

Vigor2930 Series Dual-WAN Security Firewall User's Guide

Version: 1.2 Date: 2008/03/10

Copyright 2008 All rights reserved.

This publication contains information that is protected by copyright. No part may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language without written permission from the copyright holders. The scope of delivery and other details are subject to change without prior notice.

Microsoft is a registered trademark of Microsoft Corp. Windows, Windows 95, 98, Me, NT, 2000, XP, Vista and Explorer are trademarks of Microsoft Corp. Apple and Mac OS are registered trademarks of Apple Inc. Other products may be trademarks or registered trademarks of their respective manufacturers.

Copyright Information

Copyright Information				
Copyright Declarations	Copyright 2008 All rights reserved. This publication contains information that is protected by copyright. No part may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language without written permission from the copyright holders.			
Trademarks	 The following trademarks are used in this document: Microsoft is a registered trademark of Microsoft Corp. Windows, Windows 95, 98, Me, NT, 2000, XP, Vista and Explorer are trademarks of Microsoft Corp. Apple and Mac OS are registered trademarks of Apple Inc. Other products may be trademarks or registered trademarks of their respective manufacturers. 			
Safety Instruction	s and Approval			
Safety Instructions	 Read the installation guide thoroughly before you set up the router. The router is a complicated electronic unit that may be repaired only be authorized and qualified personnel. Do not try to open or repair the router yourself. Do not place the router in a damp or humid place, e.g. a bathroom. The router should be used in a sheltered area, within a temperature range of +5 to +40 Celsius. Do not expose the router to direct sunlight or other heat sources. The housing and electronic components may be damaged by direct sunlight or heat sources. Do not deploy the cable for LAN connection outdoor to prevent electronic shock hazards. Keep the package out of reach of children. When you want to dispose of the router, please follow local regulations on conservation of the environment 			
Warranty	conservation of the environment. We warrant to the original end user (purchaser) that the router will be free from any defects in workmanship or materials for a period of two (2) years from the date of purchase from the dealer. Please keep your purchase receipt in a safe place as it serves as proof of date of purchase. During the warranty period, and upon proof of purchase, should the product have indications of failure due to faulty workmanship and/or materials, we will, at our discretion, repair or replace the defective products or components, without charge for either parts or labor, to whatever extent we deem necessary tore-store the product to proper operating condition. Any replacement will consist of a new or re-manufactured functionally equivalent product of equal value, and will be offered solely at our discretion. This warranty will not apply if the product is modified, misused, tampered with, damaged by an act of God, or subjected to abnormal working conditions. The warranty does not cover the bundled or licensed software of other vendors. Defects which do not significantly affect the usability of the product will not be covered by the warranty. We reserve the right to revise the manual and online documentation and to make changes from time to time in the contents hereof without obligation to notify any person of such revision or changes.			
Be a Registered Owner	Web registration is preferred. You can register your Vigor router via http://www.draytek.com.			
Firmware & Tools Updates	Due to the continuous evolution of DrayTek technology, all routers will be regularly upgraded. Please consult the DrayTek web site for more information on newest firmware, tools and documents.			
	http://www.draytek.com			

http://www.draytek.com

European Community Declarations

Manufacturer: DrayTek Corp.

Address:No. 26, Fu Shing Road, HuKou County, HsinChu Industrial Park, Hsin-Chu, Taiwan 303Product:Vigor2930 Series Router

DrayTek Corp. declares that Vigor2930 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.

Regulatory Information

Federal Communication Commission Interference Statement

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

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

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

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

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

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



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

Table of Contents



Preface	1
1.1 Web Configuration Buttons Explanation	
1.2 LED Indicators and Connectors	2
1.2.1 For Vigor2930 1.2.2 For Vigor2930n	
1.2.3 For Vigor2930Vn 1.2.4 For Vigor2930VS 1.2.5 For Vigor2930VSn	
1.3 Hardware Installation	
1.4 ISDN Phone Adapter Installation	



Configuring Basic Settings	15
2.1 Changing Password	15
2.2 Quick Start Wizard	17
2.2.1 PPPoE 2.2.2 PPTP	
2.2.3 Static IP 2.2.4 DHCP	21
2.3 Online Status	23
2.4 Saving Configuration	25



Advanced Web Configuration	27
3.1 WAN	27
3.1.1 Basics of Internet Protocol (IP) Network 3.1.2 General Setup	28
3.1.3 Internet Access 3.1.4 Load-Balance Policy	
3.2 LAN	39
 3.2.1 Basics of LAN 3.2.2 General Setup 3.2.3 Static Route 3.2.4 VLAN 3.2.5 Bind IP to MAC 	41 43 46
3.3 NAT	48
3.3.1 Port Redirection 3.3.2 DMZ Host 3.3.3 Open Ports	51
3.4 Objects Settings	56

3.4.1 IP Object	
3.4.2 IP Group 3.4.3 Service Type Object	
3.4.4 Service Type Group	
3.4.5 CSM-IM Object	. 61
3.4.6 CSM-P2P Object 3.4.7 CSM-Misc Object	
3.5 CSM	
3.5.1 IM/P2P Profile	. 65
3.5.2 URL Content Filter Profile 3.5.3 Web Content Filter Profile	
3.6 Firewall	
3.6.1 Basics for Firewall 3.6.2 General Setup	
3.6.3 Filter Setup	
3.6.4 DoS Defense	. 79
3.7 Bandwidth Management	. 82
3.7.1 Sessions Limit	. 82
3.7.2 Bandwidth Limit	
3.7.3 Quality of Service	
3.8 Applications	. 92
3.8.1 Dynamic DNS	
3.8.2 Schedule	
3.8.3 RADIUS	
3.8.5 Wake on LAN	
3.9 VPN and Remote Access	100
3.9.1 Remote Access Control	100
3.9.2 PPP General Setup	
3.9.3 IPSec General Setup	
3.9.4 IPSec Peer Identity	
3.9.6 LAN to LAN	108
3.9.7 Connection Management	116
3.10 Certificate Management	117
3.10.1 Local Certificate	
3.10.2 Trusted CA Certificate	
3.10.3 Certificate Backup	
3.11 VoIP	
3.11.1 DialPlan	
3.11.2 SIP Accounts	
3.11.4 Status	
3.12 ISDN	150
3.12.1 Basic Concept	150
3.12.2 General Settings	151
3.12.3 Dial to Single/Dual ISPs 3.12.4 Call Control	
3.13 Wireless LAN	
3.13.1 Basic Concepts	
3.13.2 General Setup	101

Vigor2930 Series User's Guide

v

3.13.3 Security	
3.13.4 Access Control	
3.13.5 WPS	
3.13.6 WDS	
3.13.7 AP Discovery	
3.13.8 Station List	
3.13.9 Rate Control	174
3.14 System Maintenance	174
3.14.1 System Status	175
3.14.2 TR-069 Setting	
3.14.3 Administrator Password	177
3.14.4 Configuration Backup	177
3.14.5 Syslog/Mail Alert	
3.14.6 Time and Date	
3.14.7 Management	
3.14.8 Reboot System	
3.14.9 Firmware Upgrade	
3.15 Diagnostics	
3.15.1 Dial-out Trigger	
3.15.2 Routing Table	
3.15.3 ARP Cache Table	
3.15.4 DHCP Table	
3.15.5 NAT Sessions Table	
3.15.6 Data Flow Monitor	
3.15.7 Traffic Graph	190
3.15.8 Ping Diagnosis	191
3.15.9 Trace Route	192



Application and Examples1	193
4.1 Create a LAN-to-LAN Connection Between Remote Office and Headquarter	193
4.2 Create a Remote Dial-in User Connection Between the Teleworker and Headquarter	200
4.3 QoS Setting Example	204
4.4 LAN – Created by Using NAT	207
4.5 Calling Scenario for VoIP function	209
4.5.1 Calling via SIP Sever 4.5.2 Peer-to-Peer Calling	209 211
4.6 Upgrade Firmware for Your Router	213
4.7 Request a certificate from a CA server on Windows CA Server	215
4.8 Request a CA Certificate and Set as Trusted on Windows CA Server	219



vi

Trouble Shooting	.221
5.1 Checking If the Hardware Status Is OK or Not	221
5.2 Checking If the Network Connection Settings on Your Computer Is OK or Not	222
5.3 Pinging the Router from Your Computer	224
5.4 Checking If the ISP Settings are OK or Not	225

5.5 Backing to Factory Default Setting If Necessary	
5.6 Contacting Your Dealer	

VolPon www.voipon.co.uk sales@voipon.co.uk Tel: +44 (0)1245 808195 Fax: +44 (0)1245 808299



Vigor2930 is a broadband router with dual-WAN interface. It provides policy-based load-balance, fail-over and BOD (Bandwidth on Demand), also it integrates IP layer QoS, NAT session/bandwidth management to help users control works well with large bandwidth.

By adopting hardware-based VPN platform, hardware encryption of AES/DES/3DS and hardware key hash of SHA-1/MD5, the router increases the performance of VPN greatly, and offers several protocols (such as IPSec/PPTP/L2TP) with up to 100 VPN tunnels.

The object-originated 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.

Vigor2930 "S" series models support two ISDN ports. ISDN S0 (1) port is dedicated for ISDN phone and ISDN S0 (2) port is configurable for ISDN line and phone if required. It can support multiple SIP registrars with high flexible configuration and call handling options.

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

1.1 Web Configuration Buttons Explanation

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

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

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

1.2 LED Indicators and Connectors

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

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

Definitions for ISDN Ports

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

ISDN TE (Terminal Equipment) means an interface for transmitting analog signal through Internet between Switching and router. Such interface is also named with **ISDN S0 extern** in Germany.

ISDN NT (Network Terminator) is a port that used to connect general phone. Such interface is also named with **ISDN S0 intern** in Germany.

The **ISDN S0 (1)** port on Vigor2930 series is fixed to connect phone forever and the LED on the connecter will light orange always. However **ISDN S0 (2)** port on this device is configurable for connecting phone or accessing Internet according to the settings that you adjust on WEB UI (please refer to **VoIP>>Phone Setting** for detailed information).



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

1.2.1 For Vigor2930

VIGC	PRZ930 VAN BECURITY FIREWALL	ACT CPA MGMT Dos Want VPN CSM WAN2 Qos	Pactory Restart Restart Patrice 2 Restart Restart Restart Restart Restart
LED		Status	Explanation
ACT (Activity	y)	Blinking	The router is powered on and running normally.
		Off	The router is powered off.
DoS		On	The DoS/DDoS function is active.
		Blinking	It will blink while deleting an attack.
CSM		On	The profile of CSM (Content Security Management) for IM/P2P application is active. (It is enabled from CSM >> IM/P2P Profile).
CPA (Content	t Portal Authority)	On	The Web Content Filter is active. (It is enabled from CSM >> Web Content Filter Profile).
WAN1/2		On	The WAN1 or WAN2 port is connected.
		Blinking	It will blink while transmitting data.
MGMT		On	The router is managed (handled) by Telnet.
		Blinking	It will blink while being managed by IE browser.
VPN		On	The VPN tunnel is active.
QoS		On	The QoS function is active.
LED on Con	nector		
	Left LED	On	The port is connected.
WAN 1/2	(Green)	Off	The port is disconnected.
		Blinking	The data is transmitting.
	Right LED	On	The port is connected with 100Mbps.
	(Green)	Off	The port is disconnected with 10Mbps.
	Left LED	On	The port is connected.
LAN 1/2/3/4	(Green)	Off	The port is disconnected.
		Blinking	The data is transmitting.
	Right LED	On	The port is connected with 100Mbps.
	(Green)	Off	The port is disconnected with 10Mbps.
Interface	Descript	tion	
Factory Reset			or more than 5 seconds. When you see the ACT LED an usual, release the button. Then the router will restart
Restart			
WAN(1/2)	Connecter	Connecters for remote networked devices.	
LAN (1-4)	N (1-4) Connecters for local networked devices.		vorked devices.
PWR	WR Connecter for a power adapter.		lapter.
ON/OFF Power Switch.			

1.2.2 For Vigor2930n

LED Status Explanation ACT (Activity) Blinking The router is powered on and running normally. DoS On The router is powered off. DoS On The DoS/DDOS function is active. Blinking It will blink while deleting an attack. Blinking CSM On The DoS/DDOS function is active. WLAN On With Status while deleting an attack. WLAN On Witheless access point is ready. WAN1/2 On With With while wireless traffic goes through. It will blink while wireless traffic goes through. It will blink while wireless traffic goes through. WAN1/2 On The WAN1 or WAN2 port is connected. Blinking It will blink while transmitting data. MGMT MGMT On The port is connected. VPN On The port is connected. UPN On The port is disconnected. Green Off The port is disconnected. (Green) Off The port is disconnected. (Green) Off The port is disconnected.	VIGO	ay Tek	ACT WILAN MONT DOS WAMI VPN CSM WANZ QOS	Factory Reset Restart 2 WAN LAN
Off The router is powered off. DoS On The DoS/DDoS function is active. Blinking It will blink while deleting an attack. CSM On The profile of CSM (Content Security Management) for IM/P2P application is active. (It is enabled from CSM >> IM/P2P Profile). WLAN On Wireless access point is ready. Blinking It will blink while wireless traffic goes through. It will blink fast when WPS is working and it will return to normal condition after two minutes. (You need to setup WPS within 2 minutes.) WAN1/2 On The WAN1 or WAN2 port is connected. Blinking It will blink while being managed by IE browser. (You need to setup WPS within 2 minutes.) VPN On The YON throw IS port is connected. QoS On The port is connected. UPN On The port is connected. QoS On The port is connected. Green) Off The port is connected. (Green) Off The port is connected. (Green) Off The port is disconnected. (Green) Off The port is disconnected. (Green) Off The port	LED		Status	Explanation
DoS On The DoS/DDoS function is active. Blinking It will blink while deleting an attack. CSM CSM On The profile of CSM (Content Security Management) for IM/P2P application is active. (It is enabled from CSM >> IM/P2P Profile). WLAN On Wireless access point is ready. Blinking It will blink while wireless traffic goes through. It will blink while wireless traffic goes through. It will blink while wireless traffic goes through. It will blink while vireless traffic goes through. WAN1/2 On The value of one to setup WPS within 2 minutes.) (You need to setup WPS within 2 minutes.) WAN1/2 On The value stamaged (handled) by Telnet. Blinking MGMT On The port is connected. QoS On The port is connected. VPN On The port is disconnected. QoS On The port is disconnected. UPN Off The port is connected. G(Green) Off The port is disconnected. (Green) Off The port is disconnected. (Green) Off The port is disconnected. (Green) Off The port is disconnected.	ACT (Activity))	Blinking	The router is powered on and running normally.
Blinking It will blink while deleting an attack. CSM On The profile of CSM (Content Security Management) for IM/P2P application is active. (It is enabled from CSM >> IM/P2P Profile). WLAN On Wireless access point is ready. Blinking It will blink while wireless traffic goes through. It will blink fast when WPS is working and it will return to normal condition after two minutes.) (You need to setup WPS within 2 minutes.) WAN1/2 On The WAN1 or WAN2 port is connected. Blinking It will blink while braing managed by Telnet. Blinking It will blink while being managed by IE browser. VPN On The VPN tunnel is active. QoS On The QOS function is active. LED on Connector If will blink while stative. WAN 1/2 Off The port is connected. (Green) Off The port is disconnected. (Green) Off The port is disconnec			Off	1
CSM On The profile of CSM (Content Security Management) for IM/P2P application is active. (It is enabled from CSM >> IM/P2P Profile). WLAN On Wireless access point is ready. Blinking It will blink while wireless traffic goes through. It will blink shats when WPS is working and it will return to normal condition after two minutes. (You need to setup WPS within 2 minutes.) WAN1/2 On The WAN1 or WAN2 port is connected. Blinking It will blink while transmitting data. MGMT On The Pout is managed (handled) by Telnet. Blinking It will blink while transmitting data. VPN On The Port is connected. QoS On The port is connected. WAN 1/2 On The port is disconnected. (Green) Off The port is di	DoS		-	
Management) for IM/P2P application is active. (It is enabled from CSM >> IM/P2P Profile). WLAN On Wireless access point is ready. Blinking It will blink while wireless traffic goes through. It will blink fast when WPS is working and it will return to normal condition after two minutes. (You need to setup WPS within 2 minutes.) WAN1/2 On The WAN1 or WAN2 port is connected. MGMT On The router is managed fundidely by Telnet. MGMT On The router is managed fundidely by Telnet. QoS On The PVPN tunnel is active. QoS On The port is connected. WAN 1/2 Left LED On The port is connected. WAN 1/2 Left LED On The port is connected. WAN 1/2 Left LED On The port is connected. WAN 1/2 Left LED On The port is connected. (Green) Off The port is disconnected. (Green) <td< td=""><td></td><td></td><td>Blinking</td><td>· · · · · · · · · · · · · · · · · · ·</td></td<>			Blinking	· · · · · · · · · · · · · · · · · · ·
Blinking It will blink while wireless traffic goes through. It will blink fast when WPS is working and it will return to normal condition after two minutes. (You need to setup WPS within 2 minutes.) WAN1/2 On The WAN1 or WAN2 port is connected. Blinking It will blink while transmitting data. MGMT On The router is managed (handled) by Telnet. Blinking It will blink while bransmitting data. MGMT On The router is managed (handled) by Telnet. Blinking It will blink while bransmitting data. QoS On The QoS function is active. LED on Connector Use on the port is connected. Green WAN 1/2 Left LED On The port is connected. (Green) Off The port is disconnected.	CSM		On	Management) for IM/P2P application is active. (It
It will blink fast when WPS is working and it will return to normal condition after two minutes. (You need to setup WPS within 2 minutes.) WAN1/2 On The WAN1 or WAN2 port is connected. MGMT On The router is managed (handled) by Telnet. Blinking It will blink while transmitting data. MGMT On The router is managed (handled) by Telnet. Blinking It will blink while being managed by IE browser. VPN On The VPN tunnel is active. QoS On The QoS function is active. LED on Connector It will blink mile being managed by IE browser. WAN 1/2 Left LED On (Green) Off The port is connected. (Green) Off The port is disconnected. (Green) Off The port is disconnected. (Green) Off The port is connected. (Green) Off The port is disconnected. (Green) <td>WLAN</td> <td></td> <td>On</td> <td>Wireless access point is ready.</td>	WLAN		On	Wireless access point is ready.
WAN1/2 On The WAN1 or WAN2 port is connected. Blinking MGMT On The router is managed (handled) by Telnet. Blinking MGMT On The router is managed (handled) by Telnet. Blinking VPN On The VPN tunnel is active. QoS On The QPN tunnel is active. QoS On The port is connected. WAN 1/2 Left LED (Green) On The port is connected. WAN 1/2 Left LED (Green) On The port is disconnected. Right LED (Green) On The port is connected with 100Mbps. (Green) Off The port is connected. ULAN 1/2/3/4 Left LED (Green) On The port is connected. Blinking The data is transmitting. Blinking The data is transmitting. Right LED (Green) On The port is connected. On Off The port is disconnected. DMbps. (Green) Off The port is disconnected. (Green) Off The port is disconnected with 100Mbps. (Green) Off The port is disconnected with 100Mbps. (Green) Off			Blinking	It will blink fast when WPS is working and it will return to normal condition after two minutes.
Blinking It will blink while transmitting data. MGMT On The router is managed (handled) by Telnet. Blinking It will blink while being managed by IE browser. VPN On The VPN tunnel is active. QoS On The VPN tunnel is active. QoS On The QOS function is active. LED on Connector On The port is connected. WAN 1/2 Left LED On The port is connected. WAN 1/2 (Green) Off The port is connected. Right LED On The port is connected with 100Mbps. (Green) (Green) Off The port is connected. (DMDMS) LAN 1/2/3/4 Left LED On The port is connected. (Green) Off The port is connected. (DMDMS) (Green) Off The port is connected.	WAN1/2		On	
MGMT On The router is managed (handled) by Telnet. Blinking It will blink while being managed by IE browser. VPN On The VPN tunnel is active. QoS On The QoS function is active. LED on Connector Iteft LED On The port is connected. WAN 1/2 Left LED On The port is connected. (Green) Off The port is connected. Iter (Green) Right LED On The port is connected with 100Mbps. Iter (Green) (Green) Off The port is connected. Iter (Green) ILAN 1/2/3/4 Left LED On The port is connected. (Green) Off The port is connected. Iter (Green) (Green) Off The port is connected. Iter (Green) (Green) Off The port is disconnected. Iter (Green) (Green) Off The port is disconnected. Iter (Green) (Green) Off The port is disconnected. Iter (Green) Factory Reset Press "Factory Reset" button once to make ne				
VPN On The VPN tunnel is active. QoS On The QoS function is active. LED on Connector Itef LED On The port is connected. WAN 1/2 Left LED On The port is disconnected. Blinking The data is transmitting. Blinking The data is transmitting. Right LED On The port is connected with 100Mbps. (Green) Off The port is connected. LAN 1/2/3/4 Left LED On The port is disconnected. (Green) Off The port is disconnected. Off The port is disconnected. Off IAN 1/2/3/4 Green) Off The port is connected. (Green) Off The port is disconnected. Off (Green) Off The port is disconnected. Off (Green) Off The port is disconnected with 100Mbps. Off (Green) Off The port is disconnected with 10Mbps. Off Factory Reset Off The port is disconnected with 10Mbps. Press "Factory Reset" button twice to enable or disable WLAN function. Press "Factory Reset" button twic	MGMT			
QoS On The QoS function is active. LED on Connector Itef LED On The port is connected. WAN 1/2 Left LED On The port is disconnected. Blinking The data is transmitting. Blinking The data is transmitting. Right LED On The port is disconnected with 100Mbps. Green) LAN 1/2/3/4 Left LED On The port is disconnected. Right LED On The port is disconnected. Green) Right LED On The port is disconnected. Green) Right LED On The port is connected with 100Mbps. Green) Green) Off The port is connected with 100Mbps. Green) Green) Off The port is disconnected. Disconnected with 100Mbps. Green) Off The port is disconnected with 100Mbps. Green) Green) Off The port is disconnected with 100Mbps. Green) Fress "Factory Reset" button once to make network connection through WPS. Press "Factory Reset" button twice to enable or disable WLAN function. Press "Factory Rese			Blinking	It will blink while being managed by IE browser.
LED on Connector WAN 1/2 Left LED (Green) On The port is connected. Right LED (Green) On The port is disconnected. Right LED (Green) On The port is connected with 100Mbps. LAN 1/2/3/4 Left LED (Green) On The port is connected. LAN 1/2/3/4 Left LED (Green) On The port is connected. Right LED (Green) On The port is connected. Right LED (Green) On The port is connected. Right LED (Green) On The port is connected with 100Mbps. (Green) Off The port is connected with 100Mbps. (Green) Off The port is disconnected with 100Mbps. (Green) Off The port is disconnected with 100Mbps. (Green) Off The port is disconnected with 100Mbps. (Freen) Off The port is disconnected with 100Mbps. (Green) Off The port is disconnected with 10Mbps. (Green) Off The port is disconnected with 10Mbps. (Freen) Off The port is disconnected with 10Mbps. (Freen) Off The port is disconnected with 10Mbps. <td>VPN</td> <td></td> <td>On</td> <td>The VPN tunnel is active.</td>	VPN		On	The VPN tunnel is active.
WAN 1/2 Left LED (Green) On The port is connected. Right LED (Green) On The port is disconnected. Blinking The data is transmitting. Right LED (Green) On The port is connected with 100Mbps. Left LED (Green) On The port is connected. LAN 1/2/3/4 Left LED (Green) On The port is disconnected. Right LED (Green) On The port is disconnected. Right LED (Green) On The port is disconnected. Blinking The data is transmitting. Right LED (Green) On The port is connected with 100Mbps. Off The port is disconnected with 100Mbps. Off The port is disconnected with 100Mbps. Green) Off The port is disconnected. No The port is disconnected with 100Mbps. Off Green) Off The port is disconnected. No The port is disconnected. Ontothe port is disconnected. No Off The port is disconnected. No Off The port is disconnected. No Off The port is disconnected. <tr< td=""><td>QoS</td><td></td><td>On</td><td>The QoS function is active.</td></tr<>	QoS		On	The QoS function is active.
WAN 1/2 (Green) Off The port is disconnected. Blinking The data is transmitting. Right LED (Green) On The port is connected with 100Mbps. Left LED (Green) Off The port is disconnected. LAN 1/2/3/4 Left LED (Green) On The port is disconnected. Right LED (Green) Off The port is disconnected. Blinking The data is transmitting. Right LED (Green) On The port is disconnected with 100Mbps. (Green) Off The port is disconnected with 10Mbps. Factory Reset Off The port is disconnected with 10Mbps. Factory Reset Press "Factory Reset" button once to make network connection through WPS. Press "Factory Reset" button of or 5 seconds to do the 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 fac	LED on Conn	nector		
WAN 1/2 (Green) Off The port is disconnected. Blinking The data is transmitting. Blinking The data is transmitting. Right LED (Green) On The port is connected with 100Mbps. LAN 1/2/3/4 Left LED (Green) On The port is disconnected. Right LED (Green) On The port is disconnected. Blinking The data is transmitting. Right LED (Green) On The port is disconnected with 100Mbps. Off The port is connected with 100Mbps. Off The port is disconnected with 100Mbps. Off The port is connected with 100Mbps. Off The port is disconnected with 10Mbps. Interface Description Factory Reset Press "Factory Reset" button once to make network connection through WPS. Press "Factory Reset" button twice to enable or disable WLAN function. Press "Factory Reset" button for 5 seconds to do the 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. Restart Restart the router forcefully. Phone (1/2) Connecters for PSTN phones.		Left LED	On	The port is connected.
Right LED (Green)OnThe port is connected with 100Mbps.LAN 1/2/3/4Left LED (Green)OnThe port is disconnected with 10Mbps.LAN 1/2/3/4Left LED (Green)OnThe port is connected.Right LED (Green)OnThe port is connected with 100Mbps.Right LED (Green)OnThe port is connected with 100Mbps.Green)OffThe port is connected with 100Mbps.InterfaceDescriptionFactory ResetPress "Factory Reset" button once to make network connection through WPS. Press "Factory Reset" button twice to enable or disable WLAN function. Press "Factory Reset" button for 5 seconds to do the 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.RestartRestart the router forcefully.Phone (1/2)Connecters for PSTN phones.	WAN 1/2		Off	
(Green)OffThe port is disconnected with 10Mbps.LAN 1/2/3/4Left LED (Green)OnThe port is connected.Right LED (Green)OffThe port is disconnected with 100Mbps.Right LED (Green)OffThe port is connected with 100Mbps.InterfaceOffThe port is disconnected with 10Mbps.Factory ResetPress "Factory Reset" button once to make network connection through WPS. Press "Factory Reset" button twice to enable or disable WLAN function. Press "Factory Reset" button twice to enable or disable WLAN function. Press "Factory Reset" button 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.RestartRestart the router forcefully.Phone (1/2)Connecters for PSTN phones.			Blinking	The data is transmitting.
Left LED On The port is disconnected. LAN 1/2/3/4 Off The port is disconnected. Right LED On The port is disconnected. Right LED On The port is connected. Image: Connect of the port is disconnected. Blinking Right LED On The port is connected with 100Mbps. (Green) Off The port is disconnected with 10Mbps. Interface Description Description Factory Reset Press "Factory Reset" button once to make network connection through WPS. Press "Factory Reset" button twice to enable or disable WLAN function. Press "Factory Reset" button for 5 seconds to do the 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. Restart Restart the router forcefully. Phone (1/2) Connecters for PSTN phones.		Right LED	On	The port is connected with 100Mbps.
LAN 1/2/3/4 (Green) Off The port is disconnected. Blinking The data is transmitting. Right LED (Green) On The port is connected with 100Mbps. Off The port is disconnected with 10Mbps. Interface Description Factory Reset Press "Factory Reset" button once to make network connection through WPS. Press "Factory Reset" button twice to enable or disable WLAN function. Press "Factory Reset" button for 5 seconds to do the 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. Restart Restart the router forcefully. Phone (1/2) Connecters for PSTN phones.		(Green)	Off	The port is disconnected with 10Mbps.
On The port is disconnected. Blinking The data is transmitting. Right LED (Green) On The port is connected with 100Mbps. Interface Oescription Factory Reset Press "Factory Reset" button once to make network connection through WPS. Press "Factory Reset" button for 5 seconds to do the 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. Restart Restart the router forcefully. Phone (1/2) Connecters for PSTN phones.		Left LED	On	The port is connected.
Right LED (Green)OnThe port is connected with 100Mbps.Image: Connected with 10Mbps.OffThe port is disconnected with 10Mbps.Image: Connected with 10Mbps.Image: Connecter with 10Mbps.Image: Connected with 10Mbps.Image: Connecter with 10Mbps.Image: C	LAN 1/2/3/4	(Green)	Off	The port is disconnected.
(Green)OffThe port is disconnected with 10Mbps.InterfaceDescriptionFactory ResetPress "Factory Reset" button once to make network connection through WPS. Press "Factory Reset" button twice to enable or disable WLAN function. Press "Factory Reset" button for 5 seconds to do the 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.RestartRestart the router forcefully.Phone (1/2)Connecters for PSTN phones.			Blinking	The data is transmitting.
Interface Description Factory Reset Press "Factory Reset" button once to make network connection through WPS. Press "Factory Reset" button twice to enable or disable WLAN function. Press "Factory Reset" button twice to enable or disable WLAN function. Press "Factory Reset" button for 5 seconds to do the 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. Restart Restart the router forcefully. Phone (1/2) Connecters for PSTN phones.			On	The port is connected with 100Mbps.
InterfaceDescriptionFactory ResetPress "Factory Reset" button once to make network connection through WPS. Press "Factory Reset" button twice to enable or disable WLAN function. Press "Factory Reset" button for 5 seconds to do the 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.RestartRestart the router forcefully.Phone (1/2)Connecters for PSTN phones.		(Green)	Off	The port is disconnected with 10Mbps.
Factory ResetPress "Factory Reset" button once to make network connection through WPS. Press "Factory Reset" button twice to enable or disable WLAN function. Press "Factory Reset" button for 5 seconds to do the 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.RestartRestart the router forcefully.Phone (1/2)Connecters for PSTN phones.	Patient Ration	, E		
Factory ResetPress "Factory Reset" button once to make network connection through WPS. Press "Factory Reset" button twice to enable or disable WLAN function. Press "Factory Reset" button for 5 seconds to do the 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.RestartRestart the router forcefully.Phone (1/2)Connecters for PSTN phones.	Interface	Descri	ption	
RestartRestart the router forcefully.Phone (1/2)Connecters for PSTN phones.		 Press "Factory Reset" button once to make network connection through WPS. Press "Factory Reset" button twice to enable or disable WLAN function. Press "Factory Reset" button for 5 seconds to do the 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 		
Phone (1/2) Connecters for PSTN phones.	Restart			

LAN (1-4)	Connecters for local networked devices.
PWR	Connecter for a power adapter
ON/OFF	Power Switch.

1.2.3 For Vigor2930Vn

VIGO	Tay Tek JR2930Vn VAN BEDURITY FIREWALL	ACT WLAN MONT DOS WANI Phone1 CSM WAN2 Phone2	Image: start start start Image: start star	
LED		Status	Explanation	
ACT (Activity	y)	Blinking	The router is powered on and running normally.	
-		Off	The router is powered off.	
DoS		On	The DoS/DDoS function is active.	
		Blinking	It will blink while deleting an attack.	
CSM		On	The profile of CSM (Content Security Management) for IM/P2P application is active. (It is enabled from CSM >> IM/P2P Profile).	
WLAN		On	Wireless access point is ready.	
			It will blink while wireless traffic goes through. It will blink fast when WPS is working and it will return to normal condition after two minutes. (You need to setup WPS within 2 minutes.)	
WAN1/2		On	The WAN1 or WAN2 port is connected.	
		Blinking	It will blink while transmitting data.	
MGMT		On	The router is managed (handled) by Telnet.	
		Blinking	It will blink while being managed by IE browser.	
Phone 1/2		On	The phone connected to this port is off-hook.	
		Off	The phone connected to this port is on-hook.	
			A phone call comes.	
LED on Con	nector			
	Left LED	On	The port is connected.	
WAN 1/2	(Green)	Off	The port is disconnected.	
		Blinking	The data is transmitting.	
	Right LED	On	The port is connected with 100Mbps.	
	(Green)	Off	The port is disconnected with 10Mbps.	
	Left LED	On	The port is connected.	
LAN 1/2/3/4	(Green)	Off	The port is disconnected.	
		Blinking	The data is transmitting.	
	Right LED	On	The port is connected with 100Mbps.	
	(Green)	Off	The port is disconnected with 10Mbps.	
	ĐĘ	PWR	ON OFF	
Interface	Descrip	tion		
Factory Reset	Press "Fa Press "Fa Press "Fa Restore th Press the begins to	 Press "Factory Reset" button once to make network connection through WPS. Press "Factory Reset" button twice to enable or disable WLAN function. Press "Factory Reset" button for 5 seconds to do the 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. 		
Restart		e router forcefu		
Phone (1/2)		ers for PSTN phe	•	
WAN (1/2)	Connecte	ers for remote ne	etworked devices.	

LAN (1-4)	Connecters for local networked devices.
PWR	Connecter for a power adapter.
ON/OFF	Power Switch.

1.2.4 For Vigor2930VS

8

VIGOR	BY TEK 2930VS SECURITY FIREWALL	ACT CPA MGMT DOS WANI Phone1 CSM WAN2 Phone2	Image: start I		
LED		Status	Explanation		
ACT (Activity)		Blinking	The router is powered on and running normally.		
		Off	The router is powered off.		
DoS		On	The DoS/DDoS function is active.		
		Blinking	It will blink while deleting an attack.		
CSM		On	The profile of CSM (Content Security Management) for IM/P2P application is active. (It is enabled from CSM >> IM/P2P Profile).		
CPA (Content P	ortal Authority)	On	The Web Content Filter is active. (It is enabled from CSM >> Web Content Filter Profile)		
WAN1/2		On	The WAN1 or WAN2 port is connected.		
		Blinking	It will blink while transmitting data.		
MGMT			The router is managed (handled) by Telnet.		
			It will blink while transmitting data.		
Phone 1/2			The phone connected to this port is off-hook.		
		Off Blinking	The phone connected to this port is on-hook.		
			A phone call comes.		
LED on Conne	ector				
ISDN S0 1	Left LED	On	ISDN NT (ISDN S0 intern) mode is active and an ISDN phone adapter is connected.		
	(Orange)	Blinking	ISDN NT (ISDN S0 intern) mode is active and an ISDN phone adapter is not connected.		
	Right LED	On	A phone has been connected. If not, green LED will be off.		
	(Green)	Blinking	An ISDN phone is off-hook or a phone call comes.		
ISDN S0 2	Left LED (Orange)	On	ISDN NT (ISDN S0 intern) mode is active configured from VoIP>>Phone Settings and an ISDN phone adapter is connected.		
		Blinking	ISDN NT (ISDN S0 intern) mode configured from VoIP>>Phone Settings is active and an ISDN phone adapter is not connected.		
		Off	It means ISDN TE mode is active which is configured from VoIP>>Phone Settings .		
	Right LED (Green)	On	A phone adapter with phone set has been connected (ISDN S0 intern mode) or ISDN line has been connected (ISDN S0 extern mode). It will be off if there is nothing connected.		
		Blinking	In ISDN NT (ISDN S0 intern) mode, it means an ISDN phone is off-hook or a phone call comes. In ISDN TE mode, it means data, fax or voice (phone call) is transmitting.		
	Left LED	On	The port is connected.		
WAN 1/2	(Green)	Off	The port is disconnected.		
		Blinking	The data is transmitting.		
	Right LED	On	The port is connected with 100Mbps.		
	(Green)	Off	The port is disconnected with 10Mbps.		

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





Interface	Description
Factory Reset	Restore the default settings. Usage: Turn on the router (ACT LED is blinking). Press the hole and keep for more than 5 seconds. When you see the ACT LED begins to blink rapidly than usual, release the button. Then the router will restart with the factory default configuration.
Restart	Restart the router forcefully.
Phone $(1/2)$	Connecters for PSTN phones.
ISDN S0 1	Connecter for ISDN phone(s) only via ISDN phone adapter. Do not connect any other device to such port or connect ISDN line, otherwise the router might be damaged.
ISDN S0 2	Connecter for ISDN line or ISDN phone adapter in particular condition. Refer to section 2.2 for more details.
WAN (1/2)	Connecters for remote networked devices.
LAN (1-4)	Connecters for local networked devices.
PWR	Connecter for a power adapter.
ON/OFF	Power Switch.

1.2.5 For Vigor2930VSn

	R2930V5n VAN BEDUNITY FIREWALL	ACT WIAN NGMT DOS WANI Phone1 CSM WAN2 Phone2	Phone ISDN 50 WAN LAN		
LED		Status	Explanation		
ACT (Activity	y)	Blinking	The router is powered on and running normally.		
		Off	The router is powered off.		
DoS		On	The DoS/DDoS function is active.		
		Blinking	It will blink while deleting an attack.		
CSM		On	The profile of CSM (Content Security Management) for IM/P2P application is active. (It is enabled from CSM >> IM/P2P Profile).		
WLAN		On	Wireless access point is ready.		
		Blinking	It will blink while wireless traffic goes through. It will blink fast when WPS is working and it will return to normal condition after two minutes. (You need to setup WPS within 2 minutes.)		
WAN1/2		On	The WAN1 or WAN2 port is connected.		
W/H(1/2		Blinking	It will blink while transmitting data.		
MGMT		On	The router is managed (handled) by Telnet.		
MOMI		Blinking	It will blink while being managed by IE browser.		
Phone 1/2		On	The phone connected to this port is off-hook.		
			The phone connected to this port is on-hook.		
			A phone call comes.		
LED on Con	nector	Blinking			
ISDN S0 1	Left LED	On	ISDN NT (ISDN S0 intern) mode is active and an ISDN phone adapter is connected.		
	(Orange)	Blinking	ISDN NT (ISDN S0 intern) mode is active and an ISDN phone adapter is not connected.		
	Right LED	On	A phone has been connected. If not, green LED will be off.		
	(Green)	Blinking	An ISDN phone is off-hook or a phone call comes.		
ISDN S0 2	Left LED (Orange)	On	ISDN NT (ISDN S0 intern) mode is active configured from VoIP>>Phone Settings and an ISDN phone adapter is connected.		
		Blinking	ISDN NT (ISDN S0 intern) mode configured from VoIP>>Phone Settings is active and an ISDN phone adapter is not connected.		
		Off	It means ISDN TE mode is active which is configured from VoIP>>Phone Settings .		
	Right LED (Green)	On	A phone adapter with phone set has been connected (ISDN S0 intern mode) or ISDN line has been connected (ISDN S0 extern mode). It will be off if there is nothing connected.		
		Blinking	In ISDN NT (ISDN S0 intern) mode, it means an ISDN phone is off-hook or a phone call comes. In ISDN TE mode, it means data, fax or voice (phone call) is transmitting.		
	Left LED	On	The port is connected.		
WAN 1/2	(Green)	Off	The port is disconnected.		
		Blinking	The data is transmitting.		
	Right LED	On	The port is connected with 100Mbps.		

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



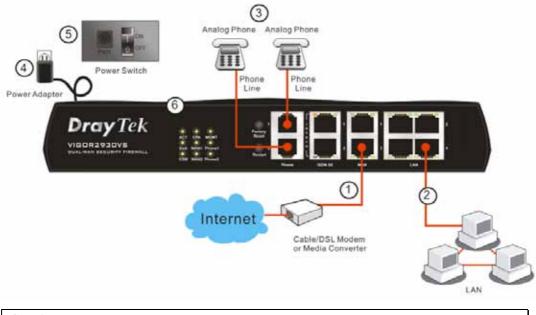
Interface	Description
Factory Reset	Press "Factory Reset" button once to make network connection through WPS Press "Factory Reset" button twice to enable or disable WLAN function. Press "Factory Reset" button for 5 seconds to do the factory reset. Restore the default settings. Usage: Turn on the router (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.
Restart	Restart the router forcefully.
Phone (1/2)	Connecters for PSTN phones.
ISDN S0 1	Connecter for ISDN phone(s) only via ISDN phone adapter. Do not connect any other device to such port or connect ISDN line, otherwise the router might be damaged.
ISDN S0 2	Connecter for ISDN line or ISDN phone adapter in particular condition. Refer to section 2.2 for more details.
WAN (1/2)	Connecters for remote networked devices.
LAN (1-4)	Connecters for local networked devices.
PWR	Connecter for a power adapter.
ON/OFF	Power Switch.

1.3 Hardware Installation

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

- 1. Connect the cable Modem/DSL Modem/Media Converter to any WAN port of router with Ethernet cable (RJ-45). The WAN1/WAN2 LED (Left or Right) will light up according to the speed (100 or 10) of the device that it connected.
- 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. The LAN LED (Left or Right) will light up according to the speed (100 or 10) of the device that it connected.
- 3. Connect the telephone sets with phone lines (for using VoIP function). For the model without phone ports, skip this step.
- 4. Connect one end of the power adapter to the router's power port on the rear panel, and the other side into a wall outlet.
- 5. Power on the device by pressing down the power switch on the rear panel.
- 6. The system starts to initiate. After completing the system test, the **ACT** LED will light up and start blinking.

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

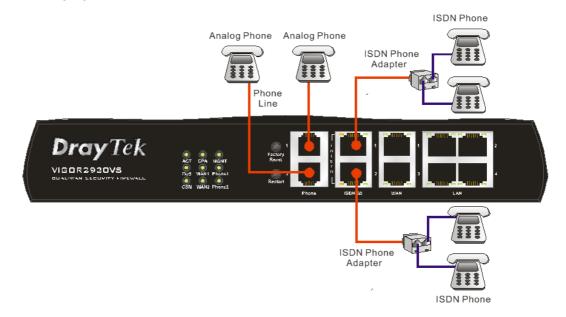


Caution: Each of the Phone ports can be connected to an analog phone only. Do not connect the phone ports to the telephone wall jack. Such connection might damage your router.

1.4 ISDN Phone Adapter Installation

Such information is provided for Vigor2930 S models (e.g., Vigor2930VS).

ISDN S0 1 is always fixed to connect ISDN phone. However, ISDN S0 2 is configurable as ISDN line or ISDN phone. When the user configures ISDN S0 2 as ISDN phone in **VoIP>> Phone Settings**, the **orange** LED will light on to indicate **ISDN2-S0** mode is selected. And by using ISDN phone adapters (coming from the router package), the user can connect several phones (the maximum is six) to Vigor2930VS for communication. Refer to the following figure for reference.



However, if the user configures ISDN S0 2 as ISDN line in **VoIP>> Phone Settings**, the **green** LED will light on to indicate ISDN2-TE mode is selected. Then, the port is specified for ISDN line only. Refer to the following figure for reference.



This page is left blank.

2 Configuring Basic Settings

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

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

2.1 Changing Password

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

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



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

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



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

Quick Start Wigard	System Status			
WAN	Model Name Firmware Version Build Date Time	: Vigor2930 series : v3,1.0_RC4 : Thu Jan 24 10:55:9.90 2008		
NAT Firewall		LAN		WAN 1
Objects Setting CSM Bardwidth Management Applications VPN and Remate Access	MAC Address 1st IP Address 1st Subnet Mask DHCP Server DNS	: 00-50-7F-C2-80-20 : 192,168.1.1 : 255.255.255.0 : Yes : 194.109.6.66	Link Status MAC Address Connection IP Address Default Gateway	: Connected : 00-50-7F-C2-80-21 : Static IP : 172.16.3.229 : 172.16.3.4
Certificate Management VotP	E	VolP		WAN 2
SDN System Maintenance Diagnostics All Rights Reserved.	Port Phone1 Phone2 ISDN1-S0 ISDN2-TE	Profile Reg. In/Out No 0/0 No 0/0 No 0/0 No 0/0 No 0/0	Link Status MAC Address Connection IP Address Default Gateway	: Disconnected : 00-50-7F-C2-80-22 : **** : **** : ****

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

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

ninistrator Password						
Old I	Password					
New	Password					
Cont	firm Password				7	

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

Connect to 19	2.168.1.1 🛛 🖓 🔀
7	A PARTY
	er Web Configurator
User name: Password:	£ <u>×</u>
	Remember my password
	OK Cancel

2.2 Quick Start Wizard

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

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

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

Quick Start Wizard

Select WAN Interface	
Select WAN Interface: Display Name: Physical Mode: Physical Type:	WAN1
	< Back Next > Finish Cancel

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

Quio	k St	art V	Viz	ard
------	------	-------	-----	-----

WAN 1		
Select one of the	following Internet Access types provided by your ISP.	
	PPPoE	
	○ РРТР	
	○ Static IP	
	O DHCP	
	•	

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

2.2.1 PPPoE

18

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

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

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

WAN 1	
Enter the user name and pa	assword provided by your ISP.
User Name	84005755@hinet.net
Password	•••••
Confirm Password	•••••

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

Click Next for viewing summary of such connection.

Quick Start Wizard

Please confirm your settings:	
WAN Interface:	WAN1
Physical Mode:	Ethernet
Physical Type:	Auto negotiation
Internet Access:	PPPoE
Click Back to modify chang settings and restart the Vig	ges if necessary. Otherwise, click Finish to save the current gor router.
	<pre>< Back Next > Finish Cancel</pre>

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

2.2.2 PPTP

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

Quick Start Wizard

WAN 1	
Enter the user name, pas your ISP.	word, WAN IP configuration and PPTP server IP provided by
User Name	
Password	
Confirm Password	
WAN IP Configuration	
🔘 Obtain an IP addres	automatically
Specify an IP addre	;
IP Address	172.16.3.229
Subnet Mask	255.255.0.0
PPTP Server IP	172.16.3.6

Click Next for viewing summary of such connection.

Quick Start Wizard

WAN Interface:	WAN1
Physical Mode:	Ethernet
Physical Type:	Auto negotiation
Internet Access:	РРТР
	nges if necessary. Otherwise, click Finish to save the current
Click Back to modify char settings and restart the V	

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

2.2.3 Static IP

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

on probided by your ISP. 172.16.3.229 255.255.255.0		
172.16.3.229		
255.255.255.0		
172.16.3.1		
168.95.1.1		
	(optional)	
		168.95.1.1 (optional)

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

Quick Start Wizard

Please confirm your settings:	
WAN Interface:	WAN1
Physical Mode:	Ethernet
Physical Type:	Auto negotiation
Internet Access:	Static IP
Click Back to modify chang	ges if necessary. Otherwise, click Finish to save the current
settings and restart the Vig	gor router.
	< Back Next > Finish Cancel

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

2.2.4 DHCP

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

Quick Start Wizard

Quick Start Wizard

HCP Client Mode	
WAN 1	
If your ISP req enter it in.	uire you to enter a specific host name or specific MAC address, please
Host Name	(optional)
MAC	00 -50 -7F -00 -00 -01 (optional)
	< Back Next > Finish Cancel

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

Please confirm your settings: WAN Interface: WAN1 Physical Mode: Ethernet Physical Type: Auto negotiation Internet Access: DHCP Click Back to modify changes if necessary. Otherwise, click Finish to save the current settings and restart the Vigor router. </

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

2.3 Online Status

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

Online status for PPPoE

Online Status

LAN Status		Primary DNS:	61.31.233.1	Secondary D	NS: 139.175.55.244
IP Address	TX Pac	kets	RX Packets		
192.168.50.111	L 240		210		
WAN 1 Status					>> <u>Drop PPPoE</u>
Enable	Line	Name	Mode	Up Time	
Yes	Ethernet		PPPoE	0:00:00	
IP	GW IP	TX Packets	TX Rate	RX Packets	RX Rate
219.81.160.205	5 211.78.218.40	6	29	6	12
WAN 2 Status					
Enable	Line	Name	Mode	Up Time	
Yes	Ethernet		Static IP	0:00:32	
IP	GW IP	TX Packets	TX Rate	RX Packets	RX Rate
192.168.4.103	192.168.4.1	1	3	1	9

Online status for PPTP (for WAN2)

Online Status

System Status					System Uptime: 0:12:
LAN Status		Primary DNS:	194.109.6.66	Secondary	DNS: 194.98.0.1
IP Address	TX Pack	ets	RX Packets		
192.168.50.111	4910		3663		
WAN 1 Status					
Enable	Line	Name	Mode	Up Time	
Yes	Ethernet	WAN1	Static IP	0:10:08	
IP	GW IP	TX Packets	TX Rate	RX Packets	RX Rate
192,168,22,111	192,168,22,105	91	21	99	3
WAN 2 Status					>> <u>Drop PPTP</u>
Enable	Line	Name	Mode	Up Time	
Yes	Ethernet	WAN2	PPTP	0:00:15	
IP	GW IP	TX Packets	TX Rate	RX Packets	RX Rate
192.168.29.202	192.168.29.1	103	119	14	6

Online status for Static IP (for WAN1) Online Status

LAN Status		Primary DNS:	194.109.6.66	Secondary	DNS: 194.98.0.1
IP Address	TX Pack	ets	RX Packets		
192.168.50.111	4910		3663		
WAN 1 Status					
Enable	Line	Name	Mode	Up Time	
Yes	Ethernet	WAN1	Static IP	0:10:08	
IP	GW IP	TX Packets	TX Rate	RX Packets	RX Rate
192.168.22.111	192,168,22,105	91	21	99	3
WAN 2 Status					>> <u>Drop PPTI</u>
Enable	Line	Name	Mode	Up Time	
Yes	Ethernet	WAN2	PPTP	0:00:15	
IP	GW IP	TX Packets	TX Rate	RX Packets	RX Rate
192.168.29.202	192.168.29.1	103	119	14	6

Online status for DHCP

Online Status

LAN Status		Primary DNS:	168.95.1.1	Secondary	DNS: 168.95.1.1
IP Address	TX Pack	ets R	X Packets		
192,168,50,111	L 856	7	83		
WAN 1 Status					>> <u>Release</u>
Enable	Line	Name	Mode	Up Time	
Yes	Ethernet		DHCP Client	0:01:49	
IP	GW IP	TX Packets	TX Rate	RX Packets	RX Rate
192,168,22,10	192,168,22,105	3	3	7	9
WAN 2 Status					>> <u>Drop PPPoE</u>
Enable	Line	Name	Mode	Up Time	
Yes	Ethernet		PPPoE	0:01:39	
IP	GW IP	TX Packets	TX Rate	RX Packets	RX Rate
202.211.100.17	76 202.211.100.17	70 35	8	46	4

Detailed explanation is shown below:

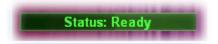
Detailed explanation is a	
Primary DNS	Displays the IP address of the primary DNS.
Secondary DNS	Displays the IP address of the secondary DNS.
LAN Status	
IP Address	Displays the IP address of the LAN interface.
TX Packets	Displays the total transmitted packets at the LAN interface.
RX Packets	Displays the total number of received packets at the LAN interface.
WAN1/2 Status	
Line	Displays the physical connection (Ethernet) of this interface.
Name	Displays the name set in WAN1/WAN web page.
Mode	Displays the type of WAN connection (e.g., PPPoE).
Up Time	Displays the total uptime of the interface.
IP	Displays the IP address of the WAN interface.
GW IP	Displays the IP address of the default gateway.
TX Packets	Displays the total transmitted packets at the WAN interface.
TX Rate	Displays the speed of transmitted octets at the WAN interface.
RX Packets	Displays the total number of received packets at the WAN interface.
RX Rate	Displays the speed of received octets at the WAN interface.
ISDN Status	
Channel Active Conn.	Displays the active connection status for each channel.
TX Pkts	Displays the total transmitted packets at the ISDN interface.
TX Rate	Displays the speed of transmitted octets at the ISDN interface.
RX Pkts	Displays the total number of received packets at the ISDN interface.
RX Rate	Displays the speed of received octets at the ISDN interface.
Up Time	Displays the total uptime of the interface.
AOC	Displays the charge information of the interface.

Dial ISDN	Allows you to dial ISDN connection.
Drop B1/B2	Allows you to drop B1 or B2 connection.

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

2.4 Saving Configuration

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



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

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

This page is left blank.



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

3.1 WAN

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

3.1.1 Basics of Internet Protocol (IP) Network

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

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

What are Public IP Address and Private IP Address

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

Get Your Public IP Address from ISP

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

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

Below shows the menu items for Internet Access.



3.1.2 General Setup

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

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

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

Note: In default, V	WAN1 a	and WAN2	are enabled.
---------------------	--------	----------	--------------

WAN >> General Setup

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

OK

Enable	Choose Yes to invoke the settings for this WAN interface. Choose No to disable the settings for this WAN interface.
Display Name	Type the description for the WAN1/WAN2 interface.
Physical Mode	For WAN1, the physical connection is done through ADSL port; yet the physical connection for WAN2 is done through an Ethernet port (P1). You cannot change it.

Physical Type	You can change the physic negotiation for determine	cal type for WAN2 or choose Auto d by the system.			
	Physical Type:	Auto negotiation Auto negotiation 10M half duplex 10M full duplex 100M half duplex 100M full duplex			
Load Balance Mode	If you know the practical bandwidth for your WAN interface, please choose the setting of According to Line Speed . Otherwise, please choose Auto Weigh to let the router reach the best load balance.				
	Load Balance Mode:	Auto Weigh Auto Weigh According to Line Speed			
Line Speed	Balance Mode, please typ	to Line Speed as the Load be the line speed for downloading AN1/WAN2. The unit is kbps.			
Active Mode	Choose Always On to make the WAN connection (WAN1/WAN2) being activated always; or choose Active on demand to make the WAN connection (WAN1/WAN2) activated if it is necessary.				
	Active Mode:	Active on demand Always On Active on demand			
	If you choose Active on demand, the Idle Timeout will be available for you to set for PPPoE and PPTP access modes in the Details Page of WAN>>Internet Access . In addition, there are three selections for you to choose for different				
	purposes. WAN2 Fail – It means the connection for WAN1 will be activated when WAN2 is failed.				
	WAN2 Upload speed exceed XX kbps – It means the connection for WAN1 will be activated when WAN2 Upload speed exceed certain value that you set in this box for 15 seconds.				
	-	exceed XX kbps– It means the l be activated when WAN2			
	for 15 seconds.	ertain value that you set in this box			
	 WAN1 Fail – It means the connection for WAN2 will be activated when WAN1 is failed. WAN1 Upload speed exceed XX kbps – It means the connection for WAN2 will be activated when WAN1 Upload speed exceed certain value that you set in this box for 15 				
	connection for WAN2 wil	exceed XX kbps – It means the l be activated when WAN1 ertain value that you set in this box			

3.1.3 Internet Access

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

WAN >> Internet Access Internet Access Physical Mode Access Mode WAN1 Ethernet Static or Dynamic IP Details Page WAN2 Ethernet None Details Page

Index	It shows the WAN modes that this router supports. WAN1 is the default WAN interface for accessing into the Internet. WAN2 is the optional WAN interface for accessing into the Internet when WAN 1 is inactive for some reason.			
Display Name	It shows the name of the WAN1/WAN2 that entered in general setup.			
Physical Mode				
Access Mode	Use the drop down list to choose a proper access mode. The details page of that mode will be popped up. If not, click Details Page for accessing the page to configure the settings. Static or Dynamic IP None PPPoE Static or Dynamic IP PPTP			
	There are three access modes provided for PPPoE, Static or Dynamic IP and PPTP.			
Details Page	This button will open different web page according to the access mode that you choose in WAN1 or WAN2.			

Details Page for PPPoE

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

PPPoE Client Mode		PPP/MP Setup	
🔘 Enable 🛛 💿 Disable	9	PPP Authentication	PAP or CHAP 🔽
ISP Access Setup Username Password		Idle Timeout IP Address Assignment Me (IPCP) WAN IP Alias Fixed IP: Yes O No]
Index(1-15) in <u>Schedul</u> =>,, ISDN Dial Backup Setup	<u>e</u> Setup: ,	Fixed IP Address	
Dial Backup Mode	None	 Default MAC Addres Specify a MAC Addres MAC Address: 	-
WAN Connection Detection	n	00 .50 .7F :22 .3	3 . 45
Mode	ARP Detect 🐱		
Ping IP	0.0.0.0		
TTL:	255		

WAN >> Internet Access

PPPoE Client Mode	Click Enable for activating this function. If you click Disable , this function will be closed and all the settings that you adjusted in this page will be invalid.
ISP Access Setup	 Enter your allocated username, password and authentication parameters according to the information provided by your ISP. If you want to connect to Internet all the time, you can check Always On. Username – Type in the username provided by ISP in this field. Password – Type in the password provided by ISP in this field. Index (1-15) in Schedule Setup - You can type in four sets of time schedule for your request. All the schedules can be set previously in Application – Schedule web page and you can use the number that you have set in that web page.
ISDN Dial Backup Setup	This setting is available for the routers supporting ISDN function only. Before utilizing the ISDN dial backup feature, you must create a dial backup profile first. Please click ISDN > Dialing to a Single ISP to create the backup profile.
	None - Disable the backup function. Packet Trigger - The backup line is not on until a packet from a local host triggers the router to establish a connection.
	This setting is available for <i>i</i> model only.
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.

PPP/MP SetupPPP Authentication – Select **PAP only** or **PAP or CHAP** for
PPP.

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

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.

🗿 WAN II	P Alias - M	icrosoft Internet Explorer						
WAN IP Alias (Multi-NAT)								
Index	Enable	Aux. WAN IP	Join NAT IP Pool					
1.	V	172.16.3.229	V					
2.								
з.								
4.								
5.								
6.								
7.								
8.								
		OK Clear All	Close					

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

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

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

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

Details Page for Static or Dynamic IP

IP Address

(IPCP)

Assignment Method

For static IP mode, you usually receive a fixed public IP address or a public subnet, namely multiple public IP addresses from your DSL or Cable ISP service providers. In most cases, a

Cable service provider will offer a fixed public IP, while a DSL service provider will offer a public subnet. If you have a public subnet, you could assign an IP address or many IP address to the WAN interface.

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

Static or Dynamic IP (DHCP Client)	WAN IP Network Setting	WAN IP Alias		
💿 Enable i 🔘 Dis	able	Obtain an IP address automatically			
ISDN Dial Backup Set	ир	Router Name			
Dial Backup Mode	·		Domain Name * * : Required for some ISPs		
Keep WAN Connection	n	Specify an IP addres	s		
Enable PING to k	eep alive	IP Address	172.16.3.229		
PING to the IP		Subnet Mask	255.255.0.0		
PING Interval	PING Interval 0 minute(s)		172.16.3.4		
WAN Connection Dete	ction	Oefault MAC Address	955		
Mode	ARP Detect 💌	🔘 Specify a MAC Add	dress		
Ping IP	0.0.0.0	MAC Address:			
TTL:	255	00 .50 .7F 22 .	33 . 45		
RIP Protocol		DNS Server IP Address			
Enable RIP		Primary IP Address			
		Secondary IP Address	5		

Static or Dynamic IP (DHCP Client)	Click Enable for activating this function. If you click Disable , this function will be closed and all the settings that you adjusted in this page will be invalid.
ISDN Dial Backup Setup	This setting is available for the routers supporting ISDN function only. Before utilizing the ISDN dial backup feature, you must create a dial backup profile first. Please click Internet Access Setup > Dialing to a Single ISP to enter the backup profile.
	None - Disable the backup function. Packet Trigger - The backup line is not on until a packet from a local host triggers the router to establish a connection.
	This setting is available for <i>i</i> model only.
Keep WAN Connection	Normally, this function is designed for Dynamic IP environments because some ISPs will drop connections if there is no traffic within certain periods of time. Check Enable PING to keep alive box to activate this function. PING to the IP - If you enable the PING function, please specify the IP address for the system to PING it for keeping alive. PING Interval - Enter the interval for the system to execute the DING
	PING operation.
RIP Protocol	Routing Information Protocol is abbreviated as RIP (RFC1058) specifying how routers exchange routing tables information. Click Enable RIP for activating this function.

WAN >> Internet Access

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.
WAN IP Network Settings	This group allows you to obtain an IP address automatically and allows you type in IP address manually.
	WAN IP Alias - If you have multiple public IP addresses and would like to utilize them on the WAN interface, please use WAN IP Alias. You can set up to 8 public IP addresses other than the

Index	Enable	Iti-NAT) Aux. WAN IP	Join NAT IP Pool
1.	v	172.16.3.229	v
2.			
з.			
4.			
5.			
6.			
7.			
8.			
		OK Clear All	Close

current one you are using. Notice that this setting is available for

Obtain an IP address automatically - Click this button to obtain the IP address automatically if you want to use Dynamic IP mode. Router Name: Type in the router name provided by ISP.

Domain Name: Type in the domain name that you have assigned. Specify an IP address – Click this radio button to specify some data if you want to use Static IP mode.

IP Address: Type the IP address.

Subnet Mask: Type the subnet mask.

Gateway IP Address: Type the gateway IP address.

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

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

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

DNS Server IP Address

necessity in the future.

Details Page for PPTP

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

WAN >> Internet Access							
WAN 1							
PPTP Client Mode		PPP Setup					
 ⊙ Enable ○ Disable PPTP Server 10.0.0.138 		PPP Authentication	PAP or CHAP 🗸				
		Idle Timeout	-1 second(s)				
		IP Address Assignme	IP Address Assignment Method				
ISP Access Setup							
Username		Fixed IP: 🔘 Yes (Fixed IP: O Yes O No (Dynamic IP)				
Password Index(1-15) in <u>Schedule</u> Setup:		Fixed IP Address					
		WAN IP Network Settings					
=> , , ,	,	🔘 Obtain an IP add	Iress automatically				
ISDN Dial Backup Setup		Specify an IP address					
Dial Backup Mode 🛛 None 💌		IP Address	10.0.0.150				
		Subnet Mask	255.0.0.0				
			233.0.0.0				
	ОК	Cancel					
		Calicer					
DDTD Cotum	DDTD I :mlr	Click Enchlate	anable o DDTD alignt to actablish a				
PPTP Setup			enable a PPTP client to establish a				
			L modem on the WAN interface.				
	PPTP Serve	r - Specify the IP a	address of the PPTP server.				
SP Access Setup	Userneme	Funa in the usarna	me provided by ISP in this field				
ISI Access Setup		Username -Type in the username provided by ISP in this field. Password -Type in the password provided by ISP in this field.					
		• •					
			p - You can type in four sets of time				
	schedule for	your request. All t	he schedules can be set previously				
	in Application	on – Schedule wel	p page and you can use the number				
	that you have	e set in that web pa	ige.				
ISDN Dial Backup			routers supporting ISDN function				
Setup	•	÷	l dial backup feature, you must				
			t. Please click Internet Access				
	Setup > Dial	Setup > Dialing to a Single ISP to enter the backup profile.					
	None Disek	None - Disable the backup function.					
		•					
			ne is not on until a packet from a				
	local nost trig	ggers the router to	establish a connection.				
	This setting i	available for <i>i</i> model only.					
PPP Setup	PPP Authent	tication - Select P	cation - Select PAP only or PAP or CHAP for PPP				
i i soup			for breaking down the Internet after				
		passing through the time without any action. This setting is active					
		Active on demand option for Active Mode is					
	selected in W	VAN>> General S	etup page.				
IP Address	Fixed IP - U	sually ISP dynami	cally assigns IP address to you				
Assignment		• •	request. In some case, your ISP				
Method(IPCP)	-						
viculou(IFCF)	-		gn you the same IP address				
	-	-	ase, you can fill in this IP address				
			ntact your ISP before you want to				
	use this funct	tion. Click Yes to r	use this function and type in a				

fixed IP address in the box.

Fixed IP Address - Type a fixed IP address.

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

WAN IP	Alias - Mi	crosoft Internet Explorer	
	Alias (Mu		
	Enable	Aux. WAN IP	Join NAT IP Pool
1.	V	172.16.3.229	V
2.			
з.			
4.			
5.			
6.			
7.			
8.			
		OK Clear All	Close
			CIUSE

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

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

WAN IP NetworkObtain an IP address automatically – Click this button to obtainSettingsthe IP address automatically.

Specify an IP address – Click this radio button to specify some data. **IP Address** – Type the IP address.

Subnet Mask – Type the subnet mask.

3.1.4 Load-Balance Policy

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

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

WAN >> Load-Balance Policy

Index	Enable	Proto	col	WAN	Src IP Start	Src IP End	Dest IP Start	Dest IP End	Dest Port Start	Dest Port End
1		any	~	WAN1 💌						
<u>2</u>		any	*	*						
<u>3</u>		any	*	~						
<u>4</u>		any	*	*						
<u>5</u>		any	*	~						
<u>6</u>		any	*	*						
Z		any	*	~						
<u>8</u>		any	*	*						
<u>9</u>		any	*	~						
<u>10</u>		any	*	~						
< <u>1-10</u>	<u>11-20</u> >	·>								<u>Next</u> >

Index	Click the number of index to access into the load-balance policy configuration web page.
Enable	Check this box to enable this policy.
Protocol	Use the drop-down menu to change the protocol for the WAN interface. any TCP UDP TCP/UDP ICMP IGMP
WAN	Use the drop-down menu to change the WAN interface.
Src IP Start	Display the IP address for the start of the source IP.
Src IP End	Display the IP address for the end of the source IP.
Dest IP Start	Display the IP address for the start of the destination IP.
Dest IP End	Display the IP address for the end of the destination IP.
Dest Port Start	Display the IP address for the start of the destination port.
Dest Port End	Display the IP address for the end of the destination port.
Click Index 1 to access	into the following page for configuring load-balance policy.

WAN >> Load-Balance Policy

🗹 Enable	
Protocol	тср 💌
Binding WAN interafce	WAN1 💌
Src IP Start	192.168.1.3
Src IP End	192.168.1.5
Dest IP Start	168.95.0.0
Dest IP End	168.95.0.100
Dest Port Start	80
Dest Port End	100

Enable

Check this box to enable this policy.

any

any TCP UDP TCP/UDP ICMP

Protocol

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

¥

Protocol	

	IGMP		
Binding WAN interface	Choose the WAN interface (WAN1 or WAN2) for binding.		
Src IP Start	Type the source IP start for the specified WAN interface.		
Src IP End	Type the source IP end for the specified WAN interface. If this field is blank, it means that all the source IPs inside the LAN will be passed through the WAN interface.		
Dest IP Start	Type the destination IP start for the specified WAN interface.		
Dest IP End	Type the destination IP end for the specified WAN interface. If this field is blank, it means that all the destination IPs will be passed through the WAN interface.		
Dest Port Start	Type the destination port start for the destination IP.		
Dest Port End	Type the destination port end for the destination IP. If this field is blank, it means that all the destination ports will be passed through the WAN interface.		

38

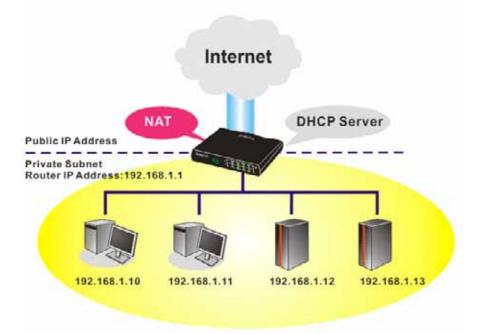
3.2 LAN

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

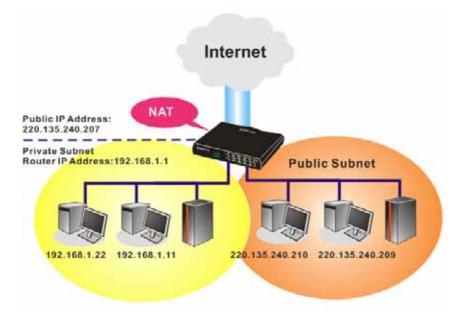


3.2.1 Basics of LAN

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



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



What is Routing Information Protocol (RIP)

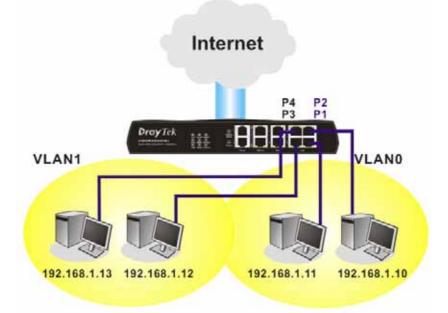
Vigor router will exchange routing information with neighboring routers using the RIP to accomplish IP routing. This allows users to change the information of the router such as IP address and the routers will automatically inform for each other.

What is Static Route

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

What are Virtual LANs and Rate Control

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



VolPon www.voipon.co.uk sales@voipon.co.uk Tel: +44 (0)1245 808195 Fax: +44 (0)1245 808299

3.2.2 General Setup

This page provides you the general settings for LAN.

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

LAN	>>	General	Setup	

AN IP Network Configurat	ion	DHCP Server Configuration)n	
For NAT Usage		💿 Enable Server 🔘 Disa	⊙Enable Server ○Disable Server	
1st IP Address 192.168.1.1		Relay Agent: 🔘 1st Su	Relay Agent: 🔿 1st Subnet 🔾 2nd Subnet	
1st Subnet Mask	255.255.255.0	Start IP Address	192.168.1.10	
For IP Routing Usage 🔘	Enable 💿 Disable	IP Pool Counts	50	
2nd IP Address	192.168.2.1	Gateway IP Address	192.168.1.1	
2nd Subnet Mask	255.255.255.0 d Subnet DHCP Server	DHCP Server IP Address for Relay Agent DNS Server IP Address		
RIP Protocol Control	Disable 👻	Force DNS manual Primary IP Address	setting	
		Secondary IP Address		

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

Start IP IP Pool C	Address	10)
Index	Matched MAC Address	given IP Address
	ress : : : : : : : : : :	

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

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

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

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

RIP Protocol Control Disable

Disable	×
Disable	
1st Subnet	
2nd Subnet	
. 1	.1

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

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

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

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

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

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

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

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

of the router, which means the router is the default gateway. DHCP Server IP Address for Relay Agent - Set the IP address of the DHCP server you are going to use so the Relay Agent can help to forward the DHCP request to the DHCP server. **DNS Server** DNS stands for Domain Name System. Every Internet host must have a unique IP address, also they may have a human-friendly, Configuration easy to remember name such as www.yahoo.com. The DNS server converts the user-friendly name into its equivalent IP address. Force DNS manual setting - Force Vigor router to use DNS servers in this page instead of DNS servers given by the Internet Access server (PPPoE, PPTP, L2TP or DHCP server). Primary IP Address - You must specify a DNS server IP address here because your ISP should provide you with usually more than one DNS Server. If your ISP does not provide it, the router will automatically apply default DNS Server IP address: 194.109.6.66 to this field. Secondary IP Address - You can specify secondary DNS server IP address here because your ISP often provides you more than one DNS Server. If your ISP does not provide it, the router will automatically apply default secondary DNS Server IP address: 194.98.0.1 to this field. The default DNS Server IP address can be found via Online Status:

System Status System Uptime: 71:47:46

System Status			System optime. / 1.47.40
LAN Status	Primary	DNS: 194.109.6.66	Secondary DNS: 168.95.1.1
IP Address	TX Packets	RX Packets	
192.168.1.1	347390	214004	

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

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

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

3.2.3 Static Route

LAN >> Static Route Setup

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

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

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

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

Diagnostics >> View Routing Table

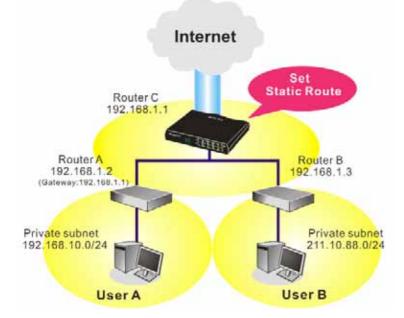
Key: C	- connected, S -	static, R - RI	P, * - default, ~ - priv	ate	
*	0.0.0.0/	0.0.0.0	via 172.16.3.1, WAN1		
С~	192.168.1.0/	255.255.255.0	is directly connected,	LAN	
с	172.16.3.0/	255.255.255.0	is directly connected,	WAN1	

Add Static Routes to Private and Public Networks

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

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

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



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

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

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

ndex No. 1		
🗹 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.

ndex 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

urrent Runr	ning Routing Table			<u>Refresh</u>
Key: C	C - connected, S -	static, R - RIP, * - default, ~ -	- private	^
s~	192.168.10.0/	255.255.255.0 via 192.168.1.2,	LAN	
С~	192.168.1.0/	255.255.255.0 is directly connect	cted, LAN	
S~	211.100.88.0/	255.255.255.0 via 192.168.1.3,	LAN	
				~

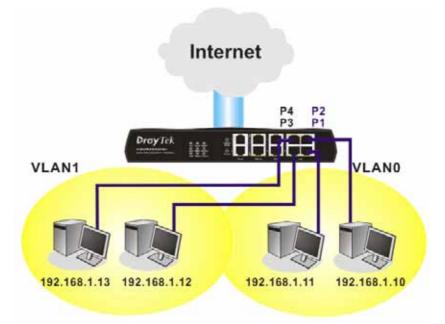
3.2.4 VLAN

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

LAN >> VLAN Configuration					
VLAN Configuration					
Enable					
	P1	P2	P3	P4	
VLAN0					
VLAN1					
VLAN2					
VLAN3					
1					
	OK	Clear	Cancel		

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

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



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

LAN Configuration				
🗹 Enable				
	P1	P2	P3	P4
VLAN0				
VLAN1			v	
VLAN2				
VLAN3				

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

3.2.5 Bind IP to MAC

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

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

LAN >> Bind IP to MAC

If you s	binding presets DHCP Allocatic elect Strict Bind, unspecified L		ne Internet.
🖲 Enable (Disable 🔘 Strict Bind		
ARP Table	<u>Select All</u> <u>Sort</u> <u>Refresh</u>	IP Bind List	Select All Sort
IP Address 192.168.1.10 192.168.1.21 192.168.1.21 192.168.1.21 192.168.1.10 192.168.1.10 192.168.1.10 192.168.1.4 192.168.1.13 192.168.1.4 Val.168.1.4 Val.168.1.4 Val.168.1.4 Val.168.1.4 Add and Edit P P Address Mac Address	Mac Address 00-0E-A6-2A-D5-A1 00-50-7F-33-F8-0B 00-13-D4-1B-B3-3D 00-0B-CD-55-CB-45 00-0D-0B-A7-86-F3 00-08-A1-36-97-5D 00-18-F73-C0-42-2C 00-E0-18-87-51-72 00-E0-18-F79-53-D5 00-85-A0-01-01-00 ♥	Index IP Address	Mac Address
	Add	Edit Delete	
		ОК	
able			his function. However, also can connect to Int

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

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

Vigor2930 Series User's Guide

47

ARP Table	This table is the LAN ARP table of this router. The information for IP and MAC will be displayed in this field. Each pair of IP and MAC address listed in ARP table can be selected and added to IP Bind List by clicking Add below.
Add and Edit	 IP Address - Type the IP address that will be used for the specified MAC address. Mac Address - Type the MAC address that is used to bind with the assigned IP address.
Refresh	It is used to refresh the ARP table. When there is one new PC added to the LAN, you can click this link to obtain the newly ARP table information.
IP Bind List	It displays a list for the IP bind to MAC information.
Add	It allows you to add the one you choose from the ARP table or the IP/MAC address typed in Add and Edit to the table of IP Bind List .
Edit	It allows you to edit and modify the selected IP address and MAC address that you create before.
Remove	You can remove any item listed in IP Bind List . Simply click and select the one, and click Remove . The selected item will be removed from the IP Bind List .
Note: Before you select St	trict Bind, you have to bind one set of IP/MAC address for one

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

3.3 NAT

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

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

The benefit of the NAT includes:

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

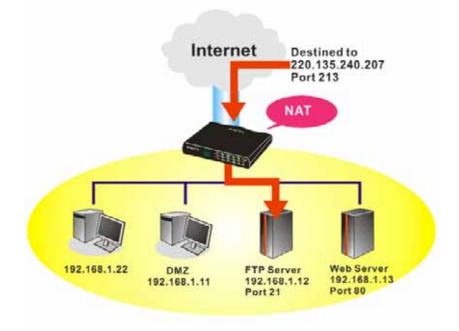
On NAT page, you will see the private IP address defined in RFC-1918. Usually we use the 192.168.1.0/24 subnet for the router. As stated before, the NAT facility can map one or more IP addresses and/or service ports into different specified services. In other words, the NAT function can be achieved by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

Below shows the menu items for NAT.



3.3.1 Port Redirection

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



The port redirection can only apply to incoming traffic.

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

NAT >> Port Redirection

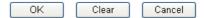
Index	Service Name	Public Port	Private IP	Status
<u>1.</u>				×
<u>2.</u>				×
<u>3.</u>				x
<u>4.</u>				х
<u>5.</u>				х
<u>6.</u>				х
<u>7.</u>				х
<u>8.</u>				х
<u>9.</u>				х
<u>10.</u>				×

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

NAT >> Port Redirection

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

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



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.

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

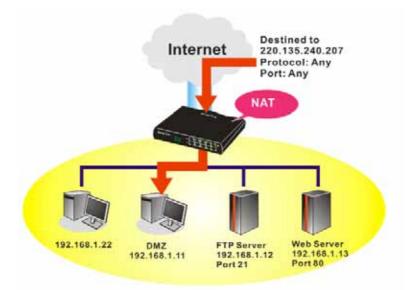
For example, the built-in web configurator in the router is with default port 80, which may conflict with the web server in the local network, http://192.168.1.13:80. Therefore, you need to **change the router's http port to any one other than the default port 80** to avoid conflict, such as 8080. This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

Management Access Control		Management Port Setup	Management Port Setup		
 Allow management from FTP Server HTTP Server HTTPS Server Telnet Server SSH Server Disable PING from the Ir 		Image: Straight of the straight	fault: 23) fault: 80) fault: 443 fault: 21) fault: 22)		
		SNMP Setup Enable SNMP Agent Get Community public Set Community Manager Host IP			
		Trap Community public Notification Host IP Trap Timeout 10 seco	inds		

System Maintenance >> Management

3.3.2 DMZ Host

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



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

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

NAT >> DMZ Host Setup

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

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

DMZ Host Setup					
WAN 1 Index	Enable	Aux. WAN IP	Private IP		
1.		172.16.3.229		Choose PC	
2.		172.16.3.89		Choose PC	
WAN 2					
	Enable		Private IP		
				Choose PC	

Vigor2930 Series User's Guide

VolPon www.voipon.co.uk sales@voipon.co.uk Tel: +44 (0)1245 808195 Fax: +44 (0)1245 808299

Enable Check to enable the DMZ Host function.

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

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



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

NAT >> DMZ Host Setup

WAN 1 Index	Enable	Aux. WAN IP	Private IP	
1.		172.16.3.229	192.168.1.10	Choose PC
2.		172.16.3.89		Choose PC
WAN 2				
	Enable		Private IP	
				Choose PC
		(OK Clear	

3.3.3 Open Ports

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

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

NAT >> Open Ports

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

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

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

NAT >> Open Ports >> Edit Open Ports

Index No. 1

🗹 Enable Open Ports							
	Co	mment	P2F)			
	W.	AN Interface	WA	N1 🔽			
	Lo	cal Computer	192	.168.1.10	Cho	ose PC	
	Protocol	Start Port	End Port		Protocol	Start Port	End Port
1.	TCP 🔽	4500	4700	6.	💙	0	0
2.	UDP 🔽	4500	4700	7.	💙	0	0
з.	💙	0	0	8.	💙	0	0
4.	💙	0	0	9.	💙	0	0
5.	🗸	0	0	10.	💙	0	0

Clear

Cancel

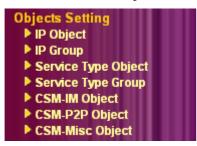
ΟK

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

55

3.4 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).



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

3.4.1 IP Object

Objects Setting >> IP Object

Objects Setting >> IP Object

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

Object Profiles: Index	Name	Index	Set to Factory Defau
	Nume		Nume
<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>	
15.		31.	
<u>16.</u>		<u>32.</u>	

Set to Factory Default Clear all profiles.

Click the number under Index column for settings in detail.

Name:	RD Department
Interface:	Any 🗸
Address Type:	Range Address 💌
Start IP Address:	192.168.1.64
End IP Address:	192.168.1.75
Subnet Mask:	0.0.0.0
Invert Selection:	

56

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

Below is an example of IP objects settings.

Objects Setting >> IP Object

-		
Index	Name	Index
<u>1.</u>	RD Department	<u>17.</u>
<u>2.</u>	Financial Dept.	<u>18.</u>
<u>3.</u>	HR Department	<u>19.</u>
<u>4.</u>		<u>20.</u>
<u>5.</u>		<u>21.</u>

3.4.2 IP Group

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

Objects Setting >> IP Group

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

Set to Factory Default Clear all profiles.

Objects Setting >> IP Group			
Profile Index : 1			
Name:	Administration		
Interface:	Any 💙		
Available IP Objects	Selected IP Objects		
1-RD Department 2-Financial Dept. 3-HR Department	» «		
	OK Clear Cancel		
Name	Type a name for this profile. Maximum 15 characters are allowed.		
nterface	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 cho above will be shown in this box.		
Selected IP Objects	Click >> button to add the selected IP objects in this box.		

3.4.3 Service Type Object

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

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 >> Service Type Object

Set to Factory Default Clear all profiles.

```
Objects Setting >> Service Type Object Setup
 Profile Index : 1
                                          www
             Name
                                          TCP
                                                  ~
             Protocol
                                                     6
                                          - -
                                               1
                                                        ~ 65535
             Source Port
                                          = ~
                                                        ~ 80
             Destination Port
                                               80
                              ΟK
                                        Clear
                                                  Cancel
                                Type a name for this profile.
Name
Protocol
                                Specify the protocol(s) which this profile will apply to.
                                 TCP
                                 Any
                                 ICMP
                                IGMP
                                TCP
                                UDP.
                                 TCP/UDP
                                 Other
Source/Destination Port
                                Source Port and the Destination Port column are available
                                for TCP/UDP protocol. It can be ignored for other protocols.
                                The filter rule will filter out any port number.
                                (=) – when the first and last value are the same, it indicates
                                one port; when the first and last values are different, it
                                indicates a range for the port and available for this profile.
```

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

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

Below is an example of service type objects settings.

Service Type Object Profiles:

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

3.4.4 Service Type Group

Objects Setting >> Service Type Group

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

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

Set to Factory Default Clear all profiles.

	Name:	VolP		
Available Service Type		Objects	Selected Service Type Objects	
	1-SIP 2-RTP			
		ок с	lear Cancel	
Name		Type a nam	e for this profile.	
• -			d IP objects from IP Objects page. A objects will be shown in this box.	ll the
Selected Service Type Click >> button to add the selected IP Objects			tton to add the selected IP objects in	this box

3.4.5 CSM-IM Object

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

1. 2. 3. 4. 5.	<u>17.</u> <u>18.</u> <u>19.</u> <u>20.</u>	
<u>3.</u> <u>4.</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 >> CSM Profile

Objects Setting >> Service Type Group Setup

Set to Factory Default

y Default Clear all profiles.

Objects Setting >> CSM-IM Object Profile

ck for Disallow:					
		Advanced	Management		
Activity / App		MSN	YahooIM	AIM(<=5.9)	ICQ
Login					
Messag				V	V
File Tran:	sfer			V	V
Game				1	¥
Video				V	
Voice				V	1
Conference					
Other Acti	vities				\checkmark
	Otł	ner IM Applicatio	n		VoIP
AIM6		iChat		/GoogleTalk	
🗌 GoogleChat 🛛 🗌 🛛 🗌		🗌 GaduGa	du 📃 Paltalk	-	Skype
Qnext	🗌 Meetro	🗌 РОСО/Р	P365 🗌 AresCh	at	SIP
	v	Veb IM (* = mor	re than one addr	ess)	
	eMessenger	WebMSN	<u>meebo*</u>	eBuddy	ILoveIM*
WehIM URI s	ICQ Java*	ICQ Flash*	<u>goowy*</u>	IMhaha*	getMessenger
	IMUnitive*	<u>Wablet*</u>	<u>mabber*</u>	<u>MSN2G0*</u>	<u>KoollM</u>
	MessengerFX*	MessengerAdi	<u>ctos WebYahoolM</u>		
	Г	ок	lear Canc	el	
file Name		Type a name	for the CSM	profile.	
	ow				device that u

3.4.6 CSM-P2P Object

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

Objects Setting >> CSM-P2P Object Profile

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

Set to Factory Default Clear all profiles.

Click the number under Index column for settings in detail.

```
Objects Setting >> CSM-P2P Object Profile
```

Profile Index: 1				
Profile Name: P2P-Forbid				
Check for Disallow:				
Protocol	Applications			
SoulSeek	SoulSeek			
🗌 eDonkey	eDonkey, eMule, Shareaza			
EastTrack	KazaA, iMesh			
🗌 Gnutella	BearShare, Limewire, Shareaza, Foxy			
BitTorrent BitTorrent, BitSpirit, BitComet				
Winny	Winny, WinMX, Share			
	Other P2P Applications			
Xunlei	Vagaa PP365 POCO			
Clubbox	Ares			
	OK Clear Cancel			
Profile Name	Type a name for the CSM profile.			
Check for Disallow	Check the items that disallow to use. Any device that uses such profile might not be allowed to access into the forbidden items.			

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

3.4.7 CSM-Misc Object

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

M-Misc Profile Ta		D GI	Set to Factory Defau
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>	

Objects Setting >> CSM-Misc Object Profile

Set to Factory Default Clear all profiles.

Click the number under Index column for settings in detail.

Objects Setting >> CSM-Misc Object Profile

Profile Index: 1							
Profile Name: Misc-F	orbid-1						
Check for Disallow:							
Tunneling							
Socks4/5	PGPNet	HTTP Proxy	TOR 🗌	VNN VNN			
SoftEther	🗌 FolderShare	🗌 MS TEREDO 🛛 🗹 Wujie/UltraSurf 🗌 Hamachi		🗌 Hamachi			
HTTP Tunnel	🗌 Ping Tunnel	🔲 Tiny VPN					
Streaming							
MMS	RTSP	TVAnts		PPStream			
🗌 PPlive	🗌 FeiDian	UUSee		NSPlayer			
PCAST	🔲 ΤΥΚοο	SopCast		UDLiveX			
TVUPlayer	🗌 MySee	🗌 Joost		FlashVideo			
OK Clear Cancel							
Profile NameType a name for the CSM profile.							
Check for Disallow Check the items that disallow to use. Any device that uses such profile might not be allowed to access into the forbidden items.							

3.5 CSM

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

3.5.1 IM/P2P Profile

IM/P2P Profile page can integrate objects profiles configured in **Objects** Setting>>CSM-IM Object/CSM-P2P Object/CSM-Misc Object into single IM/P2P profile.

CSM >> IM/P2P Profile	
Profile Index: 1	
Profile Name: CSM-Group-1	
CSM-IM Object	1-IM-forbid-1 💌
CSM-P2P Object	1-P2P-Forbid-1 💌
<u>CSM-Misc Object</u>	1-Misc-Forbid-1 💌
2	OK Cancel

Profile Name

Firewall >> General Setup

Type a name for the IM/P2P profile.

Later, in the **Firewall>>General Setup** and **Firewall>>Edit Filter Set>>Edit Filter Rule** pages, you can use **IM/P2P** drop down list to choose the proper CSM-IM profile as the standard for the host(s) to follow. See the following example.

Call Filter	💿 Enable	Start Filter S	Get Set#1 💙
	🔘 Disable		
Data Filter	💿 Enable	Start Filter 9	Set Set#2 💌
	🔘 Disable		
Actions for defaul Application	t rule:	Action/Profile	Syslog
Filter		Pass 🚩	
IM/P2P		None 🗸 🗸	
		- None	

3.5.2 URL Content Filter Profile

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

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

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

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

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

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

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

CSM >> URL Content Filter

Content Filter Setup				
Enable URL Access Contr	ol			
 Enable URL Access Lo Black List (block those White List (pass those 	e matching keyword)			
No ACT	Keyword	No	ACT	Keyword
1 🔽 gamble	-	5		
2		6		
3 🗖		7		
4		8		
Note that multiple keyw	ords are allowed to sp	i iecify in t	the blank.	For example: hotmail yahoo msn
Prevent web access from	IP address			
Enable Restrict Web Feat Java ActiveX Cookie Proxy	ure	iles	Execut	able files 🗌 Multimedia files
Enable Excepting Subnet				
No Act	IP Address			Subnet Mask
1			~	
2			~	
3			~	
4			~	
Time Schedule				
Index(1-15) in <u>Schedule</u> Note: Action and Idle Time		,,	,	
	ОК С	Clear All	Cano	el
Enable URL Access Control	Check the box to	activate	e URL A	Access Control.
Black List (block those matching keyword)				sing into the corresponding d on the box below.
White List (pass those matching keyword)				ing into the corresponding d on the box below.
Keyword	and each frame su a noun, a partial n keywords within a semicolon. In add 32-character long decline the connet matched to any us	apports oun, or a frame lition, th . After ction re ser-defi he bloc	multiple a comp are sep he maxin specifyi equest to ned key	hes for users to define keywords e keywords. The keyword could be lete URL string. Multiple arated by space, comma, or mal length of each frame is ng keywords, the Vigor router will the website whose URL string word. It should be noticed that the tword list, the more efficiently the
Prevent web access from IP address		-	-	surfing activity using IP address, son for this is to prevent someone

Vigor2930 Series User's Guide

67

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

3.5.3 Web Content Filter Profile

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

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

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

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

CSM >> Web Content Filter Setup

CPA(Content Portal Authority) Web Content Filter Setup				
Select a CPA server: glob Test a site to verify whethe				
Enable Web Content Fi		es to block. Untick to unl		
Child Protection Select All Clear All	Chat Gambling	Criminal Hacking Violence	Drugs/Alcohol Hate speech Weapons	
Leisure Select All Clear All	Advertisements Games Hobbies Personals Sports	Entertainment Glamour Lifestyle Photo Searches Streaming Media	Food Health Motor Vehicles Shopping Travel	
Business Select All Clear All	Computing/Internet Politics Remote proxies	□ Finance □ Real Estate □ Search Engine	☐ Job Search/Career ☐ Reference ☐ Web Mail	
Others Select All Clear All	 Education News Usenet news 	☐ Hosting sites ☐ Religion ☐ Block all uncategorise	☐ Kid Sites ☐ Sex Education Id sites	
Time Schedule Index(1-15) in <u>Sched</u> Note: Action and Idle Tim	ule Setup:,, eout settings will be ignor	,, ed.		
	ОК	Cancel		

3.6 Firewall

3.6.1 Basics for Firewall

Quick Start Wizard

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

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

Please enter an alpha-nu	neric string as your Passwo r	rd (Max 23 characters).
New Password	••••	
Confirm Password	••••	

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

dministrator Pa	ssword	 		
	Old Password			
	New Password			
	Confirm Password			

Firewall Facilities

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

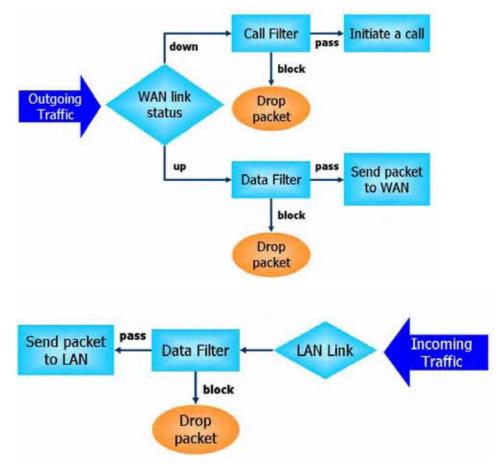
- User-configurable IP filter (Call Filter/ Data Filter).
- Stateful Packet Inspection (SPI): tracks packets and denies unsolicited incoming data
- Selectable Denial of Service (DoS) /Distributed DoS (DDoS) attacks protection

IP Filters

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

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

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



Stateful Packet Inspection (SPI)

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

Denial of Service (DoS) Defense

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

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

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

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

- 1. SYN flood attack
- 2. UDP flood attack
- 3. ICMP flood attack
- 4. TCP Flag scan
- 5. Trace route
- 6. IP options
- 7. Unknown protocol
- 8. Land attack

9. Smurf attack10. SYN fragment11. ICMP fragment12. Tear drop attack13. Fraggle attack14. Ping of Death attack

15. TCP/UDP port scan

Below shows the menu items for Firewall.

Firewall	
General Setup	
Filter Setup	
DoS Defense	

3.6.2 General Setup

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

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

Firewall >> General Setup

Call Filter	💿 Enable	Start Filter Set	Set#1 💌
	🔘 Disable		
Data Filter	💿 Enable	Start Filter Set	Set#2 💌
	🔘 Disable		
Actions for defaul Application Filter		Action/Profile Pass 💌	Syslog
IM/P2P	[None 💌	
,	r to VPN incoming p		for some games, ex. CS)

Cancel

ΟK

Call Filter	Check Enable to activate the Call Filter function. Assign a start filter set for the Call Filter.
Data Filter	Check Enable to activate the Data Filter function. Assign a start filter set for the Data Filter.
Action/Profile	Select Pass or Block for the packets that do not match with the filter rules.
Log	For troubleshooting needs you can specify the filter log and/or CSM log here by checking the box. The log will be displayed on Draytek Syslog window.
IM/P2P	Select an IM/P2P profile for global IM/P2P application blocking. All the hosts in LAN must follow the standard configured in the selected profile selected here. For detailed information, refer to the section of CSM profile setup.
Some on-line games (for	example: Half Life) will use lots of fragmented UDP packets to

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

3.6.3 Filter Setup

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

Firewal	>>	Filter	Setup
---------	----	--------	-------

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

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

Firewall	>> Filter	Setup >:	> Edit	Filter	Set

ault Call Filter			
Active	Comments	Move Up	Move Down
	Block NetBios		<u>Down</u>
		<u>UP</u>	Down
		<u>UP</u>	<u>Down</u>
		<u>UP</u>	
	Active	Active Comments Block NetBios C C C C C C C C C C C C C C C C C C	Active Comments Move Up ✓ Block NetBios UP □ UP UP

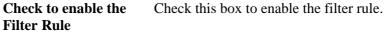
Clear	Cancel
	Clear

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

Filter Set 1 Rule 1 Check to enable the Filter Rule		
Comments:	Block NetBios	
Index(1-15) in <u>Schedule</u> Setup:		
Direction:	LAN -> WAN 🔽	
Source IP:	Any	Edit
Destination IP:	Any	Edit
Service Type:	TCP/UDP, Port: from 137~139 to undefined	Edit
Fragments:	Don't Care 🔽	
Application	Action/Profile	Syslog
Filter:	Block Immediately 💙	
Branch to Other Filter Set:	None 🔽	
IM/P2P:	None 👻	
OK	Clear Cancel	



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

Source/Destination IP Click **Edit** to access into the following dialog to choose the source/destination IP or IP ranges.

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

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



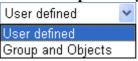
From the **IP Group** drop down list, choose the one that you want to apply. Or use the **IP Object** drop down list to choose the object that you want.

Service Type

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

Service Туре	Group and Objects 👻
Protocol	TCP/UDP
Source Port	= 🖌 137 ~ 139
Destination Port	= 🖌 1 ~ 65535
Service Group	None 🛩
r <u>Service Object</u>	None 💌
or Service Object	None 1-SIP
or Service Object	2-RTP
	OK Close

choose Group and Objects as the Service Type.



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

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

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

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

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

Service Group/Object - Use the drop down list to choose the one that you want.

Specify the action for fragmented packets. And it is used for Data Fragments Filter only. Don't care - No action will be taken towards fragmented packets. Unfragmented - Apply the rule to unfragmented packets. *Fragmented* - Apply the rule to fragmented packets. Too Short - Apply the rule only to packets that are too short to contain a complete header. Filter Specifies the action to be taken when packets match the rule. Block Immediately - Packets matching the rule will be dropped immediately. Pass Immediately - Packets matching the rule will be passed immediately. Block If No Further Match - A packet matching the rule, and that does not match further rules, will be dropped. Pass If No Further Match - A packet matching the rule, and that does not match further rules, will be passed through.

Branch to other Filter	If the packet matches the filter rule, the next filter rule will branch
Set	to the specified filter set. Select next filter rule to branch from the drop-down menu. Be aware that the router will apply the specified filter rule for ever and will not return to previous filter rule any more.
IM/P2P	All the packets/connections within the range configured in the above conditions must follow the standard configured in the IM/P2P profile selected here. For detailed information, refer to the section of IM/P2P profile setup.
SysLog	For troubleshooting needs you can specify the filter log and/or CSM log here. Check the corresponding box to enable the log function. Then, the filter log and/or CSM log will be shown on Draytek Syslog window.

Example

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

eal Setup						
Call Filter	t. O Ina	tin Start Fiter Set	Sec#1 H			
	C Disa	attle				
Data Filte	ir 💮 Ena	Die Stat Filter Set	5442			
	O Pro	Contraction of the second seco				
Actions to	er dataab role:	14.7 1 - 2015				
Applicatio	and the second se	Action Profile	Einewall >> Filter Setup			
Filter		Pate .				
BEP2P		None	Filter Setter		Satte Fa	ctory Balas
		Note:	Comments	Set	Comments	And Antes
E Apply	IP filter to VPN inco	ming packages	1. Default Call Filter	L	2.500mmin	
		prierited UDP or ICMP packets (6		
-				2		
			i.	19.		
		OR Canal	5	11.		
			6	12.		
	Senap >+ Erlh Filher Se nut Cat Filher	i				
	nut Car Film Active	Catagoria	More Up More Down			
	NI CATIN	1	A REAL PROPERTY AND A REAL	4		
	nut Car Film Active	Comments	Maren Op Maren Damm Fiscandi So Edit Filber Set So Edit Filber Po	de		
1 2 3	Active	Comments	A REAL PROPERTY AND A REAL	de		
1 2 3	Active	Comments	Firewall >> Edit Filter Set >> Edit Filter Bu			
1 2 3	Active	Comments	Filewall >> Edit Files Set >> Edit Files Po Files Set 1 Bale 1			
1 2 3 4 5	Active	Comments	Filewardt >> Edit Filmer Set >> Edit Filmer Be Filewardt >> Edit Filmer Be Glocch to enable the Filter Fole Comments			
1 2 3 4 5 6	Active	Comments	Filewardt >> Edit Filmer Set >> Edit Filmer Ro Filmer Set 1 Hade 1 S Check to enable the Filmer Ful	Flack NotBase	3	
1 2 3 4 5 6	Active	Comments	Filewardt >> Edit Filmer Set >> Edit Filmer Be Filewardt >> Edit Filmer Be Glocch to enable the Filter Fole Comments		2 3	
1 2 3 4 5 6	Active	Comments	Filewall >> Edit Filmer Set >> Edit Filmer Re Filmer Set 1 Ibale 1 Check to enable the Filmer Ful Community Index(1-13) in Scientific Betup:	Flack NotBase	, 3,	(Ess)
1 2 3 4 5 6	Active Active	Common the fact the s	Filewall >> Edit Filmer Set >> Edit Filmer Re Filmer Set 1 Ibale 1 Check to enable the Filmer Rule Commentio Index(1-13) in Scientific Betup: Directions Source IP: Destination IP-	Elact Notifies	3,	(Ea)
1 2 3 4 5 6	Active Active	Comments	Filewardt >> Edit Filmer Set >> Edit Filmer Ro Filmer Set 1 Hade 1 Scheck to enable the Filmer Role Comments Index(1=13) in Schedule Setup: Directions Source IP Destination IP-	Elact Netflan	3	
1 2 3 4 5 6	Active Active	Common the fact the s	Filewall >> Lift Files Set >> Edit Files Re Filewall >> Edit Files Set >> Edit Files Re Comments: Index(1=13) in <u>Sclashing</u> Setup: Direction: Source IP: Destination IP: Service Type:	Elack Notifies	39 to undefined	
1 2 3 4 5 6	Active Active	Common the fact the s	Filewardt >> Edit Filmer Set >> Edit Filmer Ro Filmer Set 1 Hade 1 Scheck to enable the Filmer Role Comments Index(1=13) in Schedule Setup: Directions Source IP Destination IP-	Elact Netflan	39 to undefined	
ent 1 ent t Defi	Active Active	Common the fact the s	Filewall >> Ldt Filer Set >> Edit Filer Re Files Set 1 Itale 1 Source to enable the Filer Role Comments Index(1-13) in Sclandale Setup: Direction Source IP: Destination IP: Service Type: Programmits	Hack Notifies		EAL
1 2 3 4 5 6	Active Active	Common the fact the s	Filewall >> Lift Files Set >> Lift File Po Filewall >> Lift Files Set >> Lift File Po Community Index(1>15) in Schedule Setup: Direction Source IP Destructor IP Service Type: Programmts: Application	Elect Notline LAN -> WAN W Any Any TCPAUDP, Flat, furn 127-1 Dan't Care Active Profile	54	(Ent)
1 2 3 4 5 6	Active Active	Common the fact the s	Filewall >> Ldt Filer Set >> Edit Filer Re Files Set 1 Itale 1 Source to enable the Filer Role Comments Index(1-13) in Sclandale Setup: Direction Source IP: Destination IP: Service Type: Programmits	Hack Notifies		(Ent)

3.6.4 DoS Defense

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

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

Firewall >> DoS defense Setup		<u>r</u>			_
DoS defense Setup					
Enable DoS Defense					m
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 defens	e	Threshold	50	packets / sec	
		Timeout	10	sec	
Enable Port Scan detection		Threshold	150	packets / sec	
Block IP options		📃 Block TCP flag	scan		
Block Land		🔲 Block Tear Drop	D		
🔲 Block Smurf		🔲 Block Ping of D	eath		
Block trace route		🔲 Block ICMP frag	gment		
Block SYN fragment		📃 Block Unknown	Protocol		
🔲 Block Fraggle Attack					
Enable DoS defense crackers.	function to preven	nt the attacks fr	om hacker	or 🔨	
Enable Dos Defense Enable SYN flood defense Enable UDP flood	Check the box detecting the T has exceeded t randomly disca defined in Tim packets' attem By default, the per second and	to activate the to activate the Threshold of th the defined val ard the subsequence peout. The goal pt to exhaust the threshold and 1 10 seconds, r	e SYN fl e TCP S ue, the V uent TC l for this he limite timeout espectiv	efense Function ood defense fun YN packets fro Vigor router wil P SYN packets is prevent the ' ed-resource of V values are set ely. ood defense fun	action. Once om the Internet l start to for a period TCP SYN Vigor router. to 50 packets
defense	detecting the T exceeded the c discard the sub	Threshold of th lefined value, to psequent UDP default setting	e UDP p the Vigo packets for three	backets from the r router will sta for a period def shold and timed	e Internet has art to randomly fined in
Enable ICMP flood defense	to the UDP flo packets from I will discard th	od defense fur nternet has exe e ICMP echo r for threshold a	nction, o ceeded th requests and time	flood defense funce if the Threshe defined valu coming from thous and the theory of theory of the theory of the theory of the th	shold of ICMP e, the router he Internet. The
Enable PortScan detection	many ports in Check the box	an attempt to f to activate the	ind igno Port Sc	sending lots of rant services w an detection. W behavior by mo	ould respond. henever

Vigor2930 Series User's Guide

79

	port-scanning Threshold rate, the Vigor router will send out a warning. By default, the Vigor router sets the threshold as 150 packets per second.
Block IP options	Check the box to activate the Block IP options function. The Vigor router will ignore any IP packets with IP option field in the datagram header. The reason for limitation is IP option appears to be a vulnerability of the security for the LAN because it will carry significant information, such as security, TCC (closed user group) parameters, a series of Internet addresses, routing messagesetc. An eavesdropper outside might learn the details of your private networks.
Block Land	Check the box to enforce the Vigor router to defense the Land attacks. The Land attack combines the SYN attack technology with IP spoofing. A Land attack occurs when an attacker sends spoofed SYN packets with the identical source and destination addresses, as well as the port number to victims.
Block Smurf	Check the box to activate the Block Smurf function. The Vigor router will ignore any broadcasting ICMP echo request.
Block trace router	Check the box to enforce the Vigor router not to forward any trace route packets.
Block SYN fragment	Check the box to activate the Block SYN fragment function. The Vigor router will drop any packets having SYN flag and more fragment bit set.
Block Fraggle Attack	Check the box to activate the Block fraggle Attack function. Any broadcast UDP packets received from the Internet is blocked. Activating the DoS/DDoS defense functionality might block some legal packets. For example, when you activate the fraggle attack defense, all broadcast UDP packets coming from the Internet are blocked. Therefore, the RIP packets from the Internet might be dropped.
Block TCP flag scan	Check the box to activate the Block TCP flag scan function. Any TCP packet with anomaly flag setting is dropped. Those scanning activities include <i>no flag scan</i> , <i>FIN without ACK scan</i> , <i>SYN FINscan</i> , <i>Xmas scan</i> and <i>full Xmas scan</i> .
Block Tear Drop	Check the box to activate the Block Tear Drop function. Many machines may crash when receiving ICMP datagrams (packets) that exceed the maximum length. To avoid this type of attack, the Vigor router is designed to be capable of discarding any fragmented ICMP packets with a length greater than 1024 octets.
Block Ping of Death	Check the box to activate the Block Ping of Death function. This attack involves the perpetrator sending overlapping packets to the target hosts so that those target hosts will hang once they re-construct the packets. The Vigor routers will block any packets realizing this attacking activity.
Block ICMP Fragment	Check the box to activate the Block ICMP fragment function. Any ICMP packets with more fragment bit set are dropped.
Block Unknown Protocol	Check the box to activate the Block Unknown Protocol function. Individual IP packet has a protocol field in the datagram header to indicate the protocol type running over the upper layer. However,

the protocol types greater than 100 are reserved and undefined at this time. Therefore, the router should have ability to detect and reject this kind of packets.

Warning MessagesWe 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.

SysLog / Mail Alert Se	tup				
SysLog Access Setup			Mail Alert Setup		
🗹 Enable			🔲 Enable		
Server IP Address	192.16	68.1.115	SMTP Server		
Destination Port	514		Mail To		
Enable syslog mess	aqe:		Return-Path		
🔲 Firewall Log	-		Authenticatio	n	
VPN Log			User Name		
User Access	Log		Password		
Call Log			Fassword		
WAN Log	oformation				
- Roadolybeen	Tornacies.				
		ОК	Clear Cancel	1	
🕼 DrayTek Syslog 3.7.0					
Controls	192.168.1	1 WAN	Status		
		2930 series	Gateway IP (Fixed)	TX Packets TX Rate	
LAN Status		2930 56165	172.16.3.4	32421 4	
	DV D-	ickets	WAN IP (Fixed)	RX Packets RX Rate	
TX Packets					
TX Packets 282506		308	172.16.3.229	154546 1018	1
282506	222	308		154546 1018	i
282506 Firewall Log VPN Log Use	er Access Log	308 Call Log WAN Log Other	172.16.3.229	154546 1018	
282506	222	308 Call Log WAN Log Other Message	172.16.3.229	154546 1018 State Traffic Graph	
282506 Firewall Log VPN Log Use	er Access Log	308 Call Log WAN Log Other Message	172.16.3.229	154546 1018 State Traffic Graph	
282506 Firewall Log VPN Log Use	er Access Log	308 Call Log WAN Log Other Message	172.16.3.229	154546 1018 State Traffic Graph	
282506 Firewall Log VPN Log Use	er Access Log	308 Call Log WAN Log Other Message	172.16.3.229	154546 1018 State Traffic Graph	
282506 Firewall Log VPN Log Use	er Access Log	308 Call Log WAN Log Other Message	172.16.3.229	154546 1018 State Traffic Graph	
282506 Firewall Log VPN Log Use	er Access Log	308 Call Log WAN Log Other Message	172.16.3.229	154546 1018 State Traffic Graph	
282506 Firewall Log VPN Log Use	er Access Log	308 Call Log WAN Log Other Message	172.16.3.229	154546 1018 State Traffic Graph	
282506 Firewall Log VPN Log Use	er Access Log	308 Call Log WAN Log Other Message	172.16.3.229	154546 1018 State Traffic Graph	
282506 Firewall Log VPN Log Use	er Access Log	308 Call Log WAN Log Other Message	172.16.3.229	154546 1018 State Traffic Graph	
282506 Firewall Log VPN Log Use	er Access Log	308 Call Log WAN Log Other Message	172.16.3.229	154546 1018 State Traffic Graph	
282506 Firewall Log VPN Log Use	er Access Log	308 Call Log WAN Log Other Message	172.16.3.229	154546 1018 State Traffic Graph	
282506 Firewall Log VPN Log Use	er Access Log	308 Call Log WAN Log Other Message	172.16.3.229	154546 1018 State Traffic Graph	
282506 Frewall Log VPN Log Use Time Oct 18 02:54:25	er Access Log	ADDR THE STREET	172.16.3.229	154546 1018 State Traffic Graph	
282506 Firewall Log VPN Log Use	er Access Log	308 Call Log WAN Log Other Message	172.16.3.229	154546 1018 State Traffic Graph	
282506 Firewall Log VPN Log Ux Time Oct 18 02:54:25	er Acces Log (Host 2330	aae Callog WAN Log Other Message [DoS] trace_rt Block 172.	172.16.3.229	154946 1018 State Traffic Graph PR 17(udp) len 20 72	
282506 Firewall Log VPN Log Use Oct 18 02:54:25	er Access Log	ADDR THE STREET	172.16.3.229	154546 1018 State Traffic Graph	

3.7 Bandwidth Management

Below shows the menu items for Bandwidth Management.

Bandwidth Management
Sessions Limit
Bandwidth Limit
Quality of Service

3.7.1 Sessions Limit

A PC with private IP address can access to the Internet via NAT router. The router will generate the records of NAT sessions for such connection. The P2P (Peer to Peer) applications (e.g., BitTorrent) always need many sessions for 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.

	O Enable 💿 Disable
	Default Max Sessions: 100
	Limitation List
	Index Start IP End IP Max Sessions
	Start IP: End IP:
	Maximum Sessions: Add Edit Delete
ime Scl	nedule
Ind	ex(1-15) in <u>Schedule</u> Setup:,,,
Not	e: Action and Idle Timeout settings will be ignored.

Bandwidth Management >> Sessions Limit

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

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

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

3.7.2 Bandwidth Limit

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

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

🔘 Enable	e 💿 Disable	1	
Default T>	K Limit: 200	Kbps Default RX Limit: 800 Kbps	
🔲 Allow	auto adjustn	nent to make the best utilization of <u>available band</u>	lwidth.
Limitation	List		
Index St	art IP	End IP TX limit RX limit Sh	hared
Specific Li	mitation		
Specific Li	mitation	End IP:	
Start IP:			(/h.e.=
· ·	imitation	TX Limit: Kbps RX Limit:	Kbps
Start IP:			Kbps
Start IP:		TX Limit: Kbps RX Limit:	Kbps
Start IP:		TX Limit: Kbps RX Limit:	Kbps

Bandwidth Management >> Bandwidth Limit

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

ОK

Enable	Click this button to activate the function of limit bandwidth.
Disable	Click this button to close the function of limit bandwidth.
Default TX limit	Define the default speed of the upstream for each computer in LAN.
Default RX limit	Define the default speed of the downstream for each computer in LAN.
Allow auto adjustment to make the best utilization of available bandwidth	Router will detect if there is enough bandwidth remained for using according to the bandwidth limit set by the user. If yes, the router will adjust the available bandwidth for users to enhance the total utilization.
Limitation List	Display a list of specific limitations that you set on this web page.
Start IP	Define the start IP address for limit bandwidth.
End IP	Define the end IP address for limit bandwidth.
Each/Shared	Select Each to make each IP within the range of Start IP and End IP having the same speed defined in TX limit and RX

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

3.7.3 Quality of Service

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

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

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

There are two components within Primary configuration of QoS deployment:

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

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

One more larger-scale implementation of QoS network is to apply DSCP (Differentiated Service Code Point) and IP Precedence disciplines at Layer 3. Compared with legacy IP Precedence that uses Type of Service (ToS) field in the IP header to define 8 service classes, DSCP is a successor creating 64 classes possible with backward IP Precedence compatibility. In a QoS-enabled network, or Differentiated Service (DiffServ or DS) framework, a DS domain owner should sign a Service License Agreement (SLA) with other DS domain

owners to define the service level provided toward traffic from different domains. Then each DS node in these domains will perform the priority treatment. This is called per-hop-behavior (PHB). The definition of PHB includes Expedited Forwarding (EF), Assured Forwarding (AF), and Best Effort (BE). AF defines the four classes of delivery (or forwarding) classes and three levels of drop precedence in each class.

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



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

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

Genera	Setup								
Index	Status	Bandwidth	Directon	Class 1	Class 2	Class 3	Others	UDP Bandwidth Control	
WAN1	Disable	10000Kbps/10000Kbps		25%	25%	25%	25%	Inactive	Setu
WAN2	Disable	10000Kbps/10000Kbps		25%	25%	25%	25%	Inactive	<u>Setu</u>
Class Ru Inde		N	ame				Rule	Service	Туре
Class	5 1						<u>Edit</u>		
Class	5 2						<u>Edit</u>	Edit	
	; 3						Edit		

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

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

General Setup for WAN Interface

Bandwidth Management >> Quality of Service

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.

VolPon www.voipon.co.uk sales@voipon.co.uk Tel: +44 (0)1245 808195 Fax: +44 (0)1245 808299

Bandwidth	Manad	iement	>>	Quality	of	Service

WAN1 General Setup Image: Control Contro Control Contro Control Control Control Control	· •				
WAN Inbound Ba	ndwidth	10000 Kbps			
WAN Outbound B		10000 Kbps			
	ble QoS, you should test t rk properly if the bandwidtl	the real bandwidth first.			
Index	Class Name	Reserved_bandwidth Ratio			
Class 1		25 %			
Class 2		25 %			
Class 3		25 %			
	Others	25 <mark>%</mark>			
Enable UDP Bandwidth Contr	ol	Limited_bandwidth Ratio 25 %			
🔲 Outbound TCP ACK Prioritize					
Enable the QoS Control WAN Inbound Bandwidth WAN Outbound Bandwidtl	Please also define whapply to. IN- apply to incomin OUT- apply to outgoi BOTH- apply to both Check this box and c You will see the Onli It allows you to set th For example, if your 256K upstream, please value is 10000kbps. h It allows you to set th WAN. For example, if	ing traffic only. h incoming and outgoing traffic. lick OK , then click Setup link again. ine Statistics link appearing on this pag he connecting rate of data input for WAI ADSL supports 1M of downstream and se set 1000kbps for this box. The defaul he connecting rate of data output for if your ADSL supports 1M of K upstream, please set 256kbps for this			
correct calculation of QoS. I as 80% - 85% of physical ne performance.	t is suggested to set the twork speed provided l				
Reserved Bandwidth Ratio		group index in the form of ratio of to upstream speed and reserved stream speed.			
Enable UDP Bandwidth Control	field. This is a protec	e limited bandwidth ratio on the right tion of TCP application traffic since fic such as streaming video will exhaust			
Outbound TCP ACK Prioritize	are great in ADSL2+	ndwidth between download and upload environment. For the download speed y the uploading TCP ACK, you can			

	check this box to push ACK of upload faster to speed the network traffic.						
Limited_bandwidth Ratio	The ra applic	• •	ped here is	s reserved for l	imited bandwidth of UDP		
Online Statistics	Display an online statistics for quality of service for your reference. This link will be seen only if you click OK in WAN1/WAN2 General Setup web page and click Setup again (for WAN1/WAN2) on the Bandwith Management>>Quality of Service . Bandwidth Management >> Quality of Service. Bandwidth Management >> Quality of Service						
	Indov	Direction	Class Namo Pos	oruod-bandwidth Batio	Outbound Throughput (Bytes/sec)		
	1	OUT	GIG33 Nume Kes	25%			
	2	OUT		25%	0		
	3	OUT		25%	0		
	4	OUT	Others	25%	0		
			Outbo	und Status			

Edit the Class Rule for QoS

Bandwidth Management >> Quality of Service

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.

10 (Bps)

General	Setup								
Index	Status	Bandwidth	Directon	Class 1	Class 2	Class 3	Others	UDP Bandwidth Control	
WAN1	Disable	10000Kbps/10000Kbps		25%	25%	25%	25%	Inactive	<u>Setup</u>
WAN2	Disable	10000Kbps/10000Kbps		25%	25%	25%	25%	Inactive	<u>Setup</u>
Class Ru Inde		N	ame				Rule	Service	Туре
Class	; 1						<u>Edit</u>		
Class	; 2						<u>Edit</u>	Edit	
Class	; 3						<u>Edit</u>		

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

ne	Test					
NO	Status	Local Address	Remote Address	DiffServ CodePoint	Service Type	
1	Empty	-	-	-	-	
Add Edit Delete						

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

🗹 ACT		
Local Address	Any	Edit
Remote Address	Any	Edit
DiffServ CodePoint	ANY	~
Service Type	ANY	*
Note: Please choose/set	up the Service Type	first.

OK Cancel

АСТ	Check this box to invoke these settings.						
Local Address	Click the Edit button to set the local IP address (on LAN) for the rule.						
Remote Address	Click the Edit button to set the remote IP address (on LAN/WAN) for the rule.						
Edit	It allows you to edit source address information.						
	🗿 http://192.168.1.1/doc/QosIpEdt.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 Range Address, you have to fill in Start IP address and						
	End IP address.						
	For Subnet Address , you have to fill in Start IP address and						
	Subnet Mask.						
DiffServ CodePoint	All the packets of data will be divided with different levels and will be processed according to the level type by the system. Please assign one of the levels of the data for processing with QoS control.						

Service Type

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

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

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

ne (Game					
NO	Status	Local Address	Remote Address	DiffServ CodePoint	Service Type	
1 ()	Active	Any	Any	IP precedence 2	SYSLOG(UDP:514)	
2 🔿	Active	192.168.1.15	192.168.1.65	AF Class1 (Low Drop)	FTP(TCP:20)	
Add Edit Delete						

Edit the Service Type for Class Rule

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

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

General Setup								
Index Status	Bandwidth	Directon	Class 1	Class 2	Class 3	Others	UDP Bandwidth Control	
WAN1 Disable	10000Kbps/10000Kbps		25%	25%	25%	25%	Inactive	<u>Setup</u>
WAN2 Disable	10000Kbps/10000Kbps		25%	25%	25%	25%	Inactive	<u>Setup</u>

Class Rule

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

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

Bandwidth	Managen	nent >> (Quality o	of Service

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

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

Bandwidth Management >> Quality of Service

Service Type Edit				
Service Name				
Service Type		TCP 6		
Port Configuration	n			
Type		💿 Single 🔘 Range		
Port Numbe	er	0 – 0		
Service Name	OK Type in a new	Cancel service for your request.		
ber vice i vanie				
Service Type	Choose the typ service.	e (TCP, UDP or TCP/UDP) for the new		
Port Configuration	have to type in number on the Port Number	 Range as the Type. If you select Range, you the starting port number and the end porting boxes below. Type in the starting port number and the end r here if you choose Range as the type. 		

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

3.8 Applications

Below shows the menu items for Applications.

Applications	
Dynamic DNS	
Schedule	
▶ RADIUS	
▶ UPnP	
Wake on LAN	

3.8.1 Dynamic DNS

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

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

Enable the Function and Add a Dynamic DNS Account

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

Applications >> Dynamic DNS Setup

ynamic DNS Setup			Set to Factory Defaul
🗹 Enable Dynamic	c DNS Setup	View L	og Force Update
accounts :			
Index	WAN Interface	Domain Name	Active
<u>1.</u>	WAN1 First		х
<u>2.</u>	WAN1 First		х
<u>3.</u>	WAN1 First		×



Set to Factory Default Clear all profiles and recover to factory settings.

Enable Dynamic DNS Setup Check this box to enable DDNS function.

Index	Click the number below Index to access into the setting page of DDNS setup to set account(s).
WAN Interface	Display current WAN interface used for accessing Internet.
Domain Name	Display the domain name that you set on the setting page of DDNS setup.

Active	Display if this account is active or inactive.
View Log	Display DDNS log status.
Force Update	Force the router updates its information to DDNS server.

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

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

Index : 1 Enable Dynamic DNS	S Account
WAN Interface	WAN1 First
Service Provider	dyndns.org (www.dyndns.org)
Service Type	Dynamic 💌
Domain Name	chronic6853 , dyndns.info dyndns.info 💌
Login Name	chronic6853 (max. 23 characters)
Password	•••••••••• (max. 23 characters)
🔲 Wildcards	
🔲 Backup MX	
Mail Extender	
-	OK Clear Cancel

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

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

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

Disable the Function and Clear all Dynamic DNS Accounts

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

Delete a Dynamic DNS Account

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

3.8.2 Schedule

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

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

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

Applications >> Schedule

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

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

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

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

Applications >> Schedule

Index No. 1	
🗹 Enable Schedule Setup	
Start Date (yyyy-mm-dd)	2000 🗸 - 1 🔽 - 1 🔽
Start Time (hh:mm)	0 🕶 : 0 💌
Duration Time (hh:mm)	0 💌 : 0 💌
Action	Force On
Idle Timeout	minute(s).(max. 255, 0 for default)
How Often	
Once	
💿 Weekdays	
🗌 Sun 🗹 Mon 🔽	Tue 🗹 Wed 🗹 Thu 🗹 Fri 🔲 Sat
ОК	Clear Cancel

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

Example

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



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

3.8.3 RADIUS

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

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

Applications >> RADIUS	
RADIUS Setup	
🗹 Enable	
Server IP Ad	Idress
Destination (Port 1812
Shared Secr	et
Confirm Shar	red Secret
(OK Clear Cancel
Enable	Check to enable RADIUS client feature
Server IP Address	Enter the IP address of RADIUS server
Destination Port	The UDP port number that the RADIUS server is using. The default value is 1812, based on RFC 2138.
Shared Secret	The RADIUS server and client share a secret that is used to authenticate the messages sent between them. Both sides must be configured to use the same shared secret.
Confirm Shared Secret	Re-type the Shared Secret for confirmation.

3.8.4 UPnP

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

Applications >> UPnP

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

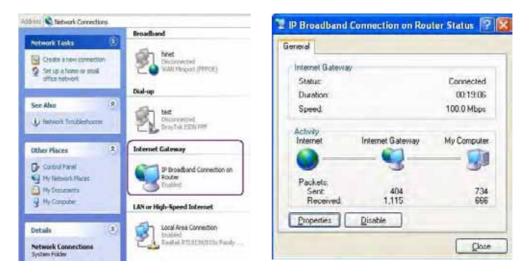
Note: If you intend running UPnP service inside your LAN, you should check the appropriate service above to allow control, as well as the appropriate UPnP settings.



Enable UPNP Service

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

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



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

ieneral	Services
Connect to the Internet using	Select the services running on your network that Internet users can access
3 IP Broadband Connection on Router	(Services
This connection allows you to connect to the Internet through a shared connection on another computer.	Ftp Example manunigr (192,168,29,11:13135) 60654 UDP manuningr (192,168,29,11:7824) 13251 UDP manuningr (192,168,29,11:8789) 63231 TCP manuningr (192,168,29,11:8789) 63231 TCP

The reminder as regards concern about Firewall and UPnP

Can't work with Firewall Software

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

Security Considerations

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

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

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

3.8.5 Wake on LAN

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

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

Application >> Wake on LAN

Wake by: MAC Address IP Address: MAC Address: Wake Up! Result	Note: Wake on L can wake up thr	AN cooperate with Bind IP to MAC function, only binded PCs ough IP.
MAC Address:	Wake by:	MAC Address 💌
	IP Address:	😪
Result	MAC Address:	Wake Up!
	Result	

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

Appl	ication	>> Wa	ke on	LAN
------	---------	-------	-------	-----

Note: Wake on L can wake up thr	AN cooperate with Bind IP to MAC function, only binded PCs ough IP.
Wake by:	MAC Address 💙
IP Address:	🔽
MAC Address:	· · · · · · · · · · · · · · · · · · ·
Result	
Send command	to client done.

3.9 VPN and Remote Access

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

Below shows the menu items for VPN and Remote Access.

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

Note: This feature can be applied for ISDN remote dial-in or ISDN LAN-to-LAN connection in *i* series models.

3.9.1 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.

emote Access	Control Setu	p
	~	Enable PPTP VPN Service
	\checkmark	Enable IPSec VPN Service
	\checkmark	Enable L2TP VPN Service
		Enable ISDN Dial-In

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

Clear

Cancel

ΟK

3.9.2 PPP General Setup

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

VPN and Remote Access >> PPP General Setup

PPP/MP Protocol		IP Address Assignment for	r Dial-In Users
Dial-In PPP Authentication	PAP or CHAP	Start IP Address	192.168.1.200
Dial-In PPP Encryption (MPPE)	Optional MPPE		
Mutual Authentication (PAP) 🔘 Yes 💽 No		
Username			
Password			

ОК

Dial-In PPP Authentication PAP Only	Select this option to force the router to authenticate dial-in users with the PAP protocol.
PAP or CHAP	Selecting this option means the router will attempt to authenticate dial-in users with the CHAP protocol first. If the dial-in user does not support this protocol, it will fall back to use the PAP protocol for authentication.
Dial-In PPP Encryption (MPPE Optional MPPE	This option represents that the MPPE encryption method will be optionally employed in the router for the remote dial-in user. If the remote dial-in user does not support the MPPE encryption algorithm, the router will transmit "no MPPE encrypted packets". Otherwise, the MPPE encryption scheme will be used to encrypt the data. Optional MPPE Require MPPE(40/128 bit) Maximum MPPE(128 bit) Require MPPE (40/128 bits) - Selecting this option will force the router to encrypt packets by using the MPPE encryption algorithm. In addition, the remote dial-in user will use 40-bit to perform encryption prior to using 128-bit for encryption. In other words, if 128-bit MPPE encryption method is not available, then 40-bit encryption scheme will be applied to encrypt the data. Maximum MPPE - This option indicates that the router will use the MPPE encryption scheme with maximum bits (128-bit) to encrypt the data.
Mutual Authentication (PAP)	The Mutual Authentication function is mainly used to communicate with other routers or clients who need bi-directional authentication in order to provide stronger security, for example, Cisco routers. So you should enable this function when your peer router requires mutual authentication. You should further specify the User Name and Password of the mutual authentication peer.
Start IP Address	Enter a start IP address for the dial-in PPP connection. You should choose an IP address from the local private network. For example, if the local private network is 192.168.1.0/255.255.255.0, you could choose 192.168.1.200 as the Start IP Address. But, you have to notice that the first two IP addresses of 192.168.1.200 and 192.168.1.201 are reserved for ISDN remote dial-in user.

3.9.3 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.

IKE Authentication Method	
Pre-Shared Key	••••
Confirm Pre-Shared Key	•••••
IPSec Security Method	
🗹 Medium (AH)	
Data will be authentic, b	out will not be encrypted.
High (ESP) 🗹 DES 📗	SDES AES
Data will be encrypted a	and authentic.

0K

VPN and Remote Access >> IPSec General Setup

IKE Authentication MethodThis usually applies to those are remote dial-in user or node
(LAN-to-LAN) which uses dynamic IP address and
IPSec-related VPN connections such as L2TP over IPSec
and IPSec tunnel.Pre-Shared Key -Currently only support Pre-Shared Key
authentication.Pre-Shared Key- Specify a key for IKE authentication
Confirm Pro Shared Key. Patyne the characters to confirm

Cancel

Confirm Pre-Shared Key- Retype the characters to confirm the pre-shared key.

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

3.9.4 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 **100** entries of digital certificates for peer dial-in users.

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

VPN and Remote Access >> IPSec Peer Identity

Set to Factory Default

Index

Click it to clear all indexes.

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

Name

Display the profile name of that index.

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

VPN and Remote Access >> IPSec Peer Ident	VPN	and	Remote	Access	>> IF	Sec	Peer	Identi
---	-----	-----	--------	--------	-------	-----	------	--------

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

VolPon www.voipon.co.uk sales@voipon.co.uk Tel: +44 (0)1245 808195 Fax: +44 (0)1245 808299

3.9.5 Remote Dial-in User

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

The router provides 100 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	Status	Index	User	Status
<u>1.</u>	???	×	<u>17.</u>	???	×
<u>2.</u>	???	×	<u>18.</u>	???	×
<u>3.</u>	???	×	<u>19.</u>	???	×
<u>4.</u>	???	×	<u>20.</u>	???	×
<u>5.</u>	???	×	<u>21.</u>	???	×
<u>6.</u>	???	×	<u>22.</u>	???	×
<u>7.</u>	???	×	<u>23.</u>	???	×
<u>8.</u>	???	×	<u>24.</u>	???	×
<u>9.</u>	???	×	<u>25.</u>	???	×
<u>10.</u>	???	×	<u>26.</u>	???	×
<u>11.</u>	???	×	<u>27.</u>	???	×
<u>12.</u>	???	Х	<u>28.</u>	???	×
<u>13.</u>	???	Х	<u>29.</u>	???	×
<u>14.</u>	???	Х	<u>30.</u>	???	×
<u>15.</u>	???	Х	<u>31.</u>	???	×
<u>16.</u>	???	×	<u>32.</u>	???	×

VPN and Remote Access >> Remote Dial-in User

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

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

VPN and Remote Access >> Remote Dial-in User

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

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

	select above will apply the authentication methods and security methods in the general settings .
User Name	This field is applicable when you select ISDN, PPTP or L2TP with or without IPSec policy above.
Password	This field is applicable when you select ISDN, PPTP or L2TP with or without IPSec policy above.
IKE Authentication Method	 d This group of fields is applicable for IPSec Tunnels and L2TP with IPSec Policy when you specify the IP address of the remote node. The only exception is Digital Signature (X.509) can be set when you select IPSec tunnel either with or without specify the IP address of the remote node. Pre-Shared Key - Check the box of Pre-Shared Key to invoke this function and type in the required characters (1-63) as the pre-shared key. Digital Signature (X.509) – Check the box of Digital Signature to invoke this function and Select one predefined Profiles set in the VPN and Remote Access >>IPSec Peer Identity.
IPSec Security Method	This group of fields is a must for IPSec Tunnels and L2TP with IPSec Policy when you specify the remote node. Check the Medium, DES, 3DES or AES box as the security method. Medium -Authentication Header (AH) means data will be authenticated, but not be encrypted. By default, this option is invoked. You can uncheck it to disable it. High-Encapsulating Security Payload (ESP) means payload (data) will be encrypted and authenticated. You may select encryption algorithm from Data Encryption Standard (DES), Triple DES (3DES), and AES. Local ID - Specify a local ID to be used for Dial-in setting in the LAN-to-LAN Profile setup. This item is optional and can be used only in IKE aggressive mode.
Callback Function	 The callback function provides a callback service only for the ISDN dial-in user (for <i>i</i> model only). The remote user will be charged the connection fee by the telecom. Check to enable Callback function-Enables the callback function. Specify the callback number-The option is for extra security. Once enabled, the router will ONLY call back to the specified Callback Number. Check to enable callback budget control-By default, the callback function has a time restriction. Once the callback budget has been exhausted, the callback mechanism will be disabled automatically. Callback Budget (Unit: minutes)- Specify the time budget for the dial-in user. The budget will be decreased automatically per callback connection.

3.9.6 LAN to LAN

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

The router provides up to **100** profiles, which also means supporting **100** VPN tunnels simultaneously. The following figure shows the summary table.

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

VPN and Remote Access >> LAN to LAN

Set to Factory Default

Click to clear all indexes.

Name

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

Status

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

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

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

Profile Index : 1 1. Common Settings						
Profile Name first		Call Direction 💿 Bo	th 🔘 Dial-Out	🔿 Dial-In		
		Always on	tii 🔾 bial-Out			
Enable this profile		Idle Timeout 300	second(s)			
VPN Connection Through: WAN1 First 💌		Enable PING to keep				
		PING to the IP				
2. Dial-Out Settings		I				
Type of Server I am calling		Link Type	64k bps 🔽			
● ISDN		Username	???			
• РРТР		Password				
O IPSec Tunnel		PPP Authentication	PAP/CHAP			
O L2TP with IPSec Policy None		VJ Compression	💿 On 🔘 Of			
Dial Number for ISDN or		·				
Server IP/Host Name for VPN.		IKE Authentication Meth	od			
(such as 5551234, draytek.com or 123.45.	.67.89)	Pre-Shared Key				
		IKE Pre-Shared Key				
		O Digital Signature(X.5	U9)			
		IPSec Security Method				
		Medium(AH)				
		O High(ESP) DES with	out Authentication	1 🗡		
		Advanced				
		Index(1-15) in Schedule	Setup:			
		,, _	,			
		Callback Eurotian (CPC)	ור			
		Callback Function (CBCI Require Remote to				
		Provide ISDN Numb				
Enable this profile	Che	nection. ock here to active the drop down a	•		monor W/	AN interface
VPN Connection Through		the drop down i this profile. This				
	VP	N Connection T	hrough:	WAN1 WAN1 WAN1 WAN2 WAN2	First Only First	
	WA	N1 First - Whil	e connecti	ing, the i	outer will	l use WAN1
	as the first channel for VPN connection. If WAN1 fails, the router will use another WAN interface instead.					
	WAN1 Only - While connecting, the router will use WAN1					
	as the only channel for VPN connection.					
	•					
	WAN2 First - While connecting, the router will use WAN2 as the first channel for VPN connection. If WAN2 fails, the					
		er will use anoth				v2 rans, the
						Luca WAND
		N2 Only - Whil		-		I use wANZ
	as ti	he only channel	tor VPN c	onnectic	on.	
Call Direction	Spec	ify the allowed	call direct	ion of th	is LAN-te	o-LAN profile.
		h:-initiator/respo				1
		l-Out- initiator of				
		l-In- responder of				
		•	•			
Always On or Idle Timeout		-	o enable r	outer alv	vays keep	O VPN
	con	nection.				

	Idle Timeout: The default value is 300 seconds. If the connection has been idled over the value, the router will drop the connection.
Enable PING to keep alive	This function is to help the router to determine the status of IPSec VPN connection, especially useful in the case of abnormal VPN IPSec tunnel disruption. For details, please refer to the note below. Check to enable the transmission of PING packets to a specified IP address.
PING to the IP	Enter the IP address of the remote host that located at the other-end of the VPN tunnel.
	Enable PING to Keep Alive is used to handle abnormal IPSec VPN connection disruption. It will help to provide the state of a VPN connection for router's judgment of redial. Normally, if any one of VPN peers wants to disconnect the connection, it should follow a serial of packet exchange procedure to inform each other. However, if the remote peer disconnect without notice, Vigor router will by no where to know this situation. To resolve this dilemma, by continuously sending PING packets to the remote host, the Vigor router can know the true existence of this VPN connection and react accordingly. This is independent of DPD (dead peer detection).
ISDN	Build ISDN LAN-to-LAN connection to remote network. You should set up Link Type and identity like User Name and Password for the authentication of remote server. You can further set up Callback (CBCP) function below. This feature is useful for <i>i</i> model only.
РРТР	Build a PPTP VPN connection to the server through the Internet. You should set the identity like User Name and Password below for the authentication of remote server.
IPSec Tunnel	Build an IPSec VPN connection to the server through Internet.
L2TP with	 Build a L2TP VPN connection through the Internet. You can select to use L2TP alone or with IPSec. Select from below: None: Do not apply the IPSec policy. Accordingly, the VPN connection employed the L2TP without IPSec policy can be viewed as one pure L2TP connection. Nice to Have: Apply the IPSec policy first, if it is applicable during negotiation. Otherwise, the dial-out VPN connection becomes one pure L2TP connection. Must: Specify the IPSec policy to be definitely applied on the L2TP connection.
User Name	This field is applicable when you select ISDN, PPTP or L2TP with or without IPSec policy above.
Password	This field is applicable when you select ISDN, PPTP or L2TP with or without IPSec policy above.
PPP Authentication	This field is applicable when you select ISDN, PPTP or L2TP with or without IPSec policy above. PAP/CHAP is the most common selection due to wild compatibility.

VJ compression	This field is applicable when you select ISDN, PPTP or L2TP with or without IPSec policy above. VJ Compression is used for TCP/IP protocol header compression. Normally set to Yes to improve bandwidth utilization.	
IKE Authentication Method	This group of fields is applicable for IPSec Tunnels and L2TF with IPSec Policy. Pre-Shared Key - Input 1-63 characters as pre-shared key. Digital Signature (X.509) - Select one predefined Profiles set in the VPN and Remote Access >> IPSec Peer Identity .	
IPSec Security Method	This group of fields is a must for IPSec Tunnels and L2TP with IPSec Policy.	
Medium	Authentication Header (AH) means data will be authenticated, but not be encrypted. By default, this option is active.	
	 High (ESP-Encapsulating Security Payload)- means payload (data) will be encrypted and authenticated. Select from below: DES without Authentication -Use DES encryption algorithm and not apply any authentication scheme. DES with Authentication-Use DES encryption algorithm and apply MD5 or SHA-1 authentication algorithm. 3DES without Authentication-Use triple DES encryption algorithm and not apply any authentication scheme. 3DES without Authentication-Use triple DES encryption algorithm and not apply any authentication scheme. 3DES with Authentication-Use triple DES encryption algorithm and apply MD5 or SHA-1 authentication scheme. 3DES with Authentication-Use triple DES encryption algorithm and apply MD5 or SHA-1 authentication algorithm and apply MD5 or SHA-1 authentication algorithm and not apply any authentication scheme. AES with Authentication-Use AES encryption algorithm and not apply any authentication scheme. 	1
Advanced	Specify mode, proposal and key life of each IKE phase, Gateway etc. The window of advance setup is shown as below:	
	Ite advanced settings - Microsoft Internet Explorer	
	IKE advanced settings - Microsoft Internet Explorer IKE advanced settings IKE phase 1 mode • Main mode • Aggressive mode IKE phase 1 proposal DES_MD5_G1/DES_SHA1_G1/3DES_MD5_G1/3DES_MD5_G2 IKE phase 2 proposal HMAC_SHA1/HMAC_MD5 IKE phase 1 key lifetime 28800 (900 ~ 86400) IKE phase 2 key lifetime 3600 (600 ~ 86400) Perfect Forward Secret Disable OK Close	

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

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

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

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

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

Callback Function (for *i* models only)

The callback function provides a callback service as a part of PPP suite only for the ISDN dial-in user. The router owner will be charged the connection fee by the telecom. **Require Remote to Callback-**Enable this to let the router to require the remote peer to callback for the connection afterwards.

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

3. Dial-In Settings		
Allowed Dial-In Type		
ISDN		Username ???
🗹 РРТР		Password
🗹 IPSec Tunnel		VJ Compression 💿 On 🔘 Off
L2TP with IPSec Poli	cy None 💌	IKE Authentication Method
	r Domoto VDN Catowa	Pre-Shared Key
Peer ISDN Number or Pe	or Remote VPN Gateway eer VPN Server IP	IKE Pre-Shared Key
		Digital Signature(X.509)
or Peer ID		None 💌
		IPSec Security Method
		Medium (AH)
		High (ESP)
		DES V 3DES V AES
		Callback Function (CBCP)
		Enable Callback Function
		Use the Following Number to Callback
		Callback Number
		Callback Budget 0 minute(s)
4. TCP/IP Network Settings	;	
My WAN IP	0.0.0.0	RIP Direction Disable 💌
Remote Gateway IP	0.0.0.0	From first subnet to remote network, you have to do
Remote Network IP	0.0.0.0	Route 🗸
Remote Network Mask	255.255.255.0	Change default route to this VPN tunnel (Only
	More	single WAN support this)
<u> </u>		
	OK (Clear Cancel
Allowed Dial-In Type	e Determine t	the dial-in connection with different types.
ISDN	Allow the r	remote ISDN LAN-to-LAN connection. You
		the User Name and Password of remote dial-in us
		s feature is useful for <i>i</i> model only. In addition, y set up Callback function below.
РРТР	Allow the r	emote dial-in user to make a PPTP VPN
		through the Internet. You should set the User
	Name and I	Password of remote dial-in user below.
PSec Tunnel	Allow the r	remote dial-in user to trigger an IPSec VPN
	connection	through Internet.

Allow the remote dial-in user to make a L2TP VPN

alone or with IPSec. Select from below:

viewed as one pure L2TP connection.

becomes one pure L2TP connection.

connection through the Internet. You can select to use L2TP

None - Do not apply the IPSec policy. Accordingly, the VPN connection employed the L2TP without IPSec policy can be

Nice to Have - Apply the IPSec policy first, if it is applicable during negotiation. Otherwise, the dial-in VPN connection

Vigor2930 Series User's Guide

L2TP

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

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

Vigor2930 Series User's Guide

interface (WAN 1 or WAN 2) on **WAN** >> General Setup for enabling such setting.

3.9.7 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

)ial-out Tool				Refres	sh Seconds	5 : 10 🔽 Refresh
			~	Dial		
PN Connection Status						
urrent Page: 1					Page M	No. GO >>
VPN Type Remote IP	Virtual Network	Tx Pkts	Tx Rate	Rx Pkts	Rx Rate	UpTime
					ata is encr ata isn't er	

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.

3.10 Certificate Management

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

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

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

Below shows the menu items for Certificate Management.

Certificate Management
Local Certificate
Trusted CA Certificate
Certificate Backup

3.10.1 Local Certificate

Certificate Management >> Local Certificate

509 Local Certificate C	Configuration		
Name	Subject	Status	Modify
Local			View Delete
GENERATE X509 Local Cer	IMPORT REFRESH		
			~
			~

Generate

Click this button to open Generate Certificate Request window.

Subject Alternative Name					
Туре	P Adress				
lb					
inbject Name					
Country (C)					
State (ST)					
Location (L)					
Orginization (0)					
Orginization Unit (OU)					
Common Name (CN)					
Email (E)					
Sey Type	REA -				
ley Size	1112a (ba (b))				

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

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

After clicking **Generate**, the generated information will be displayed on the window below:

Name	Subject	Status	Modify
Local /C=TW/O=Draytek/OU=RD/emailA		Requesting	View Delete
ENERATE	IMPORT REFRESH		
X509 Lo	cal Certificate Request		
MIIBsj BgNVBA MAOGCS blo1kt /rGhuV RZjkRM	EGIN CERTIFICATE REQUEST CCARSCAQAwUDELMAKGA1UEBhMCVFcxEDAO sTAIJEMSIwIAYJKoZIhvcNAQkBFhNzZXJ2 qGSIb3DQEBAQUAA4GNADCBiQKBgQDPioah 9cTdLUDaFk6s8d3wDeQytoV1LBJz2IDFOx TKd9j6PlcrnkP7du84t23tWBdMD4W5c8Vm aHEWpVpwIDAQABoCIwIAYJKoZIhvcNAQkO	aWN1QGRyYX1OZ u/gFQaYB1ce5O jX6ip7ev187tw SyDjShLhjdxVY MRMwETAPBgNVH	WsuY29tMIGf ERSDfWknIdH wTsg41g26Qk PWpNKVIrOT2 ≣ REECDAGhwTA
ikisNd	DGCSqGSIb3DQEBBQUAA4GBAB43O4N9nod8 ZUoUEnKcejeOndc+H83VDA23ACEJpzTPFx rvYqeZybCrSjRU1PN1Hccfo7ANJ/M/D1EP m0	qklbeZo7a+wE5	7/+0VhNagBa

Certificate Management >> Local Certificate

VoIPon www.voipon.co.uk sales@voipon.co.uk Tel: +44 (0)1245 808195 Fax: +44 (0)1245 808299

3.10.2 Trusted CA Certificate

Trusted CA certificate lists three sets of trusted CA certificate.

X509 Trusted CA Certificate Configuration

 	View Delete
 	View Delete
 	View Delete

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

Certificate Management >> Trusted CA Certificate

mport 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 - Microsoft Inter	net Explorer					
			~				
	Certificate Detail Information						
	Certificate Name:	Trusted CA-1					
	Issuer:						
	Subject:						
	Subject Alternative Name:						
	Valid From:						
	Valid To:						
		Close					
			~				

3.10.3 Certificate Backup

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

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

Certificate Mana	gement >> Certificate Backup
Certificate Back	up / 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.

3.11 VoIP

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

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

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

sip: user:password @ host: port

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

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

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

• Calling via SIP Servers

First, the Vigor V models of yours will have to register to a SIP Registrar by sending

registration messages to validate. Then, both parties' SIP proxies will forward the sequence of messages to caller to establish the session.

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



The major benefit of this mode is that you don't have to memorize your friend's IP address, which might change very frequently if it's dynamic. Instead of that, you will only have to using **dial plan** or directly dial your friend's **account name** if you are with the same SIP Registrar. Please refer to the **section 4.5.1**.

Peer-to-Peer

Before calling, you have to know your friend's IP Address. The Vigor VoIP Routers will build connection between each other. Please refer to the **section 4.5.2**.



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



3.11.1 DialPlan

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

Vigor2930 Series User's Guide

VoIP >> DialPlan Setup

DialPlan Configuration

Phone Book	
<u>Digit Map</u>	
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 2930V for setting the phone book.

VoIP >> DialPlan Setup

ndex	Phone number	Display Name	SIP URL	Loop through	Backup Phone Number	Status
<u>1.</u>	688	david	8201@iptel.org	None		v
<u>2.</u>				None		х
<u>3.</u>				None		х
<u>4.</u>				None		х
<u>5.</u>				None		х
<u>6.</u>				None		х
<u>7.</u>				None		х
<u>8.</u>				None		х
<u>9.</u>				None		х
<u>10.</u>				None		х
<u>11.</u>				None		х
<u>12.</u>				None		х
<u>13.</u>				None		х
<u>14.</u>				None		х
<u>15.</u>				None		х
<u>16.</u>				None		х
<u>17.</u>				None		х
18.				None		х
<u>19.</u>				None		х
<u>20.</u>				None		х

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

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

VoIP >> DialPl	an Setup			
Phone Book I	ndex No. 1			
🗹 Enable				
	Phone Number	688		
	Display Name	david		
	SIP URL	8201	@iptel.org	
Enable Phone Nu			Cancel nable this entry. number of this inde	ex. This can be any
I HORE I U	linder	•	ing digits 0-9 and *	•

number

Display Name	The Caller-ID that you want to be displayed on your friend's screen. This let your friend can easily know who's calling without memorizing lots of SIP URL Address.
SIP URL	Enter your friend's SIP Address

This page will differ for different models. Below is a sample page obtained from Vigor 2930VSn. The selection of **Loop through** and **Backup Phone Number** is only available for 2930VSn model.

VoIP >> DialPlan	Setup					
Phone Book Inde	x No. 1					
🗹 Enable						
	Phone Number		1	7		
	Display Name		Polly]		
	SIP URL		1112	@ fwd.pulver	r.com	
	Loop through		None 💌			
	Backup Phone Nu	umber]		
	(OK	Clear	Cancel		
Enable		Click t	his to enable thi	is entry.		
Phone Numbe	er	-	eed-dial numbe oose, using digi		idex. This can be an * .	ny number
Display Name		The Caller-ID that you want to be displayed on your friend's screen. This let your friend can easily know who's calling without memorizing lots of SIP URL Address.				
SIP URL		Enter y	your friend's SI	P Address		
Loop through	l		e model of Vigo lowing:	or 2930VS1	n, the selection sho	uld be as
		Loop) through		None None ISDN2-TE	
Backup Phon	e Number	for sor replace will be the loc switch when t telecon type in	ne reasons, the le e the VoIP phone e changed from V op through direc , the blare of ph the VoIP phone n co. might char	backup ph he number. VoIP phor tion chose one will a is switche rge you fo	ts or the Internet be one will be dialed of At this time, the p ne into PSTN call a m. Note that, during ppear for a short tin d into the PSTN ph r the connection fe PSTN number) for t	but to hone call ccording to g the phone me. And hone, the e. Please

Digit Map

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

VoIP >> DialPlan Setup

#	Enable	Prefix Number	Mode)	OP Number	Min Len	Max Len	Interface
1		03	Replace	*	8863	7	9	ISDN2-TE 🔽
2	✓	886	Strip	۷	886	8	10	ISDN2-TE 🔽
З			None	\mathbf{v}		0	0	ISDN2-TE
4			None	\sim		0	0	ISDN2-TE 🔽
5			None	\sim		0	0	ISDN2-TE
6			None	\sim		0	0	ISDN2-TE
7			None	\sim		0	0	ISDN2-TE
8			None	\sim		0	0	ISDN2-TE 🗸
9			None	\sim		0	0	ISDN2-TE
10			None	\sim		0	0	ISDN2-TE
11			None	\sim		0	0	ISDN2-TE
12			None	\sim		0	0	ISDN2-TE
13			None	\sim		0	0	ISDN2-TE
14			None	\sim		0	0	ISDN2-TE
15			None	\sim		0	0	ISDN2-TE
16			None	\sim		0	0	ISDN2-TE
١7			None	\sim		0	0	ISDN2-TE
18			None	\sim		0	0	ISDN2-TE
.9			None	\sim		0	0	ISDN2-TE
20			None	\sim		0	0	ISDN2-TE

Note: The length of Prefix Number should be between Min Len and Max Len. Min Len and Max Len should be between $0 \sim 11$.

OK Cancel

Prefix Number

Mode

Enable

The phone number set here is used to add, strip, or replace the OP number.

Check this box to invoke this setting.

None - No action. **Add** - When you choose this mode, the OP number will be added with the prefix number for calling out through the specific VoIP interface.

Strip - When you choose this mode, the OP number will be deleted by the prefix number for calling out through the specific VoIP interface. Take the above picture (Prefix Table Setup web page) as an example, the OP number of *886* will be deleted completely for the prefix number is set with *886*. **Replace** - When you choose this mode, the OP number will be replaced by the prefix number for calling out through the specific VoIP interface. Take the above picture (Prefix Table Setup web page) as an example, the prefix number of 03 will be replaced by 8863. For example: dial number of "031111111" will be changed to "88631111111" and sent to

	SIP server. Mode Replace V None Add Strip Replace
OP Number	The front number you type here is the first part of the account number that you want to execute special function (according to the chosen mode) by using the prefix number.
Min Len	Set the minimal length of the dial number for applying the prefix number settings. Take the above picture (Prefix Table Setup web page) as an example, if the dial number is between 7 and 9, that number can apply the prefix number settings here.
Max Len	Set the maximum length of the dial number for applying the prefix number settings.
Interface	Choose the one that you want to enable the prefix number settings from the saved SIP accounts. Please set up one SIP account first to make this interface available.

Call Barring

Call barring is used to block phone calls that are not welcomed.

VoIP >> DialPlan Setup

Index	Call Direction	Barring Type	Barring Number/URL/URI	Interface	Schedule	Status
<u>1.</u>						×
<u>2.</u>						×
<u>3.</u>						×
<u>4.</u>						×
<u>5.</u>						×
<u>6.</u>						×
<u>7.</u>						×
<u>8.</u>						×
<u>9.</u>						×
<u>10.</u>						×

Advanced: <u>Block Anonymous</u> <u>Block Unknown Domain</u> <u>Block IP Address</u>

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

VoIP >> DialPlan Setup

Call Barring Index No. 1	
✓ Enable	
Call Direction	IN 💌
Barring Type	Specific URI/URL 💌
Specific URI/URL	
Interface	All 💌
Index(1-15) in <u>Schedule</u> Setup	
ОК	Cancel

Enable	Click this to enable this entry.
Call Direction	Determine the direction for the phone call, IN – incoming call, OUT-outgoing call, IN & OUT – both incoming and outgoing calls.
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.
Interface	"All" means all the phone calls (including ISDN & PSTN) will be blocked with such mechanism. "ISDN" means only ISDN phone call will be blocked with such mechanism. All All ISDN
Index (1-15) in Schedule	Enter the index of schedule profiles to control the call barring according to the preconfigured schedules. Refer to section

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.

3.5.2 Schedule for detailed configuration.

For **Block Anonymous** – this function can block the incoming calls without caller ID on the interface (Phone 1 or Phone 2 or both) specified in the following window. Such controlling also can be done based on preconfigured schedules.

VolPon www.voipon.co.uk sales@voipon.co.uk Tel: +44 (0)1245 808195 Fax: +44 (0)1245 808299

VoIP >> Dialf	Plan Setup			
Call Barring	Block Anonymous			
🗹 Enable				
]]	interface		🗌 Phone1	Phone2
]	index(1-15) in <u>Schedule</u>	Setup	,	
Note:Block t	he incoming calls which (do not have tl	he caller ID.	
		ОК	Cancel	

For **Block Unknown Domain** – this function can block incoming calls from unrecognized domain that is not specified in SIP accounts. Such controlling also can be done based on preconfigured schedules.

VoIP >> Dia	IPIan Setup	
Call Barrin	g Block Unknown Domain	
🗹 Enable		
	Interface	Phone1 Phone2
	Index(1-15) in <u>Schedule</u> Setup	
Note:If the be blocked		t from the domain found in SIP accounts,the call should
	OK	Cancel

For **Block IP Address** – this function can block incoming calls coming from IP address. Such controlling also can be done based on preconfigured schedules.

VoIP >> DialPlan Setup	
Call Barring Block IP Address	
🗹 Enable	
Interface	Phone1 Phone2
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.
0	K Cancel

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

Regional		Se	<u>t to Factory Default</u>
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		
	OK	Cancel	

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.
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.

3.11.2 SIP Accounts

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

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

VoIP >> SIP Accounts

IP Acco	unts List						Refresh
index	Profile	Domain/Realm	Proxy	Account Name	Ring P	ort	Statu
1				change_me	Phone1 ISDN1-SO	Phone2	-
2				change_me	Phone1	Phone2	-
<u>3</u>				change_me	Phone1 ISDN1-SO	Phone2	-
<u>4</u>				change_me	Phone1	Phone2	-
<u>5</u>				change_me	Phone1 ISDN1-S0	Phone2	-
<u>6</u>				change_me	Phone1	Phone2	-
Z				change_me	Phone1 ISDN1-SO	Phone2	-
<u>8</u>				change_me	Phone1	Phone2	-
<u>9</u>				change_me	Phone1 ISDN1-SO	Phone2	-
<u>10</u>				change_me	Phone1 ISDN1-SO	Phone2	-
<u>11</u>				change_me	Phone1 ISDN1-SO	Phone2	-
<u>12</u>				change_me	Phone1	Phone2	-
	1.0.00				R: success regi -: fail to registe	stered on S er on SIP se	IP serv rver
AT Trav	ersal Settin STUN S						
	External	I IP:					
	SIP PIN	G Interval:	150	sec			

130

Index	Click this link to access into next page for setting SIP account.
Profile	Display the profile name of the account.
Domain/Realm	Display the domain name or IP address of the SIP registrar server.
Proxy	Display the domain name or IP address of the SIP proxy server.
Account Name	Display the account name of SIP address before @.
Ring Port	Specify which port will ring when receiving a phone call. Set Phone1, Phone2, ISDN1-S0 or ISDN-TE as the default ring port for the SIP account. If you choose Phone1, Phone2 or ISDN1-S0, the ISDN2-TE selection will be dimmed, vice versa. There are ten internal lines with numbers $(30 - 39)$ offered for ISDN-S0 . You can specify any one of them as ring port for specified SIP account. By the way, ISDN-S0 can be used by mapping with MSN numbers.
STUN Server	Type in the IP address or domain of the STUN server.
External IP	Type in the gateway IP address.
SIP PING interval	The default value is 150 (sec). It is useful for a Nortel server NAT Traversal Support.
Status	Show the status for the corresponding SIP account. \mathbf{R} means such account is registered on SIP server successfully. – means the account is failed to register on SIP server.
VolP >> SIP Accounts	

VoIP >> SIP Accounts

P Account Index No. 1		
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 proxy		
Display Name	(23 char max	.)
Account Number/Name	change_me	(63 char max.)
Authentication ID		(63 char max.)
Password		(63 char max.)
Expiry Time	1 hour 💌 3600 sec	
NAT Traversal Support	None 💌	
	Phone1 Phone2	
Ring Port	🗌 ISDN1-SO Any 🔽	
	ISDN2-TE	
Ring Pattern	1 🗸	

Assign a name for this profile for identifying. You can type similar name with the domain. For example, if the domain name is *draytel.org*, then you might set *draytel-1* in this field.

Vigor2930 Series User's Guide

Profile Name

Register via	If you want to make VoIP call winformation, please choose Non the goal. Some SIP server allow without registering. For such see Call without registration . Cho The system will select a proper	e and check the box to achieve s user to use VoIP function rver, please check the box of osing Auto is recommended. way for your VoIP call.
	Na Au W	one Y ne AN 1 AN 2 N//PN
SIP Port	Set the port number for sending building a session. The default set the same value in his/her Re	value is 5060. Your peer must
Domain/Realm	Set the domain name or IP addr	ess of the SIP Registrar server.
Proxy	Set domain name or IP address time you can type :port numbe specify that port as the destinati nat.draytel.org:5065)	r after the domain name to
Act as Outbound Proxy	Check this box to make the prov	xy acting as outbound proxy.
Display Name	The caller-ID that you want to b screen.	be displayed on your friend's
Account Number/Name	Enter your account name of SIP before @.	Address, e.g. every text
Authentication ID	Check the box to invoke this fur number used for SIP Authorizat setting value is the same as Acc for you to check the box and set	ion with SIP Registrar. If this ount Name, it is not necessary
Password	The password provided to you v service.	when you registered with a SIP
Expiry Time	The time duration that your SIP registration record. Before the ti send another register request to	ime expires, the router will
NAT Traversal Support	If the router (e.g., broadband rou internet by other device, you ha necessity.	· · · ·
	NAT Traversal Support	None None Stun Manual Nortel
	None – Disable this function.	re is Stun cerver provided for
	Stun – Choose this option if the your router.	are is stull server provided for
	Manual – Choose this option if	
	external IP address as the NAT	
	Nortel – If the soft-switch that y solution, you can choose this op	

Ring Port	or ISDN1-S0, the ISDN2-TE sversa. There are ten internal li	If you choose Phone 1, Phone 2 selection will be dimmed, vice ines with numbers $(30 - 39)$ a specify one of them or choose SIP account. By the way,
Ring Pattern	Choose a ring tone type for the Ring Pattern	e VoIP phone call. 1

3.11.3 Phone Settings

This page allows user to set phone settings for Phone1, Phone2, ISDN1-S0 and ISDN2-TE/S0 respectively.

VoIP >> Phone Settings

Index	Port	Call Feature	Codec	Tone	Gain (Mic/Speaker)	Default SIP Account	DTMF Relay
1	Phone1		G.729A/B	User Defined	5/5		InBand
2	Phone2		G.729A/B	User Defined	5/5		InBand
<u>3</u>	ISDN1-SO		G.729A/B	User Defined	5/5		InBand
<u>4</u>	ISDN2-TE 💌		G.729A/B	User Defined	5/5		InBand

RTP		
	Symmetric RTP	
	Dynamic RTP Port Start	10050
	Dynamic RTP Port End	15000
	RTP TOS	IP precedence 5
		ОК

Phone List

Port – There are four phone ports provided here for you to configure. Three (Index 1 to 3) are fixed and one (Index 4) is configurable. Phone1 and Phone2 allow you to set general settings for PSTN phones. ISDN1-S0 and ISDN2-TE allow you to set common settings for ISDN network connection. ISDN2 port is configurable. Please use the drop down list to choose ISDN2-TE for Internet connection or choose ISDN2-S0 (ISDN intern) for ISDN phone. In addition, you can connect six phones to this router in certain case. Please refer to Section 4-1 for detailed information of ISDN phone/network connection. If you want to enable function of ISDN On-Net/Off-Net, you have to choose ISDN2-TE. Call Feature – A brief description for call feature will be shown in this field for your reference. Codec – The default Codec setting for each port will be

6

Vigor2930 Series User's Guide

shown in this field for your reference. You can click the number below the Index field to change it for each phone port. **Tone** - Display the tone settings that configured in the advanced settings page of Phone Index.

Gain - Display the volume gain settings for Mic/Speaker that configured in the advanced settings page of Phone Index. **Default SIP Account** – "draytel_1" is the default SIP account. You can click the number below the Index field to change SIP account for each phone port.

DTMF Relay – Display DTMF mode that configured in the advanced settings page of Phone Index.

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

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

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

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

Manual	
IP precedence 1	
IP precedence 2	
IP precedence 3	
IP precedence 4	
IP precedence 5	
IP precedence 6	
IP precedence 7	
AF Class1 (Low Drop)	
AF Class1 (Medium Drop)	
AF Class1 (High Drop)	
AF Class2 (Low Drop)	
AF Class2 (Medium Drop)	
AF Class2 (High Drop)	
AF Class3 (Low Drop)	
AF Class3 (Medium Drop)	
AF Class3 (High Drop)	
AF Class4 (Low Drop)	
AF Class4 (Medium Drop)	
AF Class4 (High Drop)	
EF Class	
Manual	~

RTP TOS

Detailed Settings for Phone1/Phone2 Port

Click the number link of each port, you can access into the following page for configuring Phone settings. Below is the sample page for Phone1.

RTP

VoIP >> Phone Settings

Phone1				
Call Feature		Codecs		
🔲 Hotline		Prefer Codec	G.729A/B (8Kbps) 🔽	
Session Timer	3600 sec		Single Codec	
🔲 T.38 Fax Function		Packet Size	20ms 💙	
Call Forwarding	Disable 💌	Voice Active Detector	Off 🔽	
SIP URL		Default SIP Account		
Time Out	30 sec		nen account registered	
🔲 DND(Do Not Disturb) M	ode	Play utal torie only wr	ien account registereu	
Index(1-15) in <u>Scheo</u>	<u>lule</u> Setup:	Default Call Route		
		🔿 To ISDN: Dial 🛛 *#	for VoIP	
Note: Action and Idle be ignored.	e Timeout settings will	⊙ To VoIP: Dial #	for ISDN	
Index(1-60) in <u>Phone</u>	Book as Exception List:			
	,,,,,			
🔲 CLIR (hide caller ID)				
🔲 Call Waiting				
🔲 Call Transfer				
	OK Car	ncel Advanced		
Hotline	Check the box to enable it. Type in the SIP URL in the field for dialing automatically when you pick up the phone set.			
Session Timer		Check the box to enable the function. In the limited time that		

you set in this field, if there is no response, the connecting call will be closed automatically.

Call ForwardingThere are four options for you to choose. Disable is to close
call forwarding function. Always means all the incoming calls
will be forwarded into SIP URL without any reason. Busy
means the incoming calls will be forwarded into SIP URL
only when the local system is busy. No answer means if the
incoming calls do not receive any response, they will be
forwarded to the SIP URL by the time out.

Disable	*
Disable	
Always	
Busy	
No Answer	

SIP URL – Type in the SIP URL (e.g., aaa@draytel.org or abc@iptel.org) as the site for call forwarded. **Time Out** – Set the time out for the call forwarding. The default setting is 30 sec.

DND (Do Not Disturb) mode

Set a period of peace time without disturbing by VoIP phone call. During the period, the one who dial in will listen busy tone, yet the local user will not listen any ring tone.

Index (1-15) in Schedule - Enter the index of schedule profiles to control the DND mode according to the preconfigured schedules. Refer to section **3.5.2 Schedule** for

	detailed configuration. Index (1-60) in Phone Book - Enter the index of phone book profiles. Refer to section 3.11.1 DialPlan – Phone Book for detailed configuration.	
CLIR (hide caller ID)	Check this box to hide the car phone set.	ller ID on the display panel of the
Call Waiting	appear to tell the user new ph	function. A notice sound will one call is waiting for your pick up the waiting phone call.
Call Transfer		function. Click hook flash to hen the phone call connection The other two sides can
Prefer Codec	The codec used for each call party before each session, and choice. The default codec is of bandwidth while maintaining If your upstream speed is onl codec. It is better for you to h you would like to use G.711.	G.729A/B; it occupies little good voice quality. y 64Kbps, do not use G.711 have at least 256Kbps upstream if
	Prefer Codec	G.711A (64Kbps) 💙 G.711MU (64Kbps)

G.711A (64Kbps) G.711MU (64Kbps) G.729A/B (8Kbps) G.723 (6.4kbps) G.726_32 (32kbps)

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

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

Packet Size

20ms	*
10ms	
20ms	
30ms	
40ms	
50ms	
60ms	

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

Voice Active Detector



Default SIP Account You can set SIP accounts (up to six groups) on SIP Account page. Use the drop down list to choose one of the profile names for the accounts as the default one for this phone setting.

	Play dial tone only when account registered - Check this box to invoke the function.
Default Call Route	It determines the default direction for the call route of the router.
	To ISDN (for VoIP) - The router is set by using ISDN call.
	To change ISDN call into VoIP call, please dial the character
	in this field for transferring. The character that you can type
	can be *, #, and 0~9.
	To VoIP (for ISDN) - The router is set by using VoIP call. To
	change VoIP call into ISDN call, please dial the character in
	this field for transferring. The character that you can type can
	be *, #, and 0~9.

. . .

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

VoIP >> Phone Settings

Tone Sett	ings						
Region	User Defined	*					
		Low Freq (Hz)	High Freq (Hz)	T on 1 (msec)	T off 1 (msec)	T on 2 (msec)	T off 2 (msec)
Dia	l tone	350	440	0	0	0	0
Ringi	ing tone	400	450	400	200	400	2000
Bus	y tone	400	0	375	375	0	0
Conges	stion tone	0	0	0	0	0	0
Volume G	Gain			DTMF			
Mic Gain(1-10) 5		DTMF Mod	de	InBand	4		
Speaker Gain(1-10) 5		Payload T	ype(RFC2833)) 101			
MISC							
Dial Tone	Power Level	1 2	7				
Ring Freq	luency	2	5				

Region

Select the proper region which you are located. The common settings of **Caller ID Type**, **Dial tone**, **Ringing tone**, **Busy tone** and **Congestion tone** will be shown automatically on the page. If you cannot find out a suitable one, please choose **User Defined** and fill out the corresponding values for dial tone, ringing tone, busy tone, congestion tone by yourself for VoIP phone.

Tone Setti	ings	
Region	User Defined 🔽]
···· 9····	User Defined	ow
	UK	(H
Dia	US Denmark	0
Ringi	ltalγ	10
Bus	Germany Netherlands	10
Conges	Portugal Sweden	
	Australia	
Mic Gain(Slovenia Czech	
Speaker (
MISC		

Also, you can specify each field for your necessity. It is recommended for you to use the default settings for VoIP communication. Volume Gain Mic Gain (1-10)/Speaker Gain (1-10) - Adjust the volume of microphone and speaker by entering number from 1-10. The larger of the number, the louder the volume is. MISC Dial Tone Power Level - This setting is used to adjust the loudness of the dial tone. The smaller the number is, the louder the dial tone is. It is recommended for you to use the default setting. **Ring Frequency** - This setting is used to drive the frequency of the ring tone. It is recommended for you to use the default setting. DTMF DTMF Mode – There are four DTMF modes for you to choose. InBand - Choose this one then the Vigor will send the DTMF tone as audio directly when you press the keypad on the phone **OutBand** - Choose this one then the Vigor will capture the keypad number you pressed and transform it to digital form then send to the other side; the receiver will generate the tone according to the digital form it receive. This function is very useful when the network traffic congestion occurs and it still can remain the accuracy of DTMF tone. SIP INFO- Choose this one then the Vigor will capture the DTMF tone and transfer it into SIP form. Then it will be sent to the remote end with SIP message. DTMF mode InBand InBand OutBand (RFC2833)

Payload Type (rfc2833) - Choose a number from 96 to 127, the default value was 101. This setting is available for the OutBand (RFC2833) mode.

SIP INFO (cisco format) SIP INFO (nortel format)

VolPon www.voipon.co.uk sales@voipon.co.uk Tel: +44 (0)1245 808195 Fax: +44 (0)1245 808299

Detailed Settings for ISDN1-S0 Port

VoIP >> Phone Settings

Click the number link of Index 3 (ISDN1-S0), you can access into the following page for configuring Phone settings.

Call Feature	Codecs	
Hotline	Prefer Codec	G.729A/B (8Kbps) 🛛 🖌
Session Timer 3600 sec		Single Codec
Call Forwarding Disable 🔽	Packet Size	20ms 🚩
SIP URL	Voice Active Detector	Off 🔽
Time Out 30 sec	Default SIP Account	~
🔲 DND(Do Not Disturb) Mode	SIP Account for MSN30	×
Index(1-15) in <u>Schedule</u> Setup:	SIP Account for MSN31	×
	SIP Account for MSN32	×
Note: Action and Idle Timeout settings will be ignored.	SIP Account for MSN33	~
Index(1-60) in <u>Phone Book</u> as Exception List:	SIP Account for MSN34	~
	SIP Account for MSN35	×
CLIR (hide caller ID)	SIP Account for MSN36	×
Call Waiting	SIP Account for MSN37	×
Call Transfer	SIP Account for MSN38	×
	SIP Account for MSN39	×
	🔲 Play dial tone only w	hen account registered
	Default Call Route	
	◯ To ISDN: Dial *#	for VoIP
	⊙ To VoIP: Dial #*	for ISDN

Hotline	Check the box to enable it. Type in the SIP URL in the field for dialing automatically when you pick up the phone set.
Session Timer	Check the box to enable the function. In the limited time that you set in this field, if there is no response, the connecting call will be closed automatically.
Call Forwarding	There are four options for you to choose. Disable is to close call forwarding function. Always means all the incoming calls will be forwarded into SIP URL without any reason. Busy means the incoming calls will be forwarded into SIP URL only when the local system is busy. No answer means if the incoming calls do not receive any response, they will be forwarded to the SIP URL by the time out.

Disable	*
Disable	
Always	
Busy	
No Answer	

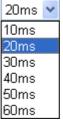
SIP URL – Type in the SIP URL (e.g., aaa@draytel.org or

	abc@iptel.org) as the site Time Out – Set the time default setting is 30 sec.	e for call forwarded. out for the call forwarding. The			
DND (Do Not Disturb) mode	call. During the period, th	Set a period of peace time without disturbing by VoIP phone call. During the period, the one who dial in will listen busy tone, yet the local user will not listen any ring tone.			
	profiles to control the DN preconfigured schedules. detailed configuration. Index (1-60) in Phone B	 e - Enter the index of schedule ID mode according to the Refer to section 3.5.2 Schedule for ook - Enter the index of phone book 3.10.1 DialPlan – Phone Book for 			
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.				
Prefer Codec	The codec used for each of party before each session choice. The default codec bandwidth while maintain If your upstream speed is	only 64Kbps, do not use G.711 to have at least 256Kbps upstream if			
	Prefer Codec	G.711A (64Kbps) G.711MU (64Kbps) G.711A (64Kbps) G.729A/B (8Kbps) G.723 (6.4kbps) G.726_32 (32kbps)			
	Single Codec – If the box is checked, only the selected Codec				

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

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

Packet Size



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.

Off <mark>∨</mark> Off On

Default SIP Account You can set SIP accounts (up to six groups) on SIP Account page. Use the drop down list to choose one of the profile names for the accounts as the default one for this phone setting. ISDN-S0 port can pick up multiple incoming calls simultaneously. Therefore different phone sets (MSN30 to MSN39) can use different SIP accounts to call out through this port. Play dial tone only when account registered - Check this box to invoke the function. **Default Call Route** It determines the default direction for the call route of the router. To ISDN (for VoIP) - The router is set by using ISDN call. To change ISDN call into VoIP call, please dial the character in this field for transferring. The character that you can type can be *, #, and 0~9. To VoIP (for ISDN) - The router is set by using VoIP call. To change VoIP call into ISDN call, please dial the character in this field for transferring. The character that you can type can be *, #, and 0~9.

Voice Active Detector

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

141

VoIP >> Phone Settings

Advance Settings >>	> ISDN1-S0
---------------------	------------

Tone Setting	js						
Region U	ser Defined	~					
		Low Freq (Hz)	High Freq (Hz)	T on 1 (msec)	T off 1 (msec)	T on 2 (msec)	T off 2 (msec)
Dial t	one	350	440	0	0	0	0
Ringing	j tone	400	450	400	200	400	2000
Busy	tone	400	0	375	375	0	0
Congesti	on tone	0	0	0	0	0	0
Volume Gai	n			DTMF			
Mic Gain(1-	10)	5		DTMF Mod	de	InBand	
Speaker Ga	in(1-10)	5		Payload T	ype(RFC2833)	101	
MISC							
Dial Tone P	ower Level	27					
Ring Freque	ency	25					
MSN Alias							
MSN 30		50		MSN 35			
MSN 31				MSN 36			
MSN 32				MSN 37			
MSN 33				MSN 38			
MSN 34				MSN 39			

ΟK

Region

Select the proper region which you are located. The common settings of **Caller ID Type**, **Dial tone**, **Ringing tone**, **Busy tone** and **Congestion tone** will be shown automatically on the page. If you cannot find out a suitable one, please choose **User Defined** and fill out the corresponding values for dial tone, ringing tone, busy tone, congestion tone by yourself for VoIP phone.

Tone Setti	ings	
Region	User Defined 💌	
	User Defined	ow I
	UK	(H)
Dia	US Denmark	0
Ringi	ltalγ	10
Bus	Germany Netherlands	0
Conges	Portugal Sweden	
	Australia	
Mic Gain(Slovenia Czech	
Speaker (
MISC		

Cancel

Also, you can specify each field for your necessity. It is recommended for you to use the default settings for VoIP communication.

Volume Gain	Mic Gain (1-10)/Speaker Gain (1-10) - Adjust the volume of microphone and speaker by entering number from 1- 10. The larger of the number, the louder the volume is.		
MISC	 Dial Tone Power Level - This setting is used to adjust the loudness of the dial tone. The smaller the number is, the louder the dial tone is. It is recommended for you to use the default setting. Ring Frequency - This setting is used to drive the frequency of the ring tone. It is recommended for you to use the default setting. 		
DTMF	setting. DTMF Mode – There are four DTMF modes for you to choose. InBand - Choose this one then the Vigor will send the tone as audio directly when you press the keypad on the OutBand - Choose this one then the Vigor will captured keypad number you pressed and transform it to digital then send to the other side; the receiver will generate the according to the digital form it receive. This function is useful when the network traffic congestion occurs and can remain the accuracy of DTMF tone. SIP INFO- Choose this one then the Vigor will captured DTMF tone and transfer it into SIP form. Then it will be to the remote end with SIP message. DTMF mode InBand OutBand (RFC2833) SIP INFO (cisco format) SIP INFO (nortel format)		send the DTMF pad on the phone Il capture the to digital form enerate the tone function is very cours and it still ill capture the en it will be sent
	Payload Type (rfc283) the default value was 10 OutBand (RFC2833) m	01. This setting is avai	
MSN Alias	You can modify the MS 30 – 39) with any numb the box of MSN 30.	-	
	MSN Alias		

MSN Alias		
MSN 30	50	MSN 35
MSN 31		MSN 36
MSN 32		MSN 37
MSN 33		MSN 38
MSN 34		MSN 39

Later you will find MSN 30 has been replaced with MSN50 in all related pages. See the following figures for examples (pages of **VoIP>>SIP Accounts** and **VoIP>>Phone Settings**).

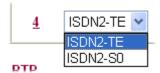
VoIP >> SIP Account

Index	Profile	Domain/Realm	Proxy	Account Name	Ring Port
					Phone1 Phone2
1				change_me	ISDN1-S0 Any 💙
					ISDN2-TE Any
<u>2</u>				change_me	Phone1 31 ne2 32 ISDN1-S0 33
					ISDN2-TE 34

ISDN1-S0					
Call Feature				Codecs	
🔲 Hotline				Prefer Codec	G.729A/B (8Kbps) 🛛 🖌
🔲 Session Timer	3600	sec			Single Codec
Call Forwarding	Disable	*		Packet Size	20ms 💌
SIP URL				Voice Active Detector	Off 💙
Time Out	30	sec		Default SIP Account	*
DND(Do Not Disturb)	Mode			SIP Account for	
Index(1-15) in <u>Schedule</u> Setup:			MSN 50	~	
				MSN 31	*
Note: Action and Id	dle Timeou	t settinas wi			

Detailed Settings for ISDN2-TE Port (Available for VSn model only)

Vigor2930VSn allows users to switch the function of ISDN2 port between TE or S0 mode. Please use the drop down list to choose the one you want.



144

If you choose ISDN2-S0, please refer to Detailed Settings for Phone1, Phone2, ISDN1-S0 for the configuration. However, if you choose ISDN-TE and click the number link for that port, you will see the following page.

VoIP	>>	Phone	Settings
		1 HOHE	Settings

ISDN2-TE							
Call Feature		Codecs					
🔲 Hotline	ISDN->VoIP 🔽	Prefer Codec	G.729A/B (8Kbps) 💌				
			Single Codec				
🔲 Session Timer	3600 sec	Packet Size	20ms 💌				
Call Forwarding	Disable 👻	Voice Active Detector	Off 🖌				
SIP URL							
Time Out	30 sec	Default SIP Account					
DND(Do Not Distur	b) Mode	Play dial tone only	when account registered				
Index(1-15) in §	· · · · · · · · · · · · · · · · · · ·	EXO feature	EX0 feature				
		Enable VoIP to ISDN	(Off-Net) Calls				
Note: Action and	d Idle Timeout settings will		Enable ISDN to VoIP (On-Net) Calls				
be ignored	1. –	Loop Through to Phone Port					
Index(1-60) in P	hone Book as Exception List		MSN mapping ring port is				
		not set then this will take effect. Broadcast call Phone1 Phone2					
🔲 CLIR (hide caller ID))						
		🔘 Loop Through to	ISDN1-S0 Port				
	ОК С	ancel Advanced					
Iotline		• •	n the SIP URL in the field u pick up the phone set.				
Session Timer	you set in th		on. In the limited time that response, the connecting cal				
Call Forwarding	call forward	ing function. Always	hoose. Disable is to close means all the incoming calls ithout any reason. Busy				

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



SIP URL – Type in the SIP URL (e.g., aaa@draytel.org or abc@iptel.org) as the site for call forwarded. **Time Out** – Set the time out for the call forwarding. The default setting is 30 sec.

DND (Do Not Disturb)Set a period of peace time without disturbing by VoIP phone
call. During the period, the one who dial in will listen busy
tone, yet the local user will not listen any ring tone.

Index (1-15) in Schedule - Enter the index of schedule profiles to control the DND mode according to the preconfigured schedules. Refer to section **3.5.2 Schedule** for detailed configuration.

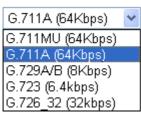
Index (1-60) in Phone Book - Enter the index of phone book

profiles. Refer to section **3.10.1 DialPlan – Phone Book** for detailed configuration.

CLIR (hide caller ID) Check this box to hide the caller ID on the display panel of the phone set.

Prefer CodecSelect one of five codecs as the default for your VoIP calls.
The codec used for each call will be negotiated with the peer
party before each session, and so may not be your default
choice. The default codec is G.729A/B; it occupies little
bandwidth while maintaining good voice quality.
If your upstream speed is only 64Kbps, do not use G.711
codec. It is better for you to have at least 256Kbps upstream if
you would like to use G.711.

Prefer Codec



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

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

Packet Size

20ms	*
10ms	
20ms	
30ms	
40ms	
50ms	
60ms	

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

Voice Active Detector



Default SIP AccountYou can set SIP accounts (up to six groups) on SIP Account
page. Use the drop down list to choose one of the profile
names for the accounts as the default one for this phone
setting.Play dial tone only when account registered - Check this

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

Enable ISDN to VoIP (On-Net) Calls – Check this box to make all the outgoing calls from ISDN line to be forwarded to receivers by Internet.

Enable VoIP to ISDN (Off-Net) Calls –Check this box to make all the incoming calls coming from Internet to be forwarded to receivers by ISDN line.

Loop Through to Phone Port – Choose this radio button to make all the calls controlled by traditional PSTN phone. It will tack effect only if MSN mapping ring port is not

FXO Feature

configured. In addition, you can specify which port (both phone 1 and phone 2, phone 1 only or phone 2 only) will ring. **Loop Through to ISDN1-S0 Port** – Choose this radio button to make all the calls controlled by ISDN line.

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

Tone Settings								
Region User Defined	*							
	Low Freq (Hz)	High Freq (Hz)	T on 1 (msec)	T off 1 (msec)	T on 2 (msec)	T off 2 (msec)		
Dial tone	350	440	0	0	0	0		
Ringing tone	400	450	400	200	400	2000		
Busy tone	400	0	375	375	0	0		
Congestion tone	0	0	0	0	0	0		
Volume Gain DTMF								
Mic Gain(1-10)	5		DTMF Mode		InBand	InBand 🖌 🖌		
Speaker Gain(1-10)	5		Payload T	ype(RFC2833)) 101			
MISC								
Dial Tone Power Leve	1 27	7						
Authentication PIN Code								
Check for ISDN to VoIP Calls 0000								
🔲 Check for VoIP to	Check for VoIP to ISDN Calls 0000							
				_				
		OK	Cancel					

Advance Settings >> ISDN2-TE

Region

Select the proper region which you are located. The common settings of **Caller ID Type**, **Dial tone**, **Ringing tone**, **Busy tone** and **Congestion tone** will be shown automatically on the page. If you cannot find out a suitable one, please choose **User Defined** and fill out the corresponding values for dial tone, ringing tone, busy tone, congestion tone by yourself for VoIP phone.

Tone Sett	ings	
Region	User Defined	*
	User Defined	ow
	UK	(H
Dia	US Denmark	0
Ringi	Italy	10
Bus	Germany Netherlands	0
Conges	Portugal Sweden	
Volume G	Australia	
Mic Gain(Slovenia Czech	
Speaker (Slovakia	

MISC

Also, you can specify each f recommended for you to use communication.	field for your necessity. It is the default settings for VoIP			
	Gain (1-10) - Adjust the volume of entering number from 1- 10. The ider the volume is.			
loudness of the dial tone. The	his setting is used to adjust the ne smaller the number is, the recommended for you to use the			
 Check for ISDN to VoIP Calls – Set a pin code for the router to authenticate which one is allowed to dial ISDN to VoIP call. The figure that you can type in this field is limited from three to eight with digits from zero to nine. Check for VoIP to ISDN Calls - Set a pin code for the router to authenticate which one is allowed to dial VoIP to ISDN call. The figure that you can type in this field is limited from three to eight with digits from zero to nine. 				
tone as audio directly when OutBand: Choose this one keypad number you pressed then send to the other side; t according to the digital form useful when the network tra can remain the accuracy of I SIP INFO: Choose this one	en the Vigor will send the DTMF you press the keypad on the phone then the Vigor will capture the and transform it to digital form he receiver will generate the tone in it receive. This function is very ffic congestion occurs and it still DTMF tone. then the Vigor will capture the nto SIP form. Then it will be sent			
	recommended for you to use communication. Mic Gain (1-10)/Speaker C microphone and speaker by larger of the number, the low Dial Tone Power Level - T loudness of the dial tone. The louder the dial tone is. It is r default setting. Check for ISDN to VoIP C to authenticate which one is The figure that you can type to eight with digits from zer Check for VoIP to ISDN C to authenticate which one is The figure that you can type to eight with digits from zer DTMF mode – There are for InBand:Choose this one the tone as audio directly when OutBand: Choose this one keypad number you pressed then send to the other side; the according to the digital form useful when the network tra can remain the accuracy of I SIP INFO: Choose this one DTMF tone and transfer it in to the remote end with SIP r			

Vigor2930 Series User's Guide

SIP INFO (nortel format)

VolPon www.voipon.co.uk sales@voipon.co.uk Tel: +44 (0)1245 808195 Fax: +44 (0)1245 808299

Payload Type (rfc2833) - Choose a number from 96 to 127, the default value was 101. This setting is available for the OutBand (RFC2833) mode.

3.11.4 Status

From this page, you can find codec, connection and other important call status for each port.

VoIP >> Status

Status Refresh Seconds: 10 💌									Refresh		
Port	Status	Codec	PeerID	Elapse (hh:mm:ss)	Tx Pkts	Rx Pkts	Rx Losts	Rx Jitter (ms)	In Calls	Out Calls	Speaker Gain
Phone1	IDLE			00:00:00	0	0	0	0	0	0	5
Phone2	IDLE			00:00:00	0	0	0	0	0	0	5
ISDN1-B1	IDLE			00:00:00	0	0	0	0	0	0	5
ISDN1-B2	IDLE			00:00:00	0	0	0	0	0	0	5
ISDN2-B1	IDLE			00:00:00	0	0	0	0	0	0	5
ISDN2-B2	IDLE			00:00:00	0	0	0	0	0	0	5

Log						
Date		Time	Duration	In/Out/Miss	Account ID	Peer ID
(mm-dd-y	уууу)	(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-	Ο	00:00:00	00:00:00	-	-	
00-00-	0	00:00:00	00:00:00	-	-	

Refresh Seconds

Specify the interval of refresh time to obtain the latest VoIP calling information. The information will update immediately when the Refresh button is clicked.

Refresh Seconds :	10	*
	5	
	10	
	30	

Port	It shows current connection status for the port of Phone1, Phone2, ISDN1 and ISDN2. The ISDN1/2 appears only when the router is equipped with ISDN interface. ISDN1 means B1 channel for the physical ISDN port; ISDN2 means B2 channel for the physical ISDN port. Be aware that ISDN1/2 port is available for the users living in Europe and using Vigor 2930VSn only. For other V models, only the status for VoIP1 and VoIP2 will be shown in this page.
Status	It shows the VoIP connection status. IDLE - Indicates that the VoIP function is idle. HANG_UP - Indicates that the connection is not established (busy tone). CONNECTING - Indicates that the user is calling out. WAIT_ANS - Indicates that a connection is launched and waiting for remote user's answer.

	ALERTING - Indicates that a call is coming. ACTIVE- Indicates that the VoIP connection is launched.
Codec	Indicates the voice codec employed by present channel.
PeerID	The present in-call or out-call peer ID (the format may be IP or Domain).
Elapse	The format is represented as 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	The accumulating in-call times.
Out Calls	The accumulating out-call times.
Speaker Gain	The volume of present call.
Log	Display logs of VoIP calls.

3.12 ISDN

3.12.1 Basic Concept

ISDN means integrated services digital network that is an international communications standard for sending voice, video, and data over digital telephone lines or normal telephone wires.

Below shows the menu items for ISDN.



3.12.2 General Settings

This web page allows you to enable ISDN function.

ISDN >> General Setup

ISDN P	Port	📀 Enable Di	isable	Blocked MSN r	numbers for the	router	
Countr	y Code	International 🛛 👻			1.		
D-Char	nnel Mode		-		2.		
ISDN	11	 ○ Point-to-Point ● Point-to-Mult 			3.		
ISDN	12	 ○ Point-to-Point ● Point-to-Mult 			4		
Own N	umber						
remote		hat the router wi umber when it's p					
Goto <mark>P</mark> type.	<u>'hone Settings</u> to	change ISDN TE	->NT				
Index	MSN numbers the router	for	Mapping	to Phone Por	ts	Phone CL	IR/CLIF
1.		Phone1	Phone2	ISDN1-SO	Any 🔽		
2.		Phone1	Phone2	ISDN1-SO	Any 🔽		
з.		Phone1	Phone2	ISDN1-S0	Any 🔽		
4.		Phone1	Phone2	ISDN1-SO	Any 🔽		
5.		Phone 1	Phone2	ISDN1-SO	Any 🔽		
6.		Phone1	Phone2	ISDN1-SO	Any 🔽		
7.		Phone1	Phone2	ISDN1-SO	Any 🔽		
		Phone1	Phone2	ISDN1-SO	Any 🔽		
8.			_	ISDN1-SO	Any 🗸		
8. 9.		Phone 1	Phone2	LIDDIAL DO			
			_	ISDN1-S0			



ISDN Port	Click Enable to open the ISDN port and Disable to close it.
Country Code	For proper operation on your local ISDN network, you should choose the correct country code.
D-Channel Mode	It allows you to configure ISDN layer2 protocol as: Point-to-Point - Configure ISDN port to use static TEI (Terminal Endpoint Identifier). Point-to-Multipoint - Configure ISDN port to use Dynamic TEI.
Own Number	Enter your ISDN number that you got from ISDN service provider (To have such number, you have offer your request from ISDN service provider first). Every outgoing call will carry the number to the receiver.
Blocked MSN Numbers for the router	Enter the specified MSN number into the fields to prevent the router from dialing the specific MSN number
MSN Numbers for the Router	MSN Numbers mean that the router is able to accept only number-matched incoming calls. In addition, local ISDN network provider should support MSN services. The router

Vigor2930 Series User's Guide

151

provides ten fields for MSN numbers. Note that MSN service must be acquired from your local telecom operators. By default, MSN function is disabled. If you leave the fields blank, all incoming calls will be accepted without number matching.

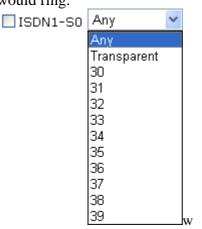
1-10 fields – Fill in the portion that is different with the own number.

For example, the own number is **1234567** and MSN numbers are **1234550**, **1234517** and **1234582** respectively. You can type in **1234567** in the filed of own number. Fill in **50**, **17** and **67** on the fields of 1, 2 and 3 one by one without typing 12345.

Mapping to Phone Ports Fo

For loop through phone calls, you can assign Phone 1, Phone 2, ISDN1-S0 as ring ports if incoming calls correspond with settings on MSN number field.

There are ten internal lines (30-39) under ISDN1-S0 for you to configure as dedicated line. You can setup your ISDN phone with one of these 10 different internal MSN numbers. **Transparent** means MSN on TE port can connect to NT port without limitation on the number among 30 ~ 39. **Any** means all the phones under ISDN1-S0 would ring.



If you choose **Any** as ISDN-S0 port, when the router receives the incoming phone call with certain number for reaching ISDN-S0, all the phone sets connected to ISDN-S0 will ring at the same time.

Phone CLIR/CLIPCLIR means "Calling Line Identification Restriction". If you
choose this item, we will not let remote side see your phone
number. Such function depends on environment that ISP
offers to you. Usually, hidden telephone number is not
permitted under many real circumstances.

CLIP means "Calling Line Identification Presentation". Usually the router will send "Own Number" to the remote side. However **Own number** will restrict the router displaying only one number on remote side. Vigor2930 series can connect up to 6

phones at the same time. Therefore, if **CLIP** is selected, the **external MSN numbers that you setup will be displayed to remote side**.

VolPon www.voipon.co.uk sales@voipon.co.uk Tel: +44 (0)1245 808195 Fax: +44 (0)1245 808299

Application Example

You got ISDN numbers with *5972720~5972729* from your ISP, and you try to connect ISDN-TE port to ISDN network. Please refer to the following configuration.

Open ISDN>> General Setup and set as the following:

ISDN >>	General	Setu
---------	---------	------

ISDN S	etup							
ISON P	Part	Inable O Dis	able	Blocked MSN	numbers for	the	router	
Countr	ry Code	International 😪			1.			
D-Cha	nnel Mode				2.			
ISDA	41	 Point-to-Point Point-to-Multip 	point		з.			
ISDN	10	O Point-to-Point	COMPT-		4.			
1901	42	Point-to-Multip	point		5.			
Own N	lumber	5972726						
remote outgoir	e end the ISDN r ng call.	that the router will number when it's p o change ISDN TE-	lacing an					
Index	MSN numbers the router		Mapping	to Phone Por	ts		Phone Cl	IR/CLIP
1.	5972727	Phone 1	Phone2	ISDN1-50	Any	*		
2.	5972728	Phone 1	Phone2	ISON1-SO	32	×	1	
З.	5972729	Phone 1	Phone2	ISDN1-50	Transparent	~	171	
4.	5972720	Phone1	Phane2	ISDN1-S0	Any	×	11	

When remote user calls you by dialing 5972727, the router will make Phone1 port ringing.

When remote user calls you by dialing *5972728*, the router will make ISDN phone under ISDN1-S0 port and configured with internal MSN number 32 ringing.

When remote user calls you by dialing *5972729*, the router will make ISDN phones under ISDN1-S0 port and configured with internal MSN number *5972729* ringing.

When remote user calls you by dialing *5972720*, the router will make all of ISDN phones under ISDN1-S0 port ringing.

When remote user calls you by dialing **5972722**, the router will make no phone ringing for the number is not specified in such page.

If you use Phone1 to dial an outgoing call: remote user will see the telephone number - 5972726 because CLIP is not checked.

If you use ISDN1-S0 with **MSN 32** to dial an outgoing call: remote user will see "Withheld Number" from the telephone display panel because Phone CLIR is checked.

If you use **ISDN1-S0 with MSN 5972729** to dial an outgoing call: remote user will see the number 5972729 because Phone CLIP is checked.

If you use **ISDN1-S0 without MSN Setup** to dial an outgoing call: remote user will see the number 5972720 because Phone CLIP is checked.

3.12.3 Dial to Single/Dual ISPs

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

ISDN	>>	Dialing	to a	Sina	le	ISP

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

ISP Access Setup	 ISP Name - Enter your ISP name such as Seednet, Hinet and so on. Dial Number -Enter the ISDN access number provided by your ISP. Username - Enter the username provided by your ISP. Password - Enter the password provided by your ISP. Require ISP Callback (CBCP) -If your ISP supports the callback function, check this box to activate the Callback Control Protocol during the PPP negotiation. Scheduler (1-15) - Enter the index of schedule profiles to control the Internet access according to the preconfigured schedules. Refer to section 3.8.2 Schedule for detailed configuration.
PPP/MP Setup	 Link Type – There are three link types provided here for different purpose. Link Disable disables the ISDN dial-out function. Dialup 64Kbps allows you to use one ISDN B channel for Internet access. Dialup 128Kbps allows you to use both ISDN B channels for Internet access. Dialup BOD (for detailed information of configuration, please refer to section 3.12.4) stands for bandwidth-on-demand. The router will use only one B channel in low traffic situations. Once the single B channel bandwidth is fully used, the other B channel will be activated automatically through the dialup. For more detailed BOD parameter settings, please refer to the section of Call Control. PPP Authentication - PAP only allows you to configure the PPP session to use the PAP or CHAP is to configure the PPP session to use the PAP or CHAP protocols to negotiate the username and password with the ISP. Idle Timeout - Idle timeout means the router will be
	disconnect after being idle for a preset amount of time. The default is 180 seconds. If you set the time to 0, the ISDN connection to the ISP will always remain on.

IP Address Assignment Method (IPCP)

In most environments, you should not change these settings as most ISPs provide a dynamic IP address for the router when it connects to the ISP. If your ISP provides a fixed IP address, check **Yes** and enter the IP address in the field of **Fixed IP Address**.

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

ISDN >> Dialing to Dual ISPs

Dual ISP				
Common Settings			PPP/MP Setup	
1. 🔲 Enable Dual ISPs Function			Link Type	Dialup BOD 🛛 🔽
2. 🗌 Require ISP callback (CBCP)		PPP Authentication	PAP or CHAP 🔽	
			Idle Timeout	180 second(s)
Primary ISP Setup			Secondary ISP Setu)
ISP Name			ISP Name	
Dial Number			Dial Number	
Username			Username	84005755@hinet.net
Password			Password	•••••
IP Address Assignment Method (IPCP)		IP Address Assignment Method (IPCP)		
Fixed IP	🔘 Yes 💿 No (Dynamic	IP)	Fixed IP	🔘 Yes 💿 No (Dynamic IP)
Fixed IP Address			Fixed IP Address	

0K	
UK	
	OK

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

different purpose. Link Disable disables the ISDN dial-out function. Dialup 128Kbps allows you to use both ISDN B channels for Internet access. Dialup BOD (for detailed information of configuration, please refer to section 3.12.4) stands for bandwidth-on-demand. The router will use only one B channel in low traffic situations. Once the single B channel bandwidth is fully used, the other B channel will be activated automatically through the dialup.

PPP Authentication - PAP only allows you to configure the PPP session to use the PAP protocol to negotiate the username and password with the ISP. **PAP or CHAP** can configure the PPP session to use the PAP or CHAP protocols to negotiate the username and password with the ISP.

Idle Timeout - Idle timeout means the router will be disconnect after being idle for a preset amount of time. The default is 180 seconds. If you set the time to 0, the ISDN connection to the ISP will always remain on.

Primary ISP Setup	 ISP Name - Enter your ISP name. Dial Number -Enter the ISDN access number provided by your ISP. Username - Enter the username provided by your ISP. Password - Enter the password provided by your ISP.
IP Address Assignment Method (IPCP) for primary ISP setup	In most environments, you should not change these settings as most ISPs provide a dynamic IP address for the router when it connects to the ISP. If your ISP provides a fixed IP address, check Yes and enter the IP address in the field of Fixed IP Address .
Secondary ISP Setup)	 ISP Name - Enter the secondary ISP name. Dial Number -Enter the ISDN access number provided by the ISP. Username - Enter the username provided by your ISP. Password - Enter the password provided by your ISP.
IP Address Assignment Method (IPCP) for secondary ISP setup	In most environments, you should not change these settings as most ISPs provide a dynamic IP address for the router when it connects to the ISP. If your ISP provides a fixed IP address, check Yes and enter the IP address in the field of Fixed IP Address .

After entering the necessary settings and clicking **OK**, you will see **Goto ISDN Diagnostic** link appears on the bottom of the webpage. To have an ISDN connection, please click this link.

ISP Access Setup		PPP/MP Setup	
ISP Name		Link Type	Dialup 128Kbps 🔽
Dial Number	30	PPP Authentication	PAP or CHAP 🗸
Siai Number		Idle Timeout	180 second(s)
Username	vivian	IP Address Assignmen	nt Method (IPCP)
Password		Fixed IP	🔿 Yes 💿 No (Dynamic IP)
🗌 Require ISP cal	lback	Fixed IP Address	
Index(1-15) in <u>Sc</u>	hedule Setup:		
=>	, , , , , , , , , , , , , , , , , , , ,		
>> Goto ISDN Diag	Inostic		

Now, the system will guide you to click **Dial ISDN**. Wait for a moment after clicking the dial link. Then, a successful ISDN connection will be shown as the following.

Online Status

System Status						Syste	m Uptime: 0:0:49
LAN Status		Primary DN	S: 168.95	.1.1	Sec	ondary DNS:	168.95.192.1
IP Address	TX P	ackets	RX Pac	kets			
192.168.1.1	419		360				
WAN 1 Status							
Enable	Line	Name	M	ode	Up Time	e	
No	Ethernet			-	00:00:0	00	
IP	GW IP	TX Packets	s TX	(Rate	RX Pac	kets R	X Rate
		0	0		0	0	
WAN 2 Status							
Enable	Line	Name	M	ode	Up Time	е	
No	Ethernet			-	00:00:0	00	
IP	GW IP	TX Packets	s TX	(Rate	RX Pac	kets R	X Rate
		0	0		0	0	
ISDN Status				>>	Dial ISDN	>> Drop B1	>> Drop B2
Channel Activ	e Connection	TX Pkts	TX Rate	RX Pkts	RX Rate	Up Time	AOC
B1 [192	.168.225.200]	19	4	18	4	0:0:46	0
B2 [192	.168.225.200]	13	3	14	3	0:0:43	0
D UP							

3.12.4 Call Control

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

ISDN >> Call Control

Call Control Setup

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

0K

Dial Retry - It specifies the dial retry counts per triggered packet. A triggered packet is the packet whose destination is outside the local network. The default setting is no dial retry. If set to 5, for each triggered packet, the router will dial 5 times until it is connected to the ISP or remote access router.
Dial Delay Interval - It specifies the interval between dialup retries. By default, the interval is 0 second.
Remote Activation – It can help users who would like to access the server which is off the Internet in the head office.

Vigor2930 Series User's Guide

157

To remotely make the server to be available on the Internet, i.e. make the router in the head office activating its Internet access either by dialing-up or starting broadband connection, users can make a regular phone call (the number is set in the Remote Activation field) to the router as signaling it for activation. The phone call will be soon disconnected once the router is on line.

Note that **Dialing to a Single ISP** should be pre-configured properly.

Basic Setup Link Type - Because ISDN has two B channels (64Kbps/per channel), you can specify whether you would like to have single B channel, two B channels or BOD (Bandwidth on Demand). Four options are available: Link Disable, Dialup 64Kbps, Dialup 128Kbps, Dialup BOD.

Link Type

Dialup BOD	~
Link Disable	
Dialup 64Kbps	
Dialup 128Kbps	
Dialup BOD	

PPP Authentication - It specifies the PPP authentication method for PPP/MP connections. Normally you can set it to PAP/CHAP for better compatibility.

TCP Header Compression - VJ Compression: It is used for TCP/IP protocol header compression. Normally it is set to Yes to improve bandwidth utilization.

Idle Timeout - Because our IDSN link type is Dial On **Demand**, the connection will be initiated only when needed.

Bandwidth-On-Demand Bandwidth-On-Demand is for Multiple-Link PPP \(ML-PPP or MP). The parameters are only applied when you set the Link Type to Dialup BOD. The ISDN usually use one B channel to access the Internet or remote network when you choose the Dialup BOD link type. The router will use the parameters here to decide on when you activate/drop the additional B channel. Note that **cps** (characters-per-second) measures the total link utilization.

> High Water Mark and High Water Time - These parameters specify the situation in which the second channel will be activated. With the first connected channel, if its utilization exceeds the High Water Mark and such a channel is being used over the High Water Time, the additional channel will be activated. Thus, the total link speed will be 128kbps (two B channels).

Low Water Mark and Low Water Time - These parameters specify the situation in which the second channel will be dropped. In terms of the two B channels, if their utilization is under the Low Water Mark and these two channels are being used over the High Water Time, the additional channel will be dropped. As a result, the total link speed will be 64kbps (one B channel).

(BOD) Setup

3.13 Wireless LAN

This function is used for "n" models only.

3.13.1 Basic Concepts

Over recent years, the market for wireless communications has enjoyed tremendous growth. Wireless technology now reaches or is capable of reaching virtually every location on the surface of the earth. Hundreds of millions of people exchange information every day via wireless communication products. The Vigor "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.



3.13.2 General Setup

Wireless LAN >> 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.

	IS LAN		
Mode :		Mixed(11b+11g+	+11n) 🛩
Index(1-15) in <u>Schedule</u>	Setup:,	,,
Enable	Hide SSID	SSID	Isolate LAN Member
1 🗹		default	
2			
3 🔲			
4			
Isolate Men Wireless cl Isolate LAN	ients (stations I:) with the same SSID cannot acc) with the same SSID cannot acc	
Wireless cl	Channel 6, 2437N Ible: necessary	/Hz ▼ Long Preamble: y for some old 802.11 b devices o	
Wireless cl	ible: necessar		
Channel: C Long Pream Packet-OV	nble: necessary ERDRIVE™		
Channel: C Long Pream Packet-OV T x Burs Note:	nble: necessary ERDRIVE™	y for some old 802.11 b devices o	

OK Cancel

Enable Wireless LAN Mode 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 Applications >> Schedule
	setup. The default setting of this filed is blank and the

function will always work.

Hide SSID	 Check it to prevent from wireless sniffing and make it harder for unauthorized clients or STAs to join your wireless LAN. Depending on the wireless utility, the user may only see the information except SSID or just cannot see any thing about Vigor wireless router while site surveying. The system allows you to set four sets of SSID for different usage. In default, the first set of SSID will be enabled. You can hide it for your necessity. Means the identification of the wireless LAN. SSID can 			
SSID	Means the identification of the wireless LAN. SSID can be any text numbers or various special characters. The default SSID is "default". We suggest you to change it.			
Isolate	 LAN – Check this box to make the wireless clients (stations) with the same SSID cannot access wired PCs on LAN. Member –Check this box to make the wireless clients (stations) with the same SSID not accessing for each other. 			
Channel	Means the channel of frequency of the wireless LAN. The default channel is 6. You may switch channel if the selected channel is under serious interference. If you have no idea of choosing the frequency, please select Auto to let system determine for you. Channel: Channel 6, 2437MHz Auto Channel 1, 2412MHz Channel 2, 2417MHz Channel 3, 2422MHz Channel 4, 2427MHz Channel 5, 2432MHz Channel 5, 2432MHz Channel 6, 2437MHz Channel 7, 2442MHz Channel 8, 2447MHz Channel 9, 2452MHz Channel 10, 2457MHz Channel 10, 2457MHz Channel 11, 2462MHz			
Long Preamble	This option is to define the length of the sync field in an 802.11 packet. Most modern wireless network uses short preamble with 56 bit sync filed instead of long preamble with 128 bit sync field. However, some original 11b wireless network devices only support long preamble. Check it to use Long Preamble if needed to communicate with this kind of devices.			
Packet-OVERDRIVE	This feature can enhance the performance in data transmission about 40%* more (by checking Tx Burs 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. Note: Vigor N61 wireless adapter supports this function. Therefore, you can use and install it into your PC for matching with Packet-OVERDRIVE (refer to the			

following picture of Vigor N61 wireless utility window, choose **Enable** for activating TxBurst).

onformation Status Option About			
Orosid Dethia Auto lemach when Hindows glart up Remember main status gontion Auto jule mini status Set gain status obseys on top Enable (F Setting and Proxy Setting in Profile Quorp Rooming Ad-base HLAH type to consect O Infrastructure and Ad-loc getwork Infrastructure and Ad-loc getwork Ad-base retwork only Ad-base retwork only	Advance Defing Double Botos Esigneratutos Threshold : RTE Threshold Frequency : Ad-hos Quarael Proger Save Mode Ta Boust	23 23 802.11 kgm - 2.40 H 1 Dashle Dashle	47
Automatically consect to non-performed networks			
	OK	Cancel	10

Note: * means the real transmission rate depends on the environment of the network.

3.13.3 Security

This page allows you to set security with different modes for SSID 1, 2, 3 and 4 respectively. After configuring the correct settings, please click **OK** to save and invoke it.

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

SID 1	SSID 2	SSID 3	SSID 4		
r	Mode:		Disable	*	
WPA:					
F	Pre-Shared Key(I	PSK):	*****		
	Type 8~63 ASCI 'cfgs01a2" or "			igits leading by	/ "Ox", for example
WEP:					
E	Encryption Mode	:	64-Bit 💌		
	⊙Key 1 :		*****		
	○Key 2 :		*****		
	○Key 3 :		******		
	◯Кеу 4 :		*****		
Type 5	b it WEP key ASCII character 2333132".	r or 10 Hexade	cimal digits leadir	g by "Ox", for (example "AB312" or
Type 1			lecimal digits lead 536373839414243		example

Mode	There are several modes provided for you to Disable WEP WPA/PSK WPA2/PSK Mixed(WPA+WPA2)/PSK) choose.
	 Disable - Turn off the encryption mechanism WEP - Accept WEP client and the encryption be entered in WEP filed below. WPA/PSK - Accepts WPA clients and the encryption be entered in PSK. WPA2/PSK-Accepts only WPA2 clients and encryption key should be entered in PSK. Mixed (WPA+WPA2)/PSK - Accepts WPA clients simultaneously and the encryption key entered in PSK. 	on key should encryption ad the A and WPA2
WPA	The WPA encrypts each frame transmitted f using the key, which either PSK entered man field below or automatically negotiated via a authentication. Pre-Shared Key (PSK) - Either 8~63 ASCI such as 012345678(or 64 Hexadecimal dig 0x, such as "0x321253abcde").	nually in this 802.1x II characters,
WEP	 64-Bit - For 64 bits WEP key, either 5 ASC such as 12345 (or 10 hexadecimal digitals lesuch as 0x4142434445.) 128-Bit - For 128 bits WEP key, either 13 A characters, such as ABCDEFGHIJKLM (or hexadecimal digits leading by 0x, such as 0x4142434445464748494A4B4C4D). 	eading by 0x, ASCII
	Encryption Mode: 64-Bit 64-Bit 128-Bit	~
	All wireless devices must support the same encryption bit size and have the same key. F be entered here, but only one key can be sele time. The keys can be entered in ASCII or H Check the key you wish to use.	Four keys can ected at a

3.13.4 Access Control

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

	Policy :	Activate MA	C address filter 🔽		
	Enable Mac Address			9	
	SSID 1	SSID 2	SSID 3	SSID 4	
		MAC Addre	ess Filter		
	Index Attribut	te MAC Addr	ess		
	Client's MAC A Attribute : s: Isola	ddress : : :	:	:	
	Add	Delete	Edit	Cancel	
		OK	Clear All		
Policy		Activate M address list address no selected sta isolated fro LAN. Blocked M address list	IAC address t for accessin t listed above ation with Ma om LAN by c IAC address t for denying	e of the followin filter- Allow to g Access Point. cannot access A AC address lister hecking Isolate f filter- Allow to access AP. How isted above are a	o set MAC PCs with MAC AP. In addition, d above can be the station from o set MAC vever, stations
		AP. Policy :		Activate MAC a Activate MAC a Blocked MAC a	address filter 💌 address filter

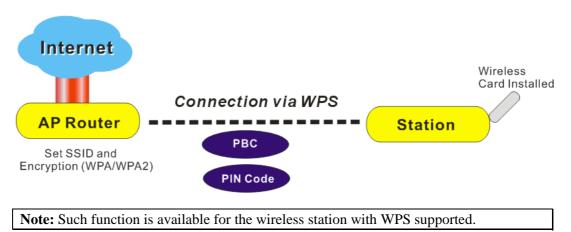
Wireless LAN >> Access Control

ess LAN identified with SSID 1 to 4 respectively. All the clients (expressed by MAC addresses) listed in the box can be grouped under different wireless LAN. For example, they can be grouped under SSID 1 and SSID 2 at the same time if you check SSID 1 and SSID 2. **MAC Address Filter** Display all MAC addresses that are edited before. Client's MAC Address - Manually enter the MAC address of wireless client. Attribute s: Isolate the station from LAN - select to isolate the wireless connection of the wireless client of the MAC address from LAN. Add Add a new MAC address into the list.

Delete	Delete the selected MAC address in the list.
Edit	Edit the selected MAC address in the list.
Cancel	Give up the access control set up.
ОК	Click it to save the access control list.
Clear All	Clean all entries in the MAC address list.

3.13.5 WPS

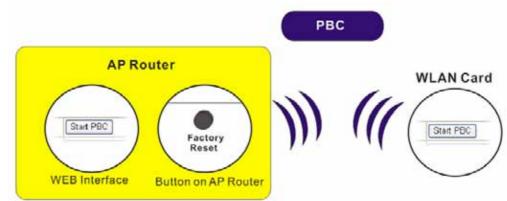
WPS (Wi-Fi Protected Setup) provides easy procedure to make network connection between wireless station and wireless access point (vigor router) with the encryption of WPA and WPA2.



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 2930 series which served as an AP, press **Factory Reset** 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.	PIN	Code
AP Router Start PIN PIN Code of Station WEB Interface	M	WLAN Card Define a PIN Code

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.

Microsoft Internet Explorer			
♪	WPS only supports in WPA/WPA2-PSK Mode.		
	OK		

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	WPA2/PSK

Device Configure

Configure via Push Button	Start PBC
Configure via Client PinCode	Start PIN

Status: Ready

Note: WPS can help your wireless client automatically connect to the Access point.

🗅: WPS is Disabled.

🖸: WPS is Enabled.

 ${f Q}_{:}$ Waiting for WPS requests from wireless clients.

Enable WPS	Check this box to enable WPS setting.
WPS Status	Display related system information for WPS. If the wireless security (encryption) function of the router is properly configured, you can see 'Configured' message here.
SSID	Display the SSID1 of the router. WPS is supported by SSID1 only.

Vigor2930 Series User's Guide

167

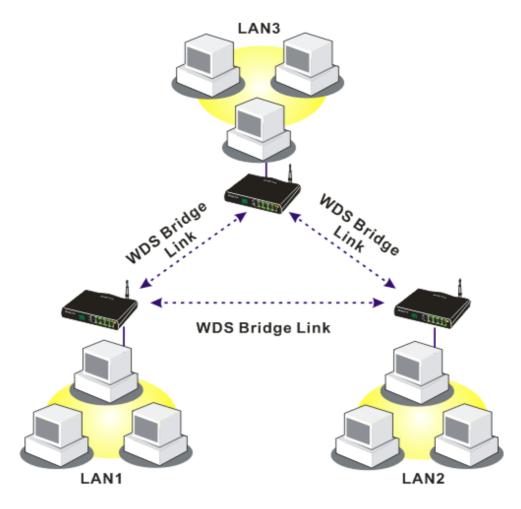
Authentication Mode	Display current authentication mode of the router. Only WPA2/PSK and WPA/PSK support WPS.
Configure via Push Button	Click Start PBC to invoke Push-Button style WPS setup procedure. The router will wait for WPS requests from wireless clients about two minutes. The WLAN LED on the router will blink fast when WPS is in progress. It will return to normal condition after two minutes. (You need to setup WPS within two minutes)
Configure via Client PinCode	Please input the PIN code specified in wireless client you wish to connect, and click Start PIN button. The WLAN LED on the router will blink fast when WPS is in progress. It will return to normal condition after two minutes. (You need to setup WPS within two minutes)

3.13.6 WDS

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

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

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



VolPon www.voipon.co.uk sales@voipon.co.uk Tel: +44 (0)1245 808195 Fax: +44 (0)1245 808299

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



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

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



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

Wireless LAN >> WDS Settings

WDS Settings		Set to Factory Default		
Mode:	Disable 🗸	Bridge Enable Peer MAC Address		
Security: • Disable • W WEP:		Image: Second		
	: TKIP : ************************************	Repeater Enable Peer MAC Addess		
		Access Point Function:		
Mode	invo			
Security	Pre folle	There are three types for security, Disable , WEP and Pre-shared key . The setting you choose here will make the following WEP or Pre-shared key field valid or not. Choose one of the types for the router.		
WEP	pag	Check this box to use the same key set in Security Settings page. If you did not set any key in Security Settings page, this check box will be dimmed.		
Settings	WE the set t Key sele	 Encryption Mode - If you checked the box of Use the same WEP key, you do not need to choose 64-bit or 128-bit as the Encryption Mode. If you do not check that box, you can set the WEP key now in this page. Key Index - Choose the key that you want to use after selecting the proper encryption mode. Key - Type the content for the key. 		
Pre-shared K		e 8 ~ 63 ASCII characters or 64 hexadecimal digits ling by "0x".		
Bridge	the	ou choose Bridge as the connecting mode, please type in peer MAC address in these fields. Four peer MAC resses are allowed to be entered in this page at one time.		

170

	Yet please disable the unused link to get better performance. If you want to invoke the peer MAC address, remember to check Enable box in the front of the MAC address after typing.
Repeater	If you choose Repeater as the connecting mode, please type in the peer MAC address in these fields. Four peer MAC addresses are allowed to be entered in this page at one time. Similarly, if you want to invoke the peer MAC address, remember to check Enable box in the front of the MAC address after typing.
Access Point Function	Click Enable to make this router serving as an access point; click Disable to cancel this function.
Status	It allows user to send "hello" message to peers. Yet, it is valid only when the peer also supports this function.

3.13.7 AP Discovery

Vigor router can scan all regulatory channels and find working APs in the neighborhood. Based on the scanning result, users will know which channel is clean for usage. Also, it can be used to facilitate finding an AP for a WDS link. Notice that during the scanning process (about 5 seconds), no client is allowed to connect to Vigor.

This page is used to scan the existence of the APs on the wireless LAN. Yet, only the AP which is in the same channel of this router can be found. Please click **Scan** to discover all the connected APs.

Wireless LAN >> Ac	cess Point Discovery	y		
Access Point List				
Access I offic List	BSSID	Channel	SSID	
	·	Scan		
See <u>St</u>	atistics.			
	uring the scanning router.	process (~5 secor	nds), no station is allowe	ed to connect
Add to	NDS Settings :			
AP's MA	C address			
Add t	0	💿 Bridge	○ Repeater	

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

3.13.8 Station List

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

Wireless LAN >> Station List

	Status MAC Address	
	Refresh Status Codes : C: Connected, No encryption. E: Connected, WEP. P: Connected, WPA. A: Connected, WPA2. B: Blocked by Access Control.	
	 N: Connecting. F: Fail to pass 802.1X or WPA/PSK authentication. Note: After a station connects to the router successfully, it may be turned off without notice. In that case, it will still be on the list until the connection expires. 	
	Add to Access Control :	1.
	Client's MAC address	
	Add	
Refresh	Click this button to refresh the status o	f station list.
Add	Click this button to add current selecte into Access Control.	d MAC address

3.13.9 Rate Control

Wireless LAN >> Rate Control

This page allows you to control the upload and download rate of each wireless client (station) and SSID1-4. Please check the box of **Enable** to invoke this setting. The range for the rate is between $100 \sim 100,000$ kbps.

nable					
Upload Ra	ate :		10000	Kbps	
Download	l Rate :		10000) Kbps	
			rement: 100 K to each asso	bps. :iated wireless client.	
SID Rate Control	Enable	Upload		Download	
SID Rate Control	Enable	Upload	kbps	Download	
	Enable	· · · · · · · · · · · · · · · · · · ·	kbps kbps		
SSID 1	Enable	100000	Ξ.	100000 kbps	
SSID 1 SSID 2	Enable	100000 100000	kbps	100000 kbps 100000 kbps	

SSID rate control controls the data transmission rate through wireless connection.

OK |

Enable	Check Enable for typing upload and download rate.
Upload	Type the transmitting rate for data upload. Default value is 30,000 kbps.
Download	Type the transmitting rate for data download. Default value is 30,000 kbps.

Cancel

3.14 System Maintenance

For the system setup, there are several items that you have to know the way of configuration: Status, Administrator Password, Configuration Backup, Syslog, Time setup, Reboot System, Firmware Upgrade.

Below shows the menu items for System Maintenance.

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

174

3.14.1 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 irmware Version uild Date/Time	1 : v3.1.0		es :55:9.90 2008		
	LAN				WAN 1
MAC Address	; : 0	D-50-7F	-C2-80-20	Link Status	: Connected
1st IP Addre:	ss : 1'	92.168.1	1	MAC Address	: 00-50-7F-C2-80-21
1st Subnet N	/lask : 2.	55.255.2	255.0	Connection	: Static IP
DHCP Server	:)	'es		IP Address	: 172.16.3.229
DNS	: 1	94.109. 6	.66	Default Gateway	: 172.16.3.4
	Vol)			WAN 2
Port	Profile	Req.	In/Out	Link Status	: Disconnected
Phone1	FIOINE	No	0/0	MAC Address	: 00-50-7F-C2-80-22
Phone2		No	0/0	Connection	:
ISDN1-SO		No	0/0	IP Address	
ISDN1-30		No	0/0	Default Gateway	
130/02 10		140	0/0		•
				W	/ireless LAN
				MAC Address	: 00-50-7f-c2-80-20

Frequency Domain Firmware Version

: Europe : v1.04.12.14.7.5

Model Name	Display the model name of the router.
Firmware Version	Display the firmware version of the router.
Build Date/Time	Display the date and time of the current firmware build.
MAC Address	Display the MAC address of the LAN Interface.
1 st IP Address	Display the IP address of the LAN interface.
1 st Subnet Mask	Display the subnet mask address of the LAN interface.
DHCP Server	Display the current status of DHCP server of the LAN interface.
MAC Address	Display the MAC address of the WAN Interface.
IP Address	Display the IP address of the WAN interface.
Default Gateway	Display the assigned IP address of the default gateway.
DNS	Display the assigned IP address of the primary DNS.
MAC Address	Display the MAC address of the wireless LAN.
Frequency Domain	It can be Europe (13 usable channels), USA (11 usable channels) etc. The available channels supported by the wireless products in different countries are various.
Firmware Version	It indicates information about equipped WLAN miniPCi card. This also helps to provide availability of some features that are bound with some WLAN miniPCi card.

3.14.2 TR-069 Setting

System Maintenance >> TR-069 Setting

Vigor router with TR-069 is available for matching with VigorACS server. Such page provides VigorACS and CPE settings under TR-069 protocol. All the settings configured here is for CPE to be controlled and managed with VigorACS server. Users need to type URL, username and password for the VigorACS server that such device will be connected. However URL, username and password under CPE client are fixed that users cannot change it. The default CPE username and password are "vigor" and "password". You will need it when you configure VigorACS server.

ACS Server	
URL	
Username	
Password	
CPE Client	
🔘 Enable 🛛 💿 Disable	
URL	http://172.16.3.229:8069/cwm/CRN.html
Port	8069
Username	vigor
Password	
c Inform Settings	
🔘 Disable	
💿 Enable	
Interval Time	900 second(s)
	ОК

Such data must be typed according to the ACS (Auto Configuration Server) you want to link. Please refer to VigorACS user's manual for detailed information. URL - Type the URL for VigorACS server. If the connected CPE needs to be authenticated, please set URL as the following and type username and password for VigorACS server: http://{IP address of VigorACS}:8080/ACSServer/services/ACSServlet If the connected CPE does not need to be authenticated please set URL as the following: http://{IP address of VigorACS}:8080/ACSServer/services/UnAuthACSServ let Username/Password - Type username and password for ACS Server for authentication. For example, if you want

ACS Server for authentication. For example, if you want to use such CPE with VigorACS, you can type as the following: Username: acs Password: password

CPE Client	 It is not necessary for you to type them. Such information is useful for Auto Configuration Server. Enable/Disable – Sometimes, port conflict might be occurred. To solve such problem, you might want to change port number for CPE. Please click Enable and change the port number.
Periodic Inform Settings	 Disable – The system will not send inform message to ACS server. Enable – The system will send inform message to ACS server periodically (with the time set in the box of interval time). The default setting is Enable. Please set interval time or schedule time for the router to send notification to CPE. Or click Disable to close the mechanism of notification.

3.14.3 Administrator Password

This page allows you to set new password.

System Maintenance >> Administrator Password Setup

Old Password	•••••
New Password	•••••
Confirm Password	•••••

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

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

3.14.4 Configuration Backup

Backup the Configuration

Follow the steps below to backup your configuration.

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

System Maintenance >> 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.			
	Backup Cancel			

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

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

ave As					_	?
Save in:	Desktop		~	00	P	
My Recent Documents Desktop My Documents	My Documen My Compute My Network I RVS-COM Lit Annex A Immm MWSnap300 TeleDanmark Tools I config I v2k2_232_cc I v2k6_250_cc	Places e infig_1				
My Computer	File name:	contig			× [Save
My Network	Save as type:	Configuration file				Cancel

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

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

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

Restore Configuration

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

System Maintenance >> Configuration Backup					
Configuration	Backup / Restoration				
Restoration					
	Select a configuration file.				
	Browse.,				
	Click Restore to upload the file.				
	Restore				
Backup					
	Click Backup to download current running configurations as a file.				
	Backup Cancel				

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

3.14.5 Syslog/Mail Alert

System Maintenance >> SysLog / Mail Alert Setup

SysLog function is provided for users to monitor router. There is no bother to directly get into the Web Configurator of the router or borrow debug equipments.

SysLog Access Setup	Mail Alert Setup	
🗌 Enable	Enable	
Router Name	SMTP Server	
Server IP Address	Mail To	
Destination Port 514	Return-Path	
Enable syslog message:	Authentication	
Firewall Log	User Name	
VPN Log	Password	
 User Access Log Call Log 		
V WAN Log		
Router/DSL information		
	lick " Enable " to activate this function.	
Router Name	ype a name to represent the router.	
yslog Server IPThe IP address of the Syslog server.		
Destination Port A	ssign a port for the Syslog protocol.	
SMTP Server T	he IP address of the SMTP server.	
Aail To A	ssign a mail address for sending mails out.	
	ssight a mail address for schuling mails out.	
	ssign a path for receiving the mail from outside.	
Return-PathAAuthenticationC	ssign a path for receiving the mail from outside.	
Return-PathAAuthenticationCe-	ssign a path for receiving the mail from outside. heck this box to activate this function while using	
Return-PathAAuthenticationCe-User NameT	ssign a path for receiving the mail from outside. heck this box to activate this function while using mail application.	

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	G	iateway IP (Fixed)	TX Packets	TX Rate
Status TX Pac		RX Packets 1470		WAN IP (Fixed)	RX Packets	RX Rate
vall Log VPN In Line Routers		ess Log Call Log	WAN Log Others Host Name:	Network Information Network	et State	
IP Address 192.168.1.1	Mask 255.255.2	MAC 00-50-7F-54-6	NIC Description:	SiS 900-Based	PCI Fast Ethernet Adapt	ter - Packet St 🔽
			MAC Address: IP Address:	00-11-D8-E4-58-CE	Default Geteway: DHCP Server:	192.168.1.1
			Subnet Mask:	255.255.255.0	Lease Obtained:	Mon Jan 22 01:28:23 2007
	Refresh	>	DNS Servers:	168.95.1.1	Lease Expires:	Thu Jan 25 01:28:23 2007

3.14.6 Time and Date

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

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

Current System Time	2007 Oct 17 Wed 8 : 3 : 19 Inquire Time
Time Setup	
🔘 Use Browser Time	
💿 Use Internet Time Client	
Time Protocol	NTP (RFC-1305) 💌
Server IP Address	pool.ntp.org
Time Zone	(GMT) Greenwich Mean Time : Dublin
Enable Daylight Saving	
Automatically Update Inte	erval 30 min 💌
Current System Time	Click Inquire Time to get the current time.
Jse Browser Time	Select this option to use the browser time from the remote administrator PC host as router's system time.
Jse Internet Time	Select to inquire time information from Time Server of the Internet using assigned protocol.
ime 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.
Automatically Update Inte	erval Select a time interval for updating from the NTP serve

3.14.7 Management

This page allows you to manage the settings for access control, access list, port setup, and SMP setup. For example, as to management access control, the port number is used to send/receive SIP message for building a session. The default value is 5060 and this must match with the peer Registrar when making VoIP calls.

Management Access Control	Management Po	ort Setup		
	🛛 💿 User Define	e Ports 🔘 Default Ports		
Allow management from the Internet	Telnet Port	23 (Default: 23)		
FTP Server	HTTP Port	80 (Default: 80)		
HTTP Server	HTTPS Port			
HTTPS Server Image: Telnet Server	FTP Port	21 (Default: 21)		
SSH Server	SSH Port	22 (Default: 22)		
Disable PING from the Internet		(Derbard, 22)		
	SNMP Setup			
Access List	📃 Enable SNI	iMP Agent		
List IP Subnet Mask	Get Communit	ity public		
	Set Communit	ity private		
3	Manager Host	t IP		
	Trap Commun	nity public		
	Notification H	Host IP		
	Trap Timeout	t 10 seconds		
Disable PING from the Interne	t Check the checkbox	het. Check the box (es) to specify.x to reject all PING packets from the ty issue, this function is enabled by defa		
Access List	login from a specie A maximum of the List IP - Indicate a router.	y that the system administrator can c ific host or network defined in the li ree IPs/subnet masks is allowed. an IP address allowed to login to th epresent a subnet mask allowed to l		
Default Ports	Check to use stand HTTP servers.	dard port numbers for the Telnet and		
Jser Defined Ports	Check to specify u Telnet and HTTP	user-defined port numbers for the servers.		
Cnable SNMP Agent	Check it to enable	e this function.		
Get Community	-	he name for getting community by typing a proper acter. The default setting is public.		
Set Community	Set community by	y typing a proper name. The default		

System Maintenance >> Management

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

3.14.8 Reboot System

System Maintenance >> Reboot System

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

Reboot System	
	Do You want to reboot your router ?
	Osing current configuration
	O Using factory default configuration
	OK

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

Note: When the system pops up Reboot System web page after you configure web settings, please click **OK** to reboot your router for ensuring normal operation and preventing unexpected errors of the router in the future.

3.14.9 Firmware Upgrade

Before upgrading your router firmware, you need to install the Router Tools. The **Firmware Upgrade Utility** is included in the tools. The following web page will guide you to upgrade firmware by using an example. Note that this example is running over Windows OS (Operating System).

Download the newest firmware from DrayTek's web site or FTP site. The DrayTek web site is www.draytek.com (or local DrayTek's web site) and FTP site is ftp.draytek.com.

Click System Maintenance>> Firmware Upgrade to launch the Firmware Upgrade Utility.

System Maintenance >> Firmware Upgrade

Web Firmware Upgrade

Select a firmware file.			
		Browse	
Click Upgrade to upload the file.	Upgrade		

TFTP Firmware Upgrade from LAN

Curre	ent Firmware Version: v3.1.0_RC4
Firm	ware Upgrade Procedures:
2. 3. 4.	Click "OK" to start the TFTP server. Open the Firmware Upgrade Utility or other 3-party TFTP client software. Check that the firmware filename is correct. Click "Upgrade" on the Firmware Upgrade Utility to start the upgrade. After the upgrade is compelete, the TFTP server will automatically stop running.
Do ye	ou want to upgrade firmware ? OK

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



For the detailed information about firmware update, please go to Chapter 4.

3.15 Diagnostics

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

Below shows the menu items for Diagnostics.

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

3.15.1 Dial-out Trigger

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

Diagnostics >> Dial-out Trigger

HEX Format:	
00 50 7F 22 33 44-00 0E A6 2A D5 A1-08 00	
45 00 00 48 BE 54 00 00-7F 11 12 3B CO A8 01 0A	
A8 5F 01 01 05 CB 00 35-00 37 E3 91 01 74 01 00	
00 01 00 00 00 00 00 00-07 67 61 74 65 77 61 79	
09 6D 65 73 73 65 6E 67-65 72 07 68 6F 74 6D 61	
69 6C 03 63 6F 6D 00 00-01 00 01 E6 84 1A 00 00	
Decoded Format:	_
192.168.1.10,1483 -> 168.95.1.1,domain	
Pr udp HLen 20 TLen 75	

Decoded Format

It shows the source IP address (local), destination IP (remote) address, the protocol and length of the package.

Refresh

Click it to reload the page.

3.15.2 Routing Table

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

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

```
Current Running Routing Table | Refresh |

Key: C - connected, S - static, R - RIP, * - default, ~ - private

* 0.0.0.0/ 0.0.0.0 via 172.16.3.1, WAN1

C~ 192.168.1.0/ 255.255.255.0 is directly connected, LAN

C 172.16.3.0/ 255.255.255.0 is directly connected, WAN1
```

Refresh

Click it to reload the page.

3.15.3 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.

Diagnostics >> View ARP Cache Table

thernet ARP Cache	Table	<u>Clear</u> <u>Refresh</u>
IP Address	MAC Address	
192.168.1.10	00-0E-A6-2A-D5-A1	
172.16.3.112	00-40-CA-6B-56-BA	
172.16.3.132	00-05-5D-E4-ED-86	
172.16.3.20	00-0D-60-6F-83-BC	
172.16.3.121	00-0C-6E-E7-79-99	
172.16.3.141	00-11-2F-C7-39-0B	
172.16.3.133	00-50-7F-23-4D-B1	
172.16.3.179	00-11-2F-4B-15-F2	
172.16.3.21	00-05-5D-A1-2B-FF	
172.16.3.2	00-11-D8-68-0D-AE	
172.16.3.18	00-50-FC-2F-3D-17	
172.16.3.151	00-50-7F-2F-33-FF	
172.16.3.19	00-0D-60-6F-89-CA	•

Refresh

Clear

Click it to reload the page.

Click it to clear the whole table.

3.15.4 DHCP Table

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

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

DHCP IP Assignment Table <u>Refresh</u>					
DHCP se Index 1	erver: Running IP Address 192.168.1.10	MAC Address 00-0E-A6-2A-D5-A1	Leased Time 0:00:02.630	HOST ID ok-leegjyiy075u	
					×
ndex		It dis	plays the conn	ection item numb	er.
P Address			It displays the IP address assigned by this router for specified PC.		
AC Address			It displays the MAC address for the specified PC that DHCP assigned IP address for it.		
eased	Time	It dis	It displays the leased time of the specified PC.		
IOST	ID	It dis	It displays the host ID name of the specified PC.		

3.15.5 NAT Sessions Table

Refresh

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

Diagnostics >> NAT Sessions Table

Active Sessions	Table					<u>Refres</u>
Private IP	:Port	#Pseudo Port	Peer IP	:Port	Interface	
192.168.1.11	2491	 52078	24.9.93.189	443	 WAN1	
192.168.1.11	2493	52080	207.46.25.2	80	WAN1	
192.168.1.10	3079	52665	207.46.5.10	80	WAN1	

Click it to reload the page.

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.

3.15.6 Data Flow Monitor

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

imit Session			
Enable	🔘 Disable		
Default Max	< Sessions: 100		
Limitation L	ist		
Index 9	Start IP	End	IP

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

🗌 Enab	le Data Flow Mon	iitor	Refresh Seconds: 10 💌 P	age: 1 💌 🛛	Refresh
Index	IP Address	TX rate(Kbps)	RX rate(Kbps) 🗸	Sessions	Action
		Current / Deals / Succed	Current / Deals / Succed	Current / De als	
1878 MIA	170.14.0.000	Current / Peak / Speed	Current / Peak / Speed	Current / Peak	
WAN1	172.16.3.229	1 / 1655 / Auto	1 / 852 / Auto		
WAN2		0/0/Auto	0/0/Auto		
Total		1 / 1655 / Auto	1 / 852 / Auto	6 / 44	

Diagnostics >> Data Flow Monitor

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

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

- 3. (Kbps): shared bandwidth
 - + : residual bandwidth used
 - Current/Peak are average.

Enable Data Flow Check this box to enable this function. **Monitor**

Refresh Seconds	Use the drop down list to choose the time interval of refreshind 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.

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

Page: 1	*	<u>Refresh</u>
Kbps)	Sessions	Action
		<u>Block</u>

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

Page:	1 🕶	<u>Refresh</u>
s <u>)</u>	Sessions	Action
	blocked / 299	<u>Unblock</u>

Current /Peak/Speed Curr

Action

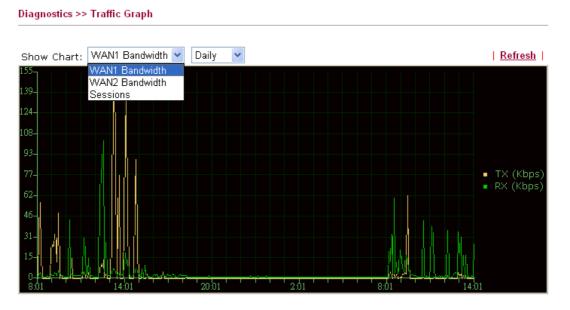
Current means current transmission rate and receiving rate for WAN1/WAN.

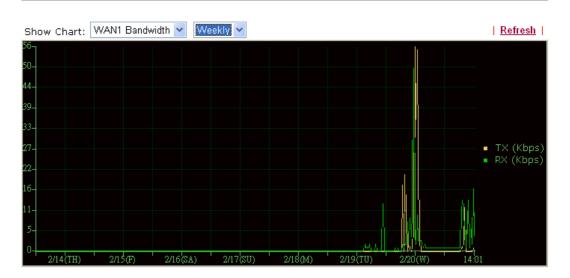
Peak means the highest peak value detected by the router in data transmission.

Speed means line speed specified in **WAN>>General**. If you do not specify any rate at that page, here will display **Auto** for instead.

3.15.7 Traffic Graph

Click **Diagnostics** and click **Traffic Graph** to pen the web page. Choose WAN1 Bandwidth/WAN2 Bandwidth, Sessions, daily or weekly for viewing different traffic graph. Click **Refresh** to renew the graph at any time. The following two figures display different charts by daily and weekly.





Diagnostics >> Traffic Graph

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

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

3.15.8 Ping Diagnosis

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

Diagnostics >> Ping Diagnosis

		LAN PC or you don't wa lease select "Unspecifie	
Ping thr	ough: WAN1	*	
Ping to:	Host / IP 🛛 💌	IP Address:	
Result	Host / IP GateWay1 GateWay2 DNS	Run	<u>Clear</u>

Ping through	Use the drop down list to choose the WAN interface that you want to ping through or choose Unspecified to be determined by the router automatically.	
	Ping through: Unspecified V Unspecified WAN1 WAN2	
Ping to	Use the drop down list to choose the destination that you want to ping.	
IP Address	Type in the IP address of the Host/IP that you want to ping.	
Run	Click this button to start the ping work. The result will be displayed on the screen.	
Clear	Click this link to remove the result on the window.	

Vigor2930 Series User's Guide

3.15.9 Trace Route

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

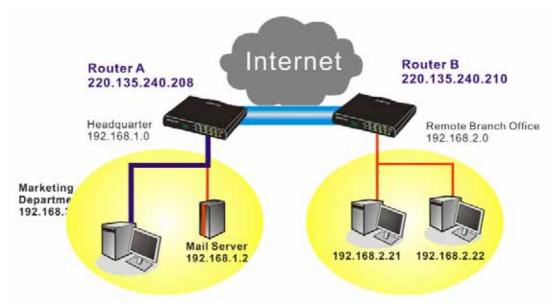
Diagnostics >>	Trace Route		
Trace Route			
	Trace through:	WAN1 💌	
	Host / IP Address:		Run
	Result		<u>Clear</u>
	Trace through WAN1. traceroute to 172.16 1 Request timed ou 2 Request timed ou Trace complete.	at. *	

Use the drop down list to choose the WAN interface that you want to ping through or choose Unspecified to be determined by the router automatically.
It indicates the IP address of the host.
Click this button to start route tracing work.
Click this link to remove the result on the window.

4 Application and Examples

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

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



Settings in Router A in headquarter:

- 1. Go to **VPN and Remote Access** and select **Remote Access Control** to enable the necessary VPN service 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 fo	or Dial-In Users
Dial-In PPP Authentication	PAP or CHAP	Start IP Address	192.168.1.200
Dial-In PPP Encryption (MPPE)	Optional MPPE		
Mutual Authentication	(PAP) 🔘 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

Vigor2930 Series User's Guide

parties have known.

PN IKE/IPSec General Setup		
	s and Dynamic IP Client (LAN to LAN).	
IKE Authentication Method		
Pre-Shared Key	••••	
Confirm Pre-Shared Key	••••	
IPSec Security Method		
🗹 Medium (AH)		
Data will be authentic, but	t will not be encrypted.	
High (ESP) 🛛 🗹 DES 📝	3DES 🔽 AES	
Data will be encrypted and	d authentic.	

- 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 Branch1	Call Direction 💿 Both 🔿 Dial-Out 🔿 Dial-In
Enable this profile	Always on
	Idle Timeout 300 second(s)
VPN Connection Through: WAN1 First 💙	Enable PING to keep alive
	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.

Type of Server I am calling	Link Type	Eda tert (m)
ISDN PPTP IPSec Tunnel I2TP with IPSec Policy films Idia Number for ISDN or Server IP/Host Name for VPN. (such as 5551234, draytek.com or 123,45,67,89) [220,136,240,250	Usemame Password PPP Authentication PAPICHAP P VJ Compression 3 On Off	
	Pre-Shared Key	
	IKE Pre-Shared Key	
	O Digital Signature(X.S09)	
	IPSec Security Method Medium(AH) High(ESP) DES with Advanced	ng Adriedcedory 🚿
	Indux(1-15) in <u>Schedule</u> Setup:	
	Callback Function (CBC	

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

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

Type of Server I am calling	Link Type	64b. hpt : 28
O ISDN	Usemame	draytek
O PPTP	Password	
IPSec Tunnel L2TP with IPSec Policy	PPP Authentication V3 Compression	PAP/CHAP
		⊙ on ○ off
Dial Number for ISDN or Server IP/Host Name for VPN. (such as 5551234, draytek.com or 123,45.67.89) 220.135.240.250	IKE Authentication Met	hed
	IKE Pre-Shanot Key	*****
	Digital Signature(X.S	(09)
	fling =	
	IPSec Security Method Medium(AH) High(ESP)	hid Adhetikation 🚿
	Index(1-15) in Schedul	setup:
	Callback Function (CBC	Callback

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

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

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

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

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

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

4. TCP/IP Network Settings	3	
My WAN IP	0.0.0.0	RIP Direction Disable 👻
Remote Gateway IP	0.0.0.0	From first subnet to remote network, you have to do
Remote Network IP	192.168.2.0	Route 🛩
Remote Network Mask	255.255.255.0	
	More	$\hfill\square$ Change default route to this VPN tunnel (Only single WAN supports this)
	ОК	Clear Cancel

Settings in Router B in the remote office:

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

PPP General Setup		
PPP/MP Protocol	IP Address Assignment f	or Dial-In Users
Dial-In PPP Authentication PAP or CHAP V	Start IP Address	192.168.2 200
Dial-In PPP Encryption (MPPE) Optional MPPE		
Mutual Authentication (PAP) 🛛 🔘 Yes 💿 No		
Username		
Password		

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

VoIPon www.voipon.co.uk sales@voipon.co.uk Tel: +44 (0)1245 808195 Fax: +44 (0)1245 808299

parties have known.

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

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

1. Common Settings			
Profile Name	Branch1	Call Direction 💿 Both 🔿 Dial-Out 🔿 Dial-In	
Enable this profile		🔲 Always on	
VPN Connection Through: WAN1 First 💌		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.

Type of Server I am calling	Link Type	Sdk hpu
O 15DN O PPTP O IPSec Tunnel O L2TP with IPSec Policy Telms Dial Number for ISDN or Server IP/Host Name for VPN. (such as 551234, draytek.com or 123,45,67,99)	Username 1777 Password PPP Authentication PARCHAP of V3 Compression on O Off IKE Authentication Method ③ Pre-Shared Key	
220.135.240.208	KE Pre-Shared Key O Digital Signature(X.5)	- Contractory
	IPSec Security Method Medium(AH) High(ESP) Internet Advanced Index(1-15) in Schedule Callback Function (CBC Require Remote to Provide ISDN Number Provide ISDN Number	e 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.

z. Diai-our setuilys		
Type of Server I am calling	Link Type	64k bps 🗸
O ISDN	Username	draytek
● PPTP	Password	••••••
O IPSec Tunnel	PPP Authentication	
O L2TP with IPSec Policy None	VJ Compression	💿 On 🔘 Off
Dial Number for ISDN or Server IP/Host Name for VPN. (such as 5551234, draytek.com or 123.45.67.89)	IKE Authentication Metho Pre-Shared Key	od
220.135.240.208	IKE Pre-Shared Key	•••••
	 Digital Signature(X.50 	19)
	None 🗸	
	IPSec Security Method Medium(AH)	
	O High(ESP) DES with	out Authentication 🔽
	Advanced	
	Index(1-15) in <u>Schedule</u>	Setup: ,,
	Callback Function (CBCP)
	🗌 Require Remote to	Callback
	Provide ISDN Number	er to Remote

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

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

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

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

3. Dial-In Settings

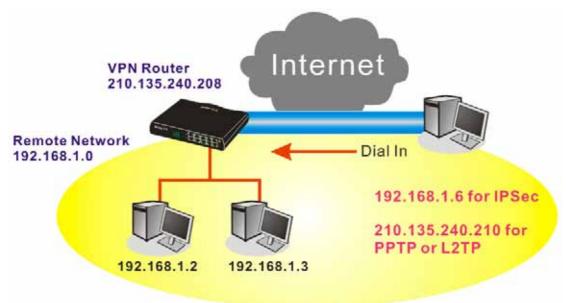
Allowed Dial-In Type		
ISDN ISDN	Username	draytek
PPTP	Password	••••
🔲 IPSec Tunnel	VJ Compression	💿 On 🔘 Off
L2TP with IPSec Policy None	IKE Authentication Method	d
Specify ISDN CLID or Remote VPN Gateway	🗹 Pre-Shared Key	
Peer ISDN Number or Peer VPN Server IP	IKE Pre-Shared Key	
220.135.240.208	Digital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

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

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

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

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



Settings in VPN Router in the enterprise office:

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

PPP General Setup		
PPP/MP Protocol	IP Address Assignment for Dial-In U	sers
Dial-In PPP Authentication	Start IP Address 192	.168.1.200
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 **IKE/IPSec General Setup**, such as the pre-shared key that both parties have known.

VPN and Remote	Access >> IP	Sec 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 I	LAN).
----------------	--------------	---------------	-------------	-----------	-----------	-------

IKE Authentication Method	
Pre-Shared Key	••••
Confirm Pre-Shared Key	•••••
IPSec Security Method	
🗹 Medium (AH)	
Data will be authentic, bu	t will not be encrypted.
High (ESP) 🛛 🔽 DES 🔽	3DES 🗹 AES
Data will be encrypted an	d authentic.
	OK Cancel

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

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

Jser account and Authentication			
🗹 Enable this account	Username ???		
Idle Timeout 300 second(s)	Password		
Allowed Dial-In Type	IKE Authentication Method		
ISDN	Pre-Shared Key		
PPTP	IKE Pre-Shared Key		
🗹 IPSec Tunnel	Digital Signature (X.509)		
📃 L2TP with IPSec Policy None 🛛 💟	None 🕶		
✓ Specify Remote Node Remote Client IP or Peer ISDN Number 210.135.240.210 or Peer ID	IPSec Security Method ✓ Medium (AH) High (ESP) ✓ DES ✓ 3DES ✓ AES Local ID (optional)		
	Callback Function		
	Check to enable Callback function		
	Specify the callback number		
	Callback Number		
	Check to enable Callback Budget Control		
	Callback Budget 30 minute(s)		

Vigor2930 Series User's Guide

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.

idex No. 1			
Jser account and Authentication			
Enable this account	Username draytek		
Idle Timeout 300 second(s)	Password •••••		
Allowed Dial-In Type	IKE Authentication Method		
ISDN	🗹 Pre-Shared Key		
PPTP	IKE Pre-Shared Key		
IPSec Tunnel	Digital Signature (X.509)		
L2TP with IPSec Policy None	None 🗸		
 Specify Remote Node Remote Client IP or Peer ISDN Number 210.135.240.210 or Peer ID 	IPSec Security Method Medium (AH) High (ESP) DES Ø 3DES Ø AES Local ID (optional)		
	Callback Function		
	Check to enable Callback function		
	Specify the callback number		
	Callback Number		
	Check to enable Callback Budget Control		
	Callback Budget 30 minute(s)		

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.

	ad the Prohibitip:	Sec registry value	to computer in
	ure a L2TP/IPSec	connection using infomation, please	a pre-shared key
		Infomation, please ledgement Base.	read the arccie
	Cor	nfigure	
and an all his	Land 1		
Step 1. Dial to		this ID you can d	in this stan
and the second se		ublic IP, you can s	kip this step.
and the second se		ublic IP, you can s	lap this step.
and the second se		ublic IP, you can s	
If you have al		۲	
If you have al	ready gotten a p	۲	Del
If you have al	ready gotten a p		

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/HO	5T Name(such as 123.45.67.89 or draytek.com)
192.168.1.1	
User Name :	die riel_ser.
Password :	******
Type of VPN	
O PPTP	OL2TP
O IPSec Tunn	el OL2TP over IPSec
PPTP Encryption No encrypt Require an	
	gateway on remote network
ОК	Cancel

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

My IP : 172.16.3.10	0			v
Type of IPSec				
O Standard IPSec Tunnel				
Remote Subnet :	U.			ų
Remote Subnet Mask :	:55	- 55	: 55	U.
Virture IP Dray	Tek Virtur	e Inter	face	~
③ Obtain an IP address .	automatic	ally (Di	HCP ove	r IPSec
O Specify an IP address		-		1
IP Address:	L.S.	160		200
Subnet Mask:		-55	-55	.0
Security Method				
	High(ES	P)		
Security Method O Medium(AH)	High(ES	iP)		*
O Medium(AH)		P)		*
Medium(AH)		P)		*
O Medium(AH)		P)		*
Medium(AH)		(P)	- Brov	¥

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

Vigor2930 Series User's Guide

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

Dial To VPN		2
Session Name:	office	
VPN Server IP/HC	ST Name(s	such as 123.45.67.89 or draytek.com)
192.168.1.1		
User Name :	drayte	k_user1
Password :	****	
Type of VPN	-	
• PPTP		OL2TP
O IPSec Tun	nel	OL2TP over IPSec
PPTP Encryption	tion	
O Maximum :		
	_	on remote network

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

4.3 QoS Setting Example

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

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

Bandwidth Management >> Quality of Service

Index	Status	Bandwidth	Directon	Class 1	Class 2	Class 3	Others	UDP Bandwidth Control	
WAN1	Disable	10000Kbps/10000Kbps		25%	25%	25%	25%	Inactive	Setup
WAN2	Disable	10000Kbps/10000Kbps		25%	25%	25%	25%	Inactive	<u>Setup</u>
Class Ru Inde		N	ame				Rule	Service	Туре
Class	51						<u>Edit</u>		
Class	52						<u>Edit</u>	<u>Edit</u>	
Class	5 3						Edit		

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

VoIPon www.voipon.co.uk sales@voipon.co.uk Tel: +44 (0)1245 808195 Fax: +44 (0)1245 808299



3. Set Inbound/Outbound bandwidth.

Bandwidth Management >> Quality of Service

WAN1 General Setup

Enable the Gos Control Donn
WAN Inbound Bandwidth
WAN Outbound Bandwidth

10000	Kbps
10000	Kbps

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

Return to previous page. Enter the Name of Index Class 1 by clicking Edit link. Type the name "E-mail" for Class 1.
 Bandwidth Management >> Quality of Service

Class Ind	lex #1						
Name	E-mail						
NO	Status	Local Address	Remote Address	DiffServ CodePoint	Service Type		
1 🔿	Inactive	Any	Any	ANY	undefined		
	Add Edit Delete						
		٢	OK Cancel	7			

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

Enable the QoS C	ontrol BOTH 🚩	
WAN	Inbound Bandwidth	10000 Kbps
WAN	Outbound Bandwidth	10000 Kbps
Index	Class Name	Reserved_bandwidth Ratio
Class 1	E-mail	25 %
Class 2		25 %
Class 3		25 %
	Others	25 %
Enable UDP Band	width Control	Limited_bandwidth Ratio 25 %
Outbound TCP AG	CK Prioritize	

Bandwidth Management >> Quality of Service

Vigor2930 Series User's Guide

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

Class Inde	x #2					
Name H	TTPS					
NO	Status	Local Address	Remote Address	DiffServ CodePoint	Service Type	
1 🔿	Active	Any	Any	ANY	ANY	
	Add Edit Delete					
			OK Cancel			

7. Click **Setup** link for WAN1.

Bandwidth Management >> Quality of Service

Bandwidth Management >> Quality of Service

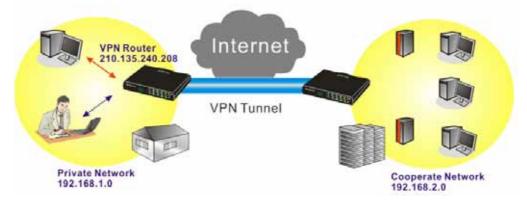
General	Setup							Set to Factory	<u>Default</u>
Index	Status	Bandwidth	Directon	Class 1	Class 2	Class 3	Others	UDP Bandwidth Control	
WAN1	Disable	10000Kbps/10000Kbps		25%	25%	25%	25%	Inactive	<u>Setup</u>
WAN2	Disable	10000Kbps/10000Kbps		25%	25%	25%	25%	Inactive	<u>Setup</u>
Class Ri									
Inde	ex	N	ame				Rule	Service	туре
Inde Class			a me -mail				Rule Edit	Service	Туре
	5 1	E						Edi	

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

WAN1 General Set		
W	/AN Inbound Bandwidth	10000 Kbps
V	/AN Outbound Bandwidth	10000 Kbps
Index	Class Name	Reserved_bandwidth Ratio
Class 1	E-mail	25 %
Class 2	HTTPS	25 %
Class 3		25 %
	Others	25 %
	andwidth Control	Limited_bandwidth Ratio 25 %
🔲 Outbound TC	P ACK Prioritize	
	OK Clear	Cancel

9. If the worker has connected to the headquarter using host to host VPN tunnel. (Please refer to Chapter 3 VPN for detail instruction), he may set up an index for it. Enter the

VolPon www.voipon.co.uk sales@voipon.co.uk Tel: +44 (0)1245 808195 Fax: +44 (0)1245 808299



Class Name of Index 3. In this index, he will set reserve bandwidth for 1 VPN tunnel.

10. Click Edit to open a new window.

Bandwidth Management >> Quality of Service

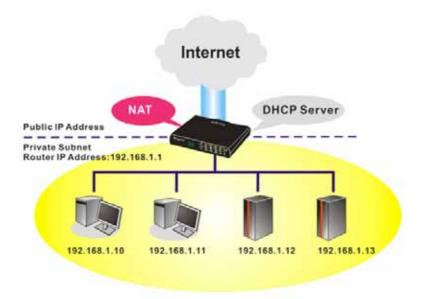
andwidth	n Managemei	nt >> Quality of Servi	ce		
lass Inde	ex #1				
ame 🛛	Fest				
NO	Status	Local Address	Remote Address	DiffServ CodePoint	Service Type
1	Empty	-	-	-	-
			Add Edit Delete	3	
		ſ	OK Cancel	1	

11. First, check the **ACT** box. Then click **Edit** of **Local Address** to set a worker's subnet address. Click **Edit** of **Remote Address** to set headquarter's subnet address. Leave other fields and click **OK**.

🗹 ACT						
Local Address	Any	Edit				
Remote Address	Any	Edit				
DiffServ CodePoint	ANY	~				
Service Type	ANY	~				
Note: Please choose/setup the Service Type first.						

4.4 LAN - Created by Using NAT

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

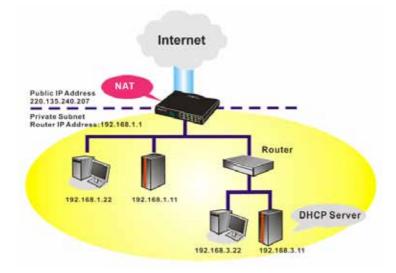


LAN >> General Setup

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

LAN IP Network Configura	tion	DHCP Server Configuration		
For NAT Usage		⊙Enable Server ○Disable Server		
1st IP Address 192.168.1.1		Relay Agent: 🔘 1st Subnet 🔾 2nd Subnet		
1st Subnet Mask	255.255.255.0	Start IP Address	192.168.1.10	
For IP Routing Usage 🔘	Enable 💿 Disable	IP Pool Counts	50	
2nd IP Address	192.168.2.1	Gateway IP Address	192.168.1.1	
2nd Subnet Mask	255.255.255.0	DHCP Server IP Address		
2n	d Subnet DHCP Server	for Relay Agent DNS Server IP Address		
		Force DNS manual setting		
RIP Protocol Control	Disable 💙	Primary IP Address		
		Secondary IP Address		

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



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

LAN >> General Setup

AN IP Network Configura	ition	DHCP Server Configuration	DHCP Server Configuration		
For NAT Usage		🔘 Enable Server 💿 Disal	ble Server		
1st IP Address	192.168.1.1	Relay Agent: 🔘 1st Sul	onet 🔾 2nd Subnet		
1st Subnet Mask	255.255.255.0	Start IP Address	192.168.1.10		
For IP Routing Usage 🤇) Enable 💿 Disable	IP Pool Counts	50		
2nd IP Address	192.168.2.1	Gateway IP Address	192.168.1.1		
2nd Subnet Mask	255.255.255.0	DHCP Server IP Address			
2	nd Subnet DHCP Server	DNS Server IP Address			
			etting		
RIP Protocol Control	Disable 💌	Primary IP Address			
		Secondary IP Address			

4.5 Calling Scenario for VoIP function

4.5.1 Calling via SIP Sever

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

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

	Display Name	David
	SIP URL	4321 @ iptel.org
	Loop through	None 💌
r .	Backup Phone Number	
	OK	Clear Cancel

Phone Number

Phone Book Index No. 1

VolP >> SIP Account

SIP Accounts Settings ----

CODEC/RTP/DTMF ----

(Use default value)

Settings for David

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

Profile Name	draytel 1	(11 char max	0
Register via	ALEO	nake call without	register
SIP Port	5060		
Domain/Realm	drayfel org		(63 char mar.)
Provy	draytel org		(63 charman.)
Act as outbound p	aug si A		
Display Name	John	(23 char mai	3
Account Number/Name	1234		(63 char max.)
Authentication 10			(63 char man.)
Password			(63 char mail.)
Expiry Time	1 hour 🗮 [HUI]	sec	
NAT Traversal Support	None 💌		
Ring Port	EValP1 EValP2	1504	
Ring Pattern	1 -		

1111

John calls David ---

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

🗹 Enable			
	Phone Number	2222	
	Display Name	John]
	SIP URL	1234	@ draytel.org
	Loop through	None 🛩	
	Backup Phone Number]
	OK	Clear	Cancel

SIP Accounts Settings ---

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

CODEC/RTP/DTMF ----(Use default value)

il⁴ Account lades No. 1 Profile Name (11 char mar.) Register via make call without register SIP Part 5060 Domary/Real iptel urg (63 char max.) stel org Proxy (63 char max.) Act as out Dripley Name David (23 char man.) Account Number/ 4321 (63 char max.) Authentication 10 (63 char mail) Password (63 char man.) 1 hour Expry Time NAT Traversal Su None . . EVOPS EVOPS ISDN **Ring Port** Ring Fatterr 1 -OK Cancel

David calls John

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

Example 2: Both John and David have SIP Addresses from the same service provider. John's SIP URL: 1234@draytel.org , David's SIP URL: 4321@draytel.org

Settings for John

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

SIP Accounts Settings ----

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

CODEC/RTP/DTMF ----

(Use default value)

Settings for David

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

SIP Accounts Settings ----

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

CODEC/RTP/DTMF----

(Use default value)

Errable				
	Phone Number	1111		
	Display Name	David		
	RUP LINE.	43/1	-Quintraylations	
	toop through	National 👾		
	Bactup Phone Number			

Volt >> SIP Assesses

Peadler Nome	invytes 1 (11 char r	nas.3
Register via	Ade 🗧 🗇 make cat with	wind impostore
SIF Port	5060	
Contain/Viealm	draytal org	(65 chiar mar.)
Penange .	shapping ang	(6.7 char max.)
Act as outbound p	roiry	
Display Name	John (23 churr	nar.)
locount Number/Name	1254	(63 that mac.)
Authentication ID	No. PI	(62 char mail.)
Fassword	****	(65 char max.)
Expiry Time:	There is a second	
NAT Traversal Support	None -	
Firig Port	Privers Tivers Ison	
Tang Pattern	1 -	

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)

E Recalifier			
Phone trumber	2222		
Display Namel	Julia		1
SIP UPL	1234		(di di sergi di sergi
Loop through	Non	-	
Backup Phone No.	mber		
off in SIP Accounts			
Profile Name	draytel 8	(11)	(har mar.)
Rogictor wia	Auto ×		il without register
1222 200 20 F	5060		
SIP Part	5060		
DomanyPealm	draytet erg		(63 char max.)
DomanyRealm Proxy	draytal org draytal org		(63 chur max.) (63 chur max.)
DomanyPealm Proxy DAct. as suttoand (draytel org draytel org draytel arg		(63 chur mar.)
DomanyPealm Proxy DAct as extracted (Display teams	draytel org draytel org rocy David	(83	(63 chur max.)
Domany/Pealm Proxy Intelligence worksound a pringing teams Account Number/Name	draytel org draytel org draytel arg	(23)	(63 chur max.) Char mai.) (63 char mai.)
Domany/Brailm Prony Mich.ac. webseuld (Utiping teams Account Number/Name Account Number/Name	draytel org draytel org rocy David	(23	(61 chur max.) char max.) (63 char max.) (63 char max.)
Contary/Bealm Proxy Dack as authorized a binplay teams Account Number/Name Account Number/Name	draytet org draytet org runy David 4321		(61 chur max.) char mail.) (63 char mail.) (63 char max.) (63 char max.)
Contary/Bealm Proxy Act as softward a piliptry Name Account Number/Name Activity Name Activity Name Repry Time	draytet org draytet org David 4221 1 hour 🖌 🕄		(61 chur max.) char max.) (63 char max.) (63 char max.)
Contary/Bealm Proxy Dack as authorized a binplay teams Account Number/Name Account Number/Name	draytet org draytet org runy David 4321	ar).	(63 chur max.) (63 chur max.) (63 chur max.) (63 chur max.) set

David calls John

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

4.5.2 Peer-to-Peer Calling

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

Phone Book Index No. 1

VolP >> DialPlan Setur

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)

Settings for Paulin

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

SIP Accounts Settings ----

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

CODEC/RTP/DTMF----

(Use default value)

Enable			
Phone Numbe	r 1111	1	
Display Name	paul	in	
SIP URL	4321	1	@ 203.69.175.24
Loop through	Non	ie 🗸	
Backup Phone	e Number		
IP >> SIP Accounts	OK	Clear	Cancel
P Account Index No. 1	10.0		
Profile Name	Paule		cher max.)
Register via	None 🖷		char max.) all without register
Register via SIP Port			all without register
Register via SIP Port DomanyRealm	None 🖷		all without register (63 char man.)
Register via SIP Port Domary/Realm Proxy	None -		all without register
Register via SIP Port Domary/Realm Proxy Act as outbou	None S000	🖸 make c	(63 char mar.) (63 char mar.)
Register via SIP Port Doman,Riealm Proxy Act as outbou Display Name	Amar	🖸 make c	(63 char mar.) (63 char mar.) (63 char mar.)
Register via SIP Port Doman/Realm Proxy Act as outbou Display Name Account Number/Nam	None S000	🖸 make c	(63 char mar.) (63 char mar.) (63 char mar.) (63 char mar.)
Register via SIP Port DomanyRealm Proxy Act as outbou Display Name Account NumberyNa Account NumberyNa	None S000	🖸 make c	(63 char mar.) (63 char mar.) (63 char mar.) (63 char mar.) (63 char mar.)
Register via SUP Port Doman/Realm Proxy Act as outbou Display Name Account Number/Na Account Number/Na Password	None S000	[] make c	(63 char man.) (63 char man.) (63 char man.) (63 char man.) (63 char man.)
Register via SIP Port Domain/Realm Proxy Act as outbou Display Name Account Number/Nae Account Number/Nae Act Act Act Act Act Act Nation D Password Expiry Time	Amar Amar net provy Amar 1224 0 1 bear	[] make c	(63 char mar.) (63 char mar.) (63 char mar.) (63 char mar.) (63 char mar.)
Register via SIP Port Doman/Realm Proxy Act as outbou Display Name Account Number/Na Account Number/Na Password	Name e 5000 Amps me 1234 D 1 haur e 1 haur e	[] make c	all without register (63 char man.) (63 char man.) (63 char man.) (63 char man.) (63 char man.) sec

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

ble					
Phone Number		2222			
Display Name		Amor			
SIP URL	SIP URL			@214.61.1	72.53
Loop through		None 🔽			
Backup Phone Nu	ımber				
Profile Name	Amur		(11 0	har.max.)	
contindex No. 1					
	210.00	(11 char max.)			
Register via	None		make cal	without re	gister
SIP Port	5060				
Domain/Realm				0	13 char man
Proce	1			0	3 char mai
EAct as outbound	A Designation of the local division of the l				
Display Name	Pain		(73 0	har max.}	
Account Number/Name	4321			(3 char mai
Authentication ID				0	13 char mai
Password				(61	char max.)
Expiry Time	1 hour	M 1101	9	ic .	
NAT Traversal Support	None	7			
Ring Port	E VolP	t ⊡votP2	: SON		

Paulin calls Arnor

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

4.6 Upgrade Firmware for Your Router

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

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

Please remember to set as follows in your DrayTek Router :

- Server IP Address : IP address of the PC that runs the Syslog
- Port Number : Default value 514

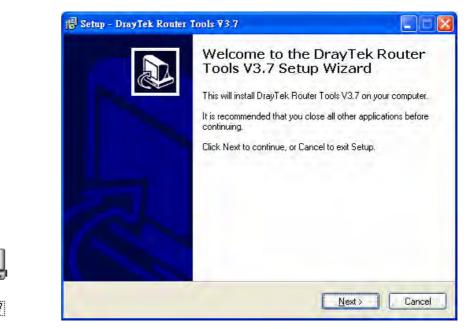
Install Now!

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

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

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

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



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

L Firmware Upgrade	Otility 3.5.2	
Operation Mode	Router IP:	
💽 Upgrade		
O Dealors Cathlers	Firmware file:	
O Backup Setting		
Time Out(Sec.)	Password:	
5		
Port		
69	Abort.	Send

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

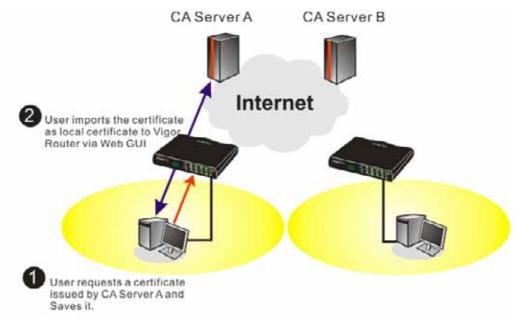
🚔 Firmware Upgrade I	Jtility 3.5.2
Operation Mode Upgrade Backup Setting	Router IP: 192.168.1.1 Firmware file: C:\Documents and Settings\Carrie
Time Out(Sec.)	Password:
5	
Port 69	Abort Send

14. Click Send.

៉ Firmware Upgrade	Utility 3.5.2 🔽 🗖 🔀
Operation Mode Upgrade Backup Setting	Router IP: 192.168.1.1 Firmware file: C:\Documents and Settings\Carrie
Time Out(Sec.)	Password:
5	
Port	
69	Abort Send
Sending	

15. Now the firmware update is finished.

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



Vigor2930 Series User's Guide

215

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

Certificate Management >> Local Certificate

Name	Subject	Status	Modify
ocal			View Delete
NERATE X509 Local Cert	IMPORT REFRESH		
			<

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

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

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

Name	Subject	Status	Modify
Local	/C=TW/O=Draytek/emailAddress	Requesting	View Delete
ENERATE	IMPORT REFRESH		
X509 Lo	al Certificate Request		
MIIBqj Bgkqhk A4GNAD 3wDeQy du84t2 oCkwJw hkiG9w uRLq4C I9Fqkj	CGIN CERTIFICATE REQUEST CCARMCAQAwQTELNAkGAIUEBhMCVFcxEDAOI (G9w0BCQEWEXByZXN2QGRyYX102W=uY29t) CBIQKBgQDPioahu/gFQaYB1ce50ERSDfWkc coV1LBJz2IDF0xjX6ip?ev187twwTsq41g; btWBdMD4W5C8VmSyDjShLhjdxVYPWpNKVI; UKoZIhvcNAQkOMRowGDAWBgNVHRED2AM, DBAQUFAAOBgQAuSBRUGt4W1hH9N6/HwToen LEi6nV4hMRytcx2pE26sMarSgRREr86RoOC INihip4TCjecSNN2jmQOSWU+Bce8TG+SCB0 D CERTIFICATE REQUEST	MIGHMADGCSqGS hIdHblo1kt9cT Z6Qk/rGhuVTKd cOT2RZjkRMaHE ggtkcmF5dGVrL mltHQbcwjXvg/ 3JxOI45560xCZ	Ib3DQEBAQUA dLUDaFk6s8d 9j6PlcrnkP7 WpVpwIDAQAB mNvbTANBgkq t7Kf1ETJiHh /NIGh9VQ911

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

Microsoft Certificate Services vigor	<u>Home</u>
Welcome	
You use this web site to request a certificate for your web browser, e-mail client, or other secure program. Once you acquire a certificate, will be able to securely identify yourself to other people over the web, sign your e-mail messages, encrypt your e-mail messages, and mor depending upon the type of certificate you request.	
Select a task:	
 ○ Retrieve the CA certificate or certificate revocation list ④ Request a certificate 	
○ Check on a pending certificate	
Next 2	>

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

Alicrosoft Centricate Services - vigor	Home
Advanced Certificate Requests	
You can request a certificate for yourself, another user, or a computer using one of the following methods. Note that the authority (CA) will determine the certificates that you can obtain.	policy 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	id PKCS #7 file
Request a certificate for a smart card on behalf of another user using the Smart Card Enrollment Station. You must have an enrolment agent certificate to submit a request for another user.	

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

Microsoft Louisco	le Gerintes - ingel		Haine
Submit A Save	d Request		
		equest or PKCS #7 renewal request generated by to the certification authority (CA).	an external application (such as a web
Saved Request			
Certificide Réquest		BirHCVFexEDA0 YTL102MenY29E //IeQw6032K++ c2dFFFVILeP3	
	Envyze for a file to insert.		
Certificate Templa	ite:		
Additional Attribu	Administrator Contract Administrator Administrator Authenticated Session Basic EFS		
Attributes	EFS Recovery Agent. User IPSEC (Offine request) Doctor (Offine request)		
	Subordinate Certification Authority Web Server		Submit 2

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

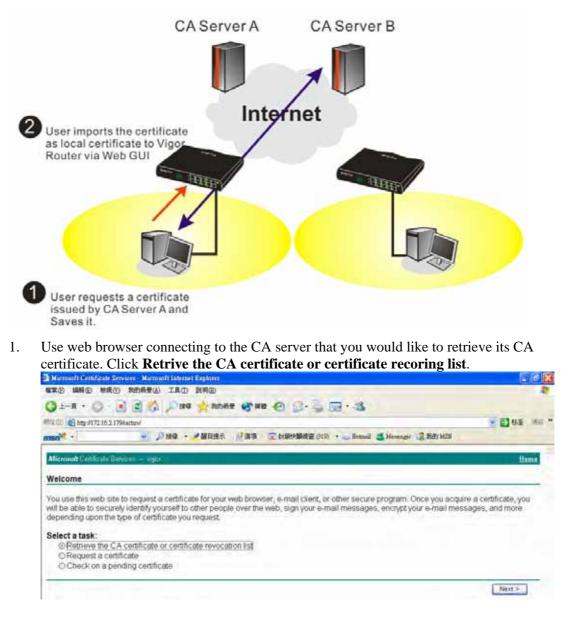
5. Back to Vigor router, go to **Local Certificate**. Click **IMPORT** button and browse the file to import the certificate (.cer file) into Vigor router. When finished, click refresh and you will find the below window showing "-----BEGINE CERTIFICATE-----...." Certificate Management >> Local Certificate

Name Subject	Status	Modify
Local /C=TW/O=Draytek/emailAddress	Not Valid Yet	View Delete
ENERATE IMPORT REFRESH		
X509 Local Certificate Request		
BEGIN CERTIFICATE REQUEST MIIBqjCCARMCAQAwQTELMAkGA1UEBhMCVFcxEDAOI BgkqhkiG9w0BCQEWEXByZXNZQGRYYX10ZWsuY29tJ A4GNADCBiQKBgQDPioahu/gFQaYBice50ERSDfWkn 3wDeQytoV1LBJz21DF0xjX6ip7ev187twwTsg4lg3 du84t23tWBdMD4W5c8VmSyDjShLhjdxVYPWpNKVIn oCkwJwYJKoZIhvcNAQkOMRowGDAWBgNVHREEDzANQ hkiG9w0BAQUFAA0BgQAuSBRUGt4W1hH9N6/HwToer uRLq4CiEi6nV4hMRytcxZpEZ6sMarSgREr86R006 ISFqkjJNihip4TCjecSNNZjmQo5WU+Bce8TG+SC80	MIGIMAOGCSqGS nIdHblo1kt9cT Z6Qk/rGhuVTKd rOT2RZjkRMaHE ggtkcmF5dGVrL m1tHQbcwjXvg/ 8JxOI45560xCZ	Ib3DQEBAQUA dLUDaFk6s8d 9j6PlcrnkP7 WpVpwIDAQAB mNvbTANBgkq t7kFlzTJiHh /NIGh9VQ9I1

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

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

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



Vigor2930 Series User's Guide

219

- 2. In **Choose file to download**, click CA Certificate **Current** and **Base 64 encoded**, and **Download CA certificate** to save the .cer. file.
 - 🗃 Marausoft Certificato Services Marausoft Internet Explore Q 1-R • Q • 🖹 🖹 🏠 🔎 00 👷 0000 😵 00 🙆 🤮 🔂 • 🚳 #12:00 @ http://172.16.2.1794.etto:v/iettoac.ett - E 4E mit - Main · 2100 • 《朝田操示 🕂 Mill 文 któlef Maltin (319) 🔹 🔜 Honseil 🙇 Mennager 👔 Roth Mills 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 Previous [vigor] ODER encoded or @Base 64 encoded Download CA certificate Download CA certification path Download latest certificate revocation list
- 3. Back to Vigor router, go to **Trusted CA Certificate**. Click **IMPORT** button and browse the file to import the certificate (.cer file) into Vigor router. When finished, click refresh and you will find the below illustration.

Certificate Management >> Trusted CA Certificate

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

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.

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 "**2.1 Hardware Installation**" for details.
- 2. Turn on the router. Make sure the **ACT LED** blink once per second and the correspondent **LAN LED** is bright.



3. If not, it means that there is something wrong with the hardware status. Simply back to **"2.1 Hardware Installation"** to execute the hardware installation again. And then, try again.

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

Sometimes the link failure occurs due to the wrong network connection settings. After trying the above section, if the link is 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.

ieneral	Authentication Ad	vanced	
Conne	t using:		
11	SUSTeK/Broadcom	440x 10/100 lr	Configure
This cg	nnection uses the fol	lowing items:	
	Client for Microsoft J File and Printer Sha QoS Packet Sched Internet Protocol (T	ring for Microsoft Ne luler	etworks
-	nstall	Limnetall	Properties
Tran wide	fiption smission Control Proto area network protoc ss diverse interconne	ol that provides com	

VolPon www.voipon.co.uk sales@voipon.co.uk Tel: +44 (0)1245 808195 Fax: +44 (0)1245 808299

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

Seneral	Alternate Configuration		
this cap		d automatically if your network eed to ask your network admi	
00	btain an IP address auto	matically	
OU	ge the following IP addre	141: 	
肥料	dels entrais		1
Sibi	net praisk in	0	
<u>(j</u>)(j)	ur nammer		
00	blain DNS server addres	is automatically	
OU	te the following DNS ser	rver addresses:	
Ente	ened 0/45 server		
22,000	HIRD DNS (8856)		
			idyanced
_		Οκ	Cancel

For MacOs

- 1. Double click on the current used MacOs on the desktop.
- 2. Open the **Application** folder and get into **Network**.
- 3. On the **Network** screen, select **Using DHCP** from the drop down list of Configure IPv4.

0.0	Network	. (
how All Display.	a Sound Network Startup Disk	
	Location: Automatic	
	Show: Built-in Ethernet	
	TCP/IP PPPoE AppleTalk Proxies Ethernet	-
Configure	IPv4: Using DHCP	
IP Add	ress: 192.168.1.10 (Renew DHCP Lease)
Subnet M	Mask: 255.255.255.0 DHCP Client ID:	
Ro	uter: 192.168.1.1	
DNS Ser	vers. IOptiona	n
Search Dom	ains: rOptiona	a .
IPv6 Add	ress: fe80:0000:0000:0000:020a 95ff fe8d:72e4	
	(Configure IPv6)	?)

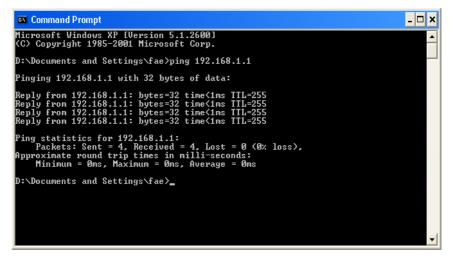
5.3 Pinging the Router from Your Computer

The default gateway IP address of the router is 192.168.1.1. For some reason, you might need to use "ping" command to check the link status of the router. **The most important thing is that the computer will receive a reply from 192.168.1.1.** If not, please check the IP address of your computer. We suggest you setting the network connection as **get IP automatically**. (Please refer to the section 4.2)

Please follow the steps below to ping the router correctly.

For Windows

- 1. Open the Command Prompt window (from Start menu> Run).
- 2. Type **command** (for Windows 95/98/ME) or **cmd** (for Windows NT/ 2000/XP). The DOS command dialog will appear.



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

For MacOs (Terminal)

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

000	Terminal - bash - 80x24	
64 bytes from 192.168 64 bytes from 192.168 64 bytes from 192.168 64 bytes from 192.168 64 bytes from 192.168 AC 192.168.1.1 ping	ng 192.168.1.1 2.168.1.1): 56 data bytes 3.1.1: icmp_seq=0 ttl=255 time=0.755 ms 3.1.1: icmp_seq=1 ttl=255 time=0.697 ms 3.1.1: icmp_seq=2 ttl=255 time=0.716 ms 3.1.1: icmp_seq=3 ttl=255 time=0.731 ms 3.1.1: icmp_seq=4 ttl=255 time=0.72 ms	8
5 packets transmitted	statištics 4, 5 packets received, 0% packet loss 1x = 0.697/0.723/0.755 mš	

5.4 Checking If the ISP Settings are OK or Not

Click **WAN>> Internet Access** and then check whether the ISP settings are set correctly. Click **Details Page** of WAN1/WAN2 to review the settings that you configured previously.

WAN >> Internet Access

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

Static or Dynamic IP 💌
None
PPPoE Static or Dynamic IP
PPTP

For PPPoE Users

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

WAN >> Internet Access

WAN 1	
PPPoE Client Mode	PPP/MP Setup
💿 Enable i 🔘 Disable	PPP Authentication PAP or CHAP 💌
	Always On
ISP Access Setup	Idle Timeout 0 second(s)
Username	IP Address Assignment Method (IPCP)
Password	Fixed IP: 🔘 Yes 📀 No (Dynamic IP)
Index(1-15) in <u>Schedule</u> Setup:	Fixed IP Address
=>,,,,	
ISDN Dial Backup Setup	Default MAC Address
Dial Backup Mode 🛛 🛛 🔽	Specify a MAC Address
	MAC Address:
	00 ·50 ·7F :00 ·00 ·01
OK	Cancel

For Static/Dynamic IP Users

- 1. Check if the **Enable** option is selected.
- 2. Check if **IP address, Subnet Mask** and **Gateway** are entered with correct values that you **got from** your **ISP**.

WAN >> Internet Access

WAN 1		
Static or Dynamic IP (DHCP Client) • Enable Obisable	WAN IP Network Settings Obtain an IP address a	WAN IP Alias
ISDN Dial Backup Setup Dial Backup Mode None 💌	Router Name Domain Name * : Required for some ISPs	
Keep WAN Connection	Specify an IP address	
Enable PING to keep alive	IP Address	172.16.3.229
PING to the IP	Subnet Mask	255.255.0.0
PING Interval 0 minute(s)	Gateway IP Address	172.16.3.4
RIP Protocol	 Default MAC Addres 	s
Enable RIP	🔘 Specify a MAC Addr	ess
	MAC Address:	F5
	DNS Server IP Address	
	Primary IP Address	
	Secondary IP Address	

For PPTP Users

WAN >> Internet Access

1. Check if the **Enable** option for **PPTP** Link is selected.

PPTP Client Mode	PPP Setup
💿 Enable 🛛 Disable	PPP Authentication PAP or CHAP 💌
PPTP Server 10.0.0.138	Idle Timeout -1 second(s)
ISP Access Setup	IP Address Assignment Method (IPCP) WAN IP Alias
Username	Fixed IP: 🔘 Yes 💿 No (Dynamic IP)
Password	Fixed IP Address
Index(1-15) in <u>Schedule</u> Setup:	WAN IP Network Settings
=>,,,	Obtain an IP address automatically
ISDN Dial Backup Setup	 Specify an IP address
Dial Backup Mode 🛛 None 💽	IP Address 10.0.0.150
	Subnet Mask 255.0.0.0

2. Check if **PPTP Server, Username, Password** and **WAN IP address** are set correctly (must identify with the values from your ISP).

5.5 Backing to Factory Default Setting If Necessary

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



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

Software Reset

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

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

System	Maintenance	>>	Reboot	System
--------	-------------	----	--------	--------

Reboot System	
	Do You want to reboot your router ?
	 Using current configuration Using factory default configuration
1	OK

Hardware Reset

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



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

5.6 Contacting Your Dealer

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