069. VoIP - It can be specified for VoIP only. If you choose VoIP, the configuration for this PVC will be effective for VoIP data transmitting and receiving.
Enable/Disable	Click Enable for activating this function. If you click Disable , this function will be closed and all the settings that you adjusted in this page will be invalid.
DSL Modem Settings	 Set up the DSL parameters required by your ISP. These are vital for building DSL connection to your ISP. VPI - Type in the value provided by ISP. VCI - Type in the value provided by ISP. QoS Type -Select a proper QoS type for the channel. Protocol - Select a proper protocol for this channel. There are three options, PPPoE, PPPoA and MPoA for you to select. The following settings will be changed according to the protocol selected here. Encapsulating Type - Drop down the list to choose the type provided by ISP. PVC Binding – Use the drop down list to specify one PVC to be bound with other channel. Add Tag – Check the box to enable the function. Type the tag number in this field for this channel.
WAN Connection Detection	 Such function allows you to verify whether network connection is alive or not through ARP Detect or Ping Detect. Mode – Choose ARP Detect or Ping Detect for the system to execute for WAN detection. Ping IP – If you choose Ping Detect as detection mode, you have to type IP address in this field for pinging. TTL (Time to Live) – Displays value for your reference. TTL value is set by telnet command.
ISP Access Setup	 Enter your allocated username, password and authentication parameters according to the information provided by your ISP. If you want to connect to Internet all the time, you can check Always On. Username – Type in the username provided by ISP in this field. Password – Type in the password provided by ISP in this field. PPP Authentication – Select PAP only or PAP or CHAP for PPP.



	Idle Timeout – Set the timeout for breaking down the Internet after passing through the time without any action. This setting is active only when the Always On option is note selected.
IP Address from ISP	Fixed IP - Click Yes to use this function and type in a fixed IP address in the box of Fixed IP Address.Fixed IP Address -Type a fixed IP address.
Obtain an IP address automatically	Click this button to obtain the IP address automatically. Router Name – Type in the router name provided by ISP. Domain Name – Type in the domain name that you have assigned.
Specify an IP address	Click this radio button to specify some data. IP Address – Type in the private IP address. Subnet Mask – Type in the subnet mask. Gateway IP Address – Type in gateway IP address.
DNS Server IP Address	Type in the primary IP address for the router. If necessary, type in secondary IP address for necessity in the future.

After finishing all the settings here, please click **OK** to save the configuration.

ATM QoS

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

ılti-PVCs General	ATM QoS	Port-based Bridge	PVC to PVC	Binding/Add Tag
Channel	QoS Type	PCR	SCR	MBS
1.	UBR 🗸	0	0	0
2.	UBR 🗸	0	0	0
з.	UBR 🗸	0	0	0
4.	UBR 🗸	0	0	0
5.	UBR 🗸	0	0	0
6.	UBR 💌	0	0	0
7.	UBR 🗸	0	0	0
	UBR 🔽	0	0	0

Available settings are explained as follows:

Item	Description
QoS Type	Select a proper QoS type for the channel according to the information that your ISP provides.
PCR	It represents Peak Cell Rate. The default setting is "0".
SCR	It represents Sustainable Cell Rate. The value of SCR must be smaller than PCR.
MBS	It represents Maximum Burst Size. The range of the value is 10 to 50.

After finishing all the settings here, please click **OK** to save the configuration.

Port-based Bridge

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

General	ATM QoS	Po	rt-based B	ridge		PVC to F	VC Binding/Add Tag
Channel	En	able	P1	P2	P3	P4	Service Type
1.							Normal 😽
2.							Normal 🐱
3.							Normal 💌
4.							Normal 💌
5.							Normal 🛩
6.							Normal 💌
7.							Normal 🐱
8.							Normal 💌



2.P1 is reserved for Nat/Route use.

OK]	Clear	Cancel

Available settings are explained as follows:

Item	Description
Enable	Check this box to enable that channel. Only channel 3 to 8 can be set in this page, for channel 1 to 2 are reserved for NAT using.
P1 to P4	It means the LAN port 1 to 4. Check the box to designate the LAN port for channel 3 to 8.
Service Type	Normally, service type is used for the service of video stream (e.g., IPTV). It can divide the packets from remote control and from video stream into different PVC. In general, the protocol used by remote control is IGMP. Normal IGMP Normal – It means that the PVC can accept all packets except IGMP. IGMP – It means that the PVC can accept packets of IGMP only.
Add Tag	To identify the usage of PVC, check this box to invoke this setting. And type the number for VLAN ID (number).
Priority	To add the packet priority number for such VLAN. The range is from 0 to 7.

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



PVC to PVC Binding/Add Tag

This feature can direct certain services (such as Internet, IPTV and so on) from other channels into a single channel.

ulti-PVCs							
General	ATM QoS	Port-ba	sed Brid	lge	PVC to F	VC Binding/A	dd Tag
Channel		PVC Bindin	g		Add Tag		Priority
1.		Disable 🗸			0		0
2.		Disable 💙			0		0
з.		Disable 💌]		0		0
4.		Disable 💌]		0		0
5.		Disable 💌]		0		0
6.		Disable 1			0		0
7.		2			0		0
8.		4			0		0
	hannels may us /C Binding only				gh the PVC Bindir 3 Bridge mode.	ng configuratior	1.
		ОК		Clear	Cancel		

Available settings are explained as follows:

Item	Description
PVC Binding	Data transmitted through the selected channel will be redirected and transmitted via the channel configured in the field of PVC Binding.
Add Tag	To identify the usage of PVC, check this box to invoke this setting. And type the number for VLAN ID (number).
Priority	To add the packet priority number for such VLAN. The range is from 0 to 7.

After finishing all the settings here, please click **OK** to save the configuration.

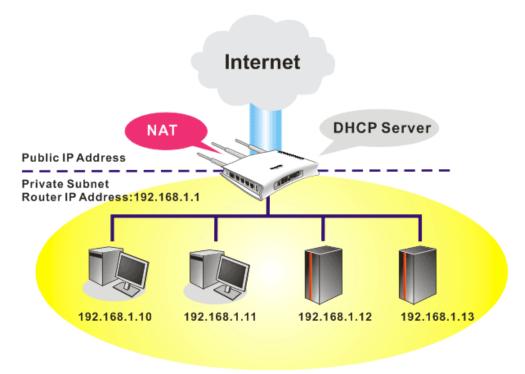
4.2 LAN

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



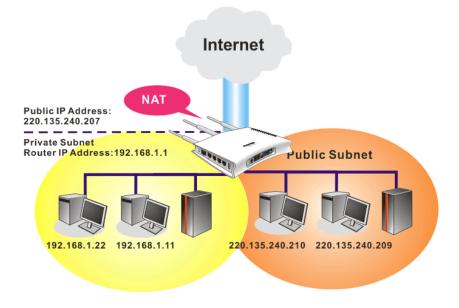
4.2.1 Basics of LAN

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



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





What is Routing Information Protocol (RIP)

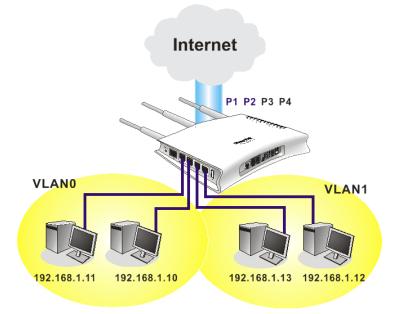
Vigor router will exchange routing information with neighboring routers using the RIP to accomplish IP routing. This allows users to change the information of the router such as IP address and the routers will automatically inform for each other.

What is Static Route

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

What are Virtual LANs

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





4.2.2 General Setup

This page provides you the general settings for LAN.

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

Details Page for Ethernet TCP/IP and DHCP Setup

Ethernet TCP / IP a	nd DHCP Setup		LAN 1 IPv6 Setup		
LAN IP Network Confi	guration		DHCP Server Configurat	tion	
For NAT Usage		_	💿 Enable Server 🔘 Disab	ole Server	
1st IP Address	192.168.1.1		Relay Agent: O 1st Subne	et 🔿 2nd Subnet	
1st Subnet Mask	255.255.255.0		DHCP Server IP Address		
For IP Routing Usage (🕽 Enable 💿 Disable		Start IP Address	192.168.1.10	
2nd IP Address	192.168.2.1		IP Pool Counts	150	
2nd Subnet Mask	255.255.255.0		Gateway IP Address	192.168.1.1	
	2nd Subnet DHCP Server		Lease Time	259200	(s)
RIP Protocol Control	Disable 💌		DNS Server IP Address		
			Primary IP Address		
			Secondary IP Address		
			Force router to use a	ddress for DNS	

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

	🗿 http://192.168.1.1 - Router Web Configurator - Microsoft Internet Explorer
	2nd DHCP Server Start IP Address IP Pool Counts 0 (max. 10) Index Matched MAC Address given IP Address MAC Address : ::::::::::::::::::::::::::::::::::::
	 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 with neighboring routers.
DHCP Server Configuration	DHCP stands for Dynamic Host Configuration Protocol. The router by factory default acts a DHCP server for your network so it automatically dispatch related IP settings to any local user configured as a DHCP client. It is highly recommended that you leave the router enabled as a DHCP



	server if you do not have a DHCP server for your network.
	If you want to use another DHCP server in the network other than the Vigor Router's, you can let Relay Agent help you to redirect the DHCP request to the specified location.
	Enable Server - Let the router assign IP address to every host in the LAN.
	Disable Server – Let you manually assign IP address to every host in the LAN.
	Relay Agent – $(1^{st} \text{ subnet}/2^{nd} \text{ subnet})$ Specify which subnet that DHCP server is located the relay agent should redirect the DHCP request to.
	DHCP Server IP Address - 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.
	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.
	Lease Time – Enter the time to determine how long the IP address assigned by DHCP server can be used.
DNS Server IP Address	DNS stands for Domain Name System. Every Internet host must have a unique IP address, also they may have a human-friendly, easy to remember name such as www.yahoo.com. The DNS server converts the user-friendly name into its equivalent IP address.
	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:
	Physical Connection System Uptime: 0day 1:36:54 IPv4 IPv6 LAN Status Primary DNS: 8.8.8.8 Secondary DNS: 8.8.4.4
	IP Address IX Packets IX Packets 192.168.1.1 37067 40850
	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.
Force router to use address for DNS - Force Vigor router to use DNS servers in this page instead of DNS servers given by the Internet Access server (PPPoE, PPTP, L2TP or DHCP server).

After finishing all the settings here, please click **OK** to save the configuration.

Details Page for LAN1 – IPv6 Setup

There are two configuration pages for LAN1, Ethernet TCP/IP and DHCP Setup (based on IPv4) and IPv6 Setup. Click the tab for each type and refer to the following explanations for detailed information. Below shows the settings page for IPv6.

LAN >> General Setup

RADVD Configuration	
Enable Obisable	
Advertisement Lifetime 1800 Seconds (Range : 600 - 9000)
OHCPv6 Server Configuration O Enable Server O Disable Server	
Start IPv6 Address	
End IPv6 Address	
DNS Server IPv6 Address	
Primary DNS Server	
Secondary DNS Server	
Static IPv6 Address configuration	
IPv6 Address	/ Prefix Length
Current IPv6 Address Table	/ Add Delete
Current IPV6 Address Table	Scope
Index IDes Address (Destin Isenth	acope
Index IPv6 Address/Prefix Length 1 FE80::250:7FFF:FE92:F500/64	Link
	Link

OK

It provides 2 daemons for LAN side IPv6 address configuration. One is **RADVD**(stateless) and the other is **DHCPv6 Server** (Stateful).

Item	Description	
RADVD Configuration	Enable – Click it to enable RADVD server. The router advertisement daemon (radvd) sends Router Advertisement messages, specified by RFC 2461, to a local Ethernet LAN periodically and when requested by a node sending a Router Solicitation message. These messages are required for IPv6 stateless auto-configuration.	
	Disable – Click it to disable RADVD server.	
	Advertisement Lifetime - The lifetime associated with the default router in units of seconds. It's used to control the lifetime of the prefix. The maximum value corresponds to 18.2 hours. A lifetime of 0 indicates that the router is not a default router and should not appear on the default router list.	
DHCPv6 Server Configuration	Enable Server –Click it to enable DHCPv6 server. DHCPv6 Server could assign IPv6 address to PC according to the Start/End IPv6 address configuration.	
	Disable Server – Click it to disable DHCPv6 server.	
	Start IPv6 Address / End IPv6 Address – Type the start and end address for IPv6 server.	
DNS Server IPv6 Address	Primary DNS Sever – Type the IPv6 address for Primary DNS server.	
	Secondary DNS Server – Type another IPv6 address for DNS server if required.	
Static IPv6 Address	IPv6 Address – Type static IPv6 address for LAN.	
configuration	Prefix Length – Type the fixed value for prefix length.	
	Add – Click it to add a new entry.	
	Delete – Click it to remove an existed entry.	
Current IPv6 Address Table	Display current used IPv6 addresses.	

Available settings are explained as follows:

After finishing all the settings here, please click **OK** to save the configuration.

4.2.3 Static Route

Go to **LAN** to open setting page and choose **Static Route**. The router offers IPv4 and IPv6 for you to configure the static route. Both protocols bring different web pages.

Static Route for IPv4

LAN >> Static Route Setup

IPv4		IPv6		<u>S</u> e	et to Factory Default View Ro	uting Table
Index	Dest	ination 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

Each item is explained as follows:

Item	Description				
Set to Factory Default	Clear all of the settings and return to factory default settings.				
Viewing Routing Table	Displays the routing table for your reference. Diagnostics >> View Routing Table Current Running Routing Table Rey: C - connected, S - static, R - RIP, * - default, ~ - private C~ 192.168.1.0/ 255.255.255.0 is directly connected, LAN				
Index	The number (1 to 10) under Index allows you to open next page to set up static route.				
Destination Address	Displays the destination address of the static route.				
Status	Displays the status of the static route.				

Static Route for IPv6

You can set up to 40 profiles for IPv6 static route. Click the IPv6 tab to open the following page:

LAN >>	Static	Route	Setu	þ
--------	--------	-------	------	---

IPv4		IPv6		Set to F	actory Default View IPv6 Ro	uting Table
Index	Desti	ination Address	Status	Index	Destination Address	Status
<u>1.</u>		::/0	х	<u>11.</u>	::/0	х
<u>2.</u>		::/0	х	<u>12.</u>	::/0	х
<u>3.</u>		::/0	х	<u>13.</u>	::/0	х
<u>4.</u>		::/0	х	<u>14.</u>	::/0	х
<u>5.</u>		::/0	х	<u>15.</u>	::/0	х
<u>6.</u>		::/0	х	<u>16.</u>	::/0	х
<u>7.</u>		::/0	х	<u>17.</u>	::/0	х
<u>8.</u>		::/0	х	<u>18.</u>	::/0	х
<u>9.</u>		::/0	x	<u>19.</u>	::/0	х
<u>10.</u>		::/0	х	<u>20.</u>	::/0	х
<< <u>1 - 20 21</u>	- 40 >>					<u>Next</u> >>

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

Each item is explained as follows:

Item	Description
Set to Factory Default	Clear all of the settings and return to factory default settings.
Viewing IPv6 Routing Table	Displays the routing table for your reference.
Index	The number (1 to 40) under Index allows you to open next page to set up static route.
Destination Address	Displays the destination address of the static route.
Status	Displays the status of the static route.

Click any underline of index number to get the following page.

LAN >> Static Route Setup

Index No. 1		
Destination IPv6 Address / Prefix Len	::	/ 0
Gateway IPv6 Address]
Network Interface	LAN 🗸	
OK	Cancel Delete	

Available settings are explained as follows:

Item	Description
Enable	Click it to enable this profile.

Dray Tek

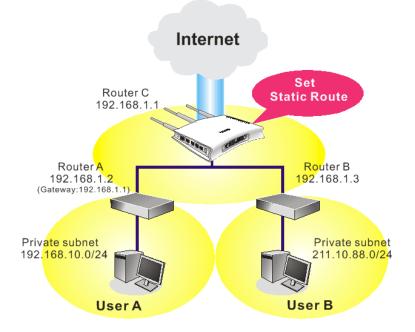
Destination IPv6 Address / Prefix Len	Type the IP address with the prefix length for this entry.
Gateway IPv6 Address	Type the gateway address for this entry.
Network Interface	Use the drop down list to specify an interface for this static route.

Add Static Routes to Private and Public Networks (based on IPv4)

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

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

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



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

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



via the router, and continuously exchange of IP routing information with different subnets.

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

🛛 Enable			
	Destination IP Address	192.168.10.0	
	Subnet Mask	255.255.255.0	
	Gateway IP Address	192.168.1.2	
	Network Interface	LAN 🔽	

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.

dex No. 1		
🗹 Enable		
	Destination IP Address	211.100.88.0
	Subnet Mask	255.255.255.0
	Gateway IP Address	192.168.1.3
	Network Interface	LAN 🔽

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

Diagnostics >> View Routing Table

LAN >> Static Route Setup

Key: C	- connected, S -	static, R - RIP, * - default, ~ - priv	vate 🔼
3~ C~		255.255.255.0 via 192.168.1.2, LA 255.255.255.0 is directly connected,	
3~	211.100.88.0/	255.255.255.0 via 192.168.1.3, LA	N
			~

Dray Tek

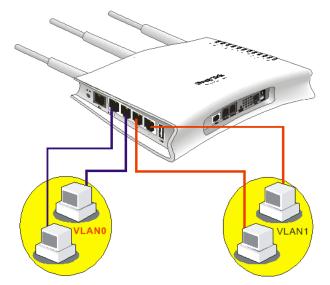
4.2.4 VLAN

Virtual LAN function provides you a very convenient way to manage hosts by grouping them based on the physical port. Go to **LAN** page and select **VLAN**. The following page will appear. Click **Enable** to invoke VLAN function.

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

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

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



LAN >> VLAN Configuration

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

🗹 Enable				
	P1	P2	P3	P4
VLANO	✓			
VLAN1				
VLAN2				
VLAN3				

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



4.2.5 Bind IP to MAC

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

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

LAN	>>	Bind	IP to	MAC
		Dillia		

○ Enable		
ARP Table Select All Sort Refresh	IP Bind List	Select All Sort
IP Address Mac Address 192.168.1.5 00-50-7F-CD-07-48 192.168.1.49 E0-CB-4E-DA-48-79	Index IP Address	Mac Address
Add or Update		
Comment	Update Delete	Show Comment

OK

Item	Description
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.
Select All	Click this link to select all the items in the ARP table.
Sort	Reorder the table based on the IP address.

Refresh	Refresh the ARP table listed below to obtain the newest ARP table information.
IP Bind List	It displays a list for the IP bind to MAC information.
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.
	Comment – Type a brief description for the entry.
	Show Comment – Check it to display the content of the comment.
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 .
Update	It allows you to edit and modify the selected IP address and MAC address that you create before.
Delete	You can remove any item listed in IP Bind List . Simply click and select the one, and click Delete . The selected item will be removed from the IP Bind List .

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

4.3 NAT

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

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

The benefit of the NAT includes:

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

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

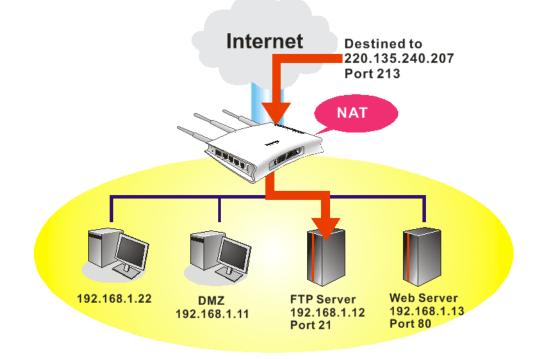


Below shows the menu items for NAT.



4.3.1 Port Redirection

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



The port redirection can only apply to incoming traffic.

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

NAT >> Port Redirection

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

Each item is explained as follows:

Item	Description
Index	Display the number of the profile.
Service Name	Display the description of the specific network service.
WAN Interface	Display the WAN IP address or interface used by the profile.
Protocol	Display the transport layer protocol (TCP or UDP).
Public Port	Display the port number which will be redirected to the specified Private IP and Port of the internal host.
Private IP	Display the IP address of the internal host providing the service.
Status	Display if the profile is enabled (v) or not (x).

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

NAT >> Port Redirection

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

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

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



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

After finishing all the settings here, please click **OK** to save the configuration.

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

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

System Maintenance >> Management

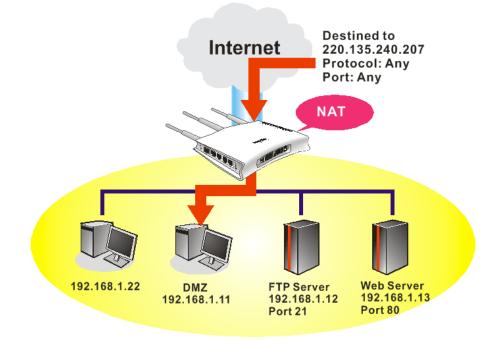
IPv4 Manageme	nt Setup IP	v6 Management Setup	
Router Name		Management Port Set	up
		Oser Define Ports	O Default Ports
Management Access C	ontrol	Telnet Port	23 (Default: 23)
Allow management from the second s	om the Internet	HTTP Port	80 (Default: 80)
FTP Server		HTTPS Port	443 (Default: 443)
HTTP Server		FTP Port	21 (Default: 21)
HTTPS Server		SSH Port	
Itelnet Server		SSH POIL	22 (Default: 22)
SSH Server		SNMP Setup	
Disable PING from the	Internet	Enable SNMP Agent	:
Access List		Get Community	public
List IP	Subnet Mask	Set Community	private
1	~	Manager Host IP	
2	~	Trap Community	public
3	~	Notification Host IP	
		Trap Timeout	10 seconds

OK

Dray Tek

4.3.2 DMZ Host

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



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

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

NAT >> DMZ Host Setup

	WAN1
AN 1	
None 🔽	
Private IP	Choose PC
MAC Address of the True IP DM	IZ Host 00 . 00 . 00 .00 .00 .00
Note: When a True-IP DMZ host be always on.	is turned on, it will force the router's WAN connection to

0K

Item	Description
WAN 1	Choose None, Private IP or Active True IP first.
None 💙	Active True IP selection is available for WAN1 only.



	None None Private IP Active True IP ft
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.

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

VAT >> D	MZ Host S	etup		
OMZ Host	Setup			
			WAN1	
WAN 1 Index	Enable	Aux. WAN IP	Private IP	
1.			0.0.0	Choose PC
2.		192.168.1.23	0.0.0	Choose PC
		(OK Clear	

Item	Description
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.
	🕋 http://19 💶 🗖 🔀
	192.168.1.10 192.168.1.18
	Without and the standard and the standard standard standard standards and the standard stan
	When you have selected one private IP from the above dialog, the IP address will be shown on the following screen. Click OK to save the setting.
	DMZ Host Setup WAN1
	WAN 1 Private IP 1. 0.0.0 Choose PC 2. I 192.168.1.23 192.168.1.11 Choose PC
	OK

4.3.3 Open Ports

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

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

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

NAT >> Open Ports

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

Each item is explained as follows:

Item	Description
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	Display the name for the defined network service.
Local IP Address	Display the private IP address of the local host offering the service.
Status	Display the state for the corresponding entry. X or V is to represent the Inactive or Active state.

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

NAT >> Open Ports >> Edit Open Ports

Inc	lex.	NO.	. 1

	С	omment	P2F)			
	W	'AN IP	192	.168.1.23	*		
	Lo	ocal Computer	192.	168.1.11	Choose	PC	
	Protocol	Start Port	End Port		Protocol	Start Port	End Port
1.	ТСР	4500	4700	6.	💌	0	0
2.	UDP	4500	4700	7.	💙	0	0
з.		0	0	8.	💙	0	0
4.		0	0	9.	💙	0	0
5.			0	10.	💙	0	0

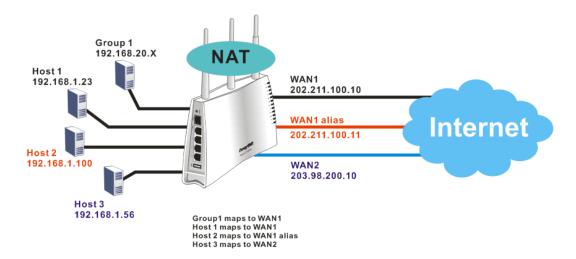
Each item is explained as follows:

Item	Description	
Enable Open Ports	Check to enable this entry.	
Comment	Make a name for the defined network application/service.	
WAN IP	Specify the WAN IP address that will be used for this entry. This setting is available when WAN IP Alias is configured.	
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.	

After finishing all the settings here, please click **OK** to save the configuration.

4.3.4 Address Mapping

Address Mapping is used to map a specified private IP or a range of private IPs of NAT subnet into a specified WAN IP (or WAN IP alias IP). Refer to the following figure.



Suppose the WAN settings for a router are configured as follows:

WAN1: 202.211.100.10, WAN1 alias: 202.211.100.11 WAN2: 203.98.200.10

Without address mapping feature, when a NAT host with an IP say "192.168.1.10" sends a packet to the WAN side (or the Internet), the source address of the NAT host will be mapped into either 202.211.100.10 or 203.98.200.10 (which IP or mapping is decided by the internal load balancing algorithm).

With address mapping feature, you can manually configure any host mapping to any WAN interface to fit the request. In the above example, you can configure NAT Host1 to always map to 202.211.100.10 (WAN1); Host2 to always map to 202.211.100.11 (WAN1 alias); Host3 always map to 203.98.200.10 (WAN2) and Group 1 to always map to 202.211.100.10 (WAN1).

Index	Protocol	Public IP	Private IP	Mask	Status
<u>1.</u>	ALL			/32	х
<u>2.</u>	ALL			/32	х
<u>3.</u>	ALL			/32	х
<u>4.</u>	ALL			/32	х
<u>5.</u>	ALL			/32	х
<u>6.</u>	ALL			/32	х
<u>7.</u>	ALL			/32	х
<u>8.</u>	ALL			/32	х
<u>9.</u>	ALL			/32	х
10.	ALL			/32	х

NAT >> Address Mapping

Item	Description	
Index	Indicate the relative number for the particular entry that you want to configure You should click the appropriate index	



	number to edit or clear the corresponding entry.	
Protocol	Display the protocol used for this address mapping.	
Public IP	Display the public IP address selected for this entry, e.g., 172.16.3.102.	
Private IP	Display the private IP set for this address mapping, e.g., 192.168.1.10.	
Mask	Display the subnet mask selected for this address mapping.	
Status	Display the status for the entry, enable or disable.	

Click the index number link to open the configuration page.

NAT >> Address Mapping

Index No. 1	
🗹 Enable	
Protocol:	ALL 💌
WAN Interface	WAN1 💌
WAN IP	×
Private IP:	
Subnet Mask:	/32 💌
-	OK Clear Cancel

Available settings are explained as follows:

Item	Description		
Enable	Check to enable this entry.		
Protocol	Specify the transport layer protocol. It could be TCP , UDP , or ALL for selection.		
WAN Interface	Choose the WAN interface for such address mapping profile.		
WAN IP	This is the source IP of a packet captured on the WAN side and sent by a NAT host specified in the Private IP field. The drop down menu contains WAN interface IPs and WAN IP alias IPs.		
Private IP	This is the source IP of a NAT host which wishes to send packets to the WAN side and have source address as configured in the WAN IP field.		
Subnet Mask	Select a value of subnet mask for private IP address.		

After finishing all the settings here, please click **OK** to save the configuration.



4.4 Firewall

4.4.1 Basics for Firewall

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

Firewall Facilities

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

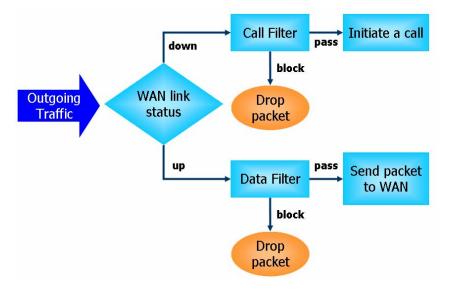
- User-configurable IP filter (Call Filter/ Data Filter).
- Stateful Packet Inspection (SPI): tracks packets and denies unsolicited incoming data
- Selectable Denial of Service (DoS) /Distributed DoS (DDoS) attacks protection

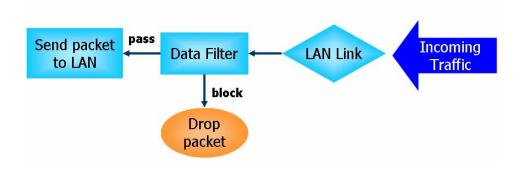
IP Filters

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

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

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





Stateful Packet Inspection (SPI)

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

Denial of Service (DoS) Defense

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

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

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

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

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

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

Below shows the menu items for Firewall.

Firewall

General Setup
Filter Setup
DoS Defense

4.4.2 General Setup

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

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

l Setup		
neral Setup	Default Rule	
Call Filter	 Enable 	Start Filter Set Set#1 🗸
	O Disable	
Data Filter	 Enable 	Start Filter Set 🛛 Set#2 💌
	🔘 Disable	
🗹 Accept large	e incoming fragmented	UDP or ICMP packets (for some games, ex. CS)
🗹 Enable Stric	t Security Firewall	

Cancel

ΟK

Item	Description
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.
Accept large incoming	Some on-line games (for example: Half Life) will use lots of fragmented UDP packets to transfer game data. Instinctively as a secure firewall, Vigor router will reject these fragmented packets to prevent attack unless you enable "Accept large incoming fragmented UDP or ICMP Packets". By checking this box, you can play these kinds of on-line games. If security concern is in higher priority, you cannot enable "Accept large incoming fragmented UDP or ICMP Packets".
Enable Strict Security	Check the box to enable such function.
Firewall	For the sake of security, the router will execute strict security checking for data transmission.
	Such feature is enabled in default. All the packets, while transmitting through Vigor router, will be filtered by firewall. If the firewall system (e.g., content filter server) does not



	make any response (pass or block) for these packets, then the router's firewall will block the packets directly.
--	--

Default Rule Page

Such page allows you to choose filtering profiles including QoS, Load-Balance policy, WCF, APP Enforcement, URL Content Filter for data transmission via Vigor router.

Firewal	>>	General	Setup

General Setup	Default Rule			
Actions for de	fault rule:			
Application		Action/Profile	Syslog	
Filter		Pass 💌		
Sessions Cont	rol	0 / 11000		
Quality of Servio	<u>:e</u>	None 💌		
APP Enforcement	<u>nt</u>	None 💌		
URL Content Filt	er	None 💌		
Web Content Fil	ter	None 💙		
Advance Settin	g	Edit		

Item	Description	
Filter	Select Pass or Block for the packets that do not match with the filter rules.	
	Filter Pass V Pass Block	
Sessions Control	The number typed here is the total sessions of the packets that do not match the filter rule configured in this page. The default setting is 60000.	
Quality of Service	Choose one of the QoS rules to be applied as firewall rule. For detailed information of setting QoS, please refer to the related section later.	

Item	Description			
	None None Class 1 Class 2 Class 3 Default			
APP Enforcement	Select an APP Enforcement profile for global IM/P2P application blocking. If there is no profile for you to selelct, please choose [Create New] from the drop down list in this page to create a new profile. All the hosts in LAN must follow the standard configured in the APP Enforcement profile selected here. For detailed information, refer to the section of APP Enforcement profile setup. For troubleshooting needs, you can specify to record information for IM/P2P by checking the Log box. It will be sent to Syslog server. Please refer to section Syslog/Mail Alert for more detailed information.			
URL Content Filter	Select one of the URL Content Filter profile settings (created in CSM>> URL Content Filter) for applying with this router. Please set at least one profile for choosing in CSM>> URL Content Filter web page first. Or choose [Create New] from the drop down list in this page to create a new profile. For troubleshooting needs, you can specify to record information for URL Content Filter by checking the Log box. It will be sent to Syslog server. Please refer to section Syslog/Mail Alert for more detailed information.			
Web Content Filter	Select one of the Web Content Filter profile settings (created in CSM>> Web Content Filter) for applying with this router. Please set at least one profile for anti-virus in CSM>> Web Content Filter web page first. Or choose [Create New] from the drop down list in this page to create a new profile. For troubleshooting needs, you can specify to record information for Web Content Filter by checking the Log box. It will be sent to Syslog server. Please refer to section Syslog/Mail Alert for more detailed information.			
Advance Setting	Click Edit to open the following window. However, it is strongly recommended to use the default settings here.			
	http://192.168.1.5/doc/ipfgenady.htm - Microsoft Internet Explorer Firewall >> General Setup Advance Setting Codepage ANSI(1252)-Latin I Window size: 65535 Session timeout: 1440 OK Close			
	Codepage - This function is used to compare the characters among different languages. Choose correct codepage can help the system obtaining correct ASCII after decoding data from			



Item	Description
	URL and enhance the correctness of URL Content Filter. The default value for this setting is ANSI 1252 Latin I. If you do not choose any codepage, no decoding job of URL will be processed. Please use the drop-down list to choose a codepage. If you do not have any idea of choosing suitable codepage, please open Syslog. From Codepage Information of Setup dialog, you will see the recommended codepage listed on the dialog box.
	Window size – It determines the size of TCP protocol $(0\sim65535)$. The more the value is, the better the performance will be. However, if the network is not stable, small value will be proper.
	Session timeout – Setting timeout for sessions can make the best utilization of network resources.

4.4.3 Filter Setup

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

Firewall >> Filter Setup

lter Se	etup		Set to Factory Defau
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.

Firewall >> Filter Setup >> Edit Filter Set

Filter Set 1						
Comments :	Default Call Filter					
Filter Rule	Active		Comments		Move Up	Move Down
1			Block NetBio	s		<u>Down</u>
2					<u>UP</u>	<u>Down</u>
3					<u>UP</u>	<u>Down</u>
4					<u>UP</u>	<u>Down</u>
5					<u>UP</u>	<u>Down</u>
6					<u>UP</u>	<u>Down</u>
7					<u>UP</u>	
					Next Filter	• Set None 💌
		OK	Clear	Cancel		

Available settings are explained as follows:

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

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

Firewall >> Edit Filter Set >> Edit Filter Rule

Check to enable the Filter Rule		
Comments:	Block NetBios	
Index(1-15) in <u>Schedule</u> Setup:	,,,,	
Clear sessions when schedule ON:	Enable	
Direction:	LAN/RT/VPN -> WAN	
Source IP:	Any	Edit
Destination IP:	Any	Edit
Service Type:	TCP/UDP, Port: from 137~139 to any	Edit
Fragments:	Don't Care 🗸	
Application	Action/Profile	Syslog
Filter:	Block Immediately	
Branch to Other Filter Set:	None 🗸	
Sessions Control	0 / 11000	
MAC Bind IP	Non-Strict 🐱	
Quality of Service	None 🗸	
APP Enforcement:	None 🗸	
URL Content Filter:	None 🗸	
Web Content Filter:	None 😽	
Advance Setting	Edit	

Available settings are explained as follows:

Item	Description	
Check to enable the Filter Rule	Check this box to enable the filter rule.	
Comments	Enter filter set comments/description. Maximum length is 14- character long.	
Index(1-15)	Set PCs on LAN to work at certain time interval only. You may choose up to 4 schedules out of the 15 schedules pre-defined in Applications >> Schedule setup. The default setting of this field is blank and the function will always work.	
Clear sessions when schedule ON	Check this box to clear all the sessions when the schedule is configured and specified above.	
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. LAN/RT/VPN -> WAN WAN -> LAN/RT/VPN LAN/RT/VPN -> LAN/RT/VPN LAN/RT/VPN -> LAN/RT/VPN LAN/RT/VPN -> LAN/RT/VPN	

Source/Destination IP	source/destination IP or IP ranges.				
	IP Address Edit - Windows Internet Explorer				
	http://192.168.1.1/doc/pfipedt.htm				
	IP Address Edit				
	Address Type Any Address 🗸				
	Start IP Address 0.0.0.0				
	End IP Address 0.0.0.0				
	Subnet Mask 0.0.0.0				
	Invert Selection				
	or IP Groupt None v				
	or IP Object None 🗸				
	or IP Object None 🗸				
	IPv6 Group				
	or IPv6 Object None v				
	or IPv6 Object None 🗸				
	OK Close				
	Type. Group and Objects Any Address Single Address Subnet Address Subnet Address Group and Objects From the IP Group drop down list, choose the one that you want to apply. Or use the IP Object drop down list to choose the object that you want. Click Edit to access into the following dialog to choose a				
Service Type	suitable service type.				
	🗿 http://192.168.1.5 - Service Type Edit - Microsoft Internet Explorer				
	Service Type Edit				
	Service Type User defined 💌				
	Protocol TCP/UDP V Source Port = V 137 ~139				
	Source Port = 137 ~139				
	Source Port = 137 ~ 139 Destination Port = 1 ~ 65535 Service Group None ~ or Service Object None ~				
	Source Port = 137 ~ 139 Destination Port = 1 ~ 665535 Service Group None or Service Object None				
	Source Port = 137 ~ 139 Destination Port = 1 ~ 65535 Service Group None ~ or Service Object None ~ or Service Object None ~ or Service Object None ~				
	Source Port = 137 ~ 139 Destination Port = 1 ~ 665535 Service Group None or Service Object None				
	Source Port = 137 ~ 139 Destination Port = 1 ~ 66535 Service Group None ~ or Service Object None ~ or Service Object None ~ or Service Object None ~				
	Source Port = 137 ~ 139 Destination Port = 1 ~ 66535 Service Group None ~ or Service Object None ~ or Service Object None ~ or Service Object None ~				



	if you want to use the service type from defined groups or objects, please choose Group and Objects as the Service
	Type.
	User defined 🛛 👻
	User defined
	Group and Objects
	Protocol - Specify the protocol(s) which this filter rule will apply to.
	Source/Destination Port –
	(=) – when the first and last value are the same, it indicates one port; when the first and last values are different, it indicates a range for the port and available for this service type.
	(!=) – when the first and last value are the same, it indicates all the ports except the port defined here; when the first and last values are different, it indicates that all the ports except the range defined here are available for this service type.
	 (>) – the port number greater than this value is available. (<) – the port number less than this value is available for this profile.
	Service Group/Object - Use the drop down list to choose the one that you want.
Fragments	Specify the action for fragmented packets. And it is used for Data Filter only.
	<i>Don't care -</i> No action will be taken towards fragmented packets.
	<i>Unfragmented</i> - Apply the rule to unfragmented packets.
	<i>Fragmented</i> - Apply the rule to fragmented packets.
	<i>Too Short</i> - Apply the rule only to packets that are too short to contain a complete header.
Filter	Specifies the action to be taken when packets match the rule.
	Block Immediately - Packets matching the rule will be dropped immediately.
	Pass Immediately - Packets matching the rule will be passed immediately.
	Block If No Further Match - A packet matching the rule, and that does not match further rules, will be dropped.
	Pass If No Further Match - A packet matching the rule, and that does not match further rules, will be passed through.
Branch to other Filter Set	If the packet matches the filter rule, the next filter rule will branch to the specified filter set. Select next filter rule to branch from the drop-down menu. Be aware that the router will apply the specified filter rule for ever and will not return to previous filter rule any more.
Sessions Control	The number typed here is the total sessions of the packets that do not match the filter rule configured in this page. The default setting is 12000 .

MAC Bind IP	 When the IP Object Profile (with specified MAC Address and IP address for Address Type) is selected for Source IP /Destination IP setting, the system will process the packet according to the following rules: If the MAC address of the packet meets the specified MAC address listed in IP Object Profile, no matter which IP address that the packet is, it can pass through Vigor router easily. If the MAC address of the packet cannot meet the specified MAC address listed in IP Object Profile, the system will consider the IP settings (Non-Strict or Strict) to determine if the packet can pass or be blocked. If Non-Strict is selected: The packet can pass.
	If Strict is selected: The packet will be blocked.
Quality of Service	Choose one of the QoS rules to be applied as firewall rule. For detailed information of setting QoS, please refer to the related section later. None Class 1 Class 2 Class 3 Default
APP Enforcement	Select an APP Enforcement profile for global IM/P2P application blocking. If there is no profile for you to selelct, please choose [Create New] from the drop down list in this page to create a new profile. All the hosts in LAN must follow the standard configured in the APP Enforcement profile selected here. For detailed information, refer to the section of APP Enforcement profile setup. For troubleshooting needs, you can specify to record information for IM/P2P by checking the Log box. It will be sent to Syslog server. Please refer to section Syslog/Mail Alert for more detailed information.
URL Content Filter	Select one of the URL Content Filter profile settings (created in CSM>> URL Content Filter) for applying with this router. Please set at least one profile for choosing in CSM>> URL Content Filter web page first. Or choose [Create New] from the drop down list in this page to create a new profile. For troubleshooting needs, you can specify to record information for URL Content Filter by checking the Log box. It will be sent to Syslog server. Please refer to section Syslog/Mail Alert for more detailed information.
Web Content Filter	Select one of the Web Content Filter profile settings (created in CSM>> Web Content Filter) for applying with this router. Please set at least one profile for anti-virus in CSM>> Web Content Filter web page first. Or choose [Create New] from the drop down list in this page to create a new profile. For troubleshooting needs, you can specify to record information for Web Content Filter by checking the

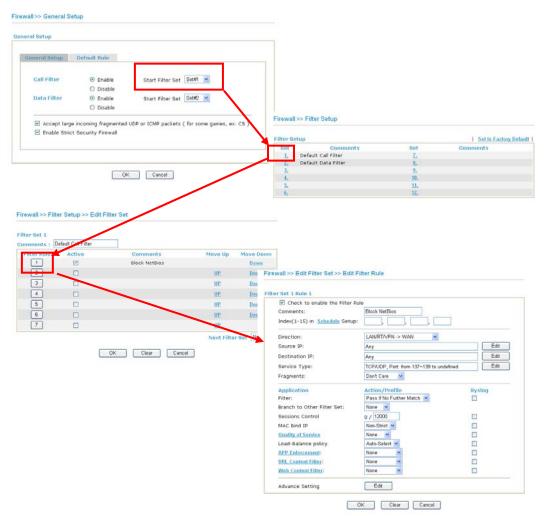


	Log box. It will be sent to Syslog server. Please refer to
	section Syslog/Mail Alert for more detailed information.
SysLog	For troubleshooting needs you can specify the filter log and/or CSM log here. Check the corresponding box to enable the log function. Then, the filter log and/or CSM log will be shown on Draytek Syslog window.
Advance Setting	Click Edit to open the following window. However, it is strongly recommended to use the default settings here.
	Firewall >> Edit Filter Set >> Edit Filter Rule
	Filter Set 1 Rule 1 Advance Setting Codepage ANSI(1252)-Latin I Window size: 65535 Session timeout: 1440 DrayTek Banner: Image: Codepage
	Strict Security Checking
	Codepage - This function is used to compare the characters
	 among different languages. Choose correct codepage can help the system obtaining correct ASCII after decoding data from URL and enhance the correctness of URL Content Filter. The default value for this setting is ANSI 1252 Latin I. If you do not choose any codepage, no decoding job of URL will be processed. Please use the drop-down list to choose a codepage. If you do not have any idea of choosing suitable codepage,
	please open Syslog. From Codepage Information of Setup dialog, you will see the recommended codepage listed on the dialog box.
	M DrayTek Syslog 3.9.1
	Controls IP2.168.1.1 WAN Information WAN1 IP (Fixed) I72.16.2.213
	TX Packets RX Packets WAN2 IP (Fixed) 28489 15285
	Setup
	Tool Setup Telnet Read-out Setup Codepage Information Codepage To Select Windows Version: 5.01.2600
	RECOMMENDED CODEPAGE: 950 (ANSI/OEM - Traditional Chinese Big5) 00a1:21 00a6:7c 00a9:63 00aa:61 00ad:2d 00ae:52 00b2:32 00b3:33 00b9:31 00ba:6f 0
	Window size – It determines the size of TCP protocol
	$(0\sim65535)$. The more the value is, the better the performance will be. However, if the network is not stable, small value
	will be proper.

Session timeout –Setting timeout for sessions can make the best utilization of network resources. However, Queue timeout is configured for TCP protocol only; session timeout is configured for the data flow which matched with the firewall rule.
DrayTek Banner – Please uncheck this box and the following screen will not be shown for the unreachable web page. The default setting is Enabled.
The requested Web page has been blocked by Web Content Filter. Please contact your system administrator for further information. [Powered by Draytek]
Strict Security Checking - All the packets, while transmitting through Vigor router, will be filtered by firewall settings configured by Vigor router. When the resource is inadequate, the packets will be blocked if Strict Security Checking is enabled. If Strict Security Checking is not enabled, then the packets will pass through the router.
<i>APP Enforcement</i> – Check this box to execute the critical checking for all the files transferred via IM/P2P.

Example

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



Dray Tek

4.4.4 DoS Defense

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

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

DoS defense Setup			
Enable DoS Defense Select All			
Enable SYN flood defense	Threshold	50	packets / sec
	Timeout	10	sec
Enable UDP flood defense	Threshold	150	packets / sec
	Timeout	10	sec
Enable ICMP flood defense	Threshold	50	packets / sec
	Timeout	10	sec
Enable Port Scan detection	Threshold	150	packets / sec
Block IP options	Block TCP flag s	scan	
Block Land	Block Tear Drop		
Block Smurf	Block Ping of Death		
Block trace route	Block ICMP frag	ment	
Block SYN fragment	Block Unassigne	ed Numbers	
Block Fraggle Attack			
			~
			~
OK	ar All Cancel		

Available settings are explained as follows:

Item	Description	
Enable Dos Defense	Check the box to activate the DoS Defense Functionality.	
Select All	Click this button to select all the items listed below.	
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. That means, when 50 packets per second received, they will be regarded as "attack event" and the session will be paused for 10 seconds.	
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	



Item	Description	
	period defined in Timeout. The default setting for threshold and timeout are 150 packets per second and 10 seconds, respectively. That means, when 150 packets per second received, they will be regarded as "attack event" and the session will be paused for 10 seconds.	
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. That means, when 50 packets per second received, they will be regarded as "attack event" and the session will be paused for 10 seconds.	
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. That means, when 150 packets per second received, they will be regarded as "attack event".	
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	

Description		
fraggle attack defense, all broadcast UDP packets coming from the Internet are blocked. Therefore, the RIP packets from the Internet might be dropped.		
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</i> <i>scan</i> , <i>SYN FINscan</i> , <i>Xmas scan</i> and <i>full Xmas scan</i> .		
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.		
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.		
Check the box to activate the Block ICMP fragment function. Any ICMP packets with more fragment bit set are dropped.		
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.		
We provide Syslog function for user to retrieve message from Vigor router. The user, as a Syslog Server, shall receive the report sending from Vigor router which is a Syslog Client. All the warning messages related to DoS Defense will be sent to user and user can review it through Syslog daemon. Look for the keyword DoS in the message, followed by a name to indicate what kind of attacks is detected. System Maintenance >> SysLog / Mail Alert Setup SysLog / Meil Alert Set		

Item	Description
	Controls 192.160.1.1 WAN 2.30.4 TX Packets Vars Series Vars Series 172.16.3.4 343 3 1417 South Sold 172.16.3.4 343 3 172.16.3.29 2050 126 126 Thread Lag Sold 172.16.3.29 2050 126
	Tense Host Message fm 10000-42 Vagor Decircup, Bood Blocks(00) 1922 (160 ± 115,10665 1122 (160 ± 112,2) 286 ± 115,10655 1122 (160 ± 112,2) 286 ± 1122 ± 1000 ± 10000 ± 1000 ± 1000 ± 1000 ± 10000 ± 10000 ± 10000 ± 10000 ± 10000 ± 10000 ± 10000 ±
	ACQ. Status State S

4.5 Objects Settings

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

Objects Setting
IP Object
IP Group
IPv6 Object
IPv6 Group
Service Type Object
Service Type Group
Keyword Object
Keyword Group
File Extension Object

4.5.1 IP Object

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

		0.44		in.		
UD,	jects	Setting	>>	I٢	OD,	ect

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

Each item is explained as follows:

Item	Description
Name	Display a name for this profile.
Set to Factory Default	Clear all profiles.

To set a new profile, please do the steps listed below:

1. Click the number (e.g., #1) under Index column for configuration in details.

Objects Setting >> IP Object		
IP Object Profile	5:	
Index	Name	
<u>1.</u>		
<u>2.</u>		
<u>3.</u>		

2. The configuration page will be shown as follows:

Objects Setting >> IP Object

Profile Index : 1 Name:	RD Department
Interface:	Any 🚩
Address Type:	Range Address 💌
Mac Address:	00:00:00:00:00:00
Start IP Address:	192.168.1.64
End IP Address:	192.168.1.75
Subnet Mask:	0.0.0.0
Invert Selection:	
	OK Clear Cancel

Available settings are explained as follows:

Item	Description	
Name	Type a name for this profile. Maximum 15 characters are allowed.	
Interface	Choose a proper interface. Any Any LAN/RT//PN WAN For example, the Direction setting in Edit Filter Rule will ask you specify IP or IP range for WAN or LAN or any IP address. If you choose LAN as the Interface here, and choose LAN as the direction setting in Edit Filter Rule , then all the IP addresses specified with LAN interface will be opened for you to choose in Edit Filter Rule page.	

Address Type	Determine the address type for the IP address. Select Single Address if this object contains one IP address only. Select Range Address if this object contains several IPs within a range. Select Subnet Address if this object contains one subnet for IP address. Select Any Address if this object contains any IP address. Select Mac Address if this object contains Mac address. Range Address Single Address Subnet Address Subnet Address Mac Address	
MAC Address	Type the MAC address of the network card which will be controlled.	
Start IP Address	Type the start IP address for Single Address type.	
End IP Address	Type the end IP address if the Range Address type is selected.	
Subnet Mask	Type the subnet mask if the Subnet Address type is selected.	
Invert Selection	If it is checked, all the IP addresses except the ones listed above will be applied later while it is chosen.	

- 3. After finishing all the settings here, please click **OK** to save the configuration.
- 4. Below is an example of IP objects settings.

Objects Setting >> IP Object

IP Object Profiles:

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

4.5.2 IP Group

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

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

Objects Setting >> IP Group

Each item is explained as follows:

Item	Description	
Set to Factory Default	Clear all profiles.	
Index	Display the profile number that you can configure.	
Name	Display the name of the group profile.	

To set a new profile, please do the steps listed below:

1. Click the number (e.g., #1) under Index column for configuration in details.

Objects Setting >> IP Group

IP Group Table:

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

Ob	iects	Setting	>>	IP	Group
~~~	,				0.000

Name:	Admin
Interface:	Any 💌
vailable IP Objects	Selected IP Objects
1-RD Department 2-Financial Dept. 3-HR Department	» «

Available settings are explained as follows:

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

3. After finishing all the settings here, please click **OK** to save the configuration.

# Objects Setting >> IP Group

## IP Group Table:

Index	Name	Index
<u>1.</u>	Administration	<u>17.</u>
<u>2.</u>		<u>18.</u>
<u>3.</u>		<u>19.</u>

# 4.5.3 IPv6 Object

You can set up to 64 sets of IPv6 Objects with different conditions.

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

Each item is explained as follows:

Item	Description	
Set to Factory Default	Clear all profiles.	
Index	Display the profile number that you can configure.	
Name	Display the name of the object profile.	

To set a new profile, please do the steps listed below:

1. Click the number (e.g., #1) under Index column for configuration in details.

## Objects Setting >> IPv6 Object

## **IPv6 Object Profiles:**

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

Objects Setting >> IPv6 Object

Name:	Games
Address Type:	Mac Address 👻
Mac Address:	00 :50 :7F :65 :45 :88
Start IP Address:	
End IP Address:	
Prefix Len:	
Invert Selection:	

Available settings are explained as follows:

Item	Description		
Name	Type a name for this profile. Maximum 15 characters are allowed.		
Address Type	Determine the address type for the IPv6 address. Select <b>Single Address</b> if this object contains one IPv6 address only.		
	Select <b>Range Address</b> if this object contains several IPv6s within a range.		
	Select <b>Subnet Address</b> if this object contains one subnet for IPv6 address.		
	Select Any Address if this object contains any IPv6 address.		
	Select Mac Address if this object contains Mac address.		
	Range Address         Any Address         Single Address         Range Address         Subnet Address         Mac Address		
MAC Address	Type the MAC address of the network card which will be controlled.		
Start IP Address	Type the start IP address for Single Address type.		
End IP Address	Type the end IP address if the Range Address type is selected.		
Prefix Len	Type the fixed value for prefix length.		
Invert Selection	If it is checked, all the IPv6 addresses except the ones listed above will be applied later while it is chosen.		



3. After finishing all the settings here, please click **OK** to save the configuration.

<u>1.</u> Games	
<u>2.</u>	

Objects Setting >> IPv6 Object

# 4.5.4 IPv6 Group

This page allows you to bind several IPv6 objects into one IPv6 group.

Obiects	Setting	>> IF	Group
00,0000	ootang	S S 10	oroup

Pv6 Group Table:			Set to Factory Default
Index	Name	Index	Name
<u>1.</u>		<u>17.</u>	
<u>2.</u>		<u>18.</u>	
<u>3.</u>		<u>19.</u>	
<u>4.</u>		<u>20.</u>	
<u>5.</u>		<u>21.</u>	
<u>6.</u>		<u>22.</u>	
<u>7.</u>		<u>23.</u>	
<u>8.</u>		<u>24.</u>	
<u>9.</u>		<u>25.</u>	
<u>10.</u>		<u>26.</u>	
<u>11.</u>		<u>27.</u>	
<u>12.</u>		<u>28.</u>	
<u>13.</u>		<u>29.</u>	
<u>14.</u>		<u>30.</u>	
<u>15.</u>		<u>31.</u>	
<u>16.</u>		<u>32.</u>	

Each item is explained as follows:

Item	Description
Set to Factory Default	Clear all profiles.
Index	Display the profile number that you can configure.
Name	Display the name of the group profile.

To set a new profile, please do the steps listed below:

1. Click the number (e.g., #1) under Index column for configuration in details.

Objects	Setting	>> IP	Group	
---------	---------	-------	-------	--

### IPv6 Group Table:

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

2. The configuration page will be shown as follows:

Objects Setting >> IPv6 Group

Name:	v6_grp1
Available IPv6 Objects	Selected IPv6 Objects
1-Games	
	~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~

Available settings are explained as follows:

Item	Description
Name	Type a name for this profile. Maximum 15 characters are allowed.
Available IPv6 Objects	All the available IPv6 objects with the specified interface chosen above will be shown in this box.
Selected IPv6 Objects	Click >> button to add the selected IPv6 objects in this box.

3. After finishing all the settings here, please click **OK** to save the configuration.

## Objects Setting >> IP Group

#### IPv6 Group Table:

Index	Name
<u>1.</u>	v6_grp1
<u>2.</u>	
<u>3.</u>	

# 4.5.5 Service Type Object

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

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

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

<< 1-32 | 33-64 | 65-96 >>

<u>Next</u> >>

Each item is explained as follows:

Item	Description
Set to Factory Default	Clear all profiles.
Index	Display the profile number that you can configure.
Name	Display the name of the object profile.

To set a new profile, please do the steps listed below:

1. Click the number (e.g., #1) under Index column for configuration in details.

## Objects Setting >> Service Type Object

### Service Type Object Profiles:

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

2. Click the number under Index column for settings in detail.

Objects S	Setting	>>	Service	Туре	Object	Setup
-----------	---------	----	---------	------	--------	-------

Name	WWW
Protocol	TCP/UDP 🗸
Source Port	= 🗸 1 ~ 65535
Destination Port	= 🗸 70 ~ 80

Available settings are explained as follows:

Item	Description
Name	Type a name for this profile.
Protocol	Specify the protocol(s) which this profile will apply to.          TCP       6         Any       6         IGMP       1         TCP       UDP         TCP/UDP       0
Source/Destination Port	<ul> <li>Source Port and the Destination Port column are available for TCP/UDP protocol. It can be ignored for other protocols. The filter rule will filter out any port number.</li> <li>(=) – when the first and last value are the same, it indicates one port; when the first and last values are different, it indicates a range for the port and available for this profile.</li> <li>(!=) – when the first and last value are the same, it indicates all the ports except the port defined here; when the first and last values are different, it indicates the range defined here are available for this service type.</li> <li>(&gt;) – the port number greater than this value is available.</li> <li>(&lt;) – the port number less than this value is available for this profile.</li> </ul>

3. After finishing all the settings here, please click **OK** to save the configuration. Below is an example of service type objects settings.

Objects Setting >> Service Type Object

#### Service Type Object Profiles:

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

# 4.5.6 Service Type Group

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

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

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

Each item is explained as follows:

Item	Description
Set to Factory Default	Clear all profiles.
Index	Display the profile number that you can configure.
Name	Display the name of the group profile.

To set a new profile, please do the steps listed below:

1. Click the number (e.g., #1) under Group column for configuration in details.

Objects Setting >> Service Type Group

Service Type G	Service Type Group Table:		
Group	Name		
<u>1.</u>			
<u>2.</u>			
<u>3.</u>			

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

Name:	VolP		
Available Service	e Type Objects	Selected Service Type Object	ts
1-SIP			
2-RTP			
		»	

Available settings are explained as follows:

Item	Description
Name	Type a name for this profile.
Available Service Type Objects	All the available service objects that you have added on <b>Objects Setting&gt;&gt;Service Type Object</b> will be shown in this box.
Selected Service Type Objects	Click >> button to add the selected IP objects in this box.

3. After finishing all the settings here, please click **OK** to save the configuration.

# Objects Setting >> Service Type Group

#### Service Type Group Table:

Group	Name
<u>1.</u>	VoIP
<u>2.</u>	
<u>3.</u>	

# 4.5.7 Keyword Object

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

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

Objects Setting >> Keyword Object

<< 1.32 | 33.64 | 65.96 | 97.128 | 129.160 | 161.192 | 193.200 >>

<u>Next</u> >>

Each item is explained as follows:

Item	Description	
Set to Factory Default	Clear all profiles.	
Index	Display the profile number that you can configure.	
Name	Display the name of the object profile.	

To set a new profile, please do the steps listed below:

1. Click the number (e.g., #1) under Index column for configuration in details.

## Objects Setting >> Keyword Object

## **Keyword Object Profiles:**

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

Objects Setting >> Keyword Object Setup

Name	
Contents	
	Limit of Contents: Max 3 Words and 63 Characters. Each word should be separated by a single space.
	You can replace a character with %HEX. Example: Contents: backdoo%72 virus keep%20out
	Result:
	1. backdoor 2. virus
	3. keep out

Available settings are explained as follows:

Item	Description         Type a name for this profile, e.g., game.	
Name		
Contents	Type the content for such profile. For example, type <i>gambling</i> as Contents. When you browse the webpage, the page with gambling information will be watched out and be passed/blocked based on the configuration on Firewall settings.	

3. After finishing all the settings here, please click **OK** to save the configuration.

Objects Setting >> Keyword Object

### Keyword Object Profiles:

Index	Name	1
<u>1.</u>	gamble	
<u>2.</u>		
<u>3.</u>		
A		

## 4.5.8 Keyword Group

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

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

Objects Setting >> Keyword Group

Each item is explained as follows:

Item	Description	
Set to Factory Default	Clear all profiles.	
Index	Display the profile number that you can configure.	
Name	Display the name of the group profile.	

To set a new profile, please do the steps listed below:

1. Click the number (e.g., #1) under Index column for configuration in details.

## Objects Setting >> Keyword Group

#### Keyword Group Table:

Index	Name
<u>1.</u>	
<u>2.</u>	
<u>3.</u>	
<u>4.</u>	

Objects Setting >> Keyword Group Setup

Name:	
Available Keyword Objects	Selected Keyword Objects(Max 16 Objects
1-Keyword-1 2-keyword-2	»
	«

Available settings are explained as follows:

Item	Description	
Name	Type a name for this group.	
Available Keyword Objects	You can gather keyword objects from <b>Keyword Object</b> page within one keyword group. All the available Keyword objects that you have created will be shown in this box.	
Selected Keyword Objects	Click button to add the selected Keyword objects in this box.	

3. After finishing all the settings here, please click **OK** to save the configuration.

## Objects Setting >> Keyword Group

### Keyword Group Table:

Index	Name
<u>1.</u>	night
<u>2.</u>	
<u>3.</u>	
4.	

# 4.5.9 File Extension Object

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

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

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

#### Objects Setting >> File Extension Object

Each item is explained as follows:

Item Description	
Set to Factory Default Clear all of the settings and return to factory defau	
<b>Index</b> Display the profile number that you can configure.	
Name	Display the name of the object profile.

To set a new profile, please do the steps listed below:

1. Click the number (e.g., #1) under Profile column for configuration in details.

## Objects Setting >> File Extension Object

#### File Extension Object Profiles:

Profile	Name
<u>1.</u>	
<u>2.</u>	
<u>3.</u>	

Objects Setting >> File Extension Object Setup

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

Available settings are explained as follows:

Item	Description
Profile Name	Type a name for this profile (maximum 7 characters).

- 3. Type a name for such profile and check all the items of file extension that will be processed in the router.
- 4. After finishing all the settings here, please click **OK** to save the configuration.

### Objects Setting >> File Extension Object

#### File Extension Object Profiles:

Profile	Name
<u>1.</u>	bigimag
<u>2.</u>	
<u>3.</u>	
4.	

# 4.6 CSM

## **Content Security Management (CSM)**

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

## **APP Enforcement Filter**

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

## **URL Content Filter**

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

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

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

## Web Content Filter

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

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



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



## 4.6.1 APP Enforcement Profile

You can define policy profiles for IM (Instant Messenger)/P2P (Peer to Peer)/Protocol/Misc application. This page allows you to set 32 profiles for different requirements. The APP Enforcement Profile will be applied in **Default Rule** of **Firewall>>General Setup** for filtering.

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

CSM >> APP Enforcement Profile

Each item is explained as follows:

Item	Description		
Set to Factory Default	Clear all profiles.		
Profile	Display the number of the profile which allows you to click to set different policy.		
Name	Display the name of the APP Enforcement Profile.		

Click the number under Index column for settings in detail.

There are three tabs IM, P2P and Misc displayed on this page. Each tab will bring out different items that you can choose to disallow people using.



### Below shows the items which are categorized under IM.

ofile Index : 1 Prof	ile Name:					
IM	P2P		Misc			
Select All Cle	ar All					
		IM Applic	ation			VoIP
MSN	🗌 YahooIM	AIM		<b>ICQ</b>		🗌 Skype 📃 Kubao
QQ/TM iChat		Jabber/GoogleTalk		GoogleChat		Gizmo SIP/RTP
Aliww						🗌 TelTel 🔲 TeamSpeal
		Web	IM ( * = more that	an one address)		
	eMessenger	WebMSN	meebo*	<u>eBuddy</u>	LovelM*	
WebIM URLs	ICQ Java*	ICQ Flash*	goowy*	<u>IMhaha*</u>	<u>getMessenger</u>	
WebIM URLS	IMUnitive*	Wablet*	<u>mabber*</u>	MSN2G0*	KoollM	
	MessengerFX*	<u>MessengerAdictos</u> <u>WebYahoolM</u>				

Available settings are explained as follows:

Item	Description	
Profile NameType a name for the CSM profile.		
Select AllClick it to choose all of the items in this page.		
Clear All	Uncheck all the selected boxes.	

The profiles configured here can be applied in the **Firewall>>General Setup** and **Firewall>>Filter Setup** pages as the standard for the host(s) to follow.

## The items categorized under P2P -----

#### CSM >> APP Enforcement Profile

IM	P2P	Misc	
Select All Clear All			
Protocol			Applications
🗌 SoulSeek		SoulSeek	
🗌 eDonkey		eDonkey, eMule, Shareaza	
🗌 FastTrack		KazaA, BearShare, iMesh	
OpenFT		KCeasy, FilePipe	
🔲 Gnutella		BearShare, Limewire, Sharea:	za, Foxy, KCeasy
OpenNap		Lopster, XNap, WinLop	
BitTorrent		BitTorrent, BitSpirit, BitCome	t

#### The items categorized under Misc -----

#### CSM >> APP Enforcement Profile

Profile Index : 1	Profile Name:				
IM	P2P	Misc			
Select All	Clear All				
Streaming					
MMS	RTSP	TVAnts	PPStream	PPTV	
🗌 FeiDian	UUSee	NSPlayer	PCAST	🔲 ΤΥΚοο	
SopCast	UDLiveX	TVUPlayer	MySee	🗖 Joost	
🗌 FlashVideo	SilverLight	🔲 Slingbox	QVOD		
		OK Car	cel		



## 4.6.2 URL Content Filter Profile

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

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

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

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

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

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

RL Content Filter	Profile Table:		Set to Factory Defaul
Profile	Name	Profile	Name
<u>1.</u>		<u>5.</u>	
<u>2.</u>		<u>6.</u>	
<u>3.</u>		<u>7.</u>	
<u>4.</u>		<u>8.</u>	

#### CSM >> URL Content Filter Profile

Administration Message (Max 255 characters)	Default Message		
<pre><body><center> The requested Web page has been blocked by URL Co Filter.Please contact your system administrator for further information.</center></body></pre>	ntent	~	
		~	

OK

Each item is explained as follows:

Item	Description
Set to Factory Default	Clear all profiles.
Profile	Display the number of the profile which allows you to click to set different policy.
Name	Display the name of the URL Content Filter Profile.

Vigor2710 Series User's Guide

Default Message	You can type the message manually for your necessity or
	click this button to get the default message which will be
	displayed on the field of Administration Message.

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

Profile Name:					
Priority:	Both : Pass		✓ Log:	None 💌	
1.URL Acces	5 Control				
🗌 Enab	le URL Access Co	ntrol	Prevent we	eb access from IP address	
Actio	n:		Group/Objec	t Selections	
Pass	~			Edit	
2.Web Featu	re				
🗌 Enab	le Restrict Web F	eature			
Actio	n:				
Pass	🗠 🗌 Cookie	Proxy	🗌 Upload	File Extension Profile: None 👻	

Available settings are explained as follows:

CSM >> URL Content Filter Profile

Item	Description
Profile Name	Type a name for the CSM profile.
Priority	It determines the action that this router will apply.
	<b>Both: Pass</b> – The router will let all the packages that match with the conditions specified in URL Access Control and Web Feature below passing through. When you choose this setting, both configuration set in this page for URL Access Control and Web Feature will be inactive.
	<b>Both:Block</b> –The router will block all the packages that match with the conditions specified in URL Access Control and Web Feature below. When you choose this setting, both configuration set in this page for URL Access Control and Web Feature will be inactive.
	<b>Either: URL Access Control First</b> – When all the packages matching with the conditions specified in URL Access Control and Web Feature below, such function can determin the priority for the actions executed. For this one, the router will process the packages with the conditions set below for URL first, then Web feature second.
	<b>Either: Web Feature First</b> –When all the packages matching with the conditions specified in URL Access Control and Web Feature below, such function can determin

	the priority for the actions executed. For this one, the router will process the packages with the conditions set below for web feature first, then URL second. Both : Pass Both : Pass Both : Block Either : URL Access Control First Either : Web Feature First
Log	<b>None</b> – There is no log file will be recorded for this profile.
	<b>Pass</b> – Only the log about Pass will be recorded in Syslog.
	<b>Block</b> – Only the log about Block will be recorded in Syslog.
	All – All the actions (Pass and Block) will be recorded in Syslog.
	None V None Pass Block All
URL Access Control	<b>Enable URL Access Control</b> - Check the box to activate URL Access Control. Note that the priority for <b>URL Access</b> <b>Control</b> is higher than <b>Restrict Web Feature</b> . If the web content match the setting set in URL Access Control, the router will execute the action specified in this field and ignore the action specified under Restrict Web Feature.
	<b>Prevent web access from IP address</b> - Check the box to deny any web surfing activity using IP address, such as http://202.6.3.2. The reason for this is to prevent someone dodges the URL Access Control. You must clear your browser cache first so that the URL content filtering facility operates properly on a web page that you visited before.
	Action – This setting is available only when Either : URL Access Control First or Either : Web Feature First is selected. <i>Pass</i> - Allow accessing into the corresponding webpage with the keywords listed on the box below.
	<ul><li><i>Block</i> - Restrict accessing into the corresponding webpage with the keywords listed on the box below.</li><li>If the web pages do not match with the keyword set here, it will be processed with reverse action.</li></ul>
	Action: Block 🕶 Pass Block
	<b>Group/Object Selections</b> – The Vigor router provides several frames for users to define keywords and each frame supports multiple keywords. The keyword could be a noun, a partial noun, or a complete URL string. Multiple keywords within a frame are separated by space, comma, or semicolon.



In addition, the maximal length of each frame is 32-character long. After specifying keywords, the Vigor router will decline the connection request to the website whose URL string matched to any user-defined keyword. It should be noticed that the more simplified the blocking keyword list is, the more efficiently the Vigor router performs.

	🗟 http://192.168.1.5 - Group/Object Edit - Microsoft Internet Explorer
	Object/Group Edit       None ♥         or Keyword Object       None ♥         or Keyword Group       None ♥
Web Feature	<ul> <li>Enable Restrict Web Feature - Check this box to make the keyword being blocked or passed.</li> <li>Action - This setting is available only when Either: URL</li> <li>Access Control First or Either: Web Feature Firs is selected. Pass allows accessing into the corresponding webpage with the keywords listed on the box below.</li> <li>Pass - Allow accessing into the corresponding webpage with the keywords listed on the box below.</li> </ul>
	<b>Block</b> - Restrict accessing into the corresponding webpage with the keywords listed on the box below. If the web pages do not match with the specified feature set here, it will be processed with reverse action.
	<b>Cookie</b> - Check the box to filter out the cookie transmission from inside to outside world to protect the local user's privacy.
	<b>Proxy</b> - 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.
	<b>Upload</b> – Check the box to reject any file upload job.
	<b>File Extension Profile</b> – Choose one of the profiles that you configured in <b>Object Setting&gt;&gt; File Extension Objects</b> previously for passing or blocking the file downloading.

None 1-default	File Extension Profile:	None	4
1-default		None	
		1-default	

After finishing all the settings here, please click **OK** to save the configuration.

# 4.6.3 Web Content Filter Profile

**Note:** Web Content Filter (WCF) service is powered by **Commtouch**, the partner of DrayTek. The product name is GlobalView WCF.

There are three ways to activate WCF on vigor router, using **Service Activation Wizard**, by means of **CSM>>Web Content Filter Profile** or via **System Maintenance>>Activation**.

Service Activation Wizard allows you to use trial version or update the license of WCF directly without accessing into the server (*MyVigor*) located on <u>http://myvigor.draytek.com</u>.

However, if you use the **Web Content Filter Profile** page to activate WCF feature, it is necessary for you to access into the server (*MyVigor*) located on http://myvigor.draytek.com. Therefore, you need to register an account on http://myvigor.draytek.com for using corresponding service. Please refer to section of creating MyVigor account.

**Note:** If you have used **Service Activation Wizard** to activate WCF service, you can skip this section.

WCF adopts the mechanism developed and offered by certain service provider (e.g., DrayTek). No matter activating WCF feature or getting a new license for web content filter, you have to click **Activate** to satisfy your request. Be aware that service provider matching with Vigor router currently offers a period of time for trial version for users to experiment. If you want to purchase a formal edition, simply contact with the channel partner or your dealer.

Click **CSM** and click **Web Content Filter Profile** to open the profile setting page. The default setting for Setup Query Server /Setup Test Server is **auto-selected**. You can choose another server for your necessity by clicking **Find more** to open http://myvigor.draytek.com for searching another qualified and suitable one.

#### CSM >> Web Content Filter Profile

Setup Query Serv	ver	auto-selected		Find more
Setup Test Serve	r	auto-selected		Find more
Web Content Filte	r Profile T	able:		Set to Factory Default
Profile		Name	Profile	Name
<u>1.</u>	l	Default	<u>5.</u>	
<u>2.</u>			<u>6.</u>	
<u>3.</u>			<u>7.</u>	
<u>4.</u>			<u>8.</u>	
Administration Ma	essage	(Max 255 characters)	Default Messa	age Cache : L1 + L2 Cache 🔨

Available settings are explained as follows:

Item	Description
Activate	Click it to access into MyVigor for activating WCF service.
Setup Query Server	It is recommended for you to use the default setting, auto-selected. You need to specify a server for categorize searching when you type URL in browser based on the web content filter profile.
Setup Test Server	It is recommended for you to use the default setting, auto-selected.
Find more	Click it to open http://myvigor.draytek.com for searching another qualified and suitable server.
Set to Factory Default	Click this link to retrieve the factory settings.
Default Message	You can type the message manually for your necessity or click this button to get the default message which will be displayed on the field of <b>Administration Message</b> .

**Dray** Tek

Cache	<b>None</b> – the router will check the URL that the user wants to access via WCF precisely, however, the processing rate is normal. Such item can provide the most accurate URL matching.
	L1 – the router will check the URL that the user wants to access via WCF. If the URL has been accessed previously, it will be stored for a short time (about 1 second) in the router to be accessed quickly if required. Such item can provide accurate URL matching with faster rate.
	L2 – the router will check the URL that the user wants to access via WCF. If the data has been accessed previously, the IP addresses of source and destination IDs will be memorized for a short time (about 1 second) in the router. When the user tries to access the same destination ID, the router will check it by comparing the record stored. If it matches, the page will be retrieved quickly. Such item can provide URL matching with the fastest rate.
	<b>L1+L2 Cache</b> – the router will check the URL with fast processing rate combining the feature of L1 and L2.

Eight profiles are provided here as Web content filters. Simply click the index number under Profile to open the following web page. The items listed in Categories will be changed according to the different service providers. If you have and activate another web content filter license, the items will be changed simultaneously. All of the configuration made for web content filter will be deleted automatically. Therefore, please backup your data before you change the web content filter license.

Profile Index: 1				
Profile Name: Default				Log: Block 🛩
Black/White List				
Enable Action:		Your Object Colections		
Block V		roup/Object Selections	Edit	
Action: Block 🕶 Groups	Categories			
Child Protection Select All Clear All	<ul> <li>✓ Alcohol &amp; Tobacco</li> <li>✓ Hate &amp; Intolerance</li> <li>✓ Porn &amp; Sexually</li> <li>✓ School Cheating</li> <li>✓ Child Abuse Images</li> </ul>	<ul> <li>✓ Criminal Activity</li> <li>✓ Illegal Drug</li> <li>✓ Violence</li> <li>✓ Sex Education</li> </ul>	♥ Gambling ♥ Nudity ♥ Weapons ♥ Tasteless	

CSM >> Web Content Filter Profile



Clear All	E Finance	🗌 Government	🗌 Health & Medicine
	News	🗌 Non-profits & NGOs	Personal Sites
	Politics	🗌 Real Estate	🗌 Religion
	🗌 Restaurants & Dining	Shopping	Translators
	🗌 General	Cults	Greeting cards
	🗌 Image Sharing	Network Errors	Parked Domains
	Private IP Addresses	Uncategorised Sites	
	ОК	Cancel	

**Note:** If the Web Content Filter (WCF) powered by Commtouch is not activated, the above settings will not be valid.

Available settings are explained as follows:

<b>Enable</b> – Activate white/black list function for such profile. <b>Group/Object Selections</b> – Click <b>Edit</b> to choose the group		
<b>Enable</b> – Activate white/black list function for such profile. <b>Group/Object Selections</b> – Click <b>Edit</b> to choose the group or object profile as the content of white/black list.		
<b>Pass - allow</b> accessing into the corresponding webpage with the characters listed on <b>Group/Object Selections</b> . If the web pages do not match with the specified feature set here, they will be processed with the categories listed on the box below.		
<b>Block - restrict</b> accessing into the corresponding webpage with the characters listed on <b>Group/Object Selections</b> . If the web pages do not match with the specified feature set here, they will be processed with the categories listed on the box below.		
<b>Pass</b> - allow accessing into the corresponding webpage with the categories listed on the box below.		
<b>Block</b> - restrict accessing into the corresponding webpage with the categories listed on the box below.		
If the web pages do not match with the specified feature set here, it will be processed with reverse action.		
None – There is no log file will be recorded for this profile.         Pass – Only the log about Pass will be recorded in Syslog.         Block – Only the log about Block will be recorded in Syslog.         All – All the actions (Pass and Block) will be recorded in Syslog.         Block ♥         None         Pass         Block		

After finishing all the settings here, please click **OK** to save the configuration.



# 4.7 Bandwidth Management

Below shows the menu items for Bandwidth Management.

Bandwidth Management
Sessions Limit
Bandwidth Limit
Quality of Service
APP QoS

## 4.7.1 Sessions Limit

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

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

Bandwidth Management >> Sessions Limit

🔘 Enable 💿 Disable			
Default Max Sessions: 100	)		
Limitation List			
Index Start IP	End IP	Max Sessions	
Specific Limitation			
Start IP:	End IP:		
Maximum Sessions:			
	Add Ed	Delete	
inistration Message (Max	256 characters)		Default Message
mise deforminessage (max	200 endractory		Delaan Meessage
e Schedule			
Index(1-15) in <u>Schedule</u> S	etup: ,	, , , , , , , , , , , , , , , , , , , ,	
		nored.	

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



Item	Description
Session Limit	<b>Enable -</b> Click this button to activate the function of limit session.
	<b>Disable</b> - Click this button to close the function of limit session.
	<b>Default Max Session -</b> 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.
Specific Limitation	Start IP- Defines the start IP address for limit session.
	End IP - Defines the end IP address for limit session.
	<b>Maximum Sessions -</b> Defines the available session number for each host in the specific range of IP addresses. If you do not set the session number in this field, the system will use the default session limit for the specific limitation you set for each index.
	<b>Add</b> - Adds the specific session limitation onto the list above.
	Edit - Allows you to edit the settings for the selected limitation.
	<b>Delete -</b> Remove the selected settings existing on the limitation list.
Administration Message	Type the words which will be displayed when reaches the maximum number of Internet sessions permitted.
	Click <b>Default Message</b> to display the default message on the screen.
Time Schedule	<b>Index (1-15) in Schedule Setup</b> - You can type in four sets of time schedule for your request. All the schedules can be set previously in <b>Application</b> >> <b>Schedule</b> 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 save the configuration.

# 4.7.2 Bandwidth Limit

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

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

🔘 Enable 🗌 Appl	ly to 2nd Subnet 💿 Disable
Default TX Limit: 2000	0 Kbps 💙 Default RX Limit: 8000 Kbps 💙
Limitation List	
Index Start IP	End IP TX limit RX limit Shared
Specific Limitation	
Start IP:	End IP:
💿 Each 🛛 Shared	
TX Limit:	Kbps 👻 RX Limit: Kbps 🗸
	Add Update Delete
Smart Bandwidth	
Smart Bandwidth	ı Limit
Smart Bandwidth	in Limitation List, whose session number exceeds 1000
Smart Bandwidth For any LAN IP Not i TX Limit : 200	in Limitation List, whose session number exceeds 1000
Smart Bandwidth For any LAN IP Not i TX Limit : 200	in Limitation List, whose session number exceeds 1000
Smart Bandwidth For any LAN IP Not i TX Limit : 200 For TX/RX, a setting of "0	in Limitation List, whose session number exceeds 1000
Smart Bandwidth For any LAN IP Not i TX Limit : 200	in Limitation List, whose session number exceeds 1000
Smart Bandwidth For any LAN IP Not i TX Limit : 200 : For TX/RX, a setting of "C	n Limit in Limitation List, whose session number exceeds 1000 Kbps ♥ RX Limit : 800 Kbps ♥ " means unlimited bandwidth.

Bandwidth Management >> Bandwidth Limit

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

Item	Description
Bandwidth Limit	<ul> <li>Enable - Click this button to activate the function of limit bandwidth.</li> <li>Apply to 2nd Subnet - Check this box to apply the bandwidth limit to the second subnet specified in LAN&gt;&gt;General Setup.</li> </ul>
	<b>Disable -</b> Click this button to close the function of limit bandwidth.
	<b>Default TX limit -</b> 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.		
Specific Limitation	Start IP - Define the start IP address for limit bandwidth.		
	<b>End IP -</b> Define the end IP address for limit bandwidth.		
	<b>Each /Shared -</b> Select <b>Each</b> to make each IP within the range of Start IP and End IP having the same speed defined in TX limit and RX limit fields; select <b>Shared</b> to make all the IPs within the range of Start IP and End IP share the speed defined in TX limit and RX limit fields.		
	<b>TX limit -</b> 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.		
	<b>RX limit -</b> 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.		
	<b>Update-</b> Allow you to edit the settings for the selected limitation.		
	<b>Delete -</b> Remove the selected settings existing on the limitation list.		
Smart Bandwidth Limit	Check this box to have the bandwidth limit determined by the system automatically.		
	<b>TX limit -</b> 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.		
	<b>RX limit -</b> 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.		
Time Schedule	<b>Index (1-15) in Schedule Setup -</b> You can type in four sets of time schedule for your request. All the schedules can be set previously in <b>Application</b> >> <b>Schedule</b> web page and you can use the number that you have set in that web page.		

After finishing all the settings here, please click  $\mathbf{O}\mathbf{K}$  to save the configuration.

# 4.7.3 Quality of Service

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

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

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

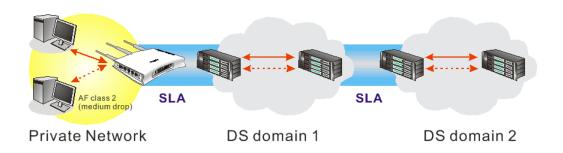
There are two components within Primary configuration of QoS deployment:

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

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

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

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



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

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

able	<b>Jandwidth</b> Kbps/Kbps Kbps/100000Kbps	Direction Outbound Outbound	25%	25%	Class 3 25% 25%	25%	UDP Bandwidth Control Inactive	Online Statistics <u>Status</u>	Setup
able 100000								<u>Status</u>	Setup
	Kbps/100000Kbps	Outbound	25%	25%	250/				
					25%	25%	Inactive	Status	Setup
		Name					Rule	Service T	уре
							Edit		
							Edit	Edit	
							<u>Edit</u>		
Enable the First Priority for VoIP SIP/RTP: SIP UDP Port: 5060 (Default: 5060)									
		the First Priority for VoIP S	the First Priority for VoIP SIP/RTP:	the First Priority for VoIP SIP/RTP:	the First Priority for VoIP SIP/RTP: Port: 5060 (Default: 5060)	the First Priority for VoIP SIP/RTP: Port: 5060 (Default: 5060)	the First Priority for VoIP SIP/RTP: Port: 5060 (Default: 5060)	the First Priority for VoIP SIP/RTP: Port: 5060 (Default: 5060)	the First Priority for VoIP SIP/RTP: Port: 5060 (Default: 5060)

Bandwidth Management >> Quality of Service

Each item is explained as follows:

Item	Description
General Setup	<b>Index</b> - Display the WAN interface number that you can edit.
	<b>Status</b> - Display the current QoS status of this WAN.
	<b>Bandwidth</b> – Display the inbound and outbound bandwidth setting for the WAN interface.
	<b>Direction</b> – Display which direction that such function will influence.
	<b>Class 1/Class2/Class 3/Others</b> – Display the bandwidth percentage for each class.
	<b>UDP Bandwidth Control</b> – Display the UDP bandwidth control is enabled or not.
	<b>Online Statistics</b> – Display an online statistics for quality of service for your reference

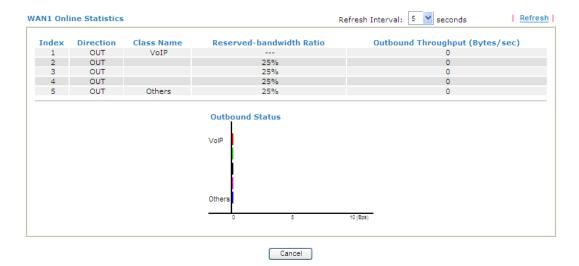
Item	Description
	<b>Setup</b> – Allow to configure general QoS setting for WAN interface.
Class Rule	<b>Index</b> – Display the class number that you can edit.
	<b>Name</b> – Display the name of the class.
	<b>Rule</b> – Allow to configure detailed settings for the selected Class.
	<b>Service Type</b> – Allow to configure detailed settings for the service type.
Enable the First Priority for VoIP SIP/RTP	When this feature is enabled, the VoIP SIP/RTP packets will be sent with highest priority.
	<b>SIP UDP Port</b> - Set a port number used for SIP.

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

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

## **Online Statistics**

Display an online statistics for quality of service for your reference. This feature is available only when the Quality of Service for WAN interface is enabled.



#### Bandwidth Management >> Quality of Service

**General Setup for WAN Interface** 

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



### Bandwidth Management >> Quality of Service

General Setup		
Enable the	QoS Control OUT 💌	
Index	Class Name	Reserved_bandwidth Ratio
Class 1		25 %
Class 2		25 %
Class 3		25 %
	Others	25 %
	Bandwidth Control CP ACK Prioritize	Limited_bandwidth Ratio 25 %
	OK Clear	Cancel

Item	Description
Enable the QoS Control	<ul> <li>The factory default for this setting is checked.</li> <li>Please also define which traffic the QoS Control settings will apply to.</li> <li>IN- apply to incoming traffic only.</li> <li>OUT- apply to outgoing traffic only.</li> <li>BOTH- apply to both incoming and outgoing traffic.</li> <li>Check this box and click OK, then click Setup link again. You will see the Online Statistics link appearing on this page.</li> </ul>
WAN Inbound Bandwidth	It allows you to set the connecting rate of data input for WAN2. For example, if your ADSL supports 1M of downstream and 256K upstream, please set 1000kbps for this box. The default value is 10000kbps.
WAN Outbound Bandwidth	It allows you to set the connecting rate of data output for WAN2. For example, if your ADSL supports 1M of downstream and 256K upstream, please set 256kbps for this box. The default value is 10000kbps. <b>Note:</b> The rate of outbound/inbound must be smaller than
	the real bandwidth to ensure correct calculation of QoS. It is suggested to set the bandwidth value for inbound/outbound as 80% - 85% of physical network speed provided by ISP to maximize the QoS performance.
Reserved Bandwidth Ratio	It is reserved for the group index in the form of ratio of <b>reserved bandwidth to upstream speed</b> and <b>reserved bandwidth to downstream speed</b> .
Enable UDP Bandwidth Control	Check this and set the limited bandwidth ratio on the right field. This is a protection of TCP application traffic since UDP application traffic such as streaming video will exhaust lots of bandwidth.

Outbound TCP ACK Prioritize	The difference in bandwidth between download and upload are great in ADSL2+ environment. For the download speed might be impacted by the uploading TCP ACK, you can check this box to push ACK of upload faster to speed the network traffic.
Limited_bandwidth Ratio	The ratio typed here is reserved for limited bandwidth of UDP application.

## Edit the Class Rule for QoS

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

Bandwidth Management >> Quality of Service

Index	Status	Bandwidth	Direction	Class 1	Class 2	Class 3	Others	UDP Bandwidth Control	Online Statistics	
WAN1	Enable	Kbps/Kbps	Outbound	25%	25%	25%	25%	Inactive	<u>Status</u>	Setup
Backup WAN	Enable	100000Kbps/100000Kbps	Outbound	25%	25%	25%	25%	Inactive	<u>Status</u>	Setup
Class R Inde Class	×		Name					Rule Edit	Service T	уре
Class	-							Edit	Edit	
Class	3							Edit		
	able the P UDP Po	First Priority for VoIP S	-							

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

Bandwidth Management >>	Quality of Service
-------------------------	--------------------

ame	Ne VolP Tag packets as: AF Class1 (High Drop)						
NO	Status	Local Address	Remote Address	DiffServ CodePoint	Service Type		
1	Empty	-	-	-	-		
		-	Add Edit Delet	е			

Item	Description
Name	Display the name of such class.
Tag packets as	Check the box to tag the packets with the header selected in the drop down list for this class.

NO	Display the number of the rules defined for such rule.
Status	Display if such rule is enabled (Active) or not.
Local Address	Display the local IP address (on LAN) for the rule.
<b>Remote Address</b>	Display the remote IP address (on LAN/WAN) for the rule.
DiffServ CodePoint	Display the levels of the data for processing with QoS control.
Service Type	Display the service type of the data for processing with QoS control.

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

### Bandwidth Management >> Quality of Service

Rule Edit			
	ACT		
	Ethernet Type	⊙ IPv4 ○ IPv6	
	Local Address	Any Edit	
	Remote Address	Any Edit	
	DiffServ CodePoint	ANY	
	Service Type	Predefined	
	Note: Please choose/setup t	he <u>Service Type</u> first.	
		OK Cancel	

Item	Description
ACT	Check this box to invoke these settings.
Ethernet Type	Please specify which protocol (IPv4 or IPv6) will be used for this rule.
Local Address	Click the <b>Edit</b> button to set the local IP address (on LAN) for the rule.
Remote Address	Click the <b>Edit</b> button to set the remote IP address (on LAN/WAN) for the rule.

Edit	It allows you to edit source address information.						
	🖹 http://192.168.1.1/doc/QoslpEdt.htm - Microsoft Internet Explorer						
	Address Type     Subnet Address       Start IP Address     0.0.0.0       End IP Address     0.0.0.0       Subnet Mask     0.0.0.0						
	OK Close						
	Address Type – Determine the address type for the source address.						
	For Single Address, you have to fill in Start IP address.						
	For <b>Range Address</b> , you have to fill in Start IP address and End IP address.						
	For <b>Subnet Address</b> , 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.						

4. After finishing all the settings here, please click **OK** to save the configuration.

Bandwidth Management >> Quality of Service

Status	Local Address	Remote Address	DiffServ		
		Keniote Address	CodePoint	Service Type	
Active Any		Any	ANY	ANY	
	A	Add Edit Delete	ן		
	Active			Add Edit Delete	

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

## Edit the Service Type for Class Rule

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



#### Bandwidth Management >> Quality of Service

Index	Status	Bandwidth	Direction	Class 1	Class 2	Class 3	Others	UDP Bandwidth Control	Online Statistics	
WAN1	Enable	Kbps/Kbps	Outbound	25%	25%	25%	25%	Inactive	<u>Status</u>	Setup
Backup WAN	Enable	100000Kbps/100000Kbps	Outbound	25%	25%	25%	25%	Inactive	Status	Setup

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

Enable the First	st Priority for VoIP SIP/RTP:
SIP UDP Port: 5	060 (Default:5060)
	ОК

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

Bandwidth Management >> Quality of Service

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

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

Bandwidth Management >> Quality of Service

Service Type Edit	
Service Name	
Service Type	TCP 🖌 6
Port Configuration	
Туре	💿 Single  🔘 Range
Port Number	0 – 0
OK	Cancel

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

Port Configuration	<b>Type</b> - Click <b>Single</b> or <b>Range</b> as the <b>Type</b> . If you select Range, you have to type in the starting port number and the	
	end porting number on the boxes below.	
	<b>Port Number</b> – Type in the starting port number and the end	
	porting number here if you choose Range as the type.	

4. After finishing all the settings here, please click **OK** to save the configuration.

Bandwidth Management >> Quality of Service

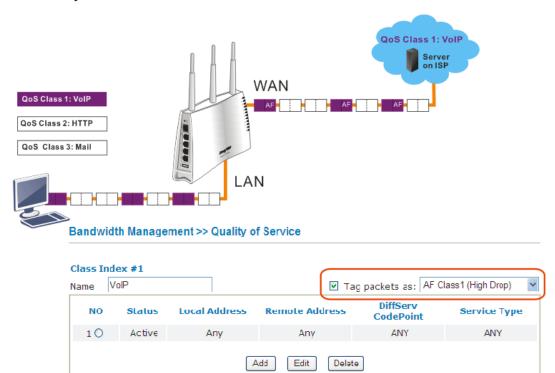
ser Defined Service Type			
NO	Name	Protocol	Port
1 ()	Audio	ТСР	0
Add Edit Delete			
		Cancel	

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

## **Retag the Packets for Identification**

Packets coming from LAN IP can be retagged through QoS setting. When the packets sent out through WAN interface, all the them will be tagged with certain header and that will be easily to be identified by server on ISP.

For example, in the following illustration, the VoIP packets in LAN go into Vigor router without any header. However, when they go forward to the Server on ISP through Vigor router, all of the packets are tagged with AF (configured in Bandwidth >>QoS>>Class) automatically.



# 4.7.4 APP QoS

The QoS function is used to do bandwidth management for the services with certain IP or port number. However, there is no effect of bandwidth management on the service such as VNC or PPTV without fixed IP or port number.

APP QoS employs the function of APP Enforcement to detect the types of software in application layer. By combining the function of QoS (adjustment on Inbound/Outbond bandwidth and bandwidth ratio), Vigor router can perform the bandwidth management for the protocols, streaming, remote control, web HD and so on.

Click **Bandwidth Management>>APP QoS** to open the following page.

0 1.11111 0	Disable		
Protocol	Misc		
Select All	Clear All	Apply to all:	QoS Class 1 (High) 🛛 🖌 Appl
Enable		Protocol	Action
	DNS		QoS Class 1 (High) 💙
	FTP		QoS Class 1 (High) 🛛 👻
	НТТР		QoS Class 1 (High) 🛛 👻
	IMAP		QoS Class 1 (High) 🛛 👻
	IRC		QoS Class 1 (High) 🛛 👻
	NNTP		QoS Class 1 (High) 🛛 👻
	POP3		QoS Class 1 (High) 🛛 👻
	SMB		QoS Class 1 (High) 🛛 👻
	SMTP		QoS Class 1 (High) 🛛 👻
	SNMP		QoS Class 1 (High) 🛛 👻
	SSH		QoS Class 1 (High) 🛛 👻
	SSL/TLS		QoS Class 1 (High) 💙

Bandwidth Management >> APP QoS

Note: Please remember to adjust Inbound/Outbound bandwidth of your network in "Quailty of Service". This will help QoS to work more efficient.



Available settings are explained as follows:

Item	Description	
Enable/Disable	Click Enable to activate APP QoS function.	
	Click <b>Disable</b> to deactivate APP QoS function.	
Protocol/Misc	Each tab offers different types of protocols to fit your request.	
Select All	Click it to select all of the protocols.	
Clear All	Click it to de-select all of the protocols.	

**Dray** Tek

Apply to all	Choose one of the actions from the drop down list. It is prepared for applying to all protocols.		
	Apply to all: QoS Class 1 (High) 🔽 Apply		
	ol QoS Class 1 (High) QoS Class 2 (Medium) QoS Class 3 (Low) ↓ ♥ DefaultClass (Lowest)		
	<b>Apply</b> – Click it to make the selected action be applied all of the selected protocols immediately.		
Action	There are many protocols which can be specified with different QoS Class.		
	Action		
	QoS Class 1 (High)		
	QoS Class 1 (High) QoS Class 2 (Medium) QoS Class 3 (Low) DefaultClass (Lowest)		

After finishing all the settings here, please click **OK** to save the configuration.

# 4.8 Applications

Below shows the menu items for Applications.

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

## 4.8.1 Dynamic DNS

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

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



### Enable the Function and Add a Dynamic DNS Account

- 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.

Dynamic DNS Setup		Set to Factory Default
🔲 Enable Dynamic DNS	3 Setup	View Log Force Update
Auto-Update interval	14400 Min(s) (1~14400)	
Accounts:		
Index	Domain Name	Active
<u>1.</u>		×
<u>2.</u>		×
<u>3.</u>		×

Applications >> Dynamic DNS Setup

ОК	Clear All
ON	Olear All

Available settings are explained as follows:

Item	Description	
Enable Dynamic DNS Setup	Check this box to enable DDNS function.	
Set to Factory Default	Clear all profiles and recover to factory settings.	
View Log	Display DDNS log status.	
Force Update	Force the router updates its information to DDNS server.	
Auto-Update interval	Set the time for the router to perform auto update for DDNS service.	
Index	Click the number below Index to access into the setting page of DDNS setup to set account(s).	
Domain Name	Display the domain name that you set on the setting page of DDNS setup.	
Active	Display if this account is active or inactive.	
Clear All	<ul> <li>Disable the Function and Clear all Dynamic DNS Accounts -</li> <li>In the DDNS setup menu, uncheck Enable Dynamic DNS Setup, and push this button to disable the function and clear all accounts from the router.</li> <li>Delete a Dynamic DNS Account -</li> <li>In the DDNS setup menu, click the Index number you want to delete and then push this button to delete the account.</li> </ul>	

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		
Service Provider	dyndns.org (www.dyndns.org)	*
Service Type	Dynamic 💌	
Domain Name	chronic6683 dyndns.org	dyndns.org 👻
Login Name	chronic6683	(max. 64 characters)
Password	•••••	(max. 23 characters)
Wildcards		
Backup MX		
Mail Extender		
Determine Real WAN IP	WAN IP	

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

Item	Description
Enable Dynamic DNS Account	Check this box to enable the current account. If you did check the box, you will see a check mark appeared on the Active column of the previous web page in step 2).
Service Provider	Select the service provider for the DDNS account.
Service Type	Select a service type (Dynamic, Custom or Static). If you choose Custom, you can modify the domain that is chosen in the Domain Name field.
Domain Name	Type in one domain name that you applied previously. Use the drop down list to choose the desired domain.
Login Name	Type in the login name that you set for applying domain.
Password	Type in the password that you set for applying domain.
Wildcard and Backup MX	The Wildcard and Backup MX (Mail Exchange) features are not supported for all Dynamic DNS providers. You could get more detailed information from their websites.
Mail Extender	If the mail server is defined with another name, please type the name in this area. Such mail server will be used as backup mail exchange.
Determine Real WAN IP	If a Vigor router is installed behind any NAT router, you can enable such function to locate the real WAN IP. When the WAN IP used by Vigor router is private IP, this function can detect the public IP used by the NAT router and use the detected IP address for DDNS update. There are two methods offered for you to choose: <b>WAN IP</b> - If it is selected and the WAN IP of Vigor router is private, DDNS update will take place right away. <b>Internet IP</b> – If it is selected and the WAN IP of Vigor router is private, it will be converted to public IP before DDNS update takes place.



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

## 4.8.2 Schedule

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

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

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

#### Applications >> Schedule

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

Each item is explained as follows:

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

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

To add a schedule:

1. Click any index, say Index No. 1.

## Applications >> Schedule

### Schedule:

Index	Status
<u>1.</u>	×
<u>2.</u>	×
<u>3.</u>	×

**Dray** Tek

2. The detailed settings of the call schedule with index 1 are shown below.

Applications >> Schedule

Index No. 1	
🗹 Enable Schedule Setup	
Start Date (yyyy-mm-dd)	2000 - 1 - 1 -
Start Time (hh:mm)	
Duration Time (hh:mm)	
Action	Force On
Idle Timeout	minute(s).(max. 255, 0 for default)
How Often	
Once	
💿 Weekdays	
🗌 Sun 🗹 Mon 🗹	Tue 🗹 Wed 🗹 Thu 🗹 Fri 🔲 Sat
OK	Clear

Available settings are explained as follows:

Item	Description	
Enable Schedule Setup	Check to enable the schedule.	
Start Date (yyyy-mm-dd)	Specify the starting date of the schedule.	
Start Time (hh:mm)	Specify the starting time of the schedule.	
Duration Time (hh:mm)	Specify the duration (or period) for the schedule.	
Action	Specify which action Call Schedule should apply during the period of the schedule.	
	Force On -Force the connection to be always on.	
	Force Down -Force the connection to be always down.	
	<b>Enable Dial-On-Demand -</b> Specify the connection to be dial-on-demand and the value of idle timeout should be specified in <b>Idle Timeout</b> field.	
	<b>Disable Dial-On-Demand -</b> 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.	
	<b>How often</b> -Specify how often the schedule will be applied <b>Once</b> -The schedule will be applied just once	
	<b>Weekdays</b> -Specify which days in one week should perform the schedule.	

3. Click **OK** button to save the settings.

### Example

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



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

# 4.8.3 RADIUS

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

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

Applications >> RADIUS

🗹 Enable	
Server IP Address	
Destination Port	1812
Shared Secret	
Confirm Shared Secret	

Available settings are explained as follows:

Item	Description	
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.	

**Dray** Tek

Shared Secret	The RADIUS server and client share a secret that is used to authenticate the messages sent between them. Both sides must be configured to use the same shared secret.	
Confirm Shared Secret	Re-type the Shared Secret for confirmation.	

After finished the above settings, click **OK** button to save the settings.

## 4.8.4 UPnP

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

Applications >> UPnP

Enable UPnP Service		Default WAN 💌
Enable	Connection control Service	
Enable	Connection Status Service	

above to allow control, as well as the appropriate UPnP settings.

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

Available settings are explained as follows:

Item	Description	
Enable UPNP Service	Accordingly, you can enable either the <b>Connection Control</b> <b>Service</b> or <b>Connection Status Service</b> .	
Default WAN	It is used to specify the WAN interface for applying such function.	
	Default WAN 💌	
	Default WAN WAN1	
	Backup WAN	

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	🔡 IP Broadband Con	and brand, says, a special	and the second s
Network Tasks         (2)           Create a new connection         (2)           Set up a home or small office network         (2)	hinet Disconnected WAN Miniport (PPPOE)	General Internet Gateway Status: Duration:		Connected 00:19:06
iee Also (*)	test Disconnected DrayTek ISDN PPP	Speed:		100.0 Mbps
Other Places 🔹	Internet Gateway	Packets:	nternet Gateway — 🧐 ——	My Computer
Hy Documents	LAN or High-Speed Internet	Sent: Received:	404 1,115	734 666
Details (*) Network Connections System Folder	Local Area Connection Enabled Realtek RTL8139/810× Family	Properties D	isable	

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.

meral	
Connect to the Internet using:	Select the services running on your network that Internet users can access.
IP Broadband Connection on Router	(Services
his connection allows you to connect to the Internet through a hared connection on another computer.	<ul> <li>□ Ftp Example</li> <li>✓ msnmsgr (192.168.29.11:13135) 60654 UDP</li> <li>✓ msnmsgr (192.168.29.11:7824) 13251 UDP</li> <li>✓ msnmsgr (192.168.29.11:8789) 63231 TCP</li> </ul>
Settings	Add., Edit., Delete

The reminder as regards concern about Firewall and UPnP

### Can't work with Firewall Software

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

## **Security Considerations**

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

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



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

# 4.8.5 IGMP

IGMP is the abbreviation of *Internet Group Management Protocol*. It is a communication protocol which is mainly used for managing the membership of Internet Protocol multicast groups.

Applications >> IGMP

IGMP					
Enable IGM	P Proxy WAN1 V				
IGMP Proxy is to act as a multicast proxy for hosts on the LAN side. Enable IGMP Proxy, if you will access any multicast group. But this function take no affect when Bridge Mode is enabled.					
Enable IGMP Snooping					
Enable IGMP Snooping, multicast traffic is only forwarded to ports that have members of that group. Disable IGMP snooping, multicast traffic is treated in the same manner as broadcast traffic.					
OK Cancel					
Refresh					
Working Multic	ast Groups				
Index	Group ID	P1	P2	P3	P4

Available settings are explained as follows:

Item	Description
Enable IGMP Proxy	Check this box to enable this function. The application of multicast will be executed through WAN port. In addition, such function is available in NAT mode.
Enable IGMP Snooping	Check this box to enable this function. Multicast traffic will be forwarded to ports that have members of that group. Disabling IGMP snooping will make multicast traffic treated in the same manner as broadcast traffic.
Refresh	Click this link to renew the working multicast group status.
Group ID	This field displays the ID port for the multicast group. The available range for IGMP starts from 224.0.0.0 to 239.255.255.254.
P1 to P4	It indicates the LAN port used for the multicast group.

After finishing all the settings here, please click **OK** to save the configuration.

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



# 4.8.6 Wake on LAN

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

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

Application >> Wake on LAN

IP Address:	Note: Wake or can wake up t	n LAN integrates with <u>Bind IP to MAC</u> function, only binded PCs nrough IP.
MAC Address:	Wake by:	MAC Address
	IP Address:	😒
Pocult.	MAC Address:	Wake Up!
Result	Result	

Item	Description	
Wake by	Two types provide for you to wake up the bound IP. If you choose Wake by MAC Address, you have to type the correct MAC address of the host in MAC Address boxes. If you choose Wake by IP Address, you have to choose the correct IP address.         Wake by:       MAC Address v         MAC Address       IP Address         IP Address       IP Address	
IP Address	The IP addresses that have been configured in <b>Firewall&gt;&gt;Bind IP to MAC</b> will be shown in this drop down list. Choose the IP address from the drop down list that you want to wake up.	
MAC Address	Type any one of the MAC address of the bound PCs.	
Wake Up	Click this button to wake up the selected IP. See the following figure. The result will be shown on the box.	

#### Application >> Wake on LAN

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

# 4.9 VPN and Remote Access

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

Below shows the menu items for VPN and Remote Access.

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

## 4.9.1 Remote Access Control

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

VPN and Remote Access >> Remote Access Control Setup

**Remote Access Control Setup** 

Enable PPTP VPN Service
Enable IPSec VPN Service
Enable L2TP VPN Service

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

OK	Clear	Cancel

# 4.9.2 PPP General Setup

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

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

#### VPN and Remote Access >> PPP General Setup

PPP General Setup	
	PPP/MP Protocol       Dial-In PPP       Authentication   PAP or CHAP
	Dial-In PPP Encryption (MPPE)
	Mutual Authentication (PAP) 🛛 🔘 Yes 💿 No
	Username
	Password
	IP Address Assignment for Dial-In Users (When DHCP Disable set)
	Assigned IP start LAN 1 192.168.1.200

OK

Item	Description
Dial-In PPP Authentication	<b>PAP Only</b> - elect this option to force the router to authenticate dial-in users with the PAP protocol.
	<b>PAP or CHAP</b> - Selecting this option means the router will attempt to authenticate dial-in users with the CHAP protocol first. If the dial-in user does not support this protocol, it will fall back to use the PAP protocol for authentication.

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

After finishing all the settings here, please click **OK** to save the configuration.

# 4.9.3 IPSec General Setup

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

There are two phases of IPSec.

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

There are two encapsulation methods used in IPSec, **Transport** and **Tunnel**. The **Transport** mode will add the AH/ESP payload and use original IP header to encapsulate the data



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

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

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

#### VPN and Remote Access >> IPSec General Setup

#### VPN IKE/IPSec General Setup

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

IKE Authentication Method	
Pre-Shared Key	••••
Confirm Pre-Shared Key	••••
IPSec Security Method	
🗹 Medium (AH)	
Data will be authentic, but will r	not be encrypted.
High (ESP) 🛛 DES 🗹 3DES	✓ AES
Data will be encrypted and auth	entic.
	OK Cancel

Available settings are explained as follows:

Item	Description
IKE Authentication Method	This usually applies to those are remote dial-in user or node (LAN-to-LAN) which uses dynamic IP address and IPSec-related VPN connections such as L2TP over IPSec and IPSec tunnel.
	<b>Pre-Shared Key -</b> Currently only support Pre-Shared Key authentication.
	<b>Pre-Shared Key-</b> Specify a key for IKE authentication <b>Confirm Pre-Shared Key-</b> Retype the characters to confirm the pre-shared key.
<b>IPSec Security Method</b>	<b>Medium</b> - Authentication Header (AH) means data will be authenticated, but not be encrypted. By default, this option is active.
	<b>High</b> - 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.

After finishing all the settings here, please click **OK** to save the configuration.

# 4.9.4 IPSec Peer Identity

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

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



Each item is explained as follows:

Item	Description
Set to Factory Default	Click it to clear all indexes.
Index	Click the number below Index to access into the setting page of IPSec Peer Identity.
Name	Display the profile name of that index.

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

#### VPN and Remote Access >> IPSec Peer Identity

Profile Index : 1	
Profile Name	??
Enable this acco	unt
Accept Any Period	er ID
O Accept Subject	Alternative Name
Туре	IP Address 💌
IP	
O Accept Subject	Name
Country (C)	
State (ST)	
Location (L)	
Orginization (O)	
Orginization Unit (	OU)
Common Name (C	۷)
Email (E)	
	OK Clear Cancel

Available settings are explained as follows:

Item	Description	
Profile Name	Type the name of the profile.	
Accept Any Peer ID	Click to accept any peer regardless of its identity.	
Accept Subject Alternative Name	Click to check one specific field of digital signature to accept the peer with matching value. The field can be <b>IP</b> <b>Address, Domain,</b> or <b>E-mail Address</b> . 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 <b>Country (C), State (ST), Location (L), Organization (O),</b> <b>Organization Unit (OU), Common Name (CN),</b> and <b>Email (E)</b> .	

After finishing all the settings here, please click **OK** to save the configuration.

## 4.9.5 Remote Dial-in User

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

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

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

VPN and Remote Access >> Remote Dial-in User

Each item is explained as follows:

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

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



#### VPN and Remote Access >> Remote Dial-in User

Index No. 1 User account and Authentication		
Enable this account	Username ???	
Idle Timeout 300 second(s)	Password(Max 19 char)	
Allowed Dial-In Type	IKE Authentication Method Pre-Shared Key	
PPTP	IKE Pre-Shared Key	
☑ IPsec Tunnel	Digital Signature(X.509)	
L2TP with IPsec Policy None	None 🗸	
Specify Remote Node		
Remote Client IP	IPsec Security Method	
	Medium(AH)	
or Peer ID	High(ESP) 🗹 DES 🗹 3DES 🗹	AES
Netbios Naming Packet 💿 Pass 🔘 Block	Local ID (optional)	
Multicast via VPN 🛛 🔿 Pass 💿 Block		
(for some IGMP, IP-Camera, DHCP Relayetc.)		
Assign Static IP Address		
0.0.0.0		

Item	Description		
User account and Authentication	<b>Enable this account</b> - Check the box to enable this function. <b>Idle Timeout-</b> 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.		
Allowed Dial-In Type	<ul> <li>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.</li> <li>IPSec Tunnel - Allow the remote dial-in user to make an IPSec VPN connection through Internet.</li> <li>L2TP with IPSec Policy - 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:</li> <li>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.</li> </ul>		
	<ul> <li>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.</li> <li>Must -Specify the IPSec policy to be definitely applied on the L2TP connection.</li> </ul>		
	<b>Specify Remote Node</b> <b>Check the checkbox-</b> You can specify the IP address of the remote dial-in user, ISDN number or peer ID (used in IKE aggressive mode).		

Item	Description				
	<b>Uncheck the checkbox-</b> This means the connection type you select above will apply the authentication methods and security methods in the <b>general settings</b> .				
	Netbios Naming Packet				
	• <b>Pass</b> – Click it to have an inquiry for data transmission between the hosts located on both sides of VPN Tunnel while connecting.				
	• <b>Block</b> – When there is conflict occurred between the hosts on both sides of VPN Tunnel in connecting, such function can block data transmission of Netbios Naming Packet inside the tunnel.				
	Multicast via VPN				
	Some programs might send multicast packets via VPN connection.				
	• <b>Pass</b> – Click this button to let multicast packets pass through the router.				
	• <b>Block</b> – This is default setting. Click this button to let multicast packets be blocked by the router.				
	<b>Assign Static IP Address</b> – Allow the IP address typed here to dial in.				
	<b>User Name</b> - This field is applicable when you select PPTP or L2TP with or without IPSec policy above. The maximum length for username is 19 characters.				
	<b>Password</b> - This field is applicable when you select PPTP or L2TP with or without IPSec policy above. The maximum length for password is 19 characters.				
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.				
	<b>Pre-Shared Key -</b> Check the box of Pre-Shared Key to invoke this function and type in the required characters (1-63) as the pre-shared key.				
	<b>Digital Signature (X.509)</b> – Check the box of Digital Signature to invoke this function and Select one predefined Profiles set in the <b>VPN and Remote Access</b> >> <b>IPSec Peer</b> <b>Identity.</b>				
IPSec Security Method	This group of fields is a must for IPSec Tunnels and L2TP with IPSec Policy when you specify the remote node. Check the Medium, DES, 3DES or AES box as the security method. <b>Medium-Authentication Header (AH)</b> means data will be authenticated, but not be encrypted. By default, this option is invoked. You can uncheck it to disable it.				
	<b>High-Encapsulating Security Payload (ESP)</b> means payload (data) will be encrypted and authenticated. You may select encryption algorithm from Data Encryption Standard (DES), Triple DES (3DES), and AES.				



Item	Description
	<b>Local ID (optional)-</b> Specify a local ID to be used for Dial-in setting in the LAN-to-LAN Profile setup. This item is optional and can be used only in IKE aggressive mode.

After finishing all the settings here, please click **OK** to save the configuration.

## 4.9.6 LAN to LAN

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

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

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

VPN and Remote Access >> LAN to LAN

Each item is explained as follows:

Item	Description	
View	<ul><li>All – Click it to display the LAN to LAN profiles.</li><li>Trunk – Click it to display the Trunk profiles.</li></ul>	
Set to Factory Default	Click to clear all indexes.	
Name	Indicate the name of the LAN-to-LAN profile. The symbol <b>???</b> represents that the profile is empty.	
Active	Check the box to enable the selected profile.	

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

To edit each profile:

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

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

VPN and Remote Access >> LAN to LAN	
Profile Index : 1 1. Common Settings	
Profile Name ??? Enable this profile VPN Dial-Out Through WAN1 First  Netbios Naming Packet  Pass  Block Multicast via VPN  Pass  Block (for some IGMP,IP-Camera,DHCP Relayetc.) 2. Dial-Out Settings	Call Direction <ul> <li>Both</li> <li>Dial-Out</li> <li>Dial-in</li> <li>Always on</li> </ul> Idle Timeout 300 second(s) <ul> <li>Enable PING to keep alive</li> <li>PING to the IP</li> </ul>
Type of Server I am calling  PPTP  IPsec Tunnel  L2TP with IPsec Policy None  Server IP/Host Name for VPN. (such as draytek.com or 123.45.67.89)	Username ??? Password(Max 15 char) PPP Authentication PAP/CHAP VJ Compression IKE Authentication Method Pre-Shared Key IKE Pre-Shared Key IKE Pre-Shared Key Digital Signature(X.509) Peer ID Local ID Alternative Subject Name First Subject Name First IPsec Security Method Medium(AH)
	High(ESP) DES without Authentication     Advanced  Index(1-15) in Schedule Setup:  , , , , , , , , , , , , , , , , , , ,

Item	Description
Common Settings	<b>Profile Name -</b> Specify a name for the profile of the LAN-to-LAN connection.
	Enable this profile - Check here to activate this profile.
	<b>VPN Dial-Out Through -</b> Use the drop down menu to choose a proper WAN interface for this profile. This setting is useful for dial-out only.



WAN1 First       WAN1 First       WAN1 Only       3G Backup Only
• WAN1 First - While connecting, the router will use WAN1 as the first channel for VPN connection. If WAN1 fails, the router will use another WAN interface instead.
• <b>WAN1 Only</b> - While connecting, the router will use WAN1 as the only channel for VPN connection.
• <b>3G Backup Only</b> - While connecting, the router will use <b>3G modem</b> as the only channel for VPN connection.
Netbios Naming Packet
• <b>Pass</b> – click it to have an inquiry for data transmission between the hosts located on both sides of VPN Tunnel while connecting.
• <b>Block</b> – When there is conflict occurred between the hosts on both sides of VPN Tunnel in connecting, such function can block data transmission of Netbios Naming Packet inside the tunnel.
<b>Multicast via VPN</b> - Some programs might send multicast packets via VPN connection.
• <b>Pass</b> – Click this button to let multicast packets pass through the router.
• <b>Block</b> – This is default setting. Click this button to let multicast packets be blocked by the router.
<b>Call Direction</b> - Specify the allowed call direction of this LAN-to-LAN profile.
Both:-initiator/responder
<b>Dial-Out-</b> initiator only
Dial-In- responder only.
<b>Always On-</b> Check to enable router always keep VPN connection.
<b>Idle Timeout:</b> The default value is 300 seconds. If the connection has been idled over the value, the router will drop the connection.
<b>Enable PING to keep alive -</b> 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.
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

	<ul> <li>disconnect without notice, Vigor router will by no where to know this situation. To resolve this dilemma, by continuously sending PING packets to the remote host, the Vigor router can know the true existence of this VPN connection and react accordingly. This is independent of DPD (dead peer detection).</li> <li>PING to the IP - Enter the IP address of the remote host that</li> </ul>
	located at the other-end of the VPN tunnel.
Dial-Out Settings	Type of Server I am calling –
	<b>PPTP</b> - 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.
	<b>IPSec Tunnel</b> - Build an IPSec VPN connection to the server through Internet.
	<b>L2TP with IPSec Policy -</b> 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.
	• <b>Must:</b> Specify the IPSec policy to be definitely applied on the L2TP connection.
	<b>User Name -</b> This field is applicable when you select, PPTP or L2TP with or without IPSec policy above. The maximum length for username is 49 characters.
	<b>Password -</b> This field is applicable when you select PPTP or L2TP with or without IPSec policy above. The maximum length for password is 15 characters.
	<b>PPP Authentication -</b> This field is applicable when you select, PPTP or L2TP with or without IPSec policy above. PAP/CHAP is the most common selection due to wild compatibility.
	<b>VJ compression -</b> This field is applicable when you select PPTP or L2TP with or without IPSec policy above. VJ Compression is used for TCP/IP protocol header compression. Normally set to <b>Yes</b> to improve bandwidth utilization.
	<b>IKE Authentication Method -</b> This group of fields is applicable for IPSec Tunnels and L2TP with IPSec Policy.
	• <b>Pre-Shared Key</b> - Input 1-63 characters as pre-shared key.
	• Digital Signature (X.509) - Click Digital Signature to invoke this function and select one predefined Profiles set in the VPN and Remote Access >>IPSec Peer Identity as Peer ID.
	<b>Local ID</b> – Specify which one will be inspected first.
	Alternative Subject Name First – The alternative



<ul> <li>subject name (configured in Certificate Management&gt;&gt;Local Certificate) will be inspected first.</li> <li>Subject Name First – The subject name (configured in Certificate Management&gt;&gt;Local Certificate) will be inspected first.</li> <li>IPSec Security Method - This group of fields is a must for IPSec Tunnels and L2TP with IPSec Policy.</li> <li>Medium AH (Authentication Header) means data wi be authenticated, but not be encrypted. By default, this option is active.</li> <li>High (ESP-Encapsulating Security Payload)- means payload (data) will be encrypted and authenticated. Select from below:</li> <li>DES without Authentication -Use DES encryption algorithm and not apply any authentication scheme.</li> <li>DES without Authentication-Use triple DES encryption algorithm and apply MD5 or SHA-1 authentication algorithm.</li> <li>3DES with Authentication-Use triple DES encryption algorithm and apply MD5 or SHA-1 authentication algorithm.</li> <li>AES without Authentication-Use triple DES encryption algorithm and paphy MD5 or SHA-1 authentication algorithm.</li> <li>AES without Authentication-Use triple DES encryption algorithm and apply MD5 or SHA-1 authentication algorithm.</li> <li>AES without Authentication-Use triple DES encryption algorithm and apply MD5 or SHA-1 authentication algorithm.</li> <li>AES without Authentication-Use AES encryption algorithm and not apply any authentication algorithm.</li> <li>AES without Authentication-Use AES encryption algorithm and not apply any authentication scheme.</li> <li>AES with Authentication-Use AES encryption algorithm.</li> <li>Advanced - Specify mode, proposal and key life of each IKI phase, Gateway, etc.</li> <li>The window of advance setup is shown as below:</li> </ul>	
<ul> <li>(configured in Certificate Management&gt;&gt;Local Certificate) will be inspected first.</li> <li>IPSec Security Method - This group of fields is a must for IPSec Tunnels and L2TP with IPSec Policy.</li> <li>Medium AH (Authentication Header) means data wi be authenticated, but not be encrypted. By default, this option is active.</li> <li>High (ESP-Encapsulating Security Payload)- means payload (data) will be encrypted and authenticated. Select from below:</li> <li>DES without Authentication -Use DES encryption algorithm and not apply any authentication scheme.</li> <li>DES with Authentication-Use DES encryption algorithm and apply MD5 or SHA-1 authentication scheme.</li> <li>3DES without Authentication-Use triple DES encryption algorithm and apply MD5 or SHA-1 authentication algorithm.</li> <li>3DES with Authentication-Use triple DES encryption algorithm and apply MD5 or SHA-1 authentication algorithm.</li> <li>AES without Authentication-Use triple DES encryption algorithm and apply MD5 or SHA-1 authentication algorithm.</li> <li>AES without Authentication-Use triple DES encryption algorithm and apply MD5 or SHA-1 authentication algorithm.</li> <li>AES with Authentication-Use AES encryption algorithm and not apply any authentication scheme.</li> <li>AES with Authentication-Use AES encryption algorithm and not apply any authentication scheme.</li> <li>AES with Authentication-Use AES encryption algorithm and apply MD5 or SHA-1 authentication algorithm.</li> <li>Advanced - Specify mode, proposal and key life of each IKH phase, Gateway, etc.</li> <li>The window of advance setup is shown as below:</li> </ul>	Management>>Local Certificate) will be
<ul> <li>IPSec Tunnels and L2TP with IPSec Policy.</li> <li>Medium AH (Authentication Header) means data wi be authenticated, but not be encrypted. By default, this option is active.</li> <li>High (ESP-Encapsulating Security Payload)- means payload (data) will be encrypted and authenticated. Select from below:</li> <li>DES without Authentication - Use DES encryption algorithm and not apply any authentication scheme.</li> <li>DES with Authentication-Use DES encryption algorithm and apply MD5 or SHA-1 authentication algorithm.</li> <li>3DES without Authentication-Use triple DES encryption algorithm and apply MD5 or SHA-1 authentication scheme.</li> <li>3DES without Authentication-Use triple DES encryption algorithm and apply MD5 or SHA-1 authentication scheme.</li> <li>3DES without Authentication-Use triple DES encryption algorithm and apply MD5 or SHA-1 authentication algorithm.</li> <li>AES without Authentication-Use AES encryption algorithm and apply MD5 or SHA-1 authentication scheme.</li> <li>AES without Authentication-Use AES encryption algorithm and not apply any authentication scheme.</li> <li>AES with Authentication-Use AES encryption algorithm and apply MD5 or SHA-1 authentication algorithm.</li> <li>ACVanced - Specify mode, proposal and key life of each IKH phase, Gateway, etc.</li> <li>The window of advance setup is shown as below:</li> </ul>	(configured in Certificate Management>>Loca
<ul> <li>be authenticated, but not be encrypted. By default, this option is active.</li> <li>High (ESP-Encapsulating Security Payload)- means payload (data) will be encrypted and authenticated. Select from below:</li> <li>DES without Authentication - Use DES encryption algorithm and not apply any authentication scheme.</li> <li>DES with Authentication-Use DES encryption algorithm and apply MD5 or SHA-1 authentication algorithm.</li> <li>3DES with Authentication-Use triple DES encryption algorithm and apply MD5 or SHA-1 authentication scheme.</li> <li>3DES with Authentication-Use triple DES encryption algorithm and apply MD5 or SHA-1 authentication algorithm.</li> <li>AES without Authentication-Use triple DES encryption algorithm and apply MD5 or SHA-1 authentication algorithm.</li> <li>AES without Authentication-Use AES encryption algorithm and not apply any authentication scheme.</li> <li>AES with Authentication-Use AES encryption algorithm and not apply any authentication scheme.</li> <li>AES with Authentication-Use AES encryption algorithm and not apply any authentication scheme.</li> <li>AES with Authentication-Use AES encryption algorithm and apply MD5 or SHA-1 authentication algorithm.</li> <li>Advanced - Specify mode, proposal and key life of each IKE phase, Gateway, etc.</li> <li>The window of advance setup is shown as below:</li> </ul>	
<ul> <li>payload (data) will be encrypted and authenticated. Select from below:</li> <li>DES without Authentication -Use DES encryption algorithm and not apply any authentication scheme.</li> <li>DES with Authentication-Use DES encryption algorithm and apply MD5 or SHA-1 authentication algorithm.</li> <li>3DES without Authentication-Use triple DES encryption algorithm and not apply any authentication scheme.</li> <li>3DES with Authentication-Use triple DES encryption algorithm and apply MD5 or SHA-1 authentication scheme.</li> <li>3DES with Authentication-Use triple DES encryption algorithm and apply MD5 or SHA-1 authentication algorithm.</li> <li>AES without Authentication-Use AES encryption algorithm and not apply any authentication scheme.</li> <li>AES with Authentication-Use AES encryption algorithm and not apply any authentication scheme.</li> <li>AES with Authentication-Use AES encryption algorithm and apply MD5 or SHA-1 authentication algorithm.</li> <li>AES with Authentication-Use AES encryption algorithm and apply MD5 or SHA-1 authentication algorithm.</li> <li>Advanced - Specify mode, proposal and key life of each IKE phase, Gateway, etc.</li> <li>The window of advance setup is shown as below:</li> </ul>	be authenticated, but not be encrypted. By default, this
<ul> <li>algorithm and not apply any authentication scheme.</li> <li>DES with Authentication-Use DES encryption algorithm and apply MD5 or SHA-1 authentication algorithm.</li> <li>3DES without Authentication-Use triple DES encryption algorithm and not apply any authentication scheme.</li> <li>3DES with Authentication-Use triple DES encryption algorithm and apply MD5 or SHA-1 authentication algorithm and apply MD5 or SHA-1 authentication algorithm.</li> <li>AES without Authentication-Use AES encryption algorithm and not apply any authentication scheme.</li> <li>AES without Authentication-Use AES encryption algorithm and not apply any authentication scheme.</li> <li>AES with Authentication-Use AES encryption algorithm and not apply any authentication scheme.</li> <li>AES with Authentication-Use AES encryption algorithm and not apply any authentication scheme.</li> <li>AES with Authentication-Use AES encryption algorithm and apply MD5 or SHA-1 authentication algorithm.</li> <li>Advanced - Specify mode, proposal and key life of each IKE phase, Gateway, etc.</li> <li>The window of advance setup is shown as below:</li> </ul>	payload (data) will be encrypted and authenticated.
<ul> <li>algorithm and apply MD5 or SHA-1 authentication algorithm.</li> <li><b>3DES without Authentication</b>-Use triple DES encryption algorithm and not apply any authentication scheme.</li> <li><b>3DES with Authentication</b>-Use triple DES encryption algorithm and apply MD5 or SHA-1 authentication algorithm.</li> <li><b>AES without Authentication</b>-Use AES encryption algorithm and not apply any authentication scheme.</li> <li><b>AES with Authentication</b>-Use AES encryption algorithm and not apply any authentication scheme.</li> <li><b>AES with Authentication</b>-Use AES encryption algorithm and not apply any authentication scheme.</li> <li><b>AES with Authentication</b>-Use AES encryption algorithm and apply MD5 or SHA-1 authentication algorithm.</li> <li><b>Ates with Authentication</b>-Use AES encryption algorithm and apply MD5 or SHA-1 authentication algorithm.</li> <li><b>Advanced</b> - Specify mode, proposal and key life of each IKE phase, Gateway, etc.</li> <li>The window of advance setup is shown as below:</li> </ul>	
<ul> <li>encryption algorithm and not apply any authentication scheme.</li> <li><b>3DES with Authentication</b>-Use triple DES encryption algorithm and apply MD5 or SHA-1 authentication algorithm.</li> <li><b>AES without Authentication</b>-Use AES encryption algorithm and not apply any authentication scheme.</li> <li><b>AES with Authentication</b>-Use AES encryption algorithm and not apply any authentication scheme.</li> <li><b>AES with Authentication</b>-Use AES encryption algorithm and apply MD5 or SHA-1 authentication algorithm.</li> <li><b>AES with Authentication</b>-Use AES encryption algorithm and apply MD5 or SHA-1 authentication algorithm.</li> <li><b>Advanced</b> - Specify mode, proposal and key life of each IKE phase, Gateway, etc.</li> <li>The window of advance setup is shown as below:</li> </ul>	• <b>DES with Authentication-</b> Use DES encryption algorithm and apply MD5 or SHA-1 authentication
<ul> <li>algorithm and apply MD5 or SHA-1 authentication algorithm.</li> <li>AES without Authentication-Use AES encryption algorithm and not apply any authentication scheme.</li> <li>AES with Authentication-Use AES encryption algorithm and apply MD5 or SHA-1 authentication algorithm.</li> <li>Advanced - Specify mode, proposal and key life of each IKH phase, Gateway, etc.</li> <li>The window of advance setup is shown as below:</li> </ul>	encryption algorithm and not apply any authentication
<ul> <li>algorithm and not apply any authentication scheme.</li> <li>AES with Authentication-Use AES encryption algorithm and apply MD5 or SHA-1 authentication algorithm.</li> <li>Advanced - Specify mode, proposal and key life of each IKE phase, Gateway, etc.</li> <li>The window of advance setup is shown as below:</li></ul>	algorithm and apply MD5 or SHA-1 authentication
algorithm and apply MD5 or SHA-1 authentication algorithm. Advanced - Specify mode, proposal and key life of each IKH phase, Gateway, etc. The window of advance setup is shown as below: <b>VE advanced settings</b> WE phase 1 mode         WE phase 1 mode         WE phase 1 proposal         Met phase 1 proposal         WE phase 2 (MS) MAL, C1, 3DES_MOS_C1, 3DES_MOS_C2, 3DES_(MS)/SMAL, C5, AES128_MS_C1(2/CS), AES256_SMA_(C2/CS), AES256_SMA_(C	
Advanced - Specify mode, proposal and key life of each IKH phase, Gateway, etc. The window of advance setup is shown as below: Image: The set of	algorithm and apply MD5 or SHA-1 authentication
The window of advance setup is shown as below:	Advanced - Specify mode, proposal and key life of each IK
INE advanced settings         INE phase 1 mode <ul> <li>Main mode</li> <li>Aggressive mode</li> <li>Et phase 1 proposal</li> <li>Ante</li> <li>INE phase 2 proposal</li> <li>INAC_SHAINMAC_MOS</li> <li>(cold &gt; 06400)</li> <li>(perfect Forward Secret</li> <li>Disable</li> <li>Cacal ID</li> </ul> Note: If you select "Auto" in IXE phase 1 proposal; the router will send the following proposals to negotiate with the remote site. The proposals include: USE_MOS_G1, 3DES_MOS_G2, 3DES_(MDS/SHA)_GS, AES128_MOS_GC2(GS), AES256_SHA_G24         OK     Close	
INE phase 1 proposal       Auto         INE phase 2 proposal       IHA4C_SHAIMAC_MOS         INE phase 1 key lifetime       2000         Perfect Porward Secret       © Disable         Local ID       Interpret Port (MSYSHA)_C1, 3DES_MOS_C1, 3DES_MOS_C2, 3DES_(MDK/SHA)_C5, AES128_MOS_(C2/C5), AES256_SHA_(C2/C5), AES256_SHA_(C2/C5)	
INE phase 1 key lifetime       2000       (coD + 06400)         INE phase 2 key lifetime       3000       (coD + 06400)         Perfect Forward Secret       Image: Code of the co	IKE phase 1 proposal Auto
Perfect Yorward Secret O Disable O Enable Cucal ID Note: If you select "Auto" in IXE phase 1 proposal; the router will send the following proposals to negotiate with the remote site. The proposals include: DES_(MDS/SHA)_G1, 3DES_MD5_G1, 3DES_MD5_G2, 3DES_(MD5/SHA)_G5, AES128_MD5_(G2/G5), AES256_SHA_(G2/G5), AES256_SHA_G14 OK Close	IKE phase 1 key lifetime 20000 (900 ~ 96400)
Note: If you select "Auto" in IKE phase 1 proposal, the router will send the following proposals to negotiate with the remote site. The proposals include: DES_(MOS/SHA)_C1, SDES_MOS_C1, 3DES_MOS_C2, 3DES_(MOS/SHA)_C5, AESIZ8_MOS_(C2/C5), AESIZ8_SHA_C1+ CK Close	Perfect Forward Secret O Disable O Enable
AE5255_SHA_G14 OK Close	Note: If you select "Auto" in IKE phase 1 proposal, the router will send the following proposals to negotiate with the remote site. The proposals
	AES256_SHA_G14
The second	
	÷ ,
mode. The ultimate outcome is to exchange security proposals to create a protected secure channel. <b>Main</b> mode is	
proposals to create a protected secure channel. <b>Main</b> mode is more secure than <b>Aggressive</b> mode since more exchanges are	done in a secure channel to set up the IPSec session.
proposals to create a protected secure channel. <b>Main</b> mode is more secure than <b>Aggressive</b> mode since more exchanges are done in a secure channel to set up the IPSec session.	
proposals to create a protected secure channel. <b>Main</b> mode is more secure than <b>Aggressive</b> mode since more exchanges are done in a secure channel to set up the IPSec session. However, the <b>Aggressive</b> mode is faster. The default value in	-
proposals to create a protected secure channel. <b>Main</b> mode is more secure than <b>Aggressive</b> mode since more exchanges are done in a secure channel to set up the IPSec session. However, the <b>Aggressive</b> mode is faster. The default value in Vigor router is Main mode.	
proposals to create a protected secure channel. <b>Main</b> mode is more secure than <b>Aggressive</b> mode since more exchanges are done in a secure channel to set up the IPSec session. However, the <b>Aggressive</b> mode is faster. The default value in	automication schemes and eneryption argorithms to the

	combinations are available for Aggressive mode and nine for <b>Main</b> mode. We suggest you select the combination that covers the most schemes.
•	<b>IKE phase 2 proposal-</b> 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.
•	<b>IKE phase 1 key lifetime-</b> 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.
•	<b>IKE phase 2 key lifetime-</b> 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.
•	<b>Perfect Forward Secret (PFS)-</b> The IKE Phase 1 key will be reused to avoid the computation complexity in phase 2. The default value is inactive this function.
•	<b>Local ID-</b> In <b>Aggressive</b> mode, Local ID is on behalf of the IP address while identity authenticating with remote VPN server. The length of the ID is limited to 47 characters.

3. Dial-In Settings		
Allowed Dial-In Type		Username ???
PPTP		Password(Max 11 char)
🗹 IPsec Tunnel		VJ Compression 💿 On 🔘 Off
L2TP with IPsec Poli	cy None 💌	
-		IKE Authentication Method
Specify Remote VPN	Gateway	Pre-Shared Key
Peer VPN Server IP		IKE Pre-Shared Key
		Digital Signature(X.509)
or Peer ID		None 🗸
		Local ID
		<ul> <li>Alternative Subject Name First</li> </ul>
		Subject Name First
		IPsec Security Method
		Medium(AH)
		High(ESP) ✓ DES ✓ 3DES ✓ AES
4. TCP/IP Network Set	tinas	
My WAN IP	0.0.0.0	RIP Direction Disable
Remote Gateway IP	0.0.0.0	From first subnet to remote network, you have to
Remote Network IP	0.0.0.0	do
Remote Network Mask	255.255.255.0	Route 💌
Local Network IP	192.168.1.1	Change default route to this VPN tunnel ( Only single WAN supports this )
Local Network Mask	255.255.255.0	
	More	
	ОК	Clear Cancel

Item Description					
Allowed Dial-In	Determine the dial-in connection with different types.				
Туре	<b>PPTP -</b> 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.				
	<b>IPSec Tunnel-</b> Allow the remote dial-in user to trigger an IPSec VPN connection through Internet.				
	<b>L2TP with IPSec Policy -</b> 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.				
	• <b>Must</b> - Specify the IPSec policy to be definitely applied on the L2TP connection.				
	<ul> <li>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. 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.</li> </ul>				
	<b>User Name -</b> This field is applicable when you select PPTP or L2TP with or without IPSec policy above. The maximum length for both username is 11 characters.				
	<b>Password -</b> This field is applicable when you select PPTP or L2TP with or without IPSec policy above. The maximum length for both username is 11 characters.				
	<b>VJ Compression -</b> VJ Compression is used for TCP/IP protocol header compression. This field is applicable when yo select PPTP or L2TP with or without IPSec policy above.				
	<b>IKE Authentication Method</b> - 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.				
	<b>Pre-Shared Key -</b> Check the box of Pre-Shared Key to invoke this function and type in the required characters (1-63) as the pre-shared key. <b>Digital Signature (X.509)</b> –Check the box of Digital Signature to invoke this function and select one predefined Profiles set in the <b>VPN and Remote Access</b> >> <b>IPSec Peer Identity</b> .				
	Local ID – Specify which one will be inspected first.				
	• Alternative Subject Name First – The alternative				

	subject name (configured in Certificate Management>>Local Certificate) will be inspected first.
	• Subject Name First – The subject name (configured in Certificate Management>>Local Certificate) will be inspected first.
	<b>IPSec Security Method</b> - This group of fields is a must for IPSec Tunnels and L2TP with IPSec Policy when you specify the remote node.
	<b>Medium-</b> Authentication Header (AH) means data will be authenticated, but not be encrypted. By default, this option is active.
	<b>High-</b> 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.
GRE over IPSec Settings	<b>Enable IPSec Dial-Out function GRE over IPSec</b> : Check this box to verify data and transmit data in encryption with GRE over IPSec packet after configuring IPSec Dial-Out setting. Both ends must match for each other by setting same virtual IP address for communication.
	Logical Traffic: Such technique comes from RFC2890. Define logical traffic for data transmission between both sides of VPN tunnel by using the characteristic of GRE. Even hacker can decipher IPSec encryption, he/she still cannot ask LAN site to do data transmission with any information. Such function can ensure the data transmitted on VPN tunnel is really sent out from both sides. This is an optional function. However, if one side wants to use it, the peer must enable it, too.
	My GRE IP: Type the virtual IP for router itself for verified by peer. Peer GRE IP: Type the virtual IP of peer host for verified by
	router.
TCP/IP Network Settings	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, which means the Vigor router will get a PPP IP address from the remote router during the IPCP negotiation phase. If the PPP IP address is fixed by remote side, specify the fixed IP address here. Do not change the default value if you do not select PPTP or L2TP.
	<b>Remote Gateway IP</b> - This field is only applicable when you select PPTP or L2TP with or without IPSec policy above. The default value is 0.0.0, which means the Vigor router will get a remote Gateway PPP IP address from the remote router during the IPCP negotiation phase. If the PPP IP address is fixed by remote side, specify the fixed IP address here. Do not change the default value if you do not select PPTP or L2TP.
	<b>Remote Network IP/ Remote Network Mask -</b> 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.				
<b>Local Network IP / Local Network Mask -</b> Add a static route to direct all traffic destined to Local Network IP Address/Local Network Mask through the VPN connection.				
<b>More -</b> Add a static route to direct all traffic destined to more Remote Network IP Addresses/ Remote Network Mask through the VPN connection. This is usually used when you find there are several subnets behind the remote VPN router.				
🤌 LAN-to-LAN Profile - Windows Internet Explorer				
http://192.168.1.1/doc//21MRt.htm				
Profile Index :1				
Remote Network				
Network IP				
Netmask				
255.255.255.255 / 32 💌				
Add Delete Edit				
OK Close				
<b>RIP Direction -</b> 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.				
<b>From first subnet to remote network, you have to do -</b> If the remote network only allows you to dial in with single IP, please choose <b>NAT</b> , otherwise choose <b>Route</b> .				
<b>Change default route to this VPN tunnel -</b> Check this box to change the default route with this VPN tunnel. Note that this setting is available only for one WAN interface is enabled. It is not available when both WAN interfaces are enabled.				

2. After finishing all the settings here, please click **OK** to save the configuration.

-

## **4.9.7 Connection Management**

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

### VPN and Remote Access >> Connection Management

Dial-out	Tool				Refre	esh Sec	onds : 10	Refresh
					✓ Dial	]		
VPN Con Current P	nection Stat age: 1	us				Pa	ge No.	Go >>
VPN	Туре	Remote IP	Virtual Network	Tx Pkts	Tx Rate (Bps)	Rx Pkts	Rx Rate (Bps)	UpTime
					××××××× : C ×××××× : C			

Item	Description				
Dial	Click this button to execute dial out function.				
Refresh Seconds	Choose the time for refresh the dial information among 5, 10, and 30.				
Refresh	Click this button to refresh the whole connection status.				

# 4.10 Certificate Management

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

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

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

Below shows the menu items for Certificate Management.



## 4.10.1 Local Certificate

Certificate Management >> Local Certificate

#### X509 Local Certificate Configuration

Name	Subject	Status	Modify
Local			View Delete
GENERATE X509 L	IMPORT REFRESH		
			<u></u>
			~

Item	Description
Generate	Click this button to open Generate Certificate Request window.

	Certificate Management >> Local Certificate			
	Generate Certificate Request			
	Subject Alternative Name			
	Туре	IP Address		
	IP			
	Subject Name			
	Country (C)			
	State (ST)			
	Location (L)			
	Orginization (O)			
	Orginization Unit (OU)			
	Common Name (CN)			
	Email (E)			
	Кеу Туре	RSA V		
	Key Size	1024 Bit 💌		
	Type in all the infor click <b>Generate</b> agai	Generate mation that the window requests. Then n.		
Import	Click this button to import a saved file as the certification information.			
Refresh	Click this button to refresh the information listed below.			
View	Click this button to view the detailed settings for certificate request.			
Delete	Click this button to delete selected name with certification information.			

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

ENERATE       IMPORT       REFRESH <b>X509 Local Certificate Request</b> BEGIN CERTIFICATE REQUEST         MIIBqjCCARMCAQAwajELMAkGA1UEBhMCVFcxCzAJBgNVBAgTAkhDMQswCQYDVQQH         EwJIQzEQMA4GA1UEChMHRHJheXR1azELMAkGA1UEC×MCUkQxIjAgBgkqhkiG9w0B         CQEWE3N1cHBvcnRAZHJheXR1ay5jb20wg28wDQYJKoZIhvcNAQEBBQADgY0AMIGJ         AoGBALMJdTsqfF97FEpYy+IqeJVJGuSRtqG6Etw8yTUSHQvXpAzcrgJBGrikTUBX         a1X//fgnEccQA2LPSQIQ85Qychwq07Bm0EDf10wHwCa1A2QoGvIi0DMC7f5w9xA8         m6+0f4xZ4QqnjXXgciC0Bj1iAa6MLScelsynZhkgnQ1QN5uFAgMBAAGgADANBgkq         nkiG9w0BAQUFAA0BgQCq3sdwVc21t9qn4U6X2BJsVzu7JHafSSeUnaYDzefCmGfX         9yojHpstNsmWsMRuAwGeKCWc8S/gLtHhr6iccMoToQFx/LWdaEPUSLqryBKKgC9t         eorpDa1/rC92wCra0t8XUmPqNoiytq8BxStTE8vULiIxmwaBvc1hWFSXKVLU7g==	Name Subject		Status	Modify
X509 Local Certificate Request BEGIN CERTIFICATE REQUEST MIIBqjCCARMCAQAwajELMAkGA1UEBhMCVFcxCzAJBgNVBAgTAkhDMQswCQYDVQQH EwJIQzEQMA4GA1UEChMHRHJheXRlazELMAkGA1UECxMCUkQxIjAgBgkqhkiG9w0B CQEWE3N1cHBvcnRA2HJheXRlay5jb20wgZ8wDQYJKoZIhvcNAQEBBQADgYOAMIGJ AoGBALMJdTsqfF97FEPYy+IqeJVJGuSRtqG6Etw8yTUSHQvXpAzcrgJBGrikTUBX a1X//fgnEccQA2LPSQIQ85Qychwq07Bm0EDf10wHwCalA2QoGvIi0DMC7f5w9xA8 m6+0f4x24QQnjXXgciC0Bj1iAa6MLScelsyn2hkgnQ1QNSuFAgMBAAGgADANBgkq hkiG9w0BAQUFAA0BgQCq3sdwVc2lt9qn4U6X2BJsVzu7JHafSSeUnaYDZefCmGfX 9yojHpstNsmWsMRuAwGeKCWc8S/gLtHhr6iccMoToQFx/LWdaEPUSLqryBKKgC9t eorpDa1/rC9ZwCra0t8XUmPqNoiytq8BxStTE8vULiIxmwaBvc1hWFSXKVLU7g==	Local	al /C=TW/ST=HC/L=HC/O=Draytek/O Requesting View D		View Delete
BEGIN CERTIFICATE REQUEST MIIBqjCCARMCAQAwajELMAkGA1UEBhMCVFcxCzAJBgNVBAgTAkhDMQswCQYDVQQH EwJIQzEQMA4GA1UEChMHRHJheXRlazELMAkGA1UECxMCUkQxIjAgBgkqhkiG9w0B CQEWE3N1cHBvcnRAZHJheXRlay5jb20wgZ8wDQYJKoZIhvcNAQEBBQADgYOAMIGJ AoGBALMJdTsqfF97FEpYy+IqeJVJGuSRtqG6Etw8yTU5HQvXpAzcrgJBGrikTUBX a1X//fgnEccQA2LPSQIQ85Qychwq07Bm0EDf10wHwCalAZQoGvIi0DMC7f5w9xA8 m6+0f4xZ4QQnjXXgciCOBj1iAa6MLScelsynZhkgnQ1QN5uFAgMBAAGgADANBgkq hkiG9w0BAQUFAAOBgQCq3sdwVc21t9qn4U6X2BJsVzu7JHafSSeUnaYDZefCmGfX 9yojHpstNsmWsMRuAwGeKCWc8S/gLtHhr6iccMoToQFx/LWdaEPUSLqryBKKgC9t eorpDa1/rC9ZwCra0t8XUmPqNoiytq8BxStTE8vULiIxmwaBvc1hWFSXKVLU7g==	ENERATE	IMPORT REFRESH		
MIIBqjCCARMCAQAwajELMAkGA1UEBhMCVFcxCzAJBgNVBAgTAkhDMQswCQYDVQQH EwJIQzEQMA4GA1UEChMHRHJheXR1azELMAkGA1UECxMCUkQxIjAgBgkqhkiG9wOB CQEWE3N1cHBvcnRAZHJheXR1ay5jb2OwgZ8wDQYJKoZIhvcNAQEBBQADgYOAMIGJ AoGBALMJdTsqfF97FEpYy+IqeJVJGuSRtqG6Etw8yTU5HQvXpAzcrgJBGrikTUBX a1X//fgnEccQA2LPSQIQ85Qychwq07BmOEDf10wHwCa1AZQoGvIiODMC7f5w9xA8 m6+Of4xZ4QQnjXXgciCOBj1iAa6MLScelsynZhkgnQ1QN5uFAgMBAAGgADANBgkq hkiG9w0BAQUFAAOBgQCq3sdwVc21t9qn4U6X2BJsVzu7JHafSSeUnaYDZefCmGfX 9yojHpstNsmWsMRuAwGeKCWc8S/gLtHhr6iccMoToQFx/LWdaEPU5LqryBKKgC9t eorpDa1/rC9ZwCra0t8XUmPqNoiytq8BxStTE8vULiIxmwaBvc1hWFSXKVLU7g==	X509 L	Local Certificate Request		
END CERTIFICATE REQUEST	MIIBq EwJIQ CQEWE AoGBAI a1X//1 m6+0f4	jCCARMCAQAwajELMAkGA1UEBhMCVFcxCzAJJ zEQMA4GA1UEChMHRHJheXRlazELMAkGA1UEC 3N1cHBvcnRAZHJheXRlay5jb2Owg28wDQYJJ LMJdTsqfF97FEpYy+IqeJVJGuSRtqG6Etw8 fgnEccQA2LPSQIQ85Qychwq07Bm0EDf10wH 4xZ4QQnjXXgciCOBj1iAa6MLScelsynZhkgn w0BAQUFAA0BgQCq3sdwVc21t9qn4U6X2BJsV	C×MCURQxIjAgB KoZIhvcNAQEBB yTU5HQvXpAzcr wCalAZQoGvIiO nQ1QN5uFAgMBA Vzu7JHafSSeUn oQFx/LWdaEPU5	gkqhkiG9w0B QADgYOAMIGJ gJBGrikTUBX DMC7f5w9xA8 AGgADANBgkq aYDZefCmGfX LqryBKKgC9t

## 4.10.2 Trusted CA Certificate

Trusted CA certificate lists three sets of trusted CA certificate.

Certificate	Management >>	Trusted	CA	Certificate
-------------	---------------	---------	----	-------------

#### **X509 Trusted CA Certificate Configuration**

Trusted CA-1 View	Modify ew Delete
	ew Delete
Trusted CA-2 View	ew Delete
Trusted CA-3 View	ew Delete

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

Certificate Management >> Trusted CA Certificate

Import X509 Trusted CA Certificate
Select a trusted CA certificate file.
Browse.
Click Import to upload the certification.
Import Cancel

For viewing each trusted CA certificate, click **View** to open the certificate detail information window. If you want to delete a CA certificate, choose the one and click **Delete** to remove all the certificate information.

Cer 🦉	tificate Information - Windows Inter	net Explorer	$\mathbf{\times}$
🥖 http	://192.168.1.200/doc/XCaCfVi2.htm		*
			^
	Certific	ate Detail Information	
	Certificate Name:	Trusted CA-2	
	Issuer:		
	Subject:		≡
	Subject Alternative Name:		
	Valid From:		
	Valid To:		
		Close	~

**Dray** Tek

## 4.10.3 Certificate Backup

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

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

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

## 4.11 VoIP

Note: This function is used for "V" models.

Outlinets Managements & Cartificate Dealeur

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/ $\mu$ -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.

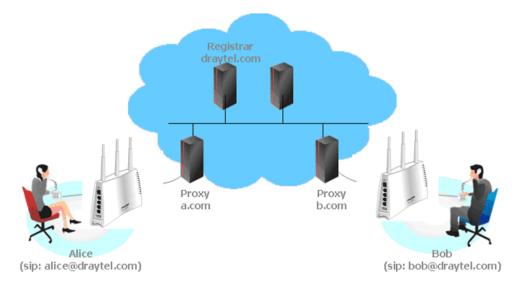
Usually there will be two types of calling scenario, as illustrated below:



### • 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.

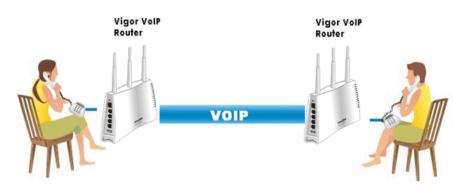
If you both register to the same SIP Registrar, then it will be illustrated as below:



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.

#### Peer-to-Peer

Before calling, you have to know your friend's IP Address. The Vigor VoIP Routers will build connection between each other.



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.

VoIP
DialPlan
SIP Accounts
Phone Settings
▶ DECT
Status

## 4.11.1 DialPlan

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

Phone Book	
<u>Digit Map</u>	
Call Barring	
<u>Regional</u>	
PSTN Setup	
	Digit Map Call Barring Regional

### **Phone Book**

In this section, you can set your VoIP contacts in the "phonebook". It can help you to make calls quickly and easily by using "speed-dial" **Phone Number**. There are total 60 index entries in the phonebook for you to store all your friends and family members' SIP addresses. **Loop through** and **Backup Phone Number** will be displayed if you are using Vigor 2710Vn/VDn for setting the phone book.



#### VoIP >> DialPlan Setup

(ndex	Phone number	Display Name	SIP URL	Dial Out Account	Loop through	Backup Phone Number	Status
1.				Default	None		x
<u>2.</u>				Default	None		x
<u>3.</u>				Default	None		х
<u>4.</u>				Default	None		x
<u>5.</u>				Default	None		х
<u>6.</u>				Default	None		х
<u>7.</u>				Default	None		х
<u>8.</u>				Default	None		x
<u>9.</u>				Default	None		х
<u>10.</u>				Default	None		х
<u>11.</u>				Default	None		х
<u>12.</u>				Default	None		×
<u>13.</u>				Default	None		х
<u>14.</u>				Default	None		х
<u>15.</u>				Default	None		х
<u>16.</u>				Default	None		х
<u>17.</u>				Default	None		х
<u>18.</u>				Default	None		х
<u>19.</u>				Default	None		х
<u>20.</u>				Default	None		х

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

To add a phone number:

Click any index number to display the dial plan setup page. 1.

Vol	P >>	DialP	lan	Setup
			10011	ootap

🗹 Enable		
	Phone Number	1
	Display Name	Polly
	SIP URL	1112 @ fwd.pulver.com
	Dial Out Account	Default 💌
	Loop through	None 💌
	Backup Phone Number	

Item	Description
Enable	Click this to enable this entry.
Phone Number	The speed-dial number of this index. This can be any number you choose, using digits <b>0-9</b> and <b>*</b> .

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	L Enter your friend's SIP Address.	
Dial Out Account	Choose one of the SIP accounts for this profile to dial out. It is useful for both sides (caller and callee) that registered to different SIP Registrar servers. If caller and callee do not use the same SIP server, sometimes, the VoIP phone call connection may not succeed. By using the specified dial out account, the successful connection can be assured.	
Loop through	Choose PSTN to enable loop through function.	
Backup Phone Number	When the VoIP phone is obstructs or the Internet breaks down for some reasons, the backup phone will be dialed out to replace the VoIP phone number. At this time, the phone call will be changed from VoIP phone into PSTN call according to the loop through direction chosen. Note that, during the phone switch, the blare of phone will appear for a short time. And when the VoIP phone is switched into the PSTN phone, the telecom co. might charge you for the connection fee. Please type in backup phone number (PSTN number/ISDN number) for this VoIP phone setting.	

2. After finishing all the settings here, please click **OK** to save the configuration.

## **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	Match Prefix	Mode		OP Number	Min Len	Max Len	Route	Move Up	Move Dowr
1	<ul><li>✓</li></ul>	03	Replace	~	8863	7	9	PSTN N	•	Down
2	<ul><li>✓</li></ul>	886	Strip	~	886	8	10	PSTN N	<u>UP</u>	Down
3			None	$\mathbf{v}$		0	0	PSTN	UP	Down
4			None	$\mathbf{v}$		0	0	PSTN N	UP	Down
5			None	$\mathbf{v}$		0	0	PSTN N	UP	Down
6			None	$\mathbf{v}$		0	0	PSTN N	UP	Down
7			None	$\mathbf{v}$		0	0	PSTN N	UP	Down
8			None	~		0	0	PSTN	UP	Down
17			None	$\sim$		0	0	PSTN	<u>UP</u>	Dowr
18			None	$\sim$		0	0	PSTN N	<u>UP</u>	Dowr
19			None	$\sim$		0	0	PSTN N	<u>UP</u>	Dowr
20			None	~		0	0	PSTN	UP	

#### VoIP >> DialPlan Setup

Note: 1. The length for Min Len and Max Len fields should be between 0~25. 2. Wildcard '?' is supported.

OK Cancel

Item	Description
Enable	Check this box to invoke this setting.
Match Prefix	It is used to match with the number you dialed and can be modified with the <b>OP Number</b> by the mode (add, strip or replace).
Mode	None - No action.
	<b>Add</b> - When you choose this mode, the OP number will be added with the prefix number for calling out through the specific VoIP interface.
	<b>Strip</b> - When you choose this mode, the OP number will be deleted by the prefix number for calling out through the specific VoIP interface. Take the above picture (Prefix Table Setup web page) as an example, the OP number of 886 will be deleted completely for the prefix number is set with 886.
	<b>Replace</b> - 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 "88631111111" and sent to SIP server. Mode Replace ✓ None Add Strip Replace	
OP Number	The front number you type here is the first part of the account number that you want to execute special function (according to the chosen mode) by using the prefix number.	
Min Len	Set the minimal length of the dial number for applying the prefix number settings. Take the above picture (Prefix Table Setup web page) as an example, if the dial number is between 7 and 9, that number can apply the prefix number settings here.	
Max Len	Set the maximum length of the dial number for applying the prefix number settings.	
Route	Choose the one that you want to enable the prefix number settings from the saved SIP accounts. Please set up one SIP account first to make this interface available. This item will be changed according to the port settings configured in <b>VoIP&gt;&gt; Phone Settings</b> .	
Move UP /Move Down	Click the link to move the selected entry up or down.	

# **Call Barring**

Call barring is used to block phone calls coming from the one that is not welcomed.

VoIP >> DialPlan Setup	Vo	IP	>>	Dia	IPlan	Setup	
------------------------	----	----	----	-----	-------	-------	--

Index	Call Direction	Barring Type	Barring Number/URL/URI	Route	Schedule	Status
<u>1.</u>				Wizard1		х
<u>2.</u>				Wizard1		x
<u>3.</u>				Wizard1		х
<u>4.</u>				Wizard1		х
<u>5.</u>				Wizard1		x
<u>6.</u>				Wizard1		х
<u>7.</u>				Wizard1		х
<u>8.</u>				Wizard1		x
<u>9.</u>				Wizard1		х
<u>10.</u>				Wizard1		х

Advanced: Block Anonymous Block Unknown Domain Block IP Address

To create a call baring profile:

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

Call Barring Index No. 1	
✓ Enable	
Call Direction	IN 💌
Barring Type	Specific URI/URL 💌
Specific URI/URL	
Route	1-Wizard1 💌
Index(1-15) in Schedule Setup	All
ote:Wildcard '?' is supported.	

Item	Description	
Enable	Check it to enable this entry.	
Call Direction	Determine the direction for the phone call, IN – incoming call, OUT-outgoing call, IN & OUT – both incoming and outgoing calls.	
Barring Type	Determine the type of the VoIP phone call, URI/URL or number. Specific URI/URL Specific URI/URL Specific Number	
Specific URI/URL or Specific Number	This field will be changed based on the type you selected for barring Type.	
Route	All means all the phone calls will be blocked with such mechanism.	
Index (1-15) in Schedule	Enter the index of schedule profiles to control the call barring according to the preconfigured schedules. Refer to section <b>Applications&gt;&gt;Schedule</b> for detailed configuration.	

2. After finishing all the settings here, please click **OK** to save the configuration.

VoIP >> DialPlan Setup

Call Bar	ring Setup			1.3	Set to Factory	Default
Index	Call Direction	Barring Type	Barring Number/URL/URI	Route	Schedule	Status
<u>1.</u>	IN	Specific URI/URL		Wizard1		v
<u>2.</u>				Wizard1		x
<u>3.</u>				Wizard1		х
4.				Wizard1		X

Additionally, you can set advanced settings for call barring such as **Block Anonymous**, **Block Unknown Domain** or **Block IP Address**. Simply click the relational links to open the web page.

For **Block Anonymous** – this function can block the incoming calls without caller ID on the interface (Phone port) specified in the following window. Such control also can be done based on preconfigured schedules.

#### Web page for Vigor2710Vn----

#### VoIP >> DialPlan Setup

Call Barring Block Anonymous					
🗹 Enable					
Route	Phone1 Phone2				
Index(1-15) in <u>Schedule</u> Setup	, , , , ,				
Note:Block the incoming calls which do not have the caller ID.					
ОК	Cancel				
Web page for Vigor2710VDn					
VoIP >> DialPlan Setup					

Call Barring Block Anonymous	
Enable	
Route	Phone
	DECT1 DECT2 DECT3
	DECT4 DECT5 DECT6
Index(1-15) in <u>Schedule</u> Setup	,,,

Note:Block the incoming calls which do not have the caller ID.

OK	Cancel
UN	Cancer

For **Block Unknown Domain** – this function can block incoming calls (through Phone port) from unrecognized domain that is not specified in SIP accounts.

### Web page for Vigor2710Vn----

Call Barring Block Unknown Domain	
🗹 Enable	
Route	Phone1 Phone2
Index(1-15) in <u>Schedule</u> Se	tup,,,
<b>lote</b> :If the domain of the incoming call hould be blocked.	is different from the domain found in SIP accounts, the call
	OK Cancel
Veb page for Vigor2710VDn	
Veb page for Vigor2710VDn olP >> DialPlan Setup Call Barring Block Unknown Domain	
olP >> DialPlan Setup	
Call Barring Block Unknown Domain	
Call Barring Block Unknown Domain	
Call Barring Block Unknown Domain	Phone
Call Barring Block Unknown Domain	Phone       DECT1     DECT2     DECT3       DECT4     DECT5     DECT6

For **Block IP Address** – this function can block incoming calls (through Phone port) coming from IP address.

#### Web page for Vigor2710Vn----

VoIP >> DialPlan Setup	
Call Barring Block IP Address	
🗹 Enable	
Route	Phone1 Phone2
Index(1-15) in Schedule	Setup , , , , ,
Note: The incoming calls by means of	f IP dialing (e.g.#192*168*1*1#) should be blocked.
	OK Cancel

### Web page for Vigor2710DVn---

VoIP >> DialPlan Setup

Call Barring Block IP Address	
Enable	
Route	Phone
	DECT1 DECT2 DECT3
	DECT4 DECT5 DECT6
Index(1-15) in <u>Schedule</u> Setup	
Note: The incoming calls by means of IP dialing	(e.g.#192*168*1*1#) should be blocked.

Cancel

ОК



## Regional

This page allows you to process incoming or outgoing phone calls by regional. Default values (common used in most areas) will be shown on this web page. You *can change* the number based on the region that the router is placed.

#### VoIP >> DialPlan Setup

🗹 Enable Regional			1	Set to Fac	tory Default
Last Call Return [Miss]:	*69	]			
Last Call Return [In]:	*12	]	Last Call Return [Out]:	*14	
Call Forward [All] [Act]:	*72	+number+#	Call Forward [Deact]:	*73	+#
Call Forward [Busy] [Act]:	*90	+number+#	Call Forward [No Ans] [Act]:	*92	+number+#
Do Not Disturb [Act]:	*78	+#	Do Not Disturb [Deact]:	*79	+#
Hide caller ID [Act]:	*67	+#	Hide caller ID [Deact]:	*68	+#
Call Waiting [Act]:	*56	+#	Call Waiting [Deact]:	*57	+#
Block Anonymous [Act]:	*77	+#	Block Anonymous [Deact]:	*87	+#
Block Unknow Domain [Act]:	*40	+#	Block Unknow Domain [Deact]:	*04	+#
Block IP Calls [Act]:	*50	+#	Block IP Calls [Deact]:	*05	+#
Block Last Calls [Act]:	*60	+#			

Cancel

ΟK

Item	Description
Enable Regional	Check this box to enable this function.
Last Call Return [Miss]	Sometimes, people might miss some phone calls. Please dial number typed in this field to know where the last phone call comes from and call back to that one.
Last Call Return [In]	You have finished an incoming phone call, however you want to call back again for some reason. Please dial number typed in this field to call back to that one.
Last Call Return [Out]	Dial the number typed in this field to call the previous outgoing phone call again.
Call Forward [All][Act]	Dial the number typed in this field to forward all the incoming calls to the specified place.
Call Forward [Deact]	Dial the number typed in this field to release the call forward function.
Call Forward [Busy][Act]	Dial the number typed in this field to forward all the incoming calls to the specified place while the phone is busy.
Call Forward [No Ans][Act]	Dial the number typed in this field to forward all the incoming calls to the specified place while there is no answer of the connected phone.
Do Not Disturb [Act]	Dial the number typed in this field to invoke the function of DND.



Item	Description
Do Not Distrub [Deact]	Dial the number typed in this field to release the DND function.
Hide caller ID [Act]	Dial the number typed in this field to make your phone number (ID) not displayed on the display panel of remote end.
Hide caller ID [Deact]	Dial the number typed in this field to release this function.
Call Waiting [Act]	Dial the number typed in this field to make all the incoming calls waiting for your answer.
Call Waiting [Deact]	Dial the number typed in this field to release this function.
Block Anonymous[Act]	Dial the number typed in this field to block all the incoming calls with unknown ID.
Block Anonymous[Deact]	Dial the number typed in this field to release this function.
Block Unknown Domain [Act]	Dial the number typed in this field to block all the incoming calls from unknown domain.
Block Unknown Domain [Deact]	Dial the number typed in this field to release this function.
Block IP Calls [Act]	Dial the number typed in this filed to block all the incoming calls from IP address.
Block IP Calls [Deact]	Dial the number typed in this field to release this function.
Block Last Calls [Act]	Dial the number typed in this field to block the last incoming phone call.

After finishing all the settings here, please click **OK** to save the configuration.

# **PSTN Setup**

Some emergency phone (e.g., 911) or special phone cannot be dialed out by using VoIP and can be called out through PSTN line only. To solve this problem, this page allows you to set five sets of PSTN number for dialing without passing through Internet. Please type the number in the field of **phone number for PSTN relay**.

#### VoIP >> PSTN Setup

Enable	phone number for PSTN relay

Then, check the **Enable** box to make the PSTN number available for dial whenever you need. After finishing all the settings here, please click **OK** to save the configuration.



**Note:** A Line port on the router allows connection to a PSTN line so the user can select either the PSTN or VoIP for the calls, and can access the PSTN line during power black-outs when VoIP is cut off (only available on port 2).

## 4.11.2 SIP Accounts

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

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

## SIP Accounts Web Page for Vigor2710 Vn ------

VolP	>>	SIP	Accounts

Index	Profile	Domain/Realm	Proxy	Account Name	Codec	Ring	Port	Status
1	Wizard1	draytel.org	draytel.org	5633s	G.729A/B	Phone1	Phone2	-
2					G.729A/B	Phone1	Phone2	-
<u>3</u>					G.729A/B	Phone1	Phone2	-
<u>4</u>					G.729A/B	Phone1	Phone2	-
<u>5</u>					G.729A/B	Phone1	Phone2	-
<u>6</u>					G.729A/B	Phone1	Phone2	-

#### NAT Traversal Setting

STUN Server:	
External IP:	
SIP PING Interval:	150 sec

OK

# SIP Accounts Web Page for Vigor2710 VDn ------

1	101	P	>>	9	P	Δ	0	0		i n	n	te
- 1	7 U I			0				•	U,	ч		ເວ

			_					
Index	Profile	Domain/Realm	Proxy	Account Name	Codec	Ring	g Port	Status
						🗌 Phone		
1					G.711MU	DECT1	DECT2	_
1					G.711MO	DECT3	DECT4	
						DECT5	DECT6	
						🗌 Phone		
						DECT1	DECT2	
2					G.711MU	DECT3	DECT4	-
						DECT5	DECT6	
						Phone		
						DECT1	DECT2	
<u>6</u>					G.711MU	DECT3	DECT4	-
						DECT5	DECT6	
					D'		qistered on S	ID corver
							ter on SIP se	
VAT Tr	aversal	Setting						
	STU	N Server:						
External IP:								
	SIP I	PING Interval:		150 sec				

## Available settings are explained as follows:

Item	Description			
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 @.			
Codec	Display the codec type for the account.			
Ring Port	Specify which port will ring when receiving a phone call.			
Status	Show the status for the corresponding SIP account. <b>R</b> means such account is registered on SIP server successfully. – means the account is failed to register on SIP server.			
STUN Server	Type in the IP address or domain of the STUN server.			
External IP	Type in the gateway IP address.			
SIP PING interval	The default value is 150 (sec). It is useful for a Nortel server			

# **Dray** Tek

Item	Description
	NAT Traversal Support.

Click any index link to open the following web page.

## SIP Accounts Web Page for Vigor2710 Vn ------

VoIP >> SIP Accounts

Profile Name	Wizard1 (11 char ma	x.)
Register via	Auto 🔽 🗌 Call without Re	egistration
SIP Port	5060	
Domain/Realm	draytel.org	(63 char max.)
Proxy	draytel.org	(63 char max.)
Act as outbound pro	ху	
Display Name	(23 char ma	x.)
Account Number/Name	5633s	(63 char max.)
Authentication ID	5633s	(63 char max.)
Password		63 char max.)
Expiry Time	1 hour 🖌 3600 sec	
NAT Traversal Support	None 🗸	
Call Forwarding	Disable 👻	
SIP URL		
Time Out	30 sec	
Ring Port	Phone1 Phone2	
Ring Pattern	1 🗸	
Prefer Codec	G.729A/B (8Kbps) 🔽 🔲 Sing	le Codec
Packet Size	20ms 💌	
Voice Active Detector	Off 🗸	

## SIP Accounts Web Page for Vigor2710 VDn ------

### VoIP >> SIP Accounts

Profile Name	(11 char max.)
Register via	None 🔽 🗌 Call without Registration
SIP Port	5060
Domain/Realm	(63 char max.)
Proxy	(63 char max.)
Act as outbound pro:	×y
Display Name	(23 char max.)
Account Number/Name	(63 char max.)
Authentication ID	(63 char max.)
Password	(63 char max.)
Expiry Time	1 hour 💌 3600 sec
NAT Traversal Support	None 💌
	Phone
Ring Port	DECT1 DECT2 DECT3
	DECT4 DECT5 DECT6
Ring Pattern	1 🕶
Prefer Codec	G.711MU (64Kbps) 💟 🗌 Single Codec
Packet Size	20ms 💌
Voice Active Detector	Off 🔽

Item	Description
Profile Name	Assign a name for this profile for identifying. You can type similar name with the domain. For example, if the domain name is <i>draytel.org</i> , then you might set <i>draytel-1</i> in this field.
Register via	If you want to make VoIP call without register personal information, please choose <b>None</b> and check the box to achieve the goal. Some SIP server allows user to use VoIP function without registering. For such server, please check the box of <b>Call without Registration</b> . Choosing <b>Auto</b> is recommended. The system will select a proper way for your VoIP call. None Auto WAN1 LAN/VPN PVC
SIP Port	Set the port number for sending/receiving SIP message for building a session. The default value is <b>5060.</b> 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 <b>:port number</b> after the domain name to



	specify that port as the destination of data transmission (e.g., <b>nat.draytel.org:5065</b> )				
Act as Outbound Proxy	Check this box to make the proxy acting as outbound proxy.				
Display Name	The caller-ID that you want to be displayed on your friend's screen.				
Account Number/Name	Enter your account name of SIP Address, e.g. every text before @.				
Authentication ID	Check the box to invoke this function and enter the name or number used for SIP Authorization with SIP Registrar. If this setting value is the same as Account Name, it is not necessary for you to check the box and set any value in this field.				
Password	The password provided to you when you registered with a SIP service.				
Expiry Time	The time duration that your SIP Registrar server keeps your registration record. Before the time expires, the router will send another register request to SIP Registrar again.				
NAT Traversal Support	If the router (e.g., broadband router) you use connects to internet by other device, you have to set this function for your necessity.				
	NAT Traversal Support None  None Stun Manual Nortel				
	<b>None</b> – Disable this function.				
	<b>Stun</b> – Choose this option if there is Stun server provided for your router.				
	<b>Manual</b> – Choose this option if you want to specify an external IP address as the NAT transversal support.				
	<b>Nortel</b> – If the soft-switch that you use supports Nortel solution, you can choose this option.				
Call Forwarding	There are four options for you to choose. <b>Disable</b> is to close call forwarding function. <b>Always</b> means all the incoming calls will be forwarded into SIP URL without any reason. <b>Busy</b> means the incoming calls will be forwarded into SIP URL only when the local system is busy. <b>No Answer</b> means if the incoming calls do not receive any response, they will be forwarded to the SIP URL by the time out.				
	Always Busy No Answer Busy or No Answer				
	<b>SIP URL</b> – Type in the SIP URL (e.g., aaa@draytel.org or abc@iptel.org) as the site for call forwarded.				



	<b>Time Out</b> – Set the time out for the call forwarding. The default setting is 30 sec.
Ring Port	Set Phone 1 and/or Phone 2 as the default ring port(s) for this SIP account.
Ring Pattern	Choose a ring tone type for the VoIP phone call. Ring Pattern  1 2 3 4 5 6
Prefer Codec	<ul> <li>Select one of five codecs as the default for your VoIP calls. The codec used for each call will be negotiated with the peer party before each session, and so may not be your default choice. The default codec is G.729A/B; it occupies little bandwidth while maintaining good voice quality.</li> <li>If your upstream speed is only 64Kbps, do not use G.711 codec. It is better for you to have at least 256Kbps upstream if you would like to use G.711.</li> <li>G.711MU (64Kbps)</li> <li>G.723 (6.4kbps)</li> <li>G.726_32 (32kbps)</li> <li>iLBC_15 (15.20kbps)</li> <li>iLBC_13 (13.20kbps)</li> <li>G.722_64 (64Kbps)</li> <li>Single Codec – If the box is checked, only the selected Codec will be applied.</li> </ul>
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 m voice information. Packet Size 20ms 10ms 20ms 30ms 40ms 50ms 60ms
Voice Active Detector	This function can detect if the voice on both sides is active or not. If not, the router will do something to save the bandwidth for other using. Click On to invoke this function; click off to close the function. Voice Active Detector Off Off On

After finishing all the settings here, please click **OK** to save the configuration.



## 4.11.3 Phone Settings

This page allows user to set phone settings for Phone 1 and Phone 2 respectively. However, it changes slightly according to different model you have.

#### Phone Settings Web Page for Vigor2710 Vn ------

VoIP >> Phone Settings

Index	Port	Call Feature	Tone	Gain (Mic/Speaker)	Default SIP Account	DTMF Relay
1	Phone1	CW,CT,	User Defined	5/5	Wizard1	InBand
<u>2</u>	Phone2	CW,CT,	User Defined	5/5	Wizard1	InBand

ONLY Phone 2 can access the PSTN line during power failure.

RTP

ixiii		
	Symmetric RTP	
	Dynamic RTP Port Start	10050
	Dynamic RTP Port End	15000
	RTP TOS	IP precedence 5 🛛 🖌 10100000
		OK

#### Phone Settings Web Page for Vigor2710 VDn ------

VoIP >> Phone Settings

Phone I	.ist					
Index	Port	Call Feature	Tone	Gain (Mic/Speaker)	Default SIP Account	DTMF Relay
1	Phone	CW,CT,	User Defined	5/5		InBand
2	DECT1		User Defined	5/5		InBand
<u>3</u>	DECT2		User Defined	5/5		InBand
<u>4</u>	DECT3		User Defined	5/5		InBand
<u>5</u>	DECT4		User Defined	5/5		InBand
<u>6</u>	DECT5		User Defined	5/5		InBand
<u>Z</u>	DECT6		User Defined	5/5		InBand

📃 Disable Port: Phone

Note: If Phone port is disabled, Phone could not be used anymore.

However, its dsp resource could be used by DECT and DECT could dial 4 voip call at the same time. Otherwise, DECT could only dial 3 voip call at the same time.

#### RTP

NTF		
	Symmetric RTP	
	Dynamic RTP Port Start	10050
	Dynamic RTP Port End	15000
	RTP TOS	IP precedence 5
		ОК

Item	Description
Phone List	<b>Port – Phone, Phone1/Phone2</b> allow you to set general settings for PSTN phones. DECT1-6 allow you to set general settings for DECT phone.
	Call Feature – A brief description for call feature will be



s DSP resource could be used by DECT and d dial 4 VoIP calls at the same time.		
<ul> <li>ttings page of Phone Index.</li> <li>lay the volume gain settings for Mic/Speaker that n the advanced settings page of Phone Index.</li> <li>Account – "draytel_1" is the default SIP u can click the number below the Index field to account for each phone port.</li> <li>ay – Display DTMF mode that configured in the ttings page of Phone Index.</li> <li>rt is disabled, Phone could not be used anymore.</li> <li>s DSP resource could be used by DECT and d dial 4 VoIP calls at the same time.</li> </ul>		
n the advanced settings page of Phone Index. • Account – "draytel_1" is the default SIP u can click the number below the Index field to account for each phone port. • ay – Display DTMF mode that configured in the ttings page of Phone Index. • tt is disabled, Phone could not be used anymore. • s DSP resource could be used by DECT and d dial 4 VoIP calls at the same time.		
ttings page of Phone Index. rt is disabled, Phone could not be used anymore. s DSP resource could be used by DECT and d dial 4 VoIP calls at the same time.		
s DSP resource could be used by DECT and d dial 4 VoIP calls at the same time.		
If Phone port is disabled, Phone could not be used anymore. However, its DSP resource could be used by DECT and DECT could dial 4 VoIP calls at the same time. Otherwise, DECT could only dial 3 VoIP calls at the same time.		
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.		
<b>Dynamic RTP Port Start</b> - Specifies the start port for RTP stream. The default value is 10050.		
<b>Dynamic RTP Port End</b> - Specifies the end port for RTP stream. The default value is 15000.		
<b>RTP TOS</b> – It decides the level of VoIP package. Use the drop down list to choose any one of them.		
Manual IP precedence 1 IP precedence 2 IP precedence 3 IP precedence 4 IP precedence 5 IP precedence 6		

After finishing all the settings here, please click **OK** to save the configuration.



### **Detailed Settings for Phone Port**

Click the *number link* for Phone/DECT port, you can access into the following page for configuring Phone settings.

### Phone Port Web Page for Vigor2710 Vn ------

VoIP >> Phone Settings

Phone1			
Call Feature		Default SIP Account	1-Wizard1 🗸
Hotline		Play dial tone only when a	count registered
Session Timer	90 sec		i i i i i i i i i i i i i i i i i i i
T.38 Fax Function			
Error Correction Mode	REDUNDANCY 🔽		
DND(Do Not Disturb) N Index(1-15) in <u>Sched</u>			
Note: Action and Idl ignored.	e Timeout settings will be		
Index(1-60) in Phone	Book as Exception List:		
CLIR (hide caller ID)			
Call Waiting			
Call Transfer			
	OK Ca	ncel Advanced	

### DECT Port Web Page for Vigor2710 VDn ------

#### VoIP >> Phone Settings

DECT1			
Call Feature		Default SIP Account	
🔲 Hotline		Play dial tone only when account registered	
🔲 Session Timer	90 sec		
T.38 Fax Function			
Call Forwarding	Disable 👻		
SIP URL			
Time Out	Time Out 30 sec		
🔲 DND(Do Not Disturb) N	Mode		
Index(1-15) in <u>Sche</u>	edule Setup:		
Note: Action and In be ignored.	dle Timeout settings will		
Index(1-60) in <u>Phon</u>	e Book as Exception List:		
CLIR (hide caller ID)			
	OK Ca	Advanced	

Item	Description
	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	Check the box to enable T.38 fax function.		
	<b>Error Correction Mode</b> – choose a mode for error correction.		
	T.38 Fax Function		
	Error Correction Mode REDUNDANCY V REDUNDANCY FEC		
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.		
	<ul> <li>Index (1-15) in Schedule - Enter the index of schedule</li> <li>profiles to control when the phone will ring and when will</li> <li>not according to the preconfigured schedules. Refer to</li> <li>section Application &gt;&gt;Schedule for detailed configuration.</li> <li>Index (1-60) in Phone Book - Enter the index of phone book</li> <li>profiles. Refer to section DialPlan – Phone Book for</li> <li>detailed configuration.</li> </ul>		
CLIR (hide caller ID)	Check this box to hide the caller ID on the display panel of the phone set.		
Call Waiting	Check this box to invoke this function. A notice sound will appear to tell the user new phone call is waiting for your response. Click hook flash to pick up the waiting phone call.		
Call Transfer	Check this box to invoke this function. Click hook flash to initiate another phone call. When the phone call connection succeeds, hang up the phone. The other two sides can communicate, then.		
Default SIP Account	You can set SIP accounts (up to six groups) on SIP Account page. Use the drop down list to choose one of the profile names for the accounts as the default one for this phone setting.		
	<b>Play dial tone only when account registered -</b> 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

Advance	Settings	>> P	hone 1
---------	----------	------	--------

Tone Settings						
Region User Defined	*		C	aller ID Type	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	400	0	400	350	225	525
Volume Gain			DTMF			
Mic Gain(1-10)	5		DTMF Mod		InBand	*
Speaker Gain(1-10)	5		Payload T (96 - 127)	ype (RFC2833	3) ₁₀₁	
MISC						
Dial Tone Power Leve	l (1 - 50) 27	•				
Ring Frequency (10 -	50HZ) 25	,				
Call Waiting Tone Pov (1 - 30)	ver Level 13	ł				
		ОК	Cancel			

Item	Description
Region	Select the proper region which you are located. The common settings of <b>Caller ID Type</b> , <b>Dial tone</b> , <b>Ringing tone</b> , <b>Busy</b> <b>tone</b> and <b>Congestion tone</b> will be shown automatically on the page. If you cannot find out a suitable one, please choose <b>User</b> <b>Defined</b> and fill out the corresponding values for dial tone, ringing tone, busy tone, congestion tone by yourself for VoIP phone.
	Tone Settings
	Region       User Defined         User Defined       0         UK       0         Dia       US         Dia       0         Dia       0         Ringi       Italy         Bus       Germany         Netherlands       00         Sweden       00
	Volume (Australia Mic Gain() Slovenia Speaker Speaker
	Slovakia         MISC         Dial Tone         France         Ring Free         UK_CCA         Call Wait         China         Taiwan

Item	Description		
	Also, you can specify each field for your necessity. It is recommended for you to use the default settings for VoIP communication.		
Volume Gain	Mic Gain (1-10)/Speaker Gain (1-10) - Adjust the volume of microphone and speaker by entering number from 1- 10. The larger of the number, the louder the volume is.		
MISC	<b>Dial Tone Power Level</b> - 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.		
	<b>Ring Frequency</b> - This setting is used to drive the frequency of the ring tone. It is recommended for you to use the default setting.		
	<b>Call Waiting Tone Power Level</b> - This setting is used to adjust the loudness of the call waiting tone. The smaller the number is, the louder the tone is. It is recommended for you to use the default setting.		
DTMF	<b>DTMF Mode</b> – There are four DTMF modes for you to choose.		
	DTMF mode InBand InBand OutBand ( RFC2833) SIP INFO (cisco format) SIP INFO (nortel format)		
	• <i>InBand</i> - Choose this one then the Vigor will send the DTMF tone as audio directly when you press the keypad on the phone.		
	• <b>OutBand</b> - 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.		
	• <i>SIP INFO</i> - 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.		
	<b>Payload Type (rfc2833)</b> - Choose a number from 96 to 127, the default value was 101. This setting is available for the OutBand (RFC2833) mode.		

After finishing all the settings here, please click  $\mathbf{OK}$  to save the configuration.

### 4.11.4 DECT

From this page, you can enable register or deregister handsets for using DECT function.

VoIP >> DECT

#### Handset Status

FwVersion: 0x100, LinkDate: 08.07.04.14.31, DectType: EU Dect

Handset	Status	PCM Channel	Deregister Handset	Wideband Voice	Ring Handset
1	HS_NOT_REGISTERED	255	Deregister	Uvideband Voice	Ring
2	HS_NOT_REGISTERED	255	Deregister	Wideband Voice	Ring
з	HS_NOT_REGISTERED	255	Deregister	Uvideband Voice	Ring
4	HS_NOT_REGISTERED	255	Deregister	Wideband Voice	Ring
5	HS_NOT_REGISTERED	255	Deregister	Uvideband Voice	Ring
6	HS_NOT_REGISTERED	255	Deregister	Wideband Voice	Ring

Refresh Seconds: 10 🔽

Refresh

Note: Please make sure your DECT handset supports wideband voice, then enable Wideband function. Otherwise, DECT incoming call may hear noisy voice. Please also setup voip codec as G.722_64 to make your voice quality better.

DECT phone access code : 1234 Note: Default DECT phone access code is 1234.

Enable Registration Mode

Deregister All Handset

Item	Description
Refresh Seconds	Specify the interval of refresh time to obtain the latest VoIP calling information. The information will update immediately when the <b>Refresh</b> button is clicked.
Handset	After DECT phone registered with router, it would be assigned one unique handset ID.
Status	It is used to indicate the DECT handset status. For example, if you have registered with router DECT module, you would get – <b>F00_REGISTERED_IDLE</b> . If you get one incoming call for this DECT handset, you would see - <b>F07_CALL_RECEIVED.</b>
PCM Channel	This field can distinguish which PCM channel is used by the handset. 255 (default setting) means it is idle and voice data is not transferred through any PCM channel.
Deregister Handset	If your handset has registered to the router, you could use this button to deregister it from router.
Wideband Voice	Check this box to enable the function to avoid hearing noisy voice.
Ring Handset	Check this box to enable the function.



DECT phone access mode	When registering with DECT phone, you will be asked to type access code. The default setting in Vigor2710VDn is <b>1234</b> .
Enable Registration Mode	If you want to use handset to register with the router, you need to enable DECT module registration mode via this button. Otherwise, you can't search our DECT base station from the air.
Deregister All Handset	Deregister all registered handset.

### Example:

Vigor 2710 VDn provides a DECT GAP/CAT-iq base module, which can facilitate 4 simultaneous wireless audio connections and 6 phone registrations.

1. Open VoIP>>DECT.

V	olP
Þ	DialPlan
Þ	SIP Accounts
Þ	Phone Settings
Þ	DECT
Þ	Status

Note: DECT menu will appear if DECT module is detected.

2. In the web page, please click **Enable Registration Mode** and wait for DECT handset to register.

VoIP >> DECT

Handset 1 is registered and idle. You could try to deregister by button.

Handset Status

FwVersion: 0x101, LinkDate: 08.08.07.16.04, DectType: EU Dect

Handse	et Status	PCM Channel	Deregister Handset
1	F00_REGISTERED_IDLE	255	Deregister
2	HS_NOT_REGISTERED	255	Deregister
3	HS_NOT_REGISTERED	255	Deregister
4	HS_NOT_REGISTERED	255	Deregister
5	HS_NOT_REGISTERED	255	Deregister
6	HS_NOT_REGISTERED	255	Deregister

Enable Registration Mode

 Waiting for DECT handset to register.
 Enable DECT registration mode by this button or press DECT button for more than 2 seconds. This state could last for 2 minutes. 3. When the registration is finished, open **VoIP>>SIP** Accounts. The Registered DECT phone will be available for you to choose. Choose the one you need.

SIP Accounts Li	Registered DECT DECT Ring Port.	handset could be		Refresh
Index Profile Do	main/RealmProxy	Account Name	Ring Port	Status
1			Phone DECT1 DECT2 DECT3 DECT4 DECT5 DECT6	4   -
2			<ul> <li>Phone</li> <li>DECT1 DECT2</li> <li>DECT3 DECT2</li> <li>DECT5 DECT6</li> </ul>	-
<u>3</u>			<ul> <li>Phone</li> <li>DECT1 DECT2</li> <li>DECT3 DECT4</li> </ul>	

4. Open **VoIP>>Status**. Information for the active DECT phone will be shown as follows.

VoIP >:	> Status	5										
Status							R	efresh	Secon	ds:	10 💌	1
Port	Status	Codec	PeerID	Elapse (hh:mm:ss)	Tx Pkts		Rx Losts	Rx Jitter (ms)	In Calls		Miss Calls	
Phone	IDLE			00:00:00	0	0	0	0	0	0	0	
DECT1	IDLE			00:00:00	0	0	0	0	0	0	0	
DECT2	IDLE			00:00:00	0	0	0	0	0	0	0	
DECT3	IDLE			00:00:00	0	0	0	0	0	0	0	
DECT4	IDLE			00:00:00	0	0	0	0	0	0	0	

0

00:00:00 0 0

0

0 0

0

2 0

0 0

DECT5 ACTIVE 729A/B 1@192.168.1.2 00:00:14 414 414

DECT6 IDLE

Vigor2710 Series User's Guide

# **Dray** Tek

5

5

5. When registering with DECT phone, you will be asked to type access code. The default setting in Vigor2710VDn is **1234**. Please open **VoIP>>Phone Settings** to modify it if required.

<u>3</u>	DECT2	G.729A/B	User Defined	5/5	InBand
4	DECT3	G.729A/B	User Defined	5/5	InBand
<u>5</u>	DECT4	G.729A/B	User Defined	5/5	InBand
<u>6</u>	DECT5	G.729A/B	User Defined	5/5	InBand
<u>7</u>	DECT6	G.729A/B	User Defined	5/5	InBand

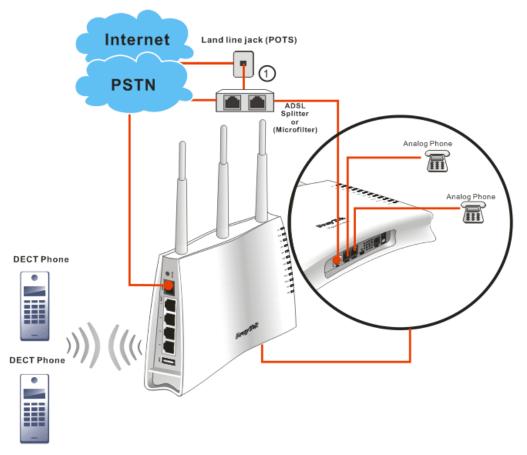
Disable Port: Phone

**Note:** If Phone port is disabled, Phone could not be used anymore. However, its dsp resource could be used by DECT and DECT could dial 4 voip call at the same time.

Otherwise, DECT could only dial 3 voip call at the same time.

DECT phone access code :	1234	Setup DECT phone access code here. Default value is 1234.
Note: Default DECT phone	access code is 1234.	

The following diagram shows the brief construction of DECT phone (handset) and Vigor router.



# 4.11.5 Status

From this page, you can find codec, connection and other important call status for each port. For Vigor2710 Vn ------

VoIP >> Status

Status								Refres	n Seco	nds:	10 🛰	Refresh
Port	Status	Codec	PeerID	Elapse (hh:mm:ss)	Tx Pkts	Rx Pkts	Rx Losts	Rx Jitter (ms)	In Calls	Out Calls		Speake Gain
Phone1	IDLE			00:00:00	0	0	0	0	0	0	0	5
Phone2	IDLE			00:00:00	0	0	0	0	0	0	0	5
Log												
Date		Time		Duration	I	n/Out	/Miss	Acc	ount :	ID	Peer	ID
(mm-dd-y	(עעע	(hh:m	m:ss)	(hh:mm:s	з)							
-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	_							

### For Vigor2710 VDn ------

VoIP >> Status

Status								Refres	n Seco	nds: [	10 🛩	Refresh
Port	Status	Codec	PeerID	Elapse (hh:mm:ss)		Rx Pkts	Rx Losts	Rx Jitter (ms)	In Calls	Out Calls		Speaker Gain
Phone	IDLE			00:00:00	0	0	0	0	0	0	0	5
DECT1	IDLE			00:00:00	0	0	0	0	0	0	0	5
DECT2	IDLE			00:00:00	0	0	0	0	0	0	0	5
DECT3	IDLE			00:00:00	0	0	0	0	0	0	0	5
DECT4	IDLE			00:00:00	0	0	0	0	0	0	0	5
DECT5	IDLE			00:00:00	0	0	0	0	0	0	0	5
DECT6	IDLE			00:00:00	0	0	0	0	0	0	0	5

Log

Date		Time	Duration	In/Out/Miss	Account ID	Peer ID
(mm-dd-	YYYY)	(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	-	-	

Each item is explained as follows:

Item	Description
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 Phone1 and Phone2.
Status	It shows the VoIP connection status.
	<b>IDLE -</b> Indicates that the VoIP function is idle.
	<b>HANG_UP</b> - Indicates that the connection is not established (busy tone).
	<b>CONNECTING -</b> Indicates that the user is calling out. <b>WAIT_ANS -</b> 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 hours:minutes: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	Accumulation for the times of in call.
Out Calls	Accumulation for the times of out call.
Miss Calls	Accumulation for the times of missing call.
Speaker Gain	The volume of present call.
Log	Display logs of VoIP calls.

# 4.12 Wireless LAN

This function is used for "n" models only.

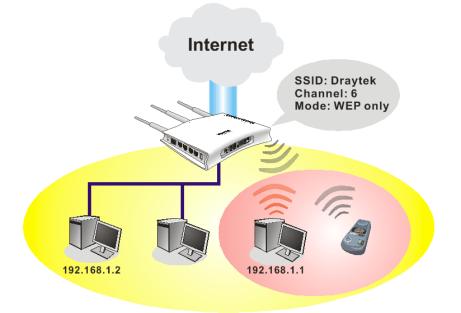
### 4.12.1 Basic Concepts

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

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

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

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



### Security Overview

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



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

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

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

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

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

**Separate the Wireless and the Wired LAN- WLAN Isolation** enables you to isolate your wireless LAN from wired LAN for either quarantine or limit access reasons. To isolate means neither of the parties can access each other. To elaborate an example for business use, you may set up a wireless LAN for visitors only so they can connect to Internet without hassle of the confidential information leakage. For a more flexible deployment, you may add filters of MAC addresses to isolate users' access from wired LAN.

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

Below shows the menu items for Wireless LAN.



## 4.12.2 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.

al Setting	( IEEE 80	)2.11)					
nable Wirele	ss LAN		_				
Mode :				Mixed(11b+1	1g+11n) 🔽		
Index(1-1	5) in <u>Sch</u>	edule Setup		,	,,	,	]
Only scheo other actio			e the action "	Force Down	n" are appli	ed to the Wi	LAN, all
Enable	Hide SSID		SSID		Isolate LAN	Isolate Member	Isolate VPN
1		DrayTek					
2							
3 🔲							
4							
Hide SSII Isolate M access fo Isolate L wired PCs	lember:V r each ot AN:Wirele on LAN.	Vireless clier her. ess clients (s	being scanne nts (stations) stations) with ith remote dia	with the sa	SSID canno	it access	_
Hide SSII Isolate M access fo Isolate L wired PCs Isolate V Channel:	lember:\ r each ot AN:Wirela on LAN. PN:isolat Channel 6	Vireless clier her. ess clients (s e wireless w , 2437MHz	nts (stations) stations) with ith remote dia	with the same s the same s al-in and LA ong Preami	SSID canno N to LAN V	ot access PN.	_
Hide SSII Isolate M access fo Isolate L wired PCs Isolate V Channel:	lember:\ r each ot AN:Wirela on LAN. PN:isolat Channel 6	Vireless clier her. ess clients (s e wireless w , 2437MHz	nts (stations) stations) with ith remote dia	with the same s the same s al-in and LA ong Preami	SSID canno N to LAN V	ot access PN.	
Hide SSII Isolate M access fo Isolate L wired PCs Isolate V Channel: [ Long Prear Packet-OV	lember:V r each ot AN:Wirele on LAN. PN:isolat Channel 6 mble: neo YERDRIVE	Vireless clier her. ess clients (s e wireless w , 2437MHz essary for s	nts (stations) stations) with ith remote dia	with the same s the same s al-in and LA ong Preami	SSID canno N to LAN V	ot access PN.	
Hide SSII Isolate M access fo Isolate L wired PCs Isolate V Channel: [ Long Prear Packet-OV T X Bur	lember:V r each ot AN:Wirele on LAN. PN:isolat Channel 6 mble: neo YERDRIVE	Vireless clier her. ess clients (s e wireless w , 2437MHz essary for s	nts (stations) stations) with ith remote dia	with the same s the same s al-in and LA ong Preami	SSID canno N to LAN V	ot access PN.	
Hide SSII Isolate M access fo Isolate L wired PCs Isolate V Channel: [ Long Prear Packet-OV T x Bur Note:	lember:V r each ot AN:Wirele on LAN. PN:isolat Channel 6 mble: nec YERDRIVE st	Vireless clier her. ess clients (s e wireless w , 2437MHz ;essary for s	nts (stations) stations) with ith remote dia	with the same same same same same same same sam	SSID canno N to LAN V ble: s only(lowe	nt access IPN. er performan	
Hide SSII Isolate M access fo Isolate L wired PCs Isolate V Channel: [ Long Prear Packet-OV Packet-OV Tx Bur Note: The same	lember:V r each ot AN:Wirele on LAN. PN:isolat Channel 6 mble: nec 'ERDRIVE st technolo	Vireless clier her. ess clients (s e wireless w , 2437MHz ;essary for s	nts (stations) stations) with ith remote dia come old 802.1	with the same same same same same same same sam	SSID canno N to LAN V ble: s only(lowe	nt access IPN. er performan	
Hide SSII Isolate M access fo Isolate L wired PCs Isolate V Channel: [ Long Prear Packet-OV T x Bur Note:	Iember:V r each ot AN:Wirele on LAN. PN:isolat Channel 6 mble: nec 'ERDRIVE st technolo	Vireless clier her. ess clients (s e wireless w , 2437MHz ;essary for s	nts (stations) stations) with ith remote dia come old 802.1	with the same same same same same same same sam	SSID canno N to LAN V ble: so only(lowe to boost W	nt access IPN. er performan	
Hide SSII Isolate M access fo Isolate L wired PCs Isolate V Channel: [ Long Prear Packet-OV Packet-OV Tx Bur Note: The same	Iember:V r each ot AN:Wirele on LAN. PN:isolat Channel 6 mble: nec 'ERDRIVE st technolo rol	Vireless clier her. ess clients (s e wireless w , 2437MHz , 2437MHz ressary for s tm gy must also	nts (stations) stations) with ith remote dia ome old 802.1	with the same same same same same same same sam	SSID canno N to LAN V ble: s only(lowe to boost W	it access IPN. er performan /LAN perform Download	
Hide SSII Isolate M access fo Isolate L wired PCs Isolate V Channel: [ Long Prear Packet-OV T X Bur Note: The same Rate Cont	lember:V r each ot AN:Wirele on LAN. PN:isolat Channel 6 mble: nec /ERDRIVE st technolo Frol Er	Vireless clier her. ess clients (s e wireless w , 2437MHz , 2437MHz , 2437MHz sessary for s m gy must also	nts (stations) stations) with ith remote dia ome old 802.1	with the same same same same same same same sam	SSID canno N to LAN V ble: s only(lowe to boost W	PN. PN. Pr performan /LAN perform Download 30000 k	nance.
Hide SSII Isolate M access fo Isolate L wired PCs Isolate V Channel: [ Long Prear Packet-OV Tx Bur Note: The same Rate Cont SSID 1	Iember:V r each ot AN:Wirele on LAN. PN:isolat Channel 6 mble: nec //ERDRIVE st technolo rol Er	vireless clier her. ess clients (s e wireless w , 2437MHz essary for s m gy must also nable □	nts (stations) stations) with ith remote dia ome old 802.1 b be supporter Upload	with the same s the same s al-in and LA ong Pream 11 b device d in clients	SSID canno N to LAN V ble: s only(lowe to boost W	PN. PN. PN. /LAN perform Download 30000 kl	hance.

Available settings are explained as follows:

Item	Description
Enable Wireless LAN	Check the box to enable wireless function.
Mode	At present, the router can connect to Mixed (11b+11g), 11g Only, 11b Only, Mixed (11g+11n), 11n Only and Mixed (11b+11g+11n) stations simultaneously. Simply choose Mix (11b+11g+11n) mode.

	Mixed(11b+11g+11n) 11b Only 11g Only 11n Only Mixed(11b+11g) Mixed(11g+11n) Mixed(11b+11g+11n)
Index(1-15)	Set the wireless LAN to work at certain time interval only. You may choose up to 4 schedules out of the 15 schedules pre-defined in <b>Applications</b> >> <b>Schedule</b> setup. The default setting of this filed is blank and the function will always work.
Hide SSID	Check it to prevent from wireless sniffing and make it harder for unauthorized clients or STAs to join your wireless LAN. Depending on the wireless utility, the user may only see the information except SSID or just cannot see any thing about Vigor wireless router while site surveying. The system allows you to set four sets of SSID for different usage. In default, the first set of SSID will be enabled. You can hide it for your necessity.
SSID	Means the identification of the wireless LAN. SSID can be any text numbers or various special characters. The default SSID is "Draytek. We suggest you to change it.
Isolate	<ul> <li>LAN – Check this box to make the wireless clients (stations) with the same SSID cannot access wired PCs on LAN.</li> <li>Member –Check this box to make the wireless clients (stations) with the same SSID not accessing for each other.</li> <li>VPN – Check this box to isolate the wireless clients with remote dial-in and LAN to LAN VPN.</li> </ul>
Channel	Means the channel of frequency of the wireless LAN. The default channel is 6. You may switch channel if the selected channel is under serious interference. If you have no idea of choosing the frequency, please select Auto to let system determine for you. Channel: Channel 6, 2437MHz Auto Channel 1, 2412MHz Channel 2, 2417MHz Channel 3, 2422MHz Channel 4, 2427MHz Channel 5, 2432MHz Channel 5, 2432MHz Channel 6, 2437MHz Channel 6, 2437MHz Channel 8, 2447MHz Channel 8, 2447MHz Channel 9, 2452MHz Channel 10, 2457MHz Channel 11, 2462MHz Channel 11, 2462MHz Channel 12, 2467MHz
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 <b>Long Preamble</b> if needed to communicate with this kind of devices.	
Packet-OVERDRIVE	This feature can enhance the performance in data transmission about 40%* more (by checking <b>Tx Burs</b> t). It is active only when both sides of Access Point and Station (in wireless client) invoke this function at the same time. That is, the wireless client must support this feature and invoke the function, too. <b>Note:</b> Vigor N61 wireless adapter supports this function. Therefore, you can use and install it into your PC for matching with Packet-OVERDRIVE (refer to the following picture of Vigor N61 wireless utility window, choose <b>Enable</b> for <b>TxBURST</b> on the tab of <b>Option</b> ).	
	Vigor N61 802.11n Wireless USB Adapter Utility	
	Configuration       Status       Option       A bout         General Setting       Advance Setting       Disable Radio         Remember mini status position       Bisable Radio       Pragmentation Threshold :       2346         A tuo hide mini status       RTS Threshold :       2347         Set mini status always on top       Boable IP Setting and Proxy Setting in Profile       Mode:       1         Group Roaming       Ad-hoc       Tx Eurst:       Disable       Tx Eurst:	
	WLAN type to connect ③ Infrastructure and Ad-hoc getwork ○ Infrastructurg network only ○ Ad-hoc network only	
	Automatically connect to non-preferred networks	
	OK Cancel Apply	
Rate Control	It controls the data transmission rate through wireless connection.	
	<b>Upload</b> – Check Enable and type the transmitting rate for data upload. Default value is 30,000 kbps.	
	<b>Download</b> – Type the transmitting rate for data download. Default value is 30,000 kbps.	

After finishing all the settings here, please click **OK** to save the configuration.

### 4.12.3 Security

This page allows you to set security with different modes for SSID 1, 2, 3 and 4 respectively. After configuring the correct settings, please click **OK** to save and invoke it.

The default security mode is **Mixed (WPA+WPA2)/PSK.** Default Pre-Shared Key (PSK) is provided and stated on the label pasted on the bottom of the router. For the wireless client who wants to access into Internet through such router, please input the default PSK value for connection.



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
```

SSID 1	SSID 2	SSID 3	SSID 4	
Ν	1ode:		Disable	~
WPA:				
Encrypt	ion Mode:		TKIP for WPA/AB	ES for WPA2
F	re-Shared Key(F	PSK):	*****	
	'ype 8~63 ASCI) cfgs01a2" or "			digits leading by "Ox", for example
WEP:				
E	ncryption Mode:		64-Bit 💙	
	◉Key 1 :		*****	
	⊖Key 2 :		*****	
	○Кеу 3:		*****	
	⊖Key 4 :		******	
Type 5 "0x4142 <b>For 128</b> Type 13	:333132". <mark>3 bit WEP key</mark> 3 ASCII characte	er or 26 Hexade	-	ng by "Ox", for example "AB312" or ing by "Ox", for example ".

Available settings are explained as follows:

Item	Description
Mode	There are several modes provided for you to choose.

Cancel

0K

	Mode:	Disable 🗸
		Disable WEP
		WPA/PSK
		WPA2/PSK Mixed(WPA+WPA2)/PSK
	Disable - Turn off the encryp	
	<b>WEP-</b> Accepts only WEP clie should be entered in WEP Ke	· · · ·
	<b>WPA/PSK-</b> Accepts only WPA clients and the encryption key should be entered in PSK.	
	<b>WPA2/PSK-</b> Accepts only WPA2 clients and the encryption key should be entered in PSK.	
	<b>Mixed (WPA+ WPA2)/PSK -</b> Accepts WPA and WPA2 clients simultaneously and the encryption key should be entered in PSK.	
WPA	802.1x authentication. Either	
	Type - Select from Mixed (W	/PA+WPA2) or WPA2 only.
	- · · · ·	her 8~63 ASCII characters, such cimal digits leading by 0x, such
WEP	<b>64-Bit</b> - For 64 bits WEP key such as 12345 (or 10 hexadec such as 0x4142434445.)	
	such as ABCDEFGHIJKLM	tey, either <b>13</b> ASCII characters, (or 26 hexadecimal digits 2434445464748494A4B4C4D).
	Encryption Mode:	64-Bit 64-Bit 128-Bit
	bit size and have the same key here, but only one key can be	port the same WEP encryption y. <b>Four keys</b> can be entered selected at a time. The keys can lecimal. Check the key you wish

After finishing all the settings here, please click  $\mathbf{OK}$  to save the configuration.

## 4.12.4 Access Control

Wireless LAN >> Access Control

In the **Access Control**, the router may restrict wireless access to certain wireless clients only by locking their MAC address into a black or white list. The user may block wireless clients by inserting their MAC addresses into a black list, or only let them be able to connect by inserting their MAC addresses into a white list.

In the **Access Control** web page, users may configure the **white/black** list modes used by each SSID and the MAC addresses applied to their lists.

nable Mac Address Fil	Iter SSID 1 White List V SSID 3 White List V	<ul> <li>✓ SSID 2 White List ▼</li> <li>✓ SSID 4 White List ▼</li> </ul>
	MAC Address Filter	
Index Attribute	MAC Address	Apply SSID
Clier	nt's MAC Address : : : :	
	nt's MAC Address : : : : : : : 5SID 2 SSID 2SSID 2SSID 2	
Apply S		

Available settings are explained as follows:

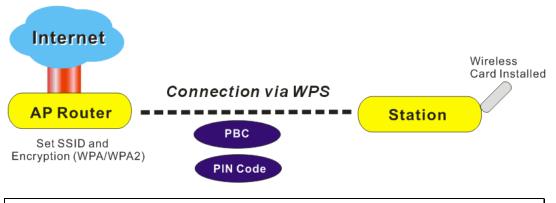
Item	Description
Enable Mac Address Filter	Select to enable the MAC Address filter for wireless LAN identified with SSID 1 to 4 respectively. All the clients (expressed by MAC addresses) listed in the box can be grouped under different wireless LAN. For example, they can be grouped under SSID 1 and SSID 2 at the same time if you check SSID 1 and SSID 2.
MAC Address Filter	Display all MAC addresses that are edited before.
Client's MAC Address	Manually enter the MAC address of wireless client.
Apply SSID	After entering the client's MAC address, check the box of the SSIDs desired to insert this MAC address into their access control list.
Attribute	<b>s: Isolate the station from LAN -</b> select to isolate the wireless connection of the wireless client of the MAC address from LAN.
Add	Add a new MAC address into the list.

Delete	Delete the selected MAC address in the list.	
Edit	Edit the selected MAC address in the list.	
Cancel	Give up the access control set up.	
ОК	Click it to save the access control list.	
Clear All	Clean all entries in the MAC address list.	

After finishing all the settings here, please click **OK** to save the configuration.

### 4.12.5 WPS

**WPS (Wi-Fi Protected Setup)** provides easy procedure to make network connection between wireless station and wireless access point (vigor router) with the encryption of WPA and WPA2.

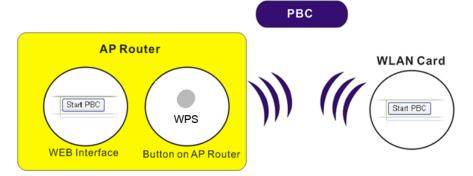


Note: Such function is available for the wireless station with WPS supported.

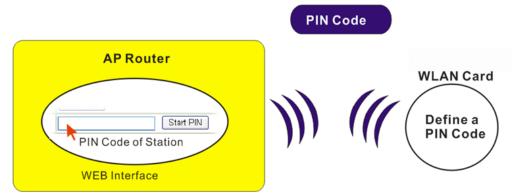
It is the simplest way to build connection between wireless network clients and vigor router. Users do not need to select any encryption mode and type any long encryption passphrase to setup a wireless client every time. He/she only needs to press a button on wireless client, and WPS will connect for client and router automatically.

There are two methods to do network connection through WPS between AP and Stations: pressing the *Start PBC* button or using *PIN Code*.

• On the side of Vigor 2710 series which served as an AP, press **WPS** button once on the front panel of the router or click **Start PBC** on web configuration interface. On the side of a station with network card installed, press **Start PBC** button of network card.



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



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

Microsof	t Internet Explorer 🛛 🔀	
⚠	WPS only supports in WPA/WPA2-PSK Mode.	
	ОК	

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

Below shows Wireless LAN>>WPS web page.

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

🗹 Enable WPS 🗘

**Wi-Fi Protected Setup Information** 

WPS Status	Configured
SSID	default
Authentication Mode	Disable

#### **Device Configure**

Configure via Push Button	Start PBC
Configure via Client PinCode	Start PIN

Status: The Authentication Mode is NOT WPA/WPA2 PSK!!

Note: WPS can help your wireless client automatically connect to the Access

point. 🗅 : WPS is Disabled.

😳 : WPS is Enabled.

arepsilon : Waiting for WPS requests from wireless clients.

### Available settings are explained as follows:

Item	Description
Enable WPS	Check this box to enable WPS setting.

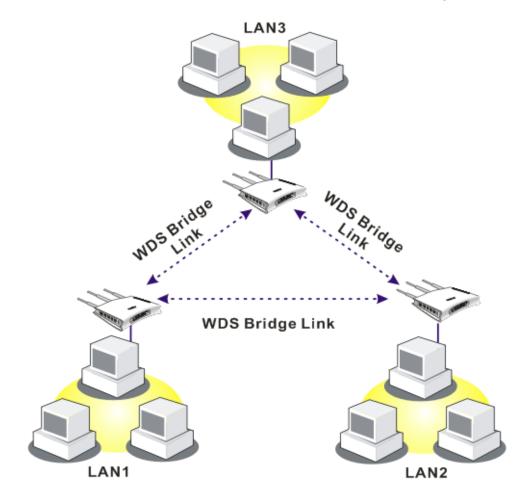
Item	Description
WPS Status	Display related system information for WPS. If the wireless security (encryption) function of the router is properly configured, you can see 'Configured' message here.
SSID	Display the SSID1 of the router. WPS is supported by SSID1 only.
Authentication Mode	Display current authentication mode of the router. Only WPA2/PSK and WPA/PSK support WPS.
Configure via Push Button	Click <b>Start PBC</b> to invoke Push-Button style WPS setup procedure. The router will wait for WPS requests from wireless clients about two minutes. The WPS LED on the router will blink fast when WPS is in progress. It will return to normal condition after two minutes. (You need to setup WPS within two minutes)
Configure via Client PinCode	Please input the PIN code specified in wireless client you wish to connect, and click <b>Start PIN</b> button. The WPS LED on the router will blink fast when WPS is in progress. It will return to normal condition after two minutes. (You need to setup WPS within two minutes)

### 4.12.6 WDS

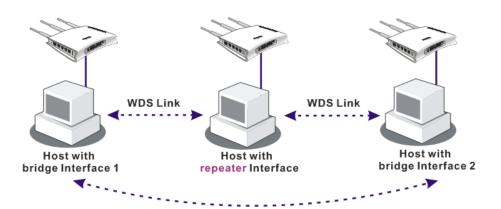
WDS means Wireless Distribution System. It is a protocol for connecting two access points (AP) wirelessly. Usually, it can be used for the following application:

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

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



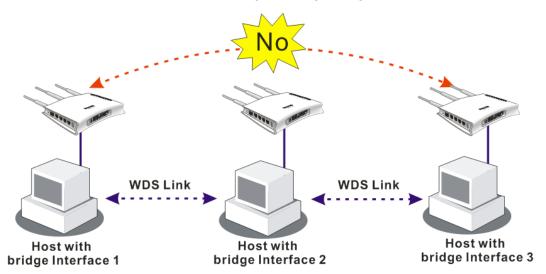
The application for the WDS-Repeater mode is depicted as below:





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

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



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



### Wireless LAN >> WDS Settings

	Public -
Mode: Bridge 💙	Bridge Enable Peer MAC Address
Security:	
💿 Disable 🔘 WEP 🔘 Pre-shared Key	
WEP:	
Use the same WEP key set in <u>Security Settings</u> .	Note: Disable unused links to get better
	performance.
Pre-shared Key:	
Туре:	Repeater Enable Peer MAC Addess
● DrayTek WPA ○ WPA ○ WPA2	
Key : **********	
Type 8~63 ASCII characters or 64 hexadecimal	
digits leading by "0x", for example "cfgs01a2" or "0x655abcd".	
	Access Point Function:
	💿 Enable 🛛 Disable
	Status:
	Send "Hello" message to peers.
	Link Status
	Note: The status is valid only when the peer also supports this function.

Available settings are explained as follows:

Item	Description	
Mode	Choose the mode for WDS setting. <b>Disable</b> mode will not invoke any WDS setting. <b>Bridge</b> mode is designed to fulfill the first type of application. <b>Repeater</b> mode is for the second one. Disable Bridge Repeater	
Security	There are three types for security, <b>Disable</b> , <b>WEP</b> and <b>Pre-shared key</b> . 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 <b>Security Settings</b> page. If you did not set any key in <b>Security Settings</b> page, this check box will be dimmed.	
Pre-shared Key	<b>Type</b> – There are some types for you to choose. <b>WPA</b> and <b>WPA2</b> are used for WDS devices (e.g.2920n wireless router, you can set the encryption mode as WPA or WPA2 to establish	

Item	Description
	your WDS system between AP and the router.
	<b>Key</b> - Type $8 \sim 63$ ASCII characters or 64 hexadecimal digits leading by "0x".
Bridge	If you choose Bridge as the connecting mode, please type in the peer MAC address in these fields. Four peer MAC addresses are allowed to be entered in this page at one time. Yet please disable the unused link to get better performance. If you want to invoke the peer MAC address, remember to check <b>Enable</b> box in the front of the MAC address after typing.
Repeater	If you choose Repeater as the connecting mode, please type in the peer MAC address in these fields. Four peer MAC addresses are allowed to be entered in this page at one time. Similarly, if you want to invoke the peer MAC address, remember to check <b>Enable</b> box in the front of the MAC address after typing.
Access Point Function	Click <b>Enable</b> to make this router serving as an access point; click <b>Disable</b> 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.

After finishing all the settings here, please click **OK** to save the configuration.

### 4.12.7 Advanced Setting

This page allows users to set advanced settings such as operation mode, channel bandwidth, guard interval, and aggregation MSDU for wireless data transmission.

Wireless	LAN >>	Advanced	Setting

HT Physical Mode	
Operation Mode	Mixed Mode ○ Green Field
Channel Bandwidth	○ 20 ④ 20/40
Guard Interval	🔘 long 💿 auto
Aggregation MSDU(A-MSDU)	O Disable 💿 Enable

OK

Item	Description
Operation Mode	<b>Mixed Mode</b> – the router can transmit data with the ways supported in both 802.11a/b/g and 802.11n standards. However, the entire wireless transmission will be slowed down if 802.11g or 802.11b wireless client is connected.
	<b>Green Field</b> – to get the highest throughput, please choose such mode. Such mode can make the data transmission happening between 11n systems only. In addition, it does not have protection mechanism to avoid the conflict with neighboring devices of 802.11a/b/g.



Item	Description
Channel Bandwidth	<ul> <li>20- the router will use 20Mhz for data transmission and receiving between the AP and the stations.</li> <li>20/40 - the router will use 20Mhz or 40Mhz for data transmission and receiving according to the station capability. Such channel can increase the performance for data transit.</li> </ul>
Guard Interval	It is to assure the safety of propagation delays and reflections for the sensitive digital data. If you choose <b>auto</b> as guard interval, the AP router will choose short guard interval (increasing the wireless performance) or long guard interval for data transmit based on the station capability.
Aggregation MSDU	Aggregation MSDU can combine frames with different sizes. It is used for improving MAC layer's performance for some brand's clients. The default setting is <b>Enable.</b>

After finishing all the settings here, please click **OK** to save the configuration.

## 4.12.8 WMM Configuration

WMM is an abbreviation of Wi-Fi Multimedia. It defines the priority levels for four access categories derived from 802.1d (prioritization tabs). The categories are designed with specific types of traffic, voice, video, best effort and low priority data. There are four accessing categories - AC_BE, AC_BK, AC_VI and AC_VO for WMM.

APSD (automatic power-save delivery) is an enhancement over the power-save mechanisms supported by Wi-Fi networks. It allows devices to take more time in sleeping state and consume less power to improve the performance by minimizing transmission latency. Such function is designed for mobile and cordless phones that support VoIP mostly.

MM Capable	e 💿 Enable 🔘 Disable					
PSD Capable		🔘 Enable	Oisable			
/MM Parame	eters of Acce	ss Point				
	Aifsn	CWMin	CWMax	Тхор	ACM	AckPolicy
AC_BE	3	4	6	0		
AC_BK	7	4	10	0		
AC_VI	1	3	4	94		
AC_VO	1	2	3	47		
/MM Parame	eters of Stati	on				
	Aifsn	CWMir	n C	WMax	Тхор	ACM
AC_BE	3	4	10		0	
AC_BK	7	4	10		0	
AC_VI	2	3	4		94	
AC_VO	2	2	3		47	

Wireless LAN >> WMM Configuration

Item	Description
WMM Capable	To apply WMM parameters for wireless data transmission, please click the <b>Enable</b> radio button.
APSD Capable	The default setting is <b>Disable</b> .
Aifsn	It controls how long the client waits for each data transmission. Please specify the value ranging from 1 to 15. Such parameter will influence the time delay for WMM accessing categories. For the service of voice or video image, please set small value for AC_VI and AC_VO categories For the service of e-mail or web browsing, please set large value for AC_BE and AC_BK categories.
CWMin/CWMax	<b>CWMin</b> means contention Window-Min and <b>CWMax</b> means contention Window-Max. Please specify the value ranging from 1 to 15. Be aware that CWMax value must be greater than CWMin or equals to CWMin value. Both values will influence the time delay for WMM accessing categories. The difference between AC_VI and AC_VO categories must be smaller; however, the difference between AC_BE and AC_BK categories must be greater.
Тхор	It means transmission opportunity. For WMM categories of AC_VI and AC_VO that need higher priorities in data transmission, please set greater value for them to get highest transmission opportunity. Specify the value ranging from 0 to 65535.
ACM	It is an abbreviation of Admission control Mandatory. It can restrict stations from using specific category class if it is checked. <b>Note:</b> Vigor router provides standard WMM configuration in the web page. If you want to modify the parameters, please refer to the Wi-Fi WMM standard specification.
AckPolicy	<ul> <li>"Uncheck" (default value) the box means the AP router will answer the response request while transmitting WMM packets through wireless connection. It can assure that the peer must receive the WMM packets.</li> <li>"Check" the box means the AP router will not answer any response request for the transmitting packets. It will have better performance with lower reliability.</li> </ul>

Available settings are explained as follows:

After finishing all the settings here, please click **OK** to save the configuration.

## 4.12.9 AP Discovery

Vigor router can scan all regulatory channels and find working APs in the neighborhood. Based on the scanning result, users will know which channel is clean for usage. Also, it can be used to facilitate finding an AP for a WDS link. Notice that during the scanning process (about 5 seconds), no client is allowed to connect to Vigor.

This page is used to scan the existence of the APs on the wireless LAN. Yet, only the AP which is in the same channel of this router can be found. Please click **Scan** to discover all the connected APs.

Access Point List				
	BSSID	Channel	SSID	
	I	Scan		
See <u>St</u>	atistics.			
	During the scanning t with the router.	process (~5 seco	onds), no station is allowed to	
Add to	WDS Settings :			
AP's MA	C address	:	:	
Add t	to	💿 Bridge	○ Repeater	

Available settings are explained as follows:

Wireless LAN >> Access Point Discovery

Item	Description
Scan	It is used to discover all the connected AP. The results will be shown on the box above this button.
Statistics	It displays the statistics for the channels used by APs. Wireless LAN >> Site Survey Statistics Recommended channels for usage: 12345678910111213
	AP number v.s. Channel 1 2 3 4 5 6 7 8 9 10 11 12 13 14 Channel
	Cancel
Add to	If you want the found AP applying the WDS settings, please type in the AP's MAC address on the bottom of the page and click Bridge or Repeater. Next, click <b>Add to</b> . Later, the MAC address of the AP will be added to Bridge or Repeater field of WDS settings page.

### 4.12.10 Station List

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

Station List				
	Status	MAC Address	Associated with	
		Refresh		
	i <mark>tus Codes :</mark> Connected, No ei	ncryption.		
	Connected, WEP. Connected, WPA.			
A:	Connected, WPA:	2.		
	Blocked by Acces Connecting.	ss Control.		
		PSK authentication.		
turi		n connects to the router suc otice. In that case, it will stil		
Ad	d to <u>Access Cont</u>	r <u>ol</u> :		
Clie	nt's MAC address		: : : : : : : : : : : : : : : : : : : :	
		Add		

Wireless LAN >> Station List

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

# 4.13 USB Application

USB disk can be regarded as an FTP server. By way of Vigor router, clients on LAN can access, write and read data stored in USB disk. After setting the configuration in **USB Application**, you can type the IP address of the Vigor router and username/password created in **USB Application>>USB User Management** on the FTP client software. Thus, the client can use the FTP site (USB disk) through Vigor router.

USB Application • USB General Settings • USB User Management • File Explorer • USB Disk Status

### 4.13.1 USB General Settings

This page will determine the number of concurrent FTP connection and default charset for FTP server. At present, the Vigor router can support USB disk with versions of FAT16 and FAT32 only. Therefore, before connecting the USB disk into the Vigor router, please make sure the memory format for the USB disk is FAT16 or FAT32. It is recommended for you to use FAT32 for viewing the filename completely (FAT16 cannot support long filename).

USB Application >> USB General Settings

General Settings		
Simultaneous FTP Connections	5 (Maximum 6)	
Default Charset	Default 💌	
Samba Service Settings(Network	Neighborhood)	
🔘 Enable 💿 Disable		
Access Mode		
● LAN Only ◯ LAN And WAN		
NetBios Name Service		
Workgroup Name	WORKGROUP	
Host Name	Vigor	

Note: 1. If Charset is set to "default", only English long file name is supported. 2. Multi-session ftp download will be banned by Router FTP server. If your ftp client have multiconnection mechanism, such as FileZilla, you may limit client connections setting to 1 to get better performance.

3. A workgroup name must not be the same as the host name. The workgroup name and the host name can have as many as 15 characters and a host name can have as many as 23 characters , but both cannot contain any of the following: .;; " <> * + = / \ | ?.

OK	OK	
----	----	--

Item	Description
General Settings	<ul> <li>Simultaneous FTP Connections - This field is used to specify the quantity of the FTP sessions. The router allows up to 6 FTP sessions connecting to USB storage disk at one time.</li> <li>Default Charset - Vigor router supports four types of</li> </ul>

Item	Description	
	character sets. Default Charset is for English based file name. English English Chinese(Simple) Chinese(Traditional) German	
Samba Service Settings	Click <b>Enable</b> to invoke samba service via the router.	
Access Mode	<ul> <li>LAN Only – Users coming from internet cannot connect to the samba server of the router.</li> <li>LAN And WAN - Both LAN and WAN users can access samba server of the router.</li> </ul>	
NetBios Name Service	For the NetBios service of USB storage disk, you have to specify a workgroup name and a host name. A workgroup name must not be the same as the host name. The workgroup name can have as many as 15 characters and the host name can have as many as 23 characters. Both them cannot contain any of the following; : $  <> * + = \setminus  $ ?.	
	Workgroup Name – Type a name for the workgroup.	
	Host Name – Type the host name for the router.	

After finishing all the settings here, please click **OK** to save the configuration.

### 4.13.2 USB User Management

This page allows you to set profiles for FTP users. Any user who wants to access into the USB disk must type the same username and password configured in this page. Before adding or modifying settings in this page, please insert a USB disk first. Otherwise, an error message will appear to warn you.

Index	Username	Home Folder	Index	Username	Home Folder
<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>		
8.			16.		

Each item is explained as follows:

Item	Description
Index	Display the number link of the profile.

Username	Display the name that FTP/Samba users will use for accessing into FTP/Samba server.	
Home Folder	Display the home folder of this entry.	
Set to Factory Default	Click it to clear all profiles settings.	

To create an account for FTP user:

1. Click any index number to access into configuration page.

# USB Application >> USB User Management

### **USB User Management**

Index	Username	Home Folder
<u>1.</u>		
<u>2.</u>		
<u>3.</u>		
<u>4.</u>		

2. The following web page will appear.

USB Application >> USB User Management

Profile Index: 1	
FTP/Samba User	⊙ Enable 🔿 Disable
Username	carrie
Password	••••••• (Maximum 11 Characters)
Confirm Password	******
Home Folder	tempstorage 🧭
Access Rule	
File	🗹 Read 🛛 Write 🗌 Delete
Directory	List Create Remove
Note: The folder name can only contain the and space.	e following characters: A-Z a-z 0-9 \$ % ' @ ~ ` ! ( ) /
OK	Clear Cancel

Item	Description	
FTP/Samba User	<ul> <li>Enable – Click this button to activate this profile (account for FTP service or Samba User service. Later, the user can use the username specified in this page to login into FTP server.</li> <li>Disable – Click this button to disable such profile.</li> </ul>	
Username	Type the username for FTP users for accessing into FTP server (USB disk). Be aware that users cannot access into USB disk in anonymity. Later, you can open FTP client software and type the username specified here for accessing	

Item	Description
	into USB storage disk.
	<b>Note:</b> "Admin" could not be typed here as username, for the word is specified for accessing into web pages of Vigor router only. Also, it is reserved for FTP firmware upgrade usage.
Password	Type the password for FTP/Samba users for accessing FTP server. Later, you can open FTP client software and type the password specified here for accessing into USB storage disk.
Confirm Password	Type the password again to make confirmation.
Home Folder	It determines the range for the client to access into. The user can enter a directory name in this field. Then, after clicking <b>OK</b> , the router will create the specific/new folder in the USB diskette. In addition, if the user types "/" here, he/she can access into all of the disk folders and files in USB diskette.
	<b>Note:</b> When write protect status for the USB disk is <b>ON</b> , you cannot type any new folder name in this field. Only "/" can be used in such case.
	You can click $\bigcirc$ to open the following dialog to add any new folder which can be specified as the Home Folder.
	Mtp://192.109.12/Moc/ftguestfolder.Ata - Microsoft Lateraset Keyberer   USB User Management   Clause Folder   Folder Name   Folder Name:   Itest   Create Note: The folder name can only contain the following characters: A-Z a-2 0-9 \$ % * @ ~ * ! ( ) and space. Only 11 characters are allowed.
Access Rule	It determines the authority for such profile. Any user, who uses such profile for accessing into USB storage disk, must follow the rule specified here. <b>File</b> – Check the items (Read, Write and Delete) for such profile.
	<b>Directory</b> –Check the items (List, Create and Remove) for such profile.

3. Before you click **OK**, you have to insert a USB disk into the USB interface of the Vigor router. Otherwise, you cannot save the configuration.



## 4.13.3 File Explorer

File Explorer offers an easy way for users to view and manage the content of USB storage disk connected on Vigor router.

t Path: /		↑ ⁽²⁾
ne Size Delete	Size Delete	Name
×	×	pstorage
×	×	g-install
4,572 KB 🗙	4,572 KB 🗙	supply-lost in I
2,775 KB 🗙	2,775 KB 🗙	stal Flower.mp3
		supply-lost in I

Note: The folder can not be deleted when it is not empty.

Item	Description
** Refresh	Click this icon to refresh files list.
★ Back	Click this icon to return to the upper directory.
📁 Create	Click this icon to add a new folder.
Current Path	Display current folder.
Upload	Click this button to upload the selected file to the USB storage disk. The uploaded file in the USB storage disk can be shared for other user through FTP.

### 4.13.4 USB Disk Status

This page is to monitor the status for the FTP users who accessing into FTP server (USB disk) via the Vigor router.

USB Application >> USB Disk Status

USB Mass Storage Device Status		
Connection Status: Disk Connected	Disconnect USB Disk	
Write Protect Status: No		
Disk Capacity: 2009 MB		
Free Capacity: 1615 MB <u>Refresh</u>		
USB Disk Users Connected	<u>Refresh</u>	
Index Service IP Address(Port)	Username	

Note: If the write protect switch of USB disk is turned on, the USB disk is in READ-ONLY mode. No data can be written to it.

Each item is explained as follows:

Item	Description
<b>Connection Status</b>	If there is no USB disk connected to Vigor router, " <b>No Disk</b> <b>Connected</b> " will be shown here. Once the USB disk has been found, the connection status will display " <b>Disk Connected</b> ".
	<b>Disconnect USB Disk</b> – click this button to disconnect the USB disk with the router.
Write Protect Status	If the USB cannot be written with any files, this field will display YES.
Disk Capacity	It displays the total capacity of the USB disk.
Free Capacity	It displays the free space of the USB disk. Click <b>Refresh</b> at any time to get new status for free capacity.
Service	It displays the service that such USB disk will serve.
IP Address	It displays the IP address of the user's host which connecting to the FTP server.
Username	It displays the username that user uses to login to the FTP server.

When you insert USB disk into the Vigor router, the system will start to find out such device within several seconds.

## 4.14 System Maintenance

For the system setup, there are several items that you have to know the way of configuration: Status, Administrator Password, User Password, Login Page Greeting, Configuration Backup, Syslog, Time and Date setup, Management, Reboot System, Firmware Upgrade and Activate.

Below shows the menu items for System Maintenance.

System Maintenance
System Status
▶ TR-069
Administrator Password
User Password
Login Page Greeting
Configuration Backup
SysLog / Mail Alert
Time and Date
Management
Reboot System
Firmware Upgrade
Activation
Diagnostics

#### 4.14.1 System Status

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

System	Status	

odel Name : Vigor2710Vn rmware Version : 3.6.3 uild Date/Time : Nov 2 2012 16:34:49 DSL Firmware Version : 211011_A Hardware: Annex	Α
LAN	WAN 1
MAC Address         : 00-50-7F-92-F5-00           1st IP Address         : 192.168.1.1           1st Subnet Mask         : 255.255.255.0           DHCP Server         : Yes           DNS         : 8.8.8.8	Link Status: DisconnectedMAC Address: 00-50-7F-92-F5-01Connection: PPPoEIP Address:Default Gateway:
VoIP	Wireless LAN
Port     Profile     Reg.     In/Out       Phone1     Wizard1     No     0/0       Phone2     Wizard1     No     0/0       ONLY Phone 2     can access the PSTN line during power failure.	MAC Address : 00-50-7F-92-F5-00 Frequency Domain : Europe Firmware Version : 2.3.2.0 SSID : DrayTek
	ΙΡν6
Address LAN FE80::250:7FFF:FE92:F500/64	Scope Internet Access Mode Link

User Mode is OFF now.

Each item is explained as follows:

Item	Description
Model Name	Display the model name of the router.

Item	Description
Firmware Version	Display the firmware version of the router.
<b>Build Date/Time</b>	Display the date and time of the current firmware build.
ADSL Firmware Version	Display the ADSL firmware version.
LAN	MAC Address - Display the MAC address of the LAN Interface.
	<b>IP Address -</b> Display the IP address of the LAN interface.
	<b>Subnet Mask -</b> Display the subnet mask address of the LAN interface.
	<b>DHCP Server -</b> Display the current status of DHCP server of the LAN interface
	<b>DNS</b> - Display the assigned IP address of the primary DNS.
WAN	Link Status - Display current connection status.
	<b>MAC Address -</b> Display the MAC address of the WAN Interface.
	<b>Connection -</b> Display the connection type.
	<b>IP Address -</b> Display the IP address of the WAN interface.
	<b>Default Gateway -</b> Display the assigned IP address of the default gateway.
VoIP	<b>Profile -</b> Display the VoIP profile for the phone port.
	<b>In/Out -</b> Display the number of incoming /outgoing phone call.
Wireless LAN	<b>MAC Address -</b> Display the MAC address of the wireless LAN.
	<b>Frequency Domain -</b> It can be Europe (13 usable channels), USA (11 usable channels) etc. The available channels supported by the wireless products in different countries are various.
	<b>Firmware Version -</b> It indicates information about equipped WLAN miniPCi card. This also helps to provide availability of some features that are bound with some WLAN miniPCi.
	<b>SSID</b> - Display the SSID of the router.
IPv6	Address - Display the IPv6 address for LAN.
	<b>Scope -</b> Display the scope of IPv6 address. For example, IPv6 <b>Link Local</b> could only be used for direct IPv6 link. It can't be used for IPv6 internet.
	<b>Internet Access Mode</b> – Display the connection mode chosen for accessing into Internet.

#### 4.14.2 TR-069

This device supports TR-069 standard. It is very convenient for an administrator to manage a TR-069 device through an Auto Configuration Server, e.g., VigorACS.

ACS Server On	Internet 💌
ACS Server	
URL	
Username	
Password	
CPE Client	
🔘 Enable 🛛 💿 Disable	
URL	
Port	8069
Username	vigor
Password	•••••
eriodic Inform Settings	
🔘 Disable	
<ul> <li>Enable</li> </ul>	
Interval Time	900 second(s)
TUN Settings	
💿 Disable	
🔘 Enable	
Server Address	
Server Port	3478
Minimum Keep Alive	Period 60 second(s)
Maximum Keep Alive	Period -1 second(s)

System Maintenance >> TR-069 Setting

Available parameters are explained as follows:

Item	Description
ACS Server On	Choose the interface for the router connecting to ACS server.
ACS Server	<b>URL/Username/Password</b> – Such data must be typed according to the ACS (Auto Configuration Server) you want to link. Please refer to Auto Configuration Server user's manual for detailed information.
CPE Client	<ul> <li>Such information is useful for Auto Configuration Server.</li> <li>Enable/Disable – Allow/Deny the CPE Client to connect with Auto Configuration Server.</li> <li>Port – Sometimes, port conflict might be occurred. To solve such problem, you might change port number for CPE.</li> </ul>
Periodic Inform Settings	The default setting is <b>Enable</b> . Please set interval time or schedule time for the router to send notification to CPE. Or click <b>Disable</b> to close the mechanism of notification.

Item	Description		
STUN Settings	The default is <b>Disable</b> . If you click <b>Enable</b> , please type the relational settings listed below:		
	<b>Server IP</b> – Type the IP address of the STUN server.		
	<b>Server Port</b> – Type the port number of the STUN server.		
	<b>Minimum Keep Alive Period</b> – If STUN is enabled, the CPE must send binding request to the server for the purpose of maintaining the binding in the Gateway. Please type a number as the minimum period. The default setting is "60 seconds".		
	Maximum Keep Alive Period – If STUN is enabled, the CPE must send binding request to the server for the purpose of maintaining the binding in the Gateway. Please type a number as the maximum period. A value of "-1" indicates that no maximum period is specified.		

After finishing all the settings here, please click **OK** to save the configuration.

# 4.14.3 Administrator Password

This page allows you to set new password.

#### System Maintenance >> Administrator Password Setup

#### Administrator Password



OK

Available parameters are explained as follows:

Item	Description
Old Password	Type in the old password. The factory default setting for password is <b>"admin"</b> .
New Password	Type in new password in this field.
<b>Confirm Password</b>	Type in the new password again.

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

## 4.14.4 User Password

Sometimes, you may want to access into User Mode to configure the web settings for some reason. Vigor router allows you to set new user password to login into the WUI to fit your request. Simply open **System Maintenance>>User Password**.

System Maintenance >> User Password	System	Maintenance	>> User	Password
-------------------------------------	--------	-------------	---------	----------

er Password				Set t	o Factory Defau
Password	đ				
Confirm F	Password				
e:Password can contain	only a-z A-Z 0-	9,;:"<>*+=	:\ ?@#^!(	)	

Available parameters are explained as follows:

Item	Description
Enable User Mode for simple web configuration	Check this box to enable user mode operation. If you do not check this box, you cannot access into the user mode operation even if you enter user password in login page.
Password	Type in new password in this field.
Confirm Password	Type in the new password again.

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

Below shows an example for accessing into User Operation with User Password.

- 1. Open System Maintenance>>User Password.
- 2. Check the box of **Enable User Mode for simple web configuration** to enable user mode operation. Type a new password in the field of New Password and click **OK**.

System Maintenance >> User Password				
Enable User Mode for simple web configu	ration	L. Cotto Francis Definite		
User Password		Set to Factory Default		
Password	••••			
Confirm Password	••••			
Note:Password can contain only a-z A-Z 0	9,;:"<>*+=\ ?	@ # ^ ! ( )		
	OK			

3. The following screen will appear.

System Maintenance >> User Password			
Active Configuration	on		
	Password	· 茶茶茶茶茶	

4. Log out Vigor router Web Configurator by clicking Logout.



5. The following window will be open to ask for username and password. It is no need to type any username. Type the new user password in the filed of **Password** and click **Login**.

J	ust for Carrie
Username	
Password	
	Login
Copyright©, DrayTek Corp. All	Rights Reserved. DrayTek

6. The main screen with User Mode will be shown as follows.

Auto Logout 👻 🛛 🛛 IRG	System Status	
Quick Start Wizard /oIP Wizard Dnline Status	Model Name : Vigor2710Vn Firmware Version : 3.6.3 Build Date/Time : Nov 2 2012 16:34:49 ADSL Firmware Version : 211011_A Hardware: Annex A	
nternet Access AN IAT Applications	LAN MAC Address : 00-50-7F-92-F5-00 1st IP Address : 192.168.1.1 1st Subnet Mask : 255.255.0	WAN 1           Link Status         : Disconnected           MAC Address         : 00-50-7F-92-F5-01           Connection         : PPPoE
/oIP Vireless LAN	DHCP Server : Yes DNS : 8.8.8	IP Address : Default Gateway :
JSB Application	VoIP	Wireless LAN
System Maintenance Diagnostics Support Area	Port         Profile         Reg.         In/Out           Phone1         Wizard1         No         0/0           Phone2         Wizard1         No         0/0 <b>ONLY Phone2</b> can access the PSTN line during power failure.	MAC Address : 00-50-7F-92-F5-00 Frequency Domain : Europe Firmware Version : 2.3.2.0 SSID : DrayTek
roduct Registration		
	IPv	/6
Logout	Address LAN FE80::250:7FF:FE92:F500/64	Scope Internet Access Mode

Settings to be configured in User Mode will be less than settings in Admin Mode. Only basic configuration settings will be available in User Mode.

#### 4.14.5 Login Page Greeting

When you want to access into the web configurator of Vigor router, the system will ask you to offer username and password first. At that moment, the background of the web page is blank and no heading will be displayed on the Login window. This page allows you to specify background message and the heading on the Login window if you have such requirement.

System Maintenance >> Login Page Greeting

Enable			
Login Page Title	Just for Carrie	(31 char max.)	
Welcome Message a	and Bulletin (Max 511 charact	ers) <u>Preview</u> <u>Set to Factory</u>	<u>Default</u>
message is displ with your own me in HTML so lists	ayed in the Login page o ssage. <ol><li>The w</li></ol>	<pre>font&gt;This welcom f the router. Replace this t elcome message can be writte created //li&gt;/li&gt;/li&gt;/li&gt;/li&gt;/li&gt;/li&gt;/li&gt;/li&gt;/li&gt;/li&gt;/li&gt;/li&gt;/li&gt;/li&gt;/li&gt;/li&gt;/li&gt;/li&gt;/li&gt;/li&gt;/li&gt;/li&gt;/li&gt;/li&gt;/li&gt;/li&gt;/li&gt;/li&gt;/li&gt;/li&gt;/li&gt;/li&gt;/li&gt;/li&gt;/li&gt;/li&gt;/li&gt;/li&gt;/li&gt;/li&gt;/li&gt;/li&gt;/li&gt;/li&gt;</pre>	ext en
	ne Message and Bulletin: r=red>Welcome Message <th>nt&gt;</th> <td></td>	nt>	

Cancel

**Dray** Tek

ΟK

Available settings are explained as follows:

Item	Description
Enable	Check this box to enable the login customization function.
Login Page Title	Type a brief description (e.g., Welcome to DrayTek) which will be shown on the heading of the login dialog.
Welcome Message and Bulletin	Type words or sentences here. It will be displayed for bulletin message. In addition, it can be displayed on the login dialog at the bottom. Note that do not type URL redirect link here.
Preview	Click it to display the preview of the login window based on the settings on this web page.
Set to Factory Default	Click to return to the factory default setting.

Below shows an example of login customization with the information typed in Login Page Title and Bulletin.



## 4.14.6 Configuration Backup

#### **Backup the Configuration**

Follow the steps below to backup your configuration.

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

System Main	tenance >> Configuration Backup
Configuration	Backup / Restoration
Restoration	
	Select a configuration file. Browse. Click Restore to upload the file. Restore
Backup	Click Backup to download current running configurations as a file.

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

File Dov	vnload 🔀
?	You are downloading the file: config.cfg from 192.168.1.1
	Would you like to open the file or save it to your computer?
	Open Save Cancel More Info
	Always ask before opening this type of file

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

Save As						? 🗙
Save in:	🞯 Desktop		~	0 Ø	• 🛄 🍤	
My Recent Documents Desktop My Documents	My Documen My Computer My Network I Annex A Annex A MWSnap300 TeleDanmark Tools Config V2k2_232_cc V2k6_250_cc	Places ∋ infig_1				
My Computer						
	File name:	config			<b>~</b> (	Save
My Network	Save as type:	Configuration file			<b>~</b> (	Cancel

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

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

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

#### **Restore Configuration**

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

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

System Maintenance >> Configuration Backup

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

## 4.14.7 Syslog/Mail Alert

SysLog function is provided for users to monitor router. There is no bother to directly get into the Web Configurator of the router or borrow debug equipments.

SysLog Access Setup		Mail Alert Setup	
Enable Syslog Save to:		Enable	Send a test e-mail
Syslog Server		SMTP Server	25
Router Name		Mail To	
Server IP Address		Return-Path	
Destination Port Mail Syslog	514 Enable	<ul> <li>Authentication</li> <li>User Name</li> </ul>	
Enable syslog message:		Password	
Firewall Log		Enable E-Mail Alert:	
VPN Log		DoS Attack	
User Access Log		M-P2P	
<ul> <li>Call Log</li> <li>WAN Log</li> </ul>		VPN LOG	
Router/DSL inform	nation		

Note: 1. Mail Syslog cannot be activated unless USB Disk is ticked for "Syslog Save to 2. Mail Syslog feature sends a Syslog file when its size reaches 1M Bytes.



Available settings are explained as follows:

System Maintenance >> SysLog / Mail Alert Setup

Item	Description
SysLog Access Setup	Enable - Check Enable to activate function of syslog.
	<b>Syslog Save to</b> – Check <b>Syslog Server</b> to save the log to Syslog server.
	Check <b>USB Disk</b> to save the log to the attached USB storage disk.
Router Name	Display the name for such router configured in <b>System</b> <b>Maintenance&gt;&gt;Management.</b>
	If there is no name here, simply lick the link to access into <b>System Maintenance&gt;&gt;Management</b> to set the router name.
	Server IP Address - The IP address of the Syslog server.
	<b>Destination Port -</b> Assign a port for the Syslog protocol.
	<b>Mail Syslog</b> – Check the box to recode the mail event on Syslog.
	<b>Enable syslog message -</b> Check the box listed on this web page to send the corresponding message of firewall, VPN, User Access, Call, WAN, Router/DSL information to Syslog.
Mail Alert Setup	Check "Enable" to activate function of mail alert.
	<b>Send a test e-mail -</b> Make a simple test for the e-mail address specified in this page. Please assign the mail address first and click this button to execute a test for verify the mail

address is available or not.
SMTP Server - The IP address of the SMTP server.
Mail To - Assign a mail address for sending mails out.
<b>Return-Path</b> - Assign a path for receiving the mail from outside.
<b>Authentication -</b> Check this box to activate this function while using e-mail application.
User Name - Type the user name for authentication.
<b>Password -</b> Type the password for authentication.
<b>Enable E-mail Alert -</b> Check the box to send alert message to the e-mail box while the router detecting the item(s) you specify here.

Click **OK** to save these settings.

For viewing the Syslog, please do the following:

- 1. Just set your monitor PC's IP address in the field of Server IP Address
- 2. Install the Router Tools in the **Utility** within provided CD. After installation, click on the **Router Tools>>Syslog** from program menu.



3. From the Syslog screen, select the router you want to monitor. Be reminded that in **Network Information**, select the network adapter used to connect to the router. Otherwise, you won't succeed in retrieving information from the router.

		192.168.1.1 Vigor series	Ge	ateway IP (Fixed)	TX Packets	TX Rate
Status TX Pao 169		RX Packets 1470		WAN IP (Fixed)	RX Packets	RX Rate
all Log VPN		ess Log Call Log	WAN Log Others Host Name:	Network Information Network Information Network	t State	
IP Address	Mask	MAC	NIC Description:	SiS 900-Based I	PCI Fast Ethernet Adapt	er - Packet S( 🗸
192.168.1.1	255.255.2	00-50-7F-54-6	NIC Information		•	
			MAC Address:	00-11-D8-E4-58-CE	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:	Mon Jan 22 01:28:23 2007
<		>	DNS Servers:	168.95.1.1	Lease Expires:	, Thu Jan 25
	Refresh					01:28:23 2007



## 4.14.8 Time and Date

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

Time Information	
Current System Time	2000 Jan 1 Sat 20 : 14 : 50 Inquire Time
Time Setup	
O Use Browser Time	
💿 Use Internet Time Client	:
Server IP Address	pool.ntp.org
Time Zone	(GMT) Greenwich Mean Time : Dublin 🛛 💌
Enable Daylight Saving	
Automatically Update Int	erval 🛛 30 min 💌
-	
	OK Cancel

Available settings are explained as follows:

Item	Description
Current System Time	Click <b>Inquire Time</b> to get the current time.
Use Browser Time	Select this option to use the browser time from the remote administrator PC host as router's system time.
Use Internet Time	Select to inquire time information from Time Server on the Internet using assigned protocol.
Time Protocol	Select a time protocol.
Server IP Address	Type the IP address of the time server.
Time Zone	Select the time zone where the router is located.
Enable Daylight Saving	Check the box to enable the daylight saving. Such feature is available for certain area.
Automatically Update Interval	Select a time interval for updating from the NTP server.

Click **OK** to save these settings.

#### 4.14.9 Management

This page allows you to manage the settings for access control, access list, port setup, and SNMP setup. For example, as to management access control, the port number is used to send/receive SIP message for building a session.

The management pages for IPv4 and IPv6 protocols are different.

#### For IPv4

System Maintenance >> Management

IPv4 Management Setup IP	v6 Management Setup	
Router Name	Management Port Setup	
	💿 User Define Ports 🛛 🔘	Default Ports
Management Access Control	Telnet Port	23 (Default: 23)
Allow management from the Internet	HTTP Port	80 (Default: 80)
FTP Server	HTTPS Port	443 (Default: 443)
HTTP Server	FTP Port	21 (Default: 21)
HTTPS Server	SSH Port	22 (Default: 22)
Interver		
SSH Server	SNMP Setup	
Disable PING from the Internet	Enable SNMP Agent	
	Get Community	public
Access List List IP Subnet Mask	Set Community	private
	Manager Host IP	
2	Trap Community	public
	Notification Host IP	
3		10 seconds
	Trap Timeout	10 seconds

Available settings are explained as follows:

Item	Description
Router Name	Type in the router name provided by ISP.
Management Access Control	Allow management from the Internet - Enable the checkbox to allow system administrators to login from the Internet. There are several servers provided by the system to allow you managing the router from Internet. Check the box(es) to specify.
	<b>Disable PING from the Internet -</b> 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.
	<b>Subnet Mask -</b> Represent a subnet mask allowed to login to the router.
Management Port Setup	User Defined Ports - Check to specify user-defined port



	numbers for the Telnet, HTTP and FTP servers. <b>Default Ports -</b> Check to use standard port numbers for the Telnet and HTTP servers.
SNMP Setup	<b>Enable SNMP Agent -</b> Check it to enable this function.
	Get Community - Set the name for getting community by typing a proper character. The default setting is <b>public</b> . Set Community - Set community by typing a proper name. The default setting is <b>private</b> .
	Manager Host IP - Set one host as the manager to execute SNMP function. Please type in IP address to specify certain host.
	<b>Trap Community -</b> Set trap community by typing a proper name. The default setting is <b>public.</b>
	<b>Notification Host IP</b> - Set the IP address of the host that will receive the trap community.
	Trap Timeout - The default setting is 10 seconds.

Click **OK** to save these settings.

#### For IPv6

System Maintenance >> Management

IPv4 Managemen	t Setup	IPv6 Management Setup	
Management Acces	s Control		
Allow management	from the Internet		
Telnet Serv	er ( Port : 23)		
HTTP Serve	r ( Port : 80)		
Enable PING fro	om the Internet		
Access List			
	s / Prefix Length		
List IPv6 Address	s / Prefix Length	/ 128	
List IPv6 Address	s / Prefix Length	/ 128	
Access List List IPv6 Address 1. 2.	s / Prefix Length		

Available settings are explained as follows:

Item	Description
Management Access Control	Enable the checkbox to allow system administrators to login from the Internet. There are several servers provided by the system to allow you managing the router from Internet. Check the box(es) to specify.
	<b>Enable PING from the Internet</b> - Check the checkbox to enable all PING packets from the Internet. For security issue, this function is disabled by default.
Access List	You could specify that the system administrator can only

ОК



login from a specific host or network defined in the list. A maximum of three IPs/subnet masks is allowed.
<b>IPv6 Address /Prefix Length-</b> Indicate the IP address(es) allowed to login to the router.

Click **OK** to save these settings.

#### 4.14.10 Reboot System

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

System Maintenance >> Reboot System

Reboot System	
	Do you want to reboot your router ?
	Osing current configuration
	O Using factory default configuration
Auto Reboot Tim	Reboot Now
Ir	ndex(1-15) in <u>Schedule</u> Setup:,,,,,
N	lote: Action and Idle Timeout settings will be ignored.
	OK Cancel

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

In addition, you can enter the index of schedule profiles to reboot your system according to the preconfigured schedules. When you finish the reboot time schedule, please click **OK** to save it. For detailed configuration of time schedule, please refer to section **Schedule**.

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

## 4.14.11 Firmware Upgrade

Before upgrading your router firmware, you need to install the Router Tools. The **Firmware Upgrade Utility** is included in the tools. The following web page will guide you to upgrade firmware by using an example. Note that this example is running over Windows OS (Operating System).

Download the newest firmware from DrayTek's web site or FTP site. The DrayTek web site is www.draytek.com (or local DrayTek's web site) and FTP site is ftp.draytek.com.

Click System Maintenance>> Firmware Upgrade to launch the Firmware Upgrade Utility.

System Maintenance >> Firmware Upgrade

Web Firmware Upgrade	
Select a firmware file.	
Browse.	
Click Upgrade to upload the file. Upgrade	
TFTP Firmware Upgrade from LAN	
Current Firmware Version: 3.6.3	
Firmware Upgrade Procedures:	
<ol> <li>Click "OK" to start the TFTP server.</li> <li>Open the Firmware Upgrade Utility or other 3-party TFTP client software.</li> <li>Check that the firmware filename is correct.</li> <li>Click "Upgrade" on the Firmware Upgrade Utility to start the upgrade.</li> </ol>	

After the upgrade is compelete, the TFTP server will automatically stop running.

Do you want to upgrade firmware ? OK

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

System Maintenance >> Firmware Upgrade

TFTP server is running. Please execute a Firmware Upgrade Utility software to upgrade router's firmware. This server will be closed by itself when the firmware upgrading finished.

## 4.14.12 Activation

There are three ways to activate WCF on vigor router, using **Service Activation Wizard**, by means of **CSM>>Web Content Filter Profile** or via **System Maintenance>>Activation**.

After you have finished the setting profiles for WCF (refer to **Web Content Filter Profile**), it is the time to activate the mechanism for your computer.

Click **System Maintenance>>Activation** to open the following page for accessing http://myvigor.draytek.com.

	Activate via interface : auto-selected Y
Web-Filter License	Activate
[Status:Not Activated]	
Authentication Message	
WebFilter, service not activate 2010-07-27 05:44:03	~
	~

OK Cancel

Each item is explained as follows:

Item	Description	
Activate via interface	Use the drop down menu to choose the interface for accessing the server. auto-selected WAN 1 WAN 2	
Activate	Click this link to access into <u>http://myvigor.draytek.com</u> for activating WCF function.	
Status	Display the mechanism (represented with code number, e.g., CT-CF) adopted by such router.	
Authentication Message	As for authentication information of <b>web filter</b> , the process of authenticating will be displayed on this field for your reference.	



Below shows the successful activation of Web Content Filter:

System Maintenance >> Activation	Activate via interface :	auto-selected	~
----------------------------------	--------------------------	---------------	---

Web-Filter License **Activate** [Status:Commtouch] [Start Date:2010-07-27 Expire Date:2010-08-27] Authentication Message Activated Wiz, Activated Wizard query license status Successful, 2010-07-27  $\wedge$ 08:47:13 Note: If you want to use email alert or syslog, please configure the SysLog/Mail Alert Setup page.

If you change the service provider, the configuration of the function will be reset.

ОК	Cancel
----	--------

Start Date	Display the starting date of WCF license activated successfully.	
Expire Date	Display the ending date of WCF license activated successfully.	

## 4.15 Diagnostics

Diagnostic Tools provide a useful way to **view** or **diagnose** the status of your Vigor router. Below shows the menu items for Diagnostics.

Diagnostics
Dial-out Triggering
Routing Table
ARP Cache Table
IPv6 Neighbour Table
DHCP Table
NAT Sessions Table
Data Flow Monitor
Traffic Graph
Ping Diagnosis
Trace Route
TSPC Status

## 4.15.1 Dial-out Triggering

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

Diagnostics >> Dial-out Trigger	
Dial-out 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	
00 00 00 00 00 00 00 00 00 00 00 00 00	
Decoded Format:	
0.0.0.0 -> 0.0.0.0	
Pr 0 len 0 (0)	

Each item is explained as follows:

Item	Description	
Decoded Format	It shows the source IP address (local), destination IP (remote) address, the protocol and length of the package.	
Refresh	Click it to reload the page.	

## 4.15.2 Routing Table

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

#### **Current Running Routing Table**

Diagnostics >> View Routing Table

Current Running Routing Table	IPv6 Routing Table	<u>Refresh</u>
Key: C - connected, S - static, R C~ 192.168.1.0/ 255.255.255		
		~

Note: WAN3, WAN4, WAN5 are router-borne WANs.

#### **IPv6 Routing Table**

Diagnostics >> View Routing Table

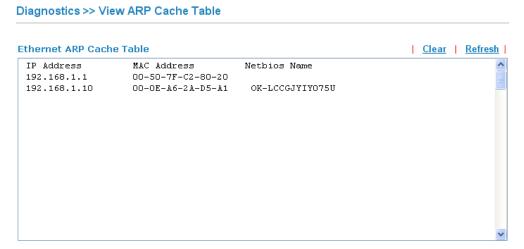
Current Running Routing Table	IPv6 Routin	g Table		Refre	sh
Destination	Interface	-	Metric	Next Hop	^
FE80::/64	LAN	U	256		
FF00::/8	LAN	U	256		
					-
<					

Available settings are explained as follows:

Item	Description
Refresh	Click it to reload the page.

## 4.15.3 ARP Cache Table

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



Available settings are explained as follows:

Diagnostics >> View IPv6 Neighbour Table

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

#### 4.15.4 IPv6 Neighbour Table

The table shows a mapping between an Ethernet hardware address (MAC Address) and an IPv6 address. This information is helpful in diagnosing network problems, such as IP address conflicts, etc.

Click **Diagnostics** and click **IPv6 Neighbour Table** to open the web page.

 IPv6 Neighbour Table
 Refresh

 IPv6 Address
 Mac Address
 Interface

 FF02::1
 33-33-00-00-001
 LAN

Available settings are explained as follows:

Item	Description
Refresh	Click it to reload the page.

#### 4.15.5 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.

## **DHCP IP Assignment Table**

```
Diagnostics >> View DHCP Assigned IP Addresses
```

D	HCP IP Assignme	nt Table	DHCPv	6 IP Assignment T	able		1	Refresh
DHCP s	erver: Running							~
Index	IP Address	MAC Address		Leased Time	HOST	ID		
1	192.168.1.10	7C-61-93-18-E	A-DF	70:58:42				
	android 807f1d	l0bfff92630						
2	192.168.1.20	68-09-27-DC-2	0-E8	71:21:11				
								~

#### **DHCPv6 IP Assignment Table**

Diagnostics >> View DHCP Assigned IP Addresses

DHCP IP Assignment Table	DHCPv6 IP Assignment Table	1	Refresh
DHCPv6 server binding client: Index IPv6 Address	MAC Address	Leased Time	~
<			>

Each item is explained as follows:

Item	Description
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.

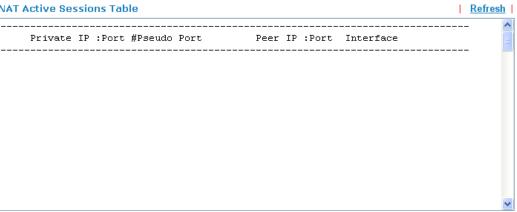
Click it to reload the page.

## 4.15.6 NAT Sessions Table

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

Diagnostics >> NAT Sessions Table

NAT Active Sessions Table



Each item is explained as follows:

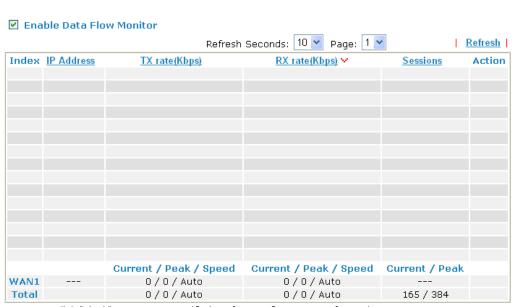
Item	Description
Private IP:Port	It indicates the source IP address and port of local PC.
#Pseudo Port	It indicates the temporary port of the router used for NAT.
Peer IP:Port	It indicates the destination IP address and port of remote host.
Interface	It displays the representing number for different interface.
Refresh	Click it to reload the page.

## 4.15.7 Data Flow Monitor

Diagnostics >> Data Flow Monitor

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

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



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

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

3. (Kbps): shared bandwidth

- + : residual bandwidth used
- Current/Peak are average.

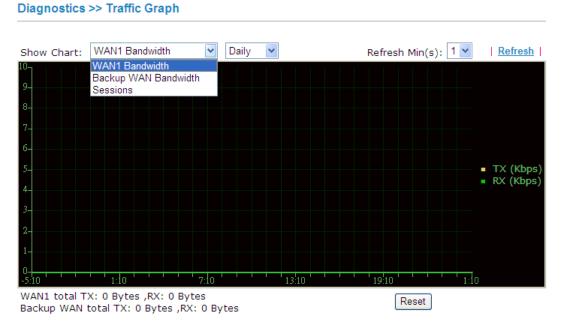
Available settings are explained as follows:

Item	Description	
Enable Data Flow Monitor	Check this box to enable this function.	
Refresh Seconds	Use the drop down list to choose the time interval of refreshing data flow that will be done by the system automatically. Refresh Seconds: 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	<b>Block</b> - can prevent specified PC accessing into Internet within 5 minutes.		
	age: 1 🖌 🛛 Refresh		
	✓ <u>Sessions</u> Action		
	7 <u>Block</u>		
	<b>Unblock</b> – the device with the IP address will be blocked in		
	five minutes. The remaining time will be shown on the session column.		
	age: 1 M Refresh		
	<u>Sessions</u> Action		
	blocked / 298 <u>Unblock</u>		
Current /Peak/Speed	<b>Current</b> means current transmission rate and receiving rate for WAN interface.		
	<b>Peak</b> means the highest peak value detected by the router in data transmission.		
	Speed means line speed specified in WAN>>General Setup.		
	If you do not specify any rate at that page, here will display		
	Auto for instead.		

## 4.15.8 Traffic Graph

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



The horizontal axis represents time. Yet the vertical axis has different meanings. For WAN1 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.

## 4.15.9 Ping Diagnosis

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

Ping Diagnosis		
● IPV4 ○ IPV6		
Ping to: Host / IP 💌	IP Address:	
	Run	
Result		Clear
		_

Each item is explained as follows:

Item	Description
IPV4 /IPV6	Choose the protocol for such function.
Ping to	Use the drop down list to choose the destination that you want to ping.
IP Address	Type in the IP address of the Host/IP that you want to ping.
Ping IPv6 Address	Type the IPv6 address that you want to ping.
Run	Click this button to start the ping work. The result will be displayed on the screen.
Clear	Click this link to remove the result on the window.

## 4.15.10 Trace Route

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

toute	
● IPV4 ○ IPV6	
Protocol: ICMP 🐱	
Host / IP Address:	
Run	
Result	Clear
	<u>~</u>

Diagnostics >> Trace Route

Each item is explained as follows:

Item	Description
IPv4 / IPv6	Choose the protocol for such function.
Protocol	Use the drop down list to choose the protocol that you want to ping through.
Host/IP Address	It indicates the IPv4 address of the host if IPv4 protocol is selected.
Trace Host/IP Address	It indicates the IPv6 address of the host if IPv6 protocol is selected.
Run	Click this button to start route tracing work.
Clear	Click this link to remove the result on the window.

# **4.16 Product Registration**

When you click it, you will be guided to visit myvigor.draytek.com and open the corresponding pages directly.



Click **Support Area>>Product Registration**, the following web page will be displayed.

UserName :			
Password :			
Auth Code :		AYi GXZ	
	If you cannot read the	word, <u>click here</u>	
	Forget passwo	ord? Login	

If you are having difficulty logging in, contact our customer service. Customer Service : (886) 3 597 2727 or email to :<u>Webmaster@draytek.com</u>



# **5** Trouble Shooting

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

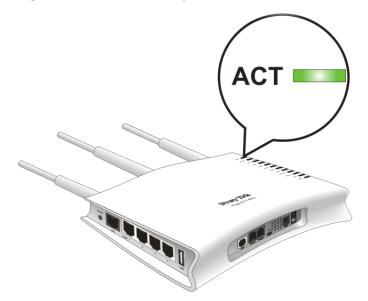
- Checking if the hardware status is OK or not.
- Checking if the network connection settings on your computer are OK or not.
- Pinging the router from your computer.
- Checking if the ISP settings are OK or not.
- Backing to factory default setting if necessary.

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

## 5.1 Checking If the Hardware Status Is OK or Not

Follow the steps below to verify the hardware status.

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



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

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

Sometimes the link failure occurs due to the wrong network connection settings. After trying the above section, if the link is 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**.

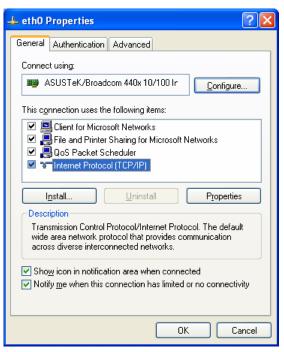
1. Go to Control Panel and then double-click on Network Connections.



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



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



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

Internet Protocol (TCP/IP) Prope	erties 🛛 💽 🔀		
General Alternate Configuration			
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.			
⊙ <u>O</u> btain an IP address automatica	lly		
Use 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 ad	dresses:		
Preferred DNS server:			
Alternate DNS server:			
	Advanced		
	OK Cancel		

#### For Mac OS

- 1. Double click on the current used Mac OS 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 Sound	Network Startup Disk		
Locat	tion: Automatic	•	
TCP/IP	PPPoE AppleTalk Pro	oxies Ethernet	
Configure IPv4:	sing DHCP	•	
IP Address: 19	2.168.1.10	Renew DHCP Lea	ise
Subnet Mask: 25	5.255.255.0 DHCP C	Client ID:	
Router: 19	2.168.1.1	(If required)	
DNS Servers:		(Ор	tional)
Search Domains:		(Op	tional)
IPv6 Address: fe8	0:0000:0000:0000:020a:95	ff:fe8d:72e4	
C	Configure IPv6		?
Click the lock to preve	nt further changes. (	Assist me Apply	Now

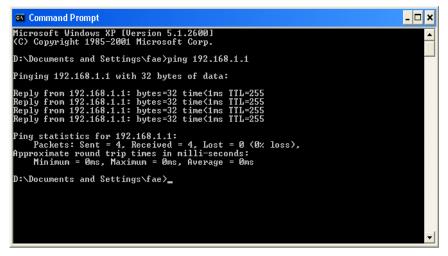
## 5.3 Pinging the Router from Your Computer

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 Mac OS (Terminal)

- 1. Double click on the current used Mac OS 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.



\varTheta 🔿 🔿 Terminal — ba	sh — 80x24
Last login: Sat Jan 3 02:24:18 on ttyp1 Welcome to Darwin! Vigor10:~ draytek\$ ping 192.168.1.1 PING 192.168.1.1 (192.168.1.1): 56 data by 64 bytes from 192.168.1.1: icmp_seq=0 ttl=2 64 bytes from 192.168.1.1: icmp_seq=1 ttl=2 64 bytes from 192.168.1.1: icmp_seq=2 ttl=2 64 bytes from 192.168.1.1: icmp_seq=3 ttl=2	255 time=0.755 ms 255 time=0.697 ms 255 time=0.716 ms
64 bytes from 192.168.1.1: icmp_seq=4 ttl=2 ^C 192.168.1.1 ping statistics 5 packets transmitted, 5 packets received, round-trip min/avg/max = 0.697/0.723/0.755 Vigor10:~ draytek\$	0% packet loss

# 5.4 Checking If the ISP Settings are OK or Not

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



#### Take PPPoE User as an Example

1. Check if the **Enable** option is selected.

Internet Access >> PPPoE / PPPoA

2. Check if **Username** and **Password** are entered with correct values that you **got from** your **ISP**.

# 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 Vigor2710. 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 Vigor2710.

#### 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.

		Court I		Getway IP (Static)	TX Packets	RX Rate
		DrayTek			0	0
AN Status TX Packets		RX Packets		WAN IP (Static)	RX Packets	TX Rate
6442		3807	1		0	0
Wall Log VPN Log	User Acces	ss Log Call Log	WAN Log	Network Infomation	Net State	
-						120
Time	Host	Message				^
Apr 12 09:17:49	Vigor			LCP(c021) ConfReq Id	entifier:0x03 ACCM:	OxO Authe:
Apr 12 09:17:49	Vigor	[3G]Modem stat	tus:a1 20 00	00 00 00 02 00 03 00		
Apr 12 09:17:49 Apr 12 09:17:49	Vigor Vigor	[3G]Modem stat WAN2 PPPoE =	tus:a1 20 00 => Protocol	00 00 00 02 00 03 00 LCP(c021) ConfReg Id		
Apr 12 09:17:49 Apr 12 09:17:49 Apr 12 09:17:49	Vigor Vigor Vigor	[3G]Modem stat WAN2 PPPoE = WAN2 PPPoE <	tus:a1 20 00 => Protocol :== V:1 T:1	00 00 00 02 00 03 00 :LCP(c021) ConfReq Id PADS ID:0		
Apr 12 09:17:49 Apr 12 09:17:49 Apr 12 09:17:49 Apr 12 09:17:49 Apr 12 09:17:49	Vigor Vigor Vigor Vigor	[3G]Modem stat WAN2 PPPoE = WAN2 PPPoE < [3G]Modem res	tus:a1 20 00 => Protocol :== V:1 T:1 ponse: CON	00 00 00 02 00 03 00 LCP(c021) ConfReq Id PADS ID:0 NECT 3600000		
Apr 12 09:17:49 Apr 12 09:17:49 Apr 12 09:17:49 Apr 12 09:17:49 Apr 12 09:17:49 Apr 12 09:17:49	Vigor Vigor Vigor Vigor Vigor	[3G]Modem stat WAN2 PPPoE = WAN2 PPPoE < [3G]Modem res [3G]Modem stat	tus:a1 20 00 => Protocol :== V:1 T:1 ponse: CON tus:a1 20 00	00 00 00 02 00 03 00 LCP(c021) ConfReg Id PADS ID:0 NECT 3600000 00 00 00 02 00 02 00		
Apr 12 09:17:49 Apr 12 09:17:49 Apr 12 09:17:49 Apr 12 09:17:49 Apr 12 09:17:49 Apr 12 09:17:49 Apr 12 09:17:49	Vigor Vigor Vigor Vigor Vigor Vigor Vigor	[3G]Modem sta WAN2 PPPoE = WAN2 PPPoE < [3G]Modem res [3G]Modem stat [3G]Modem stat	tus:a1 20 00 => Protocol :== V:1 T:1 ponse: CON tus:a1 20 00 tus:a1 20 00	00 00 00 02 00 03 00 LCP(c021) ConfReq Id PADS ID:0 NECT 3600000 00 00 00 02 00 02 00 00 00 00 02 00 02 00		
Apr 12 09:17:49 Apr 12 09:17:49	Vigor Vigor Vigor Vigor Vigor Vigor Vigor	[3G]Modem stat WAN2 PPPoE = WAN2 PPPoE < [3G]Modem stat [3G]Modem stat [3G]Modem stat [3G]Modem dia	tus:a1 20 00 => Protocol :== V:1 T:1 ponse: CON tus:a1 20 00 tus:a1 20 00 1 A TDT *99:	00 00 00 02 00 03 00 LCP(c021) ConfReq Id PADS ID:0 NECT 3600000 00 00 00 02 00 02 00 00 00 00 02 00 02 00 #		
Apr 12 09:17:49           Apr 12 09:17:49	Vigor Vigor Vigor Vigor Vigor Vigor Vigor Vigor	[3G]Modem sta WAN2 PPPoE = WAN2 PPPoE < [3G]Modem res [3G]Modem sta [3G]Modem sta [3G]Modem sta [3G]Modem dia WAN2 PPPoE =	tus:a1 20 00 => Protocol :== V:1 T:1 ponse: CON tus:a1 20 00 tus:a1 20 00 1 ATDT*99 => V:1 T:1	00 00 00 02 00 03 00 LCP(021) ConfReq Id PADS ID:0 NECT 3600000 00 00 00 02 00 02 00 00 00 00 02 00 02 00 # PADR ID:0		500 ACCM
Apr 12 09:17:49 Apr 12 09:17:49	Vigor Vigor Vigor Vigor Vigor Vigor Vigor Vigor Vigor	[3G]Modem sta WAN2 PPPoE = WAN2 PPPOE = [3G]Modem sta [3G]Modem sta [3G]Modem sta [3G]Modem dis WAN2 PPPoE = WAN2 PPPoE =	tus:a1 20 00 >> Protocol :== V:1 T:1 ponse: CON tus:a1 20 00 tus:a1 20 00 1 A TDT*999 => V:1 T:1 :== V:1 T:1	00 00 00 02 00 03 00 LCP(021) ConfReq Id PADS ID:0 NECT 3600000 00 00 00 02 00 02 00 00 00 00 02 00 02 00 # PADR ID:0		500 ACCM
Apr 12 09:17:49 Apr 12 09:17:49 Apr 12 09:17:49	Vigor Vigor Vigor Vigor Vigor Vigor Vigor Vigor	[3G]Modem stat WAN2 PPPOE = WAN2 PPPOE = [3G]Modem res [3G]Modem stat [3G]Modem stat [3G]Modem stat [3G]Modem res WAN2 PPPOE = WAN2 PPPOE = [3G]Modem res	tus:a1 20 00 => Protocol :== V:1 T:1 ponse: CON tus:a1 20 00 tus:a1 20 00 1 A TDT *999 => V:1 T:1 :== V:1 T:1 ponse: OK	00 00 00 02 00 03 00 LCP(021) ConfReq Id PADS ID:0 NECT 3600000 00 00 00 02 00 02 00 00 00 00 02 00 02 00 # PADR ID:0	entifier:0x00 MRU: 1	500 ACCM
Apr 12 09:17:49 Apr 12 09:17:49	Vigor Vigor Vigor Vigor Vigor Vigor Vigor Vigor Vigor Vigor Vigor	[3G]Modem stat WAN2 PPPOE = WAN2 PPPOE = [3G]Modem res [3G]Modem stat [3G]Modem stat [3G]Modem stat [3G]Modem res WAN2 PPPOE = WAN2 PPPOE = [3G]Modem res	tus:a1 20 00 ⇒ Protocol ≔ V:1 T:1 ponse: CON tus:a1 20 00 tus:a1 20 00 1 A TDT*999 ⇒ V:1 T:1 ≔ V:1 T:1 ponse: OK tialize A T&I	00 00 00 02 00 03 00 LCP(021) ConfReq Id PADS ID:0 NECT 3600000 00 00 00 02 00 02 00 00 00 00 02 00 02 00 # PADR ID:0 PADO ID:0 # # # # # # # # # # # # #	entifier:0x00 MRU: 1	500 ACCM
Apr 12 09:17:49 Apr 12 09:17:49	Vigor Vigor Vigor Vigor Vigor Vigor Vigor Vigor Vigor Vigor Vigor	[3G]Modem stat WAN2 PPPoE = WAN2 PPPoE = [3G]Modem stat [3G]Modem stat [3G]Modem stat [3G]Modem stat [3G]Modem stat [3G]Modem res [3G]Modem res [3G]Modem res	tus:a1 20 00 ⇒ Protocol ≔ V:1 T:1 ponse: CON tus:a1 20 00 tus:a1 20 00 1 A TDT*999 ⇒ V:1 T:1 ≔ V:1 T:1 ponse: OK tialize A T&I	00 00 00 02 00 03 00 LCP(021) ConfReq Id PADS ID:0 NECT 3600000 00 00 00 02 00 02 00 00 00 00 02 00 02 00 # PADR ID:0 PADO ID:0 # # # # # # # # # # # # #	entifier:0x00 MRU: 1	500 ACCM
Apr 12 09:17:49 Apr 12 09:17:49	Vigor Vigor Vigor Vigor Vigor Vigor Vigor Vigor Vigor Vigor Vigor	[3G]Modem stat WAN2 PPPoE = WAN2 PPPoE = [3G]Modem stat [3G]Modem stat [3G]Modem stat [3G]Modem stat [3G]Modem stat [3G]Modem res [3G]Modem res [3G]Modem res	tus:a1 20 00 ⇒ Protocol ≔ V:1 T:1 ponse: CON tus:a1 20 00 tus:a1 20 00 1 A TDT*999 ⇒ V:1 T:1 ≔ V:1 T:1 ponse: OK tialize A T&I	00 00 00 02 00 03 00 LCP(021) ConfReq Id PADS ID:0 NECT 3600000 00 00 00 02 00 02 00 00 00 00 02 00 02 00 # PADR ID:0 PADO ID:0 # # # # # # # # # # # # #	entifier:0x00 MRU: 1	500 ACCM

#### 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 Vigor2710. In addition, please refer to the manual of 3G USB Modem for LED Status to make sure if the modem connects to Internet via HSDPA mode. If you want to use the modem indoors, please put it on the place near the window to obtain better signal receiving.

# 5.6 Backing to Factory Default Setting If Necessary

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



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



#### Software Reset

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

Go to **System Maintenance** and choose **Reboot System** on the web page. The following screen will appear. Choose **Using factory default configuration** and click **Reboot Now**. 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 ?
<ul> <li>Using current configuration</li> </ul>
<ul> <li>Using factory default configuration</li> </ul>
Reboot Now
Auto Reboot Time Schedule
Index(1-15) in <u>Schedule</u> Setup:,,,,
Note: Action and Idle Timeout settings will be ignored.
OK Cancel

#### **Hardware Reset**

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



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

## **5.7 Contacting Your Dealer**

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

