

Vigor 2700 Series Firewall Router User's Guide

Version: 2.5 Date: 2007/03/19

Copyright 2006 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 and Explorer are trademarks of Microsoft Corp. Apple and Mac OS are registered trademarks of Apple Computer Inc. Other products may be trademarks or registered trademarks of their respective manufacturers.

Please visit www.draytek.com to get the newly updated manual at any time.

This page is left blank.

Table of Contents



Preface	1
1.1 LED Indicators and Connectors	2
1.1.1 Front and Rear View for Vigor2700	2
1.1.2 Front and Rear View for Vigor2700G	
1.1.3 Front and Rear View for Vigor2700Gi	
1.1.4 Front and Rear View for Vigor2700V (MODULE:2S1L)	5
1.1.5 Front and Rear View for Vigor2700V (MODULE:2S)	6
1.1.6 Front and Rear View for Vigor2700VGi	
1.1.7 Front and Rear View for Vigor2700VG (MODULE:2S1L)	8
1.1.8 Front and Rear View for Vigor2700VG (MODULE:2S)	9
1.2 Hardware Installation	10



Configuring Basic Settings	13
2.1 Changing Password	13
2.2 Quick Start Wizard	15
2.2.1 Adjusting Protocol/Encapsulation 2.2.2 PPPoE/PPPoA 2.2.3 Bridged IP 2.2.4 Routed IP	16 18
2.3 Online Status for Each Protocol	20
2.4 Status Bar	22



Advanced Web Configuration	23
3.1 Internet Access	23
3.1.1 Basics of Internet Protocol (IP) Network	
3.1.2 PPPoE/PPPoA 3.1.3 MPoA	
3.1.4 Multi-PVCs	30
3.2 LAN	33
3.2.1 Basics of LAN	
3.2.2 General Setup 3.2.3 Static Route	34 37
3.2.4 VLAN	40
3.2.5 Bind IP to MAC	41
3.3 NAT	42
3.3.1 Port Redirection	
3.3.2 DMZ Host 3.3.3 Open Ports	44 46
3.3.4 Well-Known Ports List	
3.4 Firewall	49

	49
3.4.2 General Setup 3.4.3 Filter Setup	
3.4.4 IM Blocking	
3.4.5 P2P Blocking	
3.4.6 DoS Defense	
3.4.7 URL Content Filter	
3.4.8 Web Content Filter	62
3.5 Bandwidth Management	62
3.5.1 Sessions Limit	
3.5.2 Bandwidth Limit	
3.5.3 Quality of Service	
3.6 Applications	
3.6.1 Dynamic DNS	
3.6.2 Schedule	
3.6.3 RADIUS 3.6.4 UPnP	
3.6.5 IGMP	
3.6.6 Wake on LAN	
3.7 VPN and Remote Access	
3.7.1 Remote Access Control	
3.7.2 PPP General Setup	
3.7.3 IPSec General Setup 3.7.4 IPSec Peer Identity	
3.7.5 Remote Dial-In User	
3.7.6 LAN to LAN	
3.7.7 Connection Management	
3.8 Certificate Management	97
3.8 Certificate Management	97
3.8 Certificate Management	97 98
3.8 Certificate Management 3.8.1 Local Certificate 3.8.2 Trusted CA Certificate 3.9 VoIP	97 98 99
3.8 Certificate Management 3.8.1 Local Certificate 3.8.2 Trusted CA Certificate 3.9 VoIP 3.9.1 DialPlan	97 98 99 101
3.8 Certificate Management 3.8.1 Local Certificate 3.8.2 Trusted CA Certificate 3.9 VoIP	
3.8 Certificate Management 3.8.1 Local Certificate 3.8.2 Trusted CA Certificate 3.9 VoIP 3.9.1 DialPlan 3.9.2 SIP Accounts	97 98 99 99 101 105 109
3.8 Certificate Management 3.8.1 Local Certificate 3.8.2 Trusted CA Certificate 3.9 VoIP 3.9.1 DialPlan 3.9.2 SIP Accounts 3.9.3 Phone Settings	97 98 99 101 105 109 113
3.8 Certificate Management. 3.8.1 Local Certificate	97 98 99
3.8 Certificate Management. 3.8.1 Local Certificate	
3.8 Certificate Management. 3.8.1 Local Certificate	97 98 99 99 99 101 105 109 113 113 115 115 116 117
3.8 Certificate Management. 3.8.1 Local Certificate 3.8.2 Trusted CA Certificate 3.9 VoIP. 3.9.1 DialPlan 3.9.2 SIP Accounts 3.9.3 Phone Settings 3.9.4 Status 3.10 ISDN. 3.10.1 General Setup 3.10.2 Dialing to a Single ISP 3.10.3 Dialing to Dual ISPs 3.10.4 Virtual TA	97 98 99 99 101 109 115 115 115 116 117 117
 3.8 Certificate Management. 3.8.1 Local Certificate	97 98 99 99 101 105 109 115 115 115 115 117 117 117 121
3.8 Certificate Management. 3.8.1 Local Certificate 3.8.2 Trusted CA Certificate 3.9 VoIP. 3.9.1 DialPlan 3.9.2 SIP Accounts 3.9.3 Phone Settings 3.9.4 Status 3.10 ISDN. 3.10.1 General Setup 3.10.2 Dialing to a Single ISP 3.10.3 Dialing to Dual ISPs 3.10.4 Virtual TA	97 98 99 99 101 105 109 115 115 115 115 117 117 117 121
3.8 Certificate Management. 3.8.1 Local Certificate 3.8.2 Trusted CA Certificate 3.9 VolP. 3.9.1 DialPlan 3.9.2 SIP Accounts 3.9.3 Phone Settings 3.9.4 Status. 3.10 ISDN 3.10.1 General Setup. 3.10.2 Dialing to a Single ISP. 3.10.3 Dialing to Dual ISPs. 3.10.4 Virtual TA 3.10.5 Call Control. 3.11 Wireless LAN. 3.11.1 Basic Concept.	97 98 99 99 99 101 105 109 113 115 115 115 115 115 115 121 122 122
3.8 Certificate Management	97 98 99 101 105 105 115 115 115 115 117 121 121 122 122 125
3.8 Certificate Management. 3.8.1 Local Certificate 3.8.2 Trusted CA Certificate 3.9 VolP. 3.9 I DialPlan 3.9.2 SIP Accounts 3.9.3 Phone Settings 3.9.4 Status 3.10 ISDN. 3.10.1 General Setup. 3.10.2 Dialing to a Single ISP. 3.10.4 Virtual TA 3.10.5 Call Control. 3.11 Wireless LAN. 3.11.1 Basic Concept. 3.11.3 Security.	97 98 99 99 99 101 105 109 109 113 115 115 116 117 117 117 117 121 122 122 125 127
3.8 Certificate Management. 3.8.1 Local Certificate 3.8.2 Trusted CA Certificate 3.9 VolP. 3.9 I DialPlan 3.9.2 SIP Accounts 3.9.3 Phone Settings 3.9.4 Status 3.10 ISDN. 3.10.1 General Setup. 3.10.2 Dialing to a Single ISP. 3.10.3 Dialing to Dual ISPs. 3.10.4 Virtual TA 3.10.5 Call Control. 3.11.1 Basic Concept. 3.11.2 General Settings 3.11.3 Security. 3.11.4 Access Control.	97 98 99 99 99 101 105 109 109 109 113 115 115 116 117 117 117 121 122 122 122 122 123
3.8 Certificate Management. 3.8.1 Local Certificate . 3.8.2 Trusted CA Certificate . 3.9 VoIP. 3.9.1 DialPlan . 3.9.2 SIP Accounts . 3.9.3 Phone Settings . 3.9.4 Status. 3.10 ISDN. 3.10.1 General Setup . 3.10.2 Dialing to a Single ISP . 3.10.3 Dialing to Dual ISPs . 3.10.4 Virtual TA . 3.10.5 Call Control . 3.11.1 Basic Concept . 3.11.3 Security . 3.11.4 Access Control . 3.11.5 WDS .	97 98 99 99 99 101 105 109 109 109 113 115 115 115 116 117 117 121 122 122 122 122 125 128 129
3.8 Certificate Management. 3.8.1 Local Certificate 3.8.2 Trusted CA Certificate 3.9 VolP. 3.9 I DialPlan 3.9.2 SIP Accounts 3.9.3 Phone Settings 3.9.4 Status 3.10 ISDN. 3.10.1 General Setup. 3.10.2 Dialing to a Single ISP. 3.10.3 Dialing to Dual ISPs. 3.10.4 Virtual TA 3.10.5 Call Control. 3.11.1 Basic Concept. 3.11.2 General Settings 3.11.3 Security. 3.11.4 Access Control.	97 98 99 101 105 105 109 113 115 115 115 115 116 117 121 121 122 125 127 128 129 129 129 129
3.8 Certificate Management 3.8.1 Local Certificate 3.8.2 Trusted CA Certificate 3.9 VolP 3.9.1 DialPlan 3.9.2 SIP Accounts 3.9.3 Phone Settings 3.9.4 Status 3.10 ISDN 3.10.1 General Setup 3.10.2 Dialing to a Single ISP 3.10.3 Dialing to Dual ISPs 3.10.4 Virtual TA 3.10.5 Call Control 3.11.1 Basic Concept 3.11.3 Security 3.11.4 Access Control 3.11.5 WDS 3.11.6 AP Discovery	97 98 99 101 105 105 109 113 115 115 115 115 116 117 121 122 122 125 127 128 129 129 129 129 129 129 129 129 129 129
3.8 Certificate Management 3.8.1 Local Certificate 3.8.2 Trusted CA Certificate 3.9 VoIP 3.9.1 DialPlan 3.9.2 SIP Accounts 3.9.3 Phone Settings 3.9.4 Status 3.10 ISDN 3.10.1 General Setup 3.10.2 Dialing to a Single ISP 3.10.3 Dialing to Dual ISPs 3.10.4 Virtual TA 3.10.5 Call Control 3.11.1 Basic Concept 3.11.3 Security 3.11.4 Access Control 3.11.5 WDS 3.11.6 AP Discovery 3.11.7 Station List	97 98 99 101 105 109 113 115 115 115 115 116 117 117 121 122 122 122 125 127 128 129 128 129 123 123 123

3.12.3 Configuration Backup	135
3.12.4 Syslog/Mail Alert	136
3.12.3 Configuration Backup 3.12.4 Syslog/Mail Alert 3.12.5 Time and Date	138
3.12.6 Management	
3.12.7 Reboot System	
3.12.8 Firmware Upgrade	140
3.13 Diagnostics	141
3.13.1 WAN Connection	141
3.13.2 Dial-out Trigger	142
3.13.3 Routing Table	142
3.13.4 ARP Cache Table	
3.13.5 DHCP Table	143
3.13.6 NAT Sessions Table	144
3.13.7 Ping Diagnosis	145
3.13.8 Data Flow Monitor	146
3.13.9 Trace Route	147



Application and Examples	149
4.1 Create a LAN-to-LAN Connection Between Remote Office and Headquarter	149
4.2 Create a Remote Dial-in User Connection Between the Teleworker and Headquarter	156
4.3 QoS Setting Example	160
4.4 LAN – Created by Using NAT	162
4.5 Calling Scenario for VoIP function	164
4.5.1 Calling via SIP Sever 4.5.2 Peer-to-Peer Calling	164 166
4.6 Upgrade Firmware for Your Router	167
4.7 Request a Certificate from a CA Server on Windows CA Server	170
4.8 Request a CA Certificate and Set as Trusted on Windows CA Server	174



Trouble Shooting	177
5.1 Checking If the Hardware Status Is OK or Not	177
5.2 Checking If the Network Connection Settings on Your Computer Is OK or Not	177
5.3 Pinging the Router from Your Computer	180
5.4 Checking If the ISP Settings are OK or Not	182
5.5 Backing to Factory Default Setting If Necessary	183
5.6 Contacting Your Dealer	184

This page is left blank.



Targeting requirement for residential, SOHO (Small Office and Home Office) and business users, the Vigor2700 series is an ADSL2/2+ enabled integrated access device. With downstream speed up to 12Mbps (ADSL2) or 24Mbps (ADSL2+), the Vigor2700 series provides exceptional bandwidth for Internet access.

To secure your network, the Vigor router provides an advanced firewall with advanced features, such as Stateful Packet Inspection (SPI) to offer network reliability by detecting and prohibiting malicious penetrating packets or DoS attacks, user-configurable web filtering for parental control against network abuse etc.

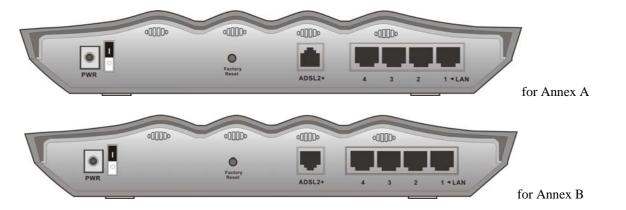
Vigor 2700 G model is embedded with an 802.11g compliant wireless module which provides wireless LAN access with data rate as much as 54Mbps. As for data privacy of wireless network, the Vigor2700 G model can encode all transmissions data with standard WEP and industrial strength WPA2 (IEEE 802.11i) encryption. Additional features include Wireless Client List and MAC Address Control for maintaining control over user's authorization in your network, and Hidden SSID for being invisible to outside intruders scanning.

1.1 LED Indicators and Connectors

1.1.1 Front and Rear View for Vigor2700

VPN VPN QoS ACT ACT 2 LAN 3 4

LED	Status	Explanation
VPN	On	The VPN tunnel is launched.
QoS	On	The QoS function is active.
	Off	The QoS function is inactive.
Firewall	On	The DoS function is enabled.
	Blinking	When encountered DoS attacks.
ADSL2+	On (Green)	ADSL is show time.
	Blinking (Green)	The device starts handshaking.
	Blinking (Orange)	The data is transmitting.
ACT (Activity)	On	The router is powered on.
	Blinking	The router is powered on and running properly.
LAN (1, 2, 3, 4)	Green	A normal connection is through its corresponding port.
	Blinking	Ethernet packets are transmitting.

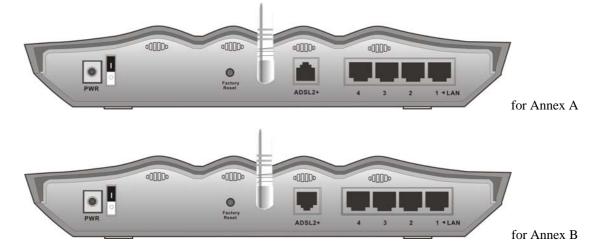


Interface	Description		
PWR	Connecter for a power adapter with 12~15VDC.		
ON/OFF	Power Switch.		
Factory Reset	Restore the default settings. Usage: Turn on the router (ACT LED is blinking). Press the hole and keep for more than 5 seconds. When you see the ACT LED begins to blink rapidly than usual, release the button. Then the router will restart with the factory default configuration.		
ADSL 2+	Connecter for accessing the Internet through ADSL2/2+.		
LAN 4 – 1	Connecter for local networked devices.		

1.1.2 Front and Rear View for Vigor2700G



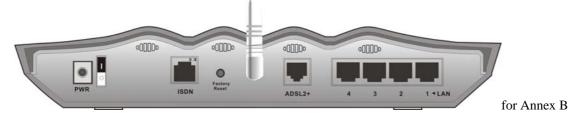
LED	Status	Explanation
WLAN	On	Wireless access point is ready.
	Blinking	Ethernet packets are transmitting over wireless LAN.
	Off	The WLAN function is inactive.
QoS	On	The QoS function is active.
	Off	The QoS function is inactive.
Firewall	On	The DoS function is enabled.
	Blinking	When encountered DoS attacks.
ADSL2+	On (Green)	ADSL is show time.
	Blinking (Green)	The device starts handshaking.
	Blinking (Orange)	The data is transmitting.
ACT (Activity)	On	The router is powered on.
	Blinking	The router is powered on and running properly.
LAN (1, 2, 3, 4)	Green	A normal connection is through its corresponding port.
	Blinking	Ethernet packets are transmitting.



Interface	Description		
PWR	Connecter for a power adapter with 12~15VDC.		
ON/OFF	Power Switch.		
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.		
ADSL 2+	Connecter for accessing the Internet through ADSL2/2+.		
LAN 4 – 1	Connecter for local networked devices.		

	WLAN	ADSL2+ ADSL2+ ACT 4 4
LED	Status	Explanation
WLAN	On	Wireless access point is ready.
	Blinking	Ethernet packets are transmitting over wireless LAN.
	Off	The WLAN function is inactive.
QoS	On	The QoS function is active.
	Off	The QoS function is inactive.
Firewall	On	The DoS function is enabled.
	Blinking	When encountered DoS attacks.
ADSL2+	On (Green)	ADSL is show time.
	Blinking (Green)	The device starts handshaking.
	Blinking (Orange)	The data is transmitting.
ACT (Activity)	On	The router is powered on.
	Blinking	The router is powered on and running properly.
LAN (1, 2, 3, 4)	Green	A normal connection is through its corresponding port.
	Blinking	Ethernet packets are transmitting.

1.1.3 Front and Rear View for Vigor2700Gi



Interface Description Connecter for a power adapter with 12~15VDC. **PWR** ON/OFF Power Switch. ISDN Connecter for NT1 (or NT1+) box provided by ISDN service provider. Factory Reset Restore the default settings. Usage: Turn on the router (ACT LED is blinking). Press the hole and keep for more than 5 seconds. When you see the ACT LED begins to blink rapidly than usual, release the button. Then the router will restart with the factory default configuration. ADSL 2+ Connecter for accessing the Internet through ADSL2/2+.

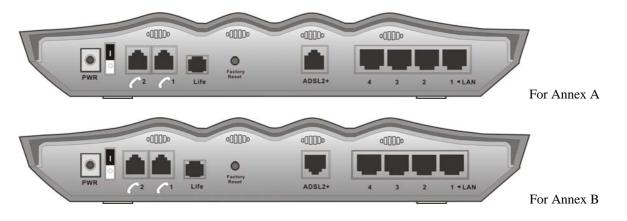
Connecter for local networked devices.

LAN 4 - 1

1.1.4 Front and Rear View for Vigor2700V (MODULE:2S1L)

	Phone 1	Phone 2	SL2+	F	LAN				
٩٧	5	C.	AD	AC	-	2	e	4	
0	0	0		\square	0		0	0	

LED	Status	Explanation
VPN	On	The VPN tunnel is launched.
Phone 1 & 2	On	The phone is off hook (the handset of phone is hanging).
(FXS1, FXS2)	Blinking	A phone call is incoming.
ADSL2+	On (Green)	ADSL is show time.
	Blinking (Green)	The device starts handshaking.
	Blinking (Orange)	The data is transmitting.
ACT (Activity)	On	The router is powered on.
	Blinking	The router is powered on and running properly.
LAN (1, 2, 3, 4)	Green	A normal connection is through its corresponding port.
	Blinking	Ethernet packets are transmitting.

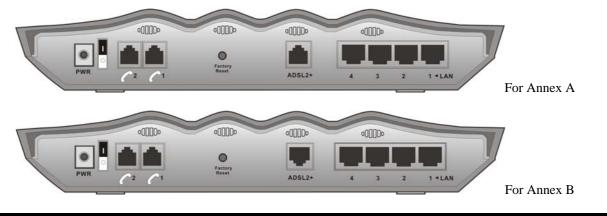


Interface	Description
PWR	Connecter for a power adapter with 12~15VDC.
ON/OFF	Power Switch.
VoIP 1/2	Connecter of analog phone for VoIP communication.
Life	Connector of analog phone for PSTN life line.
Factory Reset	Restore the default settings. Usage: Turn on the router (ACT LED is blinking). Press the hole and keep for more than 5 seconds. When you see the ACT LED begins to blink rapidly than usual, release the button. Then the router will restart with the factory default configuration.
ADSL 2+	Connecter for accessing the Internet through ADSL2/2+.
LAN 4 – 1	Connecter for local networked devices.

1.1.5 Front and Rear View for Vigor2700V (MODULE:2S)

_	Phone 1	Phone 2	SL2+	т		NA			
٩ ۲	5	5	AD	AC	-	2	en	4	
0	0	0		0	0	\cap	0		

LED	Status	Explanation
VPN	On	The VPN tunnel is launched.
Phone 1 & 2	On	The phone is off hook (the handset of phone is hanging).
(FXS1, FXS2)	Blinking	A phone call is incoming.
ADSL2+	On (Green)	ADSL is show time.
	Blinking (Green)	The device starts handshaking.
	Blinking (Orange)	The data is transmitting.
ACT (Activity)	On	The router is powered on.
	Blinking	The router is powered on and running properly.
LAN (1, 2, 3, 4)	Green	A normal connection is through its corresponding port.
	Blinking	Ethernet packets are transmitting.



Interface	Description
PWR	Connecter for a power adapter with 12~15VDC.
ON/OFF	Power Switch.
VoIP 1/2	Connecter of analog phone for VoIP communication.
Factory Reset	Restore the default settings. Usage: Turn on the router (ACT LED is blinking). Press the hole and keep for more than 5 seconds. When you see the ACT LED begins to blink rapidly than usual, release the button. Then the router will restart with the factory default configuration.
ADSL 2+	Connecter for accessing the Internet through ADSL2/2+.
LAN 4 – 1	Connecter for local networked devices.

1.1.6 Front and Rear View for Vigor2700VGi

	one 1	one 2	2+			z	1		
WLAN	C Pho	C Pho	ADSL	ACT	,	2	5 m	4	
Δ	Δ	Δ	Δ	0	Δ	0	0	0	

LED	Status	Explanation
WLAN	On	Wireless access point is ready.
	Blinking	Ethernet packets are transmitting over wireless LAN.
	Off	The WLAN function is inactive.
Phone 1 & 2	On	The phone is off hook (the handset of phone is hanging).
(FXS1, FXS2)	Blinking	A phone call is incoming.
ADSL2+	On (Green)	ADSL is show time.
	Blinking (Green)	The device starts handshaking.
	Blinking (Orange)	The data is transmitting.
ACT (Activity)	On	The router is powered on.
	Blinking	The router is powered on and running properly.
LAN (1, 2, 3, 4)	Green	A normal connection is through its corresponding port.
	Blinking	Ethernet packets are transmitting.



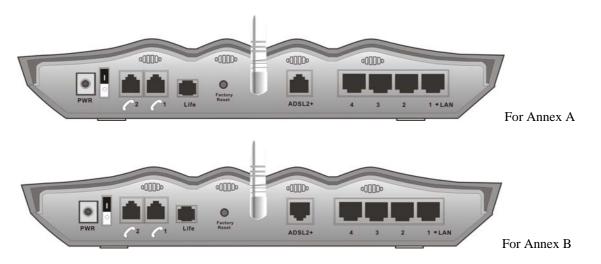
For Annex B

Interface	Description
PWR	Connecter for a power adapter with 12~15VDC.
ON/OFF	Power Switch.
VoIP 1/2	Connecter of analog phone for VoIP communication.
ISDN	Connecter for NT1 (or NT1+) box provided by ISDN service provider.
Factory Reset	Restore the default settings. Usage: Turn on the router (ACT LED is blinking). Press the hole and keep for more than 5 seconds. When you see the ACT LED begins to blink rapidly than usual, release the button. Then the router will restart with the factory default configuration.
ADSL 2+	Connecter for accessing the Internet through ADSL2/2+.
LAN 4 – 1	Connecter for local networked devices.

1.1.7 Front and Rear View for Vigor2700VG (MODULE:2S1L)

NA	Phone 1	hone 2	SL2+	F	LAN				
N	C	Ū	AD	AC	-	8	e	4	
	0	0	0		0	0	0	\square	

LED	Status	Explanation
WLAN	On	Wireless access point is ready.
	Blinking	Ethernet packets are transmitting over wireless LAN.
	Off	The WLAN function is inactive.
Phone 1 & 2	On	The phone is off hook (the handset of phone is hanging).
(FXS1, FXS2)	Blinking	A phone call is incoming.
ADSL2+	On (Green)	ADSL is show time.
	Blinking (Green)	The device starts handshaking.
	Blinking (Orange)	The data is transmitting.
ACT (Activity)	On	The router is powered on.
	Blinking	The router is powered on and running properly.
LAN (1, 2, 3, 4)	Green	A normal connection is through its corresponding port.
	Blinking	Ethernet packets are transmitting.

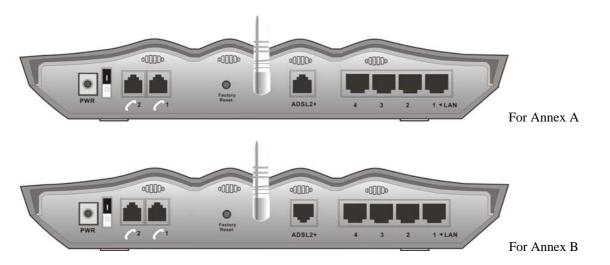


Interface	Description
PWR	Connecter for a power adapter with 12~15VDC.
ON/OFF	Power Switch.
VoIP 1/2	Connecter of analog phone for VoIP communication.
Life	Connector of analog phone for PSTN life line.
Factory Reset	Restore the default settings. Usage: Turn on the router (ACT LED is blinking). Press the hole and keep for more than 5 seconds. When you see the ACT LED begins to blink rapidly than usual, release the button. Then the router will restart with the factory default configuration.
ADSL 2+	Connecter for accessing the Internet through ADSL2/2+.
LAN 4 – 1	Connecter for local networked devices.

1.1.8 Front and Rear View for Vigor2700VG (MODULE:2S)

AN	Phone 1	hone 1 hone 2	Phone 2 SL2+ T	F	LAN				
Ň	5	5	AD	AC	-	2	ъ	4	
	Δ	Δ	0	0	Δ	0	0	0	

LED	Status	Explanation
WLAN	On	Wireless access point is ready.
	Blinking	Ethernet packets are transmitting over wireless LAN.
	Off	The WLAN function is inactive.
Phone 1 & 2	On	The phone is off hook (the handset of phone is hanging).
(FXS1, FXS2)	Blinking	A phone call is incoming.
ADSL2+	On (Green)	ADSL is show time.
	Blinking (Green)	The device starts handshaking.
	Blinking (Orange)	The data is transmitting.
ACT (Activity)	On	The router is powered on.
	Blinking	The router is powered on and running properly.
LAN (1, 2, 3, 4)	Green	A normal connection is through its corresponding port.
	Blinking	Ethernet packets are transmitting.



Interface	Description
PWR	Connecter for a power adapter with 12~15VDC.
ON/OFF	Power Switch.
VoIP 1/2	Connecter of analog phone for VoIP communication.
Factory Reset	Restore the default settings. Usage: Turn on the router (ACT LED is blinking). Press the hole and keep for more than 5 seconds. When you see the ACT LED begins to blink rapidly than usual, release the button. Then the router will restart with the factory default configuration.
ADSL 2+	Connecter for accessing the Internet through ADSL2/2+.
LAN 4 – 1	Connecter for local networked devices.

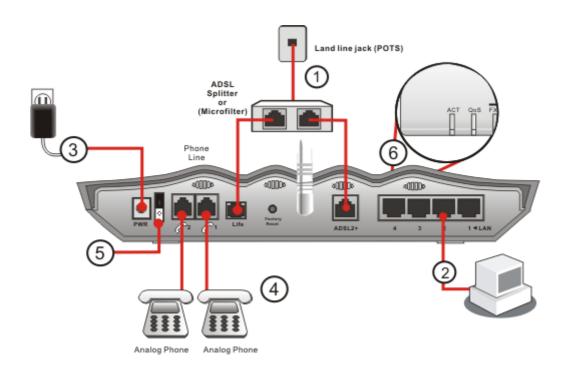
1.2 Hardware Installation

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

- 1. Connect the ADSL interface to the external ADSL splitter with an ADSL line cable for all models. For the VoIP model with MODULE:2S1L (Annex A), also connect Life interface to external ADSL splitter. (refer to Example 1 to 3)
- 2. Connect one port of 4-port switch to your computer with a RJ-45 cable.
- 3. Connect one end of the power cord to the power port of this device. Connect the other end to the wall outlet of electricity.
- 4. Connect the telephone sets with phone lines (for using VoIP function). For the user of the model without VoIP ports, skip this step.
- 5. Power on the router.
- 6. Check the ACT and ADSL2+, LAN LEDs to assure network connections.

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

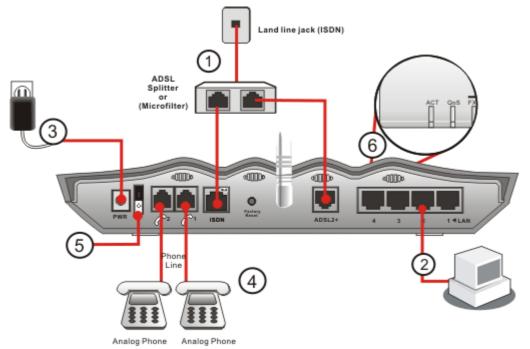
Example 1:



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

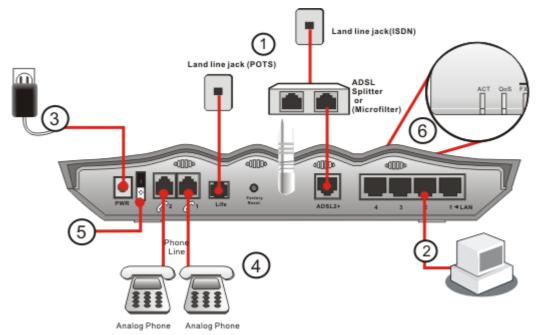
Example 2:

Connect the ADSL interface to the external ADSL splitter with an ADSL line cable. For the model of Vigor2700VGi (Annex B), also connect ISDN interface to external ADSL splitter.



Example 3:

Connect the ADSL interface to the external ADSL splitter with an ADSL line cable and connect to ISDN wall outlet. For the VoIP model with MODULE:2S1L (Annex B), also connect Life interface to POTS wall outlet.



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. The main screen will be chaged slightly according to the model you have.

	System Status					
uick Start Wizard	-					
Online Status	Model Name		VI			
nternet Access	Model Name Firmware Version		: Vigor2700 series : 2.7.2 RC4			
AN	Build Date/Time		: Mar 2 2007 09:22:10			
AT	ADSL Firmware Ven	sion	: 121201_A Annex B			
irewall						
andwidth Management						
pplications	LAN MAC Address	00-50-7	F-00-00-00	WAN Link Status	: Disconnected	
PN and Remote Access		: 192.168		MAC Address	: 00-50-7F-00-00-01	
ertificate Management oIP	1st Subnet Mask		.255.0	Connection	:	
5DN	DHCP Server	: Yes		IP Address Default Gateway		
ystem Maintenance	VoIP			DNS	: 194.109.6.66	
iagnostics	Port	: 1	2			
3	SIP registrar Account ID	: change	_me change_me			
	Register	: chango	_me_change_me			
	Codec	:				
	In Calls Out Calls	: O : O	0			

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

System Maintenance >> Administrator Password Setup

Old	Password	
New	Password	
Rety	pe New Password	

- 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 192	2.168.1.1 🛛 🖓 🔀
	A.
Login to the Route	er Web Configurator
User name:	2
Password:	••••
	Remember my password
	OK Cancel

2.2 Quick Start Wizard

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

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

2.2.1 Adjusting Protocol/Encapsulation

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

nect to Internet	
VPI	0 Auto detect
VCI	35
Protocol / Encapsulation	PPPoA VC MUX
Fixed IP	○ Yes ④ No(Dynamic IP)
IP Address	
Subnet Mask	
Default Gateway	
Primary DNS	
Second DNS	

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

VPI

Stands for **Virtual Path Identifier**. It is an 8-bit header inside each ATM cell that indicates where the cell should be routed. The ATM, is a method of sending data in small packets of fixed sizes. It is used for transferring data to client computers.

VCI	Stands for Virtual Channel Identifier. It is a 16-bit field inside ATM cell's header that indicates the cell's next destination as it travels through the network. A virtual channel is a logical connection between two end devices on the network.			
Protocol/Encapsulation	Select an IP mode for this WAN interface. There are several available modes for Internet access such as PPPoE , PPPoA , Bridged IP and Routed IP .			
	Protocol / Encapsulation	1483 Bridged IP LLC		
	Fixed IP IP Address Subnet Mask Default Gateway Primary DNS	PPPoE LLC/SNAP PPPoE VC MUX PPPoA VC MUX 1483 Bridged IP LLC 1483 Routed IP LLC 1483 Routed IP VC-Mux 1483 Routed IP VC-Mux (IPoA) 1483 Bridged IP (IPoE)		
Fixed IP	x y	For the router. Otherwise, click No er choosing a dynamic IP. If you dress, Subnet Mask and Default		
IP Address	Assign an IP address for the protocol that you select.			
Subnet Mask	Assign a subnet mask value for the protocol of Routed IP and Bridged IP .			
Default Gateway	Assign an IP address to the gate and Bridged IP .	way for the protocol of Routed IP		
Primary DNS	Assign an IP address to the prim	nary DNS.		
Second DNS	Assign an IP address to the secondary DNS.			

2.2.2 PPPoE/PPPoA

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

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

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

et PPPoE / PPPoA	
ISP Name	isp
User Name	user
Password	••••
Confirm Password	••••
🗹 Always On	
Idle Timeout	-1 Seconds

ISP Name	Assign a specific name for ISP requirement.
User Name	Assign a specific valid user name provided by the ISP.
Password	Assign a valid password provided by the ISP.
Confirm Password	Retype the password.
Always On	Check this box to allow the router connecting to Internet forever.
Idle Timeout	Type in the value (unit is second) as the idle timeout of the connection. When the time is expired, the internet connection will be dropped immediately.

Click Next for viewing summary of such connection.

Quick Start Wizard

4. Please confirm your settings:	
VPI	: 0
VCI	: 35
Protocol / Encapsulation	: PPPoA / VCMUX
Fixed IP	: No
Primary DNS	:
Secondary DNS	:
Always On	: Yes
	< Back Next > Finish Cancel

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

Online Status

System Statu	IS					Syst	em Up	otime: 210:58:20
LAN Status		Prima	ary DNS: 16	8.95.192.	1 8	econda	ry DN	S: 168.95.1.1
IP Address		TX Packets	RX RX	Packets				
192.168.1.1		35035810	31:	127516				
WAN Status			GW IP Addr	: 61.230.	192.254			Drop PPPoE
Mode	IP Addre	ess T	K Packets	TX Rate	RX Packet	s RX	Rate	Up Time
PPPoE	61.230.2	02,155 1	59	1023	97	390)	0:00:31
ADSL Informa	ation	(ADSL Firmwa	re Version:	121201_A	.)			
ATM Statist	ics TX Bl	locks	RX Blocks	;	Corrected	Blocks	Unco	orrected Blocks
	32523	37670	577675847	7	0		0	
ADSL Status	5 Mode	State	Up Spe	ed Do	own Speed	SNR M	argin	Loop Att.
	G.DMT	SHOWTIME	256000	20	48000	31		26

2.2.3 Bridged IP

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

Quick Start Wizard

2. Cc	nnect to Internet	
	VPI VCI	0 Auto detect
	Protocol / Encapsulation	1483 Bridged IP LLC
	Fixed IP IP Address	○ Yes ● No(Dynamic IP)
	Subnet Mask Default Gateway	
	Primary DNS Second DNS	
<u> </u>		<pre>< Back Next > Finish Cancel</pre>

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

VPI	: 0
VCI	: 35
Protocol / Encapsulation	: 1483 Bridge LLC
Fixed IP	: No
Primary DNS	:
Secondary DNS	:

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

Online Status

LAN Status	Primary DNS: 168.95.1.3			95.1.1	5	econda	ry DNS:	168.95.192.1	
IP Address		TX Packet	s	RX Pa	ickets				
192.168.1.1		194		215					
WAN Status			GW IP /	Addr:	202.211.	100.1			Release
Mode	IP Addres	s	TX Packe	ts 1	FX Rate	RX Packe	ets R	X Rate	Up Time
DHCP Client	202.211.1	00.54	0	(0	0	0		0:00:11
ADSL Informa	ntion (/	ADSL Firmw	are Versio	in: 12	1201_A)				
ATM Statisti	cs TX Blo	cks	RX Blo	cks	C	Corrected	Blocks	Uncori	ected Blocks
	23		42		C)		157	
ADSL Status	Mode	State	Up S	peed	Dov	vn Speed	SNR M	argin	Loop Att.
	ADSL2+ (G.992.5)	SHOWTIM	E 1008	3000	216	44000	6		0

2.2.4 Routed IP

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

Quick Start Wizard 2. Connect to Internet Auto detect VPI 0 VCI 35 Protocol / Encapsulation 1483 Routed IP LLC * Fixed IP ⊙ Yes ○No(Dynamic IP) 192.168.1.10 IP Address Subnet Mask 255.255.255.0 Default Gateway 192.168.1.1 168.95.1.1 Primary DNS Second DNS < Back Next > Finish Cancel

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

VPI	: 0
VCI	: 35
Protocol / Encapsulation	: 1483 Route LLC
Fixed IP	: Yes
IP Address	: 192.168.1.10
Subnet Mask	: 255.255.255.0
Default Gateway	: 192.168.1.1
Primary DNS	: 168.95.1.1
Secondary DNS	:

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

Online Status

System Statu LAN Status		Prim	ary DNS: 19	4.109.6.66				Uptime: 0:0:: : 194.98.0.1
IP Address		TX Packet:		Packets			, 5.10	. 15
192.168.1.1		137	191	L				
WAN Status			GW IP Add	r: 202.211	.100.1			
Mode	IP Addres	is 1	TX Packets	TX Rate	RX Pack	ets R	X Rate	Up Time
Static IP	202.211.1	00.54 2	26	36	0	0		0:00:35
ADSL Informa	ntion (/	ADSL Firmwa	are Version:	121201_A))			
ATM Statisti	cs TX Blo	cks	RX Blocks		Corrected	Blocks	Uncor	rected Blocks
	0		0		0		1	
ADSL Status	5 Mode	State	Up Spec	ed Do	wn Speed	SNR M	argin	Loop Att.
	ADSL2+ (G.992.5)	SHOWTIME	992000	24:	168000	5		0

2.3 Online Status for Each Protocol

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

Online status for PPPoA/PPPoE

Online Status

System Statu	S								otime: 210:58:2
LAN Status		Pri	mary DM	√S: 168	3.95.192.	1 5	3econda	iry DN	S: 168.95.1.1
IP Address		TX Packe	ets	RX I	Packets				
192.168.1.1		35035810)	311:	27516				
WAN Status			GW IF	Addr:	61,230,	192.254			Drop PPPoE
Mode	IP Addre	ss	TX Pac	kets	TX Rate	RX Packet	ts RX	Rate	Up Time
PPPoE	61.230.2	02.155	159		1023	97	390)	0:00:31
ADSL Informa	ation	(ADSL Firm	ware Vei	rsion: 1	121201_4	۹)			
ATM Statist	ics TX B	ocks	RX	Blocks		Corrected	Blocks	Unco	orrected Blocks
	3252:	37670	577	675847		0		0	
ADSL Status	5 Mode	State	U	p Spee	d Dr	own Speed	SNR M	argin	Loop Att.
	G.DMT	SHOWTIN	4E 2.	56000	20	048000	31		26

Online status for Bridge

Online Status

LAN Status		Prim	ary DNS:	ary DNS: 168.95.1.1			econda	ry DNS:	168.95.192.1
IP Address		TX Packet	s	RX Pack	ets				
192.168.1.1		194		215					
WAN Status			GW IP A	\ddr: 20	2.211	.100.1			Release
Mode	IP Addres	55	TX Packet	ts TX	Rate	RX Packe	ets R	X Rate	Up Time
DHCP Client	202.211.1	00.54	0	0		0	0		0:00:11
ADSL Informa	tion (a	ADSL Firmw	are Versio	n: 1212(01_A)				
ATM Statistic	cs TX Blo	cks	RX Blo	cks		Corrected	Blocks	Uncor	rected Blocks
	23		42		()		157	
ADSL Status	Mode	State	Up S	peed	Dov	vn Speed	SNR M	argin	Loop Att.
	ADSL2+ (G.992.5)	SHOWTIM	E 1008	000	216	44000	6		0

Online status for Routed IP

Online Status

System Statu	5					8	System	Uptime: 0:0:3
LAN Status Pri		Prima	ry DNS: 19	5	Seconda	194.98.0.1		
IP Address		TX Packets	RX	Packets				
192,168,1,1		137	191					
WAN Status			GW IP Add	r: 202.211	.100.1			
Mode	IP Addres	ss T	X Packets	TX Rate	RX Pack	ets R	X Rate	Up Time
Static IP	202.211.1	00.54 2	6	36	0	0		0:00:35
ADSL Informa	tion (ADSL Firmwa	re Version:	121201_A))			
ATM Statisti	cs TX Blo	cks	RX Blocks		Corrected	Blocks	Uncor	rected Blocks
	0		0		0		1	
ADSL Status	Mode	State	Up Spee	ed Do	wn Speed	SNR M	argin	Loop Att.
	ADSL2+ (G.992.5)	SHOWTIME	992000	24	168000	5		0

Primary DNS	Displays the assigned IP address of the primary DNS.
Secondary DNS	Displays the assigned IP address of the secondary DNS.
IP Address (in LAN)	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.
GW IP Addr:	Displays the assigned IP address of the default gateway.
IP Address (in WAN)	Displays the IP address of the WAN interface.
TX Rate	Displays the speed of transmitted packets at the WAN interface.
RX Rate	Displays the speed of received packets at the WAN interface.
Up Time	Displays the total system uptime of the interface.
TX Blocks	Displays the total number of transmitted ATM Blocks.
RX Blocks	Displays the total number of received ATM Blocks.
Corrected Blocks	Displays the total l number of received ATM Blocks corrupted but corrected.

Uncorrected Blocks	Displays the total number of received ATM Blocks corrupted but uncorrected.
Mode	Displays the modulation mode used: G.DMT, G.Lite, or T1.413.
State	Displays the DSL line status.
Up Speed	Displays the upstream speed (bits/ second).
Down Speed	Displays the downstream speed (bits/ second).
SNR Margin	Displays the value of Signal Noise Ratio Margin (dB). The higher value has better signal quality.
Loop Att.	Displays the value of subscribed Loop Attenuation.

2.4 Status Bar

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.

3Advanced Web Configuration

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

3.1 Internet Access

3.1.1 Basics of Internet Protocol (IP) Network

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

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 of the host PCs can share a common Internet connection.

Get Your Public IP Address from ISP

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

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

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

3.1.2 PPPoE/PPPoA

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

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

PPPoE/PPPoA Client 💿 Enable 🔘 Disa	able ISP Access Setup
DSL Modem Settings Multi-PVC channel Channel 1 VPI 0 VCI 33 Encapsulating Type LLC/SNAP ♥ Protocol PPPoE ♥ Modulation Multimode	ISP Name Username Password PPP Authentication PAP or CHAP Always On Idle Timeout 180 second(s) IP Address From ISP WAN IP Alias Fixed IP Yes ● No (Dynamic IP)
PPPoE Pass-through For Wired LAN For Wireless LAN Note: If this box is checked while using the protocol, the router will behave like a mode which only serves the PPPoE client on the I ISDN Dial Backup Setup Dial Backup Mode None	Fixed IP Address O Default MAC Address Specify a MAC Address MAC Address :

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

Internet Access >> PPPoE / PPPoA

PPPoE Pass-through The router offers PPPoE dial-up connection. Besides, you also can establish the PPPoE connection directly from local clients to your ISP via the Vigor router. When PPPoA protocol is selected, the PPPoE package transmitted by PC will be transformed into PPPoA package and sent to WAN server. Thus, the PC can access Internet through such direction.

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

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

ISDN Dial Backup Setup

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

Dial Backup Mode

	None	*
	None	
	Packet Trigger	
Ŀ	Always On	

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

None - Disable the backup function.

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

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

ISP Access SetupEnter your allocated username, password and authentication
parameters according to the information provided by your ISP. If
you want to connect to Internet all the time, you can check Always
On.**ISP Name** – Type in the ISP Name provided by ISP in this field.**Unsernance** – Type in the ISP Name provided by ISP in this field.

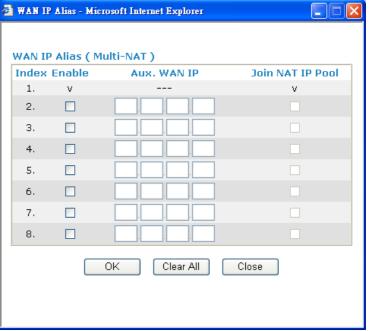
Username – Type in the username provided by ISP in this field. **Password** – Type in the password provided by ISP in this field. **PPP Authentication** – Select **PAP only** or **PAP or CHAP** for PPP. **Always On** – Check this box if you want the router keeping connecting to Internet forever.

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

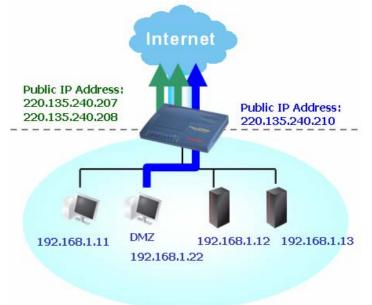
IP Address From ISP
 Usually ISP dynamically assigns IP address to you each time you connect to it and request. In some case, your ISP provides service to assign you the same IP address whenever you request. In this case, you can fill in this IP address in the Fixed IP field. Please contact your ISP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

WAN IP Alias - If you have multiple public IP addresses and would

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

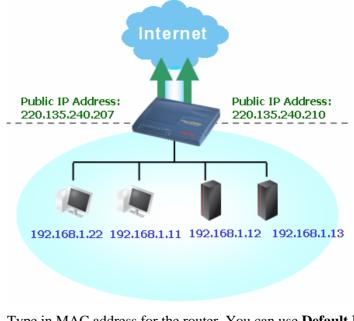


By checking the checkbox **Join NAT IP Pool**, data from NAT hosts will be round-robin forwarded on a session basis.



If you do not check Join NAT IP Pool, you can still use these public

IP addresses for other purpose, such as DMZ host, Open Ports.



Default MAC Address	Type in MAC address for the router. You can use Default MAC Address or specify another MAC address for your necessity. MAC Address – Type in the MAC address for the router manually.
Index (1-15) in Schedule Setup	You can type in four sets of time schedule for your request. All the schedules can be set previously in Application – Schedule web page and you can use the number that you have set in that web page.

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

3.1.3 MPoA

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

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

Internet Access >> MPoA (RFC1483/2684)

MPoA (RFC1483/2684)	💿 Enable	🔘 Disable	WAN IP Networ	rk Settings	
			💿 Obtain an IP	address a	utomatically
DSL Modem Settings			Router Name		*
Multi-PVC channel	Channel 2	*	Domain Name		*
Encapsulation			0.0		WAN IP Alias
1483 Br	idged IP LLC	*	O Specify an I	_	
VPI	0	7	IP Address	0.	.0.0.0
	33		Subnet Mask	0.	.0.0.0
VCI			Gateway IP Ad	ldress	
Modulation	Multimode	*			
			* : Required fo	or some ISP:	5
ISDN Dial Backup Setup			O Default M/	AC Address	
Dial Backup Mode	None	*	Specify a	MAC Addres	55
RIP Protocol			MAC Address	:	
			00 . 50	. 7F D8	FO . 01
Enable RIP					
Bridge Mode			DNS Server IP	Address	
Enable Bridge Mode			Primary IP Add	dress	
Enable bridge Mode			Secondary IP	Address	

- MPoA (RFC1483/2684) Click Enable for activating this function. If you click Disable, this function will be closed and all the settings that you adjusted in this page will be invalid.
- **DSL Modem Settings** Set up the DSL parameters required by your ISP. These are vital for building DSL connection to your ISP. Multi-PVC channel - The selections displayed here are determined by the page of Internet Access – Multi PVCs. Select M-PVCs Channel means no selection will be chosen. Encapsulating Type - Drop down the list to choose the type provided by ISP. **VPI** - Type in the value provided by ISP. VCI - Type in the value provided by ISP. **ISDN Dial Backup** This setting is available for the routers supporting ISDN function Setup only. Before utilizing the ISDN dial backup feature, you must create a dial backup profile first. Please click Internet Access **Setup** > **Dialing to a Single ISP** to enter the backup profile.

Dial Backup Mode

None	*
None	
Packet Trigger	
Always On	

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

None - Disable the backup function.

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

Always On - If the broadband connection is no longer available, the backup line will be activated automatically and always on until the broadband connection is restored. We recommend you to

	enable this feature if you host a web server for your customers' access.
RIP Protocol	Routing Information Protocol is abbreviated as RIP (RFC1058) specifying how routers exchange routing tables information. Click Enable RIP for activating this function.
Bridge Mode	If you choose Bridged IP as the protocol, you can check this box to invoke the function. The router will work as a bridge modem.
WAN IP Network Settings	This group allows you to obtain an IP address automatically and allows you type in IP address manually.
	Obtain an IP address automatically – Click this button to obtain

the IP address automatically. **Router Name** – Type in the router name provided by ISP.

Domain Name – Type in the domain name that you have assigned. **WAN IP Alias** - If you have multiple public IP addresses and would like to utilize them on the WAN interface, please use WAN IP Alias. You can set up to 8 public IP addresses other than the current one you are using.

	P <mark>Alias (</mark> Mu Enable	Aux. WAN IP	Join NAT IP Pool
1.	v		v
2.			
з.			
4.			
5.			
6.			
7.			
8.			
		OK Clear All	Close

Specify an IP address – Click this radio button to specify some data.
IP Address – Type in the private IP address.
Subnet Mask – Type in the subnet mask.
Gateway IP Address – Type in gateway IP address.

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

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

3.1.4 Multi-PVCs

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

General

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

```
Internet Access >> Multi-PVCs
```

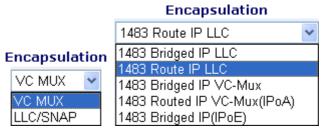
Multi-PVCs						
General	ATI	M QoS	Por	rt-based Br	idge	
Channel	Enable	VPI	VCI	QoS Type	Protocol	Encapsulation
1.		0	33	UBR 🔽	PPPoE 💌	LLC/SNAP 🔽
2.		0	34	UBR 🔽	MPoA 💌	1483 Bridged IP LLC 🛛 👻
з.		0	35	UBR 🗸	PPPoE 💌	LLC/SNAP
4.		0	36	UBR 🔽	PPPoE 💌	LLC/SNAP
5.		0	37	UBR 🔽	PPPoE 🛩	LLC/SNAP
6.		0	38	UBR 🔽	PPPoE 💌	LLC/SNAP
7.		0	39	UBR 🗸	PPPoE 🛩	LLC/SNAP
8.		0	40	UBR 🗸	PPPoE 💌	LLC/SNAP

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

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

Encapsulation

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



ATM QoS

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

```
Internet Access >> Multi-PVCs
```

Multi-PVCs				
General	ATM QoS	Port-based	l Bridge	
Channel	QoS Type	PCR	SCR	MBS
1.	UBR 🔽	0	0	0
2.	UBR 🛃	0	0	0
з.	UBR 🖌	0	0	0
4.	UBR 💌	0	0	0
5.	UBR 🖌	0	0	0
6.	UBR 💌	0	0	0
7.	UBR 🔽	0	0	0
8.	UBR 🔽	0	0	0

Note: 1.Set 0 means default value.

2.PCR(max) = ADSL Up Speed / 53 / 8.

ОК	Clear	Cancel

QoS Type

Select a proper QoS type for the channel according to the information that your ISP provides.

Qua	١Ŷ	he
UBR		*
UBR		
CBR		
ABR		
nrt∨B	R	

rt∨BR

PCR It represents Peak Cell Rate. The default setting is "0".

SCR It represents Sustainable Cell Rate. The value of SCR must be smaller than PCR.

MBSIt represents Maximum Burst Size. The range of the value is 10 to
50.

Port-based Bridge

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

Internet Access >> Multi-PVCs

Multi-PVCs								
General	ATM Qo	S	Port-based Bridge			l Bridge		
Channel	Enable	P1	P2	P3	P4	Service Type	Add Tag	
1.						Normal 😪		
2.						Normal 😪		
з.						Normal 🛩		
4.						Normal 🐱		
5.						Normal 🛩		
6.						Normal 💌		
7.						Normal 🛩		
8.						Normal 🔽		

OK Clear Cancel

Note: 1.Channel 1 to 2 are reserved for Nat/Route use.

2.P1 is reserved for Nat/Route use.

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

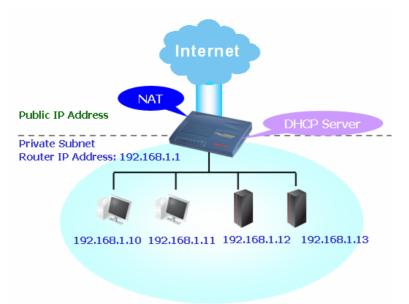
Click **Clear** to remove all the configurations in this page if you do not satisfy it. When you finish the configuration, please click **OK** to save and exit this page. Or click Cancel to abort the configuration and exit this page.

3.2 LAN

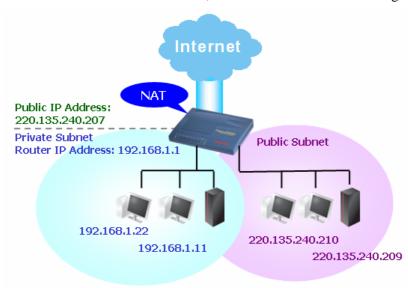
Local Area Network (LAN) is a group of subnets regulated and ruled by router. The design of network structure is related to what type of public IP addresses coming from your ISP.

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)

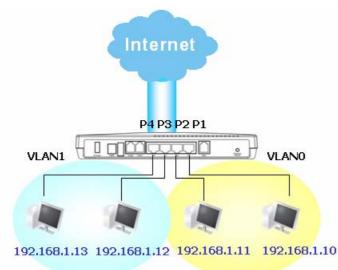
Vigor router will exchange routing information with neighboring routers using the RIP to accomplish IP routing. This allows users to change the information of the router such as IP address and the routers will automatically inform for each other.

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

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



3.2.2 General Setup

LAN >> General Setup

This page provides you the general settings for LAN.

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

AN IP Network Confi	guration	DHCP Server Configura	DHCP Server Configuration		
For NAT Usage		💿 Enable Server 🔘 Disal	⊙Enable Server ◯Disable Server		
1st IP Address 192.168.1.1 p		Relay Agent: 🔘 1st Subr	Relay Agent: 🔘 1st Subnet 🗌 2nd Subnet		
1st Subnet Mask 255.255.255.0		Start IP Address	192.168.1.10		
or IP Routing Usage 🤇) Enable 💿 Disable	IP Pool Counts	50		
2nd IP Address	192.168.2.1	Gateway IP Address	192.168.1.1		
2nd Subnet Mask 255.255.255.0		DHCP Server IP Address			
	2nd Subnet DHCP Server	for Relay Agent			
		DNS Server IP Address			
P Protocol Control 🛛 Disable 🔽		Primary IP Address			
		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 Addri IP Pool Count		0.3.1.95 (max. 10))
ndex I	Matched MAC	Address	given IP Addres
AC Address		e Edit	Cancel
		Clear All	Close

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

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

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

RIP Protocol Control

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

RIP Protocol Control

Disable 🛛 💙	
Disable	
1st Subnet	
2nd Subne	t

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

	2nd Subnet - Select the router to change the RIP information of the 2nd subnet with neighboring routers.
DHCP Server Configuration	DHCP stands for Dynamic Host Configuration Protocol. The router by factory default acts a DHCP server for your network so it automatically dispatch related IP settings to any local user configured as a DHCP client. It is highly recommended that you leave the router enabled as a DHCP server if you do not have a DHCP server for your network.
	If you want to use another DHCP server in the network other than Vigor Router's, you can let Relay Agent help you to redirect the DHCP request to the specified location. Enable Server - Let the router assign IP address to every host in the LAN.
	 Disable Server – Let you manually assign IP address to every host in the LAN. Relay Agent – (1st subnet/2nd subnet) Specify which subnet that DHCP server is located the relay agent should redirect the DHCP request to. Start IP Address - Enter a value of the IP address pool for the DHCP server to start with when issuing IP addresses. If the 1st IP address of your router is 192.168.1.1, the starting IP address must be
	 192.168.1.2 or greater, but smaller than 192.168.1.254. IP Pool Counts - Enter the maximum number of PCs that you want the DHCP server to assign IP addresses to. The default is 50 and the maximum is 253. Gateway IP Address - Enter a value of the gateway IP address for the DHCP server. The value is usually as same as the 1st IP address of the router, which means the router is the default gateway. DHCP Server IP Address for Relay Agent - Set the IP address of the DHCP server you are going to use so the Relay Agent can help to forward the DHCP request to the DHCP server.
DNS Server Configuration	DNS stands for Domain Name System. Every Internet host must have a unique IP address, also they may have a human-friendly, easy to remember name such as www.yahoo.com. The DNS server converts the user-friendly name into its equivalent IP address.
	 Primary IP Address - You must specify a DNS server IP address here because your ISP should provide you with usually more than one DNS Server. If your ISP does not provide it, the router will automatically apply default DNS Server IP address: 194.109.6.66 to this field. Secondary IP Address - You can specify secondary DNS server IP address here because your ISP often provides you more than one DNS Server. If your ISP does not provide it, the router will automatically apply default secondary DNS Server IP address: 194.98.0.1 to this field. The default DNS Server IP address can be found via Online Status:
	LAN Status Primary DNS: 194.109.6.66 Secondary DNS: 194.98.0.1 IP Address TX Packets RX Packets

192.168.1.1

1330

1187

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.

tatic Rou	ite Configuration			View R	outing Table
Index	Destination Address	Status	Index	Destination Address	Status
<u>1.</u>	???	?	<u>6.</u>	???	?
<u>2.</u>	???	?	<u>7.</u>	???	?
<u>3.</u>	???	?	<u>8.</u>	???	?
<u>4.</u>	???	?	<u>9.</u>	???	?
<u>5.</u>	???	?	<u>10.</u>	???	?
<u>2.</u>	??? ??? ??? ???	? ?	<u>7.</u> <u>8.</u> <u>9.</u>	??? ??? ??? ???	

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

Index	The number (1 to 10) under Index allows you to open next page to setup static route.
Destination Address	Displays the destination address of the static route.

Status Displays the status of the static route.

Viewing Routing Table Displays the routing table for your reference.

Diagnostics >> View Routing Table

Key: C	- connected, S -	static, R - RIP, * - default, ~ - private	
C~	192.168.1.0/	255.255.255.0 is directly connected, IFO	

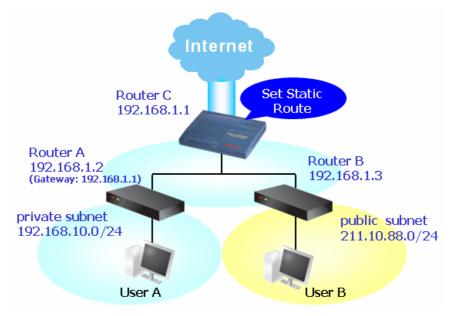
Add Static Routes to Private and Public Networks

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. Please add a static route as shown below, which regulates all packets destined to 192.168.10.0 will be forwarded to 192.168.1.2. Click OK.

LAN >> Static Route Setup

ndex N	lo. 1	
	Status/Action	Active/Add 🔽
	Destination IP Address	192.168.10.0
	Subnet Mask	255.255.255.0
	Gateway IP Address	192.168.1.2
	Network Interface	LAN 🕶

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

LAN >>	Static	Route	Setup
--------	--------	-------	-------

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

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

Diagnostics >> View Routing Table

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

Disable Static Route

LAN >> Static Route Setup

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

Status/Action	Active/Add
Destination IP Address	Empty/Clear Active/Add
Subnet Mask	Inactive/Disable
Gateway IP Address	192.168.1.3
Network Interface	LAN 🔽

3.2.4 VLAN

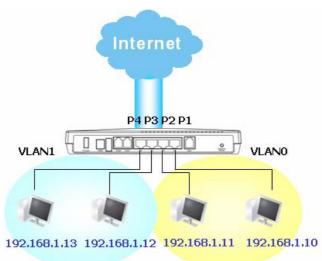
Virtual LAN function provides you a very convenient way to manage hosts by grouping them based on the physical port. You can also manage the in/out rate of each port. Go to LAN menu and select VLAN. The following page will appear. Click **Enable** to invoke VLAN function.

Enable				
	P1	P2	P3	P4
VLANO				
VLAN1				
VLAN2				
VLAN3				

LAN >> VLAN Configuration

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

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



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

LAN Configuration				
Enable				
	P1	P2	P3	P4
VLANO	V	\checkmark		
VLAN1				
VLAN2				
VLAN3				

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

3.2.5 Bind IP to MAC

LAN >> 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.

Bind IP to MAC		
Note: IP-MAC binding presets DHCP Allocat		
If you select Strict Bind, unspecified	LAN clients cannot access	the Internet.
ARP Table Select All Sort Refresh	IP Bind List	Select All Sort
IP Address Mac Address 192.168.1.10 00-0E-A6-2A-D5-A1	Index IP Address	Mac Address
Add and Edit		
IP Address		
Mac Address		
bbA	Edit Remove	

Enable	Click this radio button to invoke this function. However, IP/MAC which is not listed in IP Bind List also can connect to Internet.
Disable	Click this radio button to disable this function. All the settings on this page will be invalid.
Strict Bind	Click this radio button to block the connection of the IP/MAC which is not listed in IP Bind List.
ARP Table	This is LAN ARP table of this router. The information for IP and MAC will be displayed in this field. Each pair of IP and MAC address listed in ARP table can be selected and added to IP Bind List by clicking Add below.
Select All	Click this link to select the whole content in the ARP Table or IP Bind List.
Sort	Click this link to display the list by using the order of 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.
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.

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 .
-	select Strict Bind , you have to bind one set of IP/MAC address , no one of the PCs can access into Internet. And the web

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:

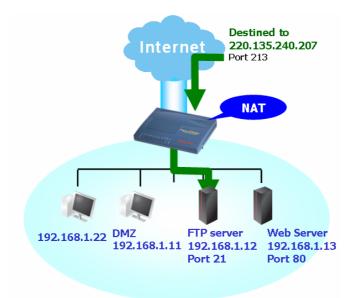
configurator of the router might not be accessed.

- 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.

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 10 port-mapping entries for the internal hosts.

NAT >> Configure Port Redirection Table

Index	Service Name	Protocol	Public Port	Private IP	Private Port	Active
1		💙	0		0	
2		💙	0		0	
3		💙	0		0	
4		💌	0		0	
5		💙	0		0	
6		💌	0		0	
7		💙	0		0	
8		💙	0		0	
9		💙	0		0	
10		💙	0		0	

ΟK

Service Name	Enter the description of the specific network service.
Protocol	Select the transport layer protocol (TCP or UDP).
Public Port	Specify which port can be redirected to the specified Private IP and Port of the internal host.
Private IP	Specify the private IP address of the internal host providing the service.
Private Port	Specify the private port number of the service offered by the internal host.
Active	Check this box to activate the port-mapping entry you have defined.

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

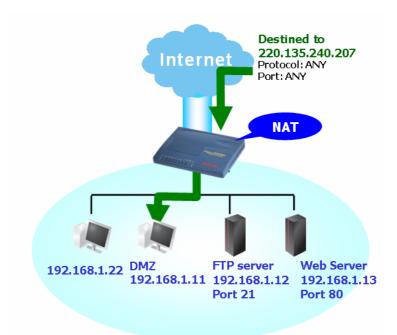
For example, the built-in web configurator in the router is with default port 80, which may conflict with the web server in the local network, http://192.168.1.13:80. Therefore, you need to **change the router's http port to any one other than the default port 80** to avoid conflict, such as 8080. This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

Management Access Control	Management Port Setup	
	 Default Ports (Telnet: 23, HTTP: 80, F443, FTP: 21) User Define Ports Telnet Port HTTP Port HTTPS Port FTP Port SNMP Setup 	

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.



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

Click DMZ Host to open the following page:

```
NAT >> DMZ Host Setup
```

DMZ Host Setup	
None 🔽	
Private IP	Choose PC
MAC Address of the True	IP DMZ Host 00 . 00 . 00 . 00 . 00 . 00
Note: When a True-IP DM2 be always on.	Z host is turned on, it will force the router's WAN connection to
	ОК
Drop Down List	The drop down list allows you to set Private IP or Active True
	IP as the DMZ host.
	None 🗸
	None
	Private IP
	Active True IP
Private IP	If you choose Private IP as the selection for DMZ host, please type in private IP or select any one by clicking the Choose PC button.
MAC Address of the True IP DMZ Host	If you choose Active True IP as the selection for DMZ host, please type in MAC address in these fields.

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

NAT >> DMZ Host Setup

	Aux. WAN IP	Private IP	
1.	220.135.240.247		Choose PC
	ОК	Clear	
Enable	Check to enable	the DMZ Host function	on.
Private IP	Enter the private select one.	IP address of the DM	Z host, or click Choose PC to
Choose PC	depicted below. To of all hosts in you the list to be the list to	The window consists of ur LAN network. Sele DMZ host.	ill automatically pop up, as of a list of private IP addresses ect one private IP address in P from the above dialog, the IP g screen. Click OK to save the

DMZ Ho	st Setup			
Index	Enable	Aux. WAN IP	Private IP	
1.		220.135.240.247	192 168 1 10	Choose PC
		ОК	Clear	,

3.3.3 Open Ports

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

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

NAT >> Open Ports Setup

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

Clear All

Index	Indicate the relative number for the particular entry that you want to offer service in a local host. You should click the appropriate index number to edit or clear the corresponding entry.
Comment	Specify the name for the defined network service.
Aux. WAN IP	Display the private IP address of the local host that you specify in WAN Alias. This field will not appear if you did not specify any WAN IP in the WAN Alias page.
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.

Index No. 1					
🗹 Enable Open F	Ports				
	Comment	P2P-Emule	WAN IP 220.1	35.240.247 💌	
	Local Computer	192 , 168 , 1	, 11 Choose PC		
Protocol	Start Port	End Port	Protocol	Start Port	End Port
1. TCP 🚩	4500	4700	6. 🖳 🖌	0	0
2. UDP 🚩	4500	4700	7 💌	0	0
3 💙	O	0	8 💙	0	0
4 🔽	0	0	9 💙	0	0
5 🚩	0	0	10. 🔜 💌	0	0
			ear Cancel		

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

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

Enable Open Ports	Check to enable this entry.
Comment	Make a name for the defined network application/service.
Local Computer	Enter the private IP address of the local host or click Choose PC to select one.

Choose PC	Click this button and, subsequently, a window having a list of private IP addresses of local hosts will automatically pop up. Select the appropriate IP address of the local host in the list.
Protocol	Specify the transport layer protocol. It could be TCP , UDP , or (none) for selection.
Start Port	Specify the starting port number of the service offered by the local host.
End Port	Specify the ending port number of the service offered by the local host.

NAT >> Open Ports Setup

Open Ports Setup

point ones oe	can be			
Index	Comment	Aux. WAN IP	Local IP Address	Status
<u>1.</u>	P2P-Emule	220.135.240.247	192.168.1.11	v
<u>2.</u>				х
<u>3.</u>				×
<u>4.</u>				х
<u>5.</u>				х
<u>6.</u>				х
<u>7.</u>				×
<u>8.</u>				х
<u>9.</u>				×
<u>10.</u>				×

Clear All

3.3.4 Well-Known Ports List

This page provides you a view of well-known ports.

NAT >> View Well-Known Ports List

Well-Known Ports List		
Service/Application	Protocol	Port Number
File Transfer Protocol (FTP)	TCP	21
SSH Remote Login Protocol (ex. pcAnyWhere)	UDP	22
Telnet	TCP	23
Simple Mail Transfer Protocol (SMTP)	TCP	25
Domain Name Server (DNS)	UDP	53
WWW Server (HTTP)	ТСР	80
Post Office Protocol ver.3 (POP3)	ТСР	110
Network News Transfer Protocol (NNTP)	ТСР	119
Point-to-Point Tunneling Protocol (PPTP)	ТСР	1723
pcANYWHEREdata	ТСР	5631
pcANYWHEREstat	UDP	5632
WinVNC	TCP	5900

3.4 Firewall

3.4.1 Basics for Firewall

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

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



1. Enter login password				
Please enter an alpha-numeric strir	ng as your Password (M	ax 23 charact	ers).	
New Password]		
Confirm Password]		
	< Back	Next >	Finish	Cancel

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

System	Maintenance >>	Administrator	Password	Setup
	in an iteritaries is a	7		outup

Old Password			
New Password			
Retype New Password			

Firewall Facilities

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

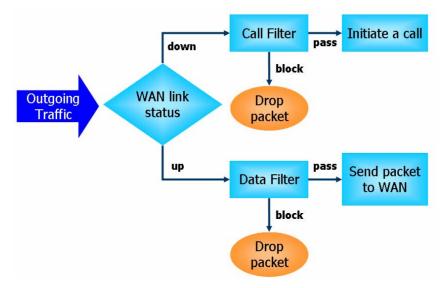
- User-configurable IP filter (Call Filter/ Data Filter).
- Stateful Packet Inspection (SPI): tracks packets and denies unsolicited incoming data
- Selectable Denial of Service (DoS) /Distributed DoS (DDoS) attacks protection
- URL Content Filter

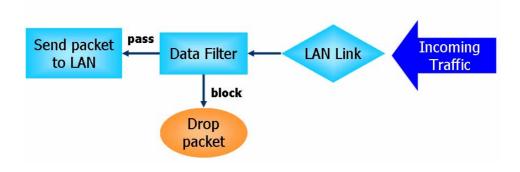
IP Filters

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

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

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





Stateful Packet Inspection (SPI)

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

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

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

Denial of Service (DoS) Defense

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

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

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

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

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

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

Content Filtering

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

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

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

Web Filtering

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

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

3.4.2 General Setup

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

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

Firewall >> General Setup

all Filter	💿 Enable	Start Filter Set	Set#1 💌		
	🔘 Disable				
)ata Filter	 Enable 	Start Filter Set	Set#2 💌		
	🔘 Disable				
.og Flag	None 💌				
🗌 Enable stateful pac	ket inspection				
Apply IP filter to VPN incoming packets					
🗌 Drop non-http conr	nection on TCP port 80	D			
🗹 Accept incoming fra	agmented UDP packet:	s (for some game	es, ex. CS)		
	og Flag Senable stateful pac Apply IP filter to VF Drop non-http conr	 Disable Disable	O Disable O Disable O Disable Start Filter Set O Disable O Disable Og Flag None In Enable stateful packet inspection		

OK

Call Filter	Check Enable to activate the Call Filter function. Assign a start filter set for the Call Filter.
Data Filter	Check Enable to activate the Data Filter function. Assign a start filter set for the Data Filter.
Log Flag	 For troubleshooting needs you can specify the filter log here. None - The log function is not activated. Block - All blocked packets will be logged. Pass - All passed packets will be logged. No Match - The log function will record all packets that are not matched. Note that the filter log will be displayed on the Telnet terminal when you type the <i>log -f</i> command.

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

3.4.3 Filter Setup

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

Firewall >> Filter Setup

lter So	etup		Set to Factory Defaul
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.

Fi	irewall	>>	Filter	Setup	>>	Edit	Filter	Set
	o ri an			outup				~~~

Filter Set 1		
Comments :	Default Call Filter	
Filter Rule	Active	Comments
1		Block NetBios
2		
3		
4		
5		
6		
7		
		Next Filter Set None 🚩
		OK Clear Cancel
Filter Rule		Click a button numbered $(1 \sim 7)$ to edit the filter rule. Click the be 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
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	Rule >>	Edit Filter Rule
-------------	-------------	---------	------------------

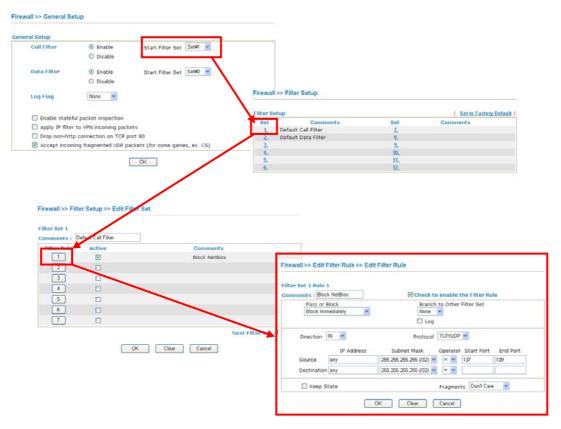
Filter Set 1 Rule 1			
Comments : Block	(NetBios	🗹 Check to	o enable the Filter Rule
Pass or B Block Imm		None	to Other Filter Set
		Log	
Direction [Ν 💌	Protocol	TCP/UDP 💌
	IP Address	Subnet Mask	Operator Start Port End Port
Source	any	255.255.255.255 (/32) 💌	= 🖌 137 139
Destination	any	255.255.255.255 (/32) 💌	= •
🗌 Keep St	ate		Fragments Don't Care 🍟
	0	IK Clear	Cancel

Comments	Enter filter set comments/description. Maximum length is 14- character long.
Check to enable the Filter Rule	Check this box to enable the filter rule.
Pass or Block	 Specifies the action to be taken when packets match the rule. Pass Immediately - Packets matching the rule will be passed immediately. Block Immediately - Packets matching the rule will be dropped immediately.

	 Pass If No Further Match - A packet matching the rule, and that does not match further rules, will be passed through. Block If No Further Match - A packet matching the rule, and that does not match further rules, will be dropped.
Branch to other Filter Set	If the packet matches the filter rule, the next filter rule will branch to the specified filter set. Select next filter rule to branch from the drop-down menu.
Log	Check this box to enable the log function. Use the Telnet command <i>log-f</i> to view the logs.
Direction	Set the direction of packet flow. It is for Data Filter only. For the Call Filter , this setting is not available since Call Filter is only applied to outgoing traffic.
Protocol	Specify the protocol(s) which this filter rule will apply to.
IP Address	Specify the source and destination IP addresses for this filter rule to apply to. Place the symbol "!" before a specific IP Address will prevent this rule from being applied to that IP address. To apply the rule to all IP address, enter any or leave the field blank.
Subnet Mask	Select the Subnet Mask for the IP Address column for this filter rule to apply from the drop-down menu.
Operator, Start Port and End Port	 The operator column specifies the port number settings. If the Start Port is empty, the Start Port and the End Port column will be ignored. The filter rule will filter out any port number. (=) If the End Port is empty, the filter rule will set the port number to be the value of the Start Port. Otherwise, the port number ranges between the Start Port and the End Port (including the Start Port and the End Port). (!=)If the End Port is empty, the port number is not equal to the value of the Start Port. Otherwise, this port number is not between the Start Port. Otherwise, this port number is not between the Start Port. Otherwise, this port number is not between the Start Port and the End Port (including the Start Port and End Port). (>) Specify the port number is larger than the Start Port (includes the Start Port). (<) Specify the port number is less than the Start Port (includes the Start Port).
Keep State	This function should work along with Direction, Protocol, IP address, Subnet Mask, Operator, Start Port and End Port settings. It is used for Data Filter only.Keep State is in the same nature of modern term Stateful Packet Inspection. It tracks packets, and accept the packets with appropriate characteristics showing its state is legal as the protocol defines. It will deny unsolicited incoming data. You may select protocols from any, TCP, UDP, TCP/UDP, ICMP and IGMP.
Fragments	 Specify the action for fragmented packets. And it is used for Data Filter only. Don't care -No action will be taken towards fragmented packets. Unfragmented - Apply the rule to unfragmented packets. Fragmented - Apply the rule to fragmented packets. Too Short - Apply the rule only to packets that are too short to contain a complete header.

Example

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



3.4.4 IM Blocking

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

Firewall >> IM Blocking Setup
Instant Messenger Applications Blocking Setup
Enable IM Blocking
Block MSN Messenger
Block Yahoo Messenger
Block ICQ/AOL
Time Schedule
Index(1-15) in <u>Schedule</u> Setup:,,,,
Note: Action and Idle Timeout settings will be ignored.
OK Cancel

3.4.5 P2P Blocking

Firewall >> P2P Blocking Setup

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

Peer-to-Peer fi	le-sharing Applications Blocking Setup			
·········	-			
Protocol	Applications	Action		
eDonkey	eDonkey, eMule, Shareaza, MLDonkey	● Allow ○ Disallow ○ Disallow upload		
FastTrack	KazaA, iMesh, MLDonkey	⊙ Allow ○ Disallow		
Gnutella	BearShare, Gnucleus, Limewire, Phex, Swapper, XoloX, Shareaza, MLDonkey	⊙ Allow ○ Disallow		
BitTorrent	BitTorrent	⊙ Allow ○ Disallow		
Time Schedule				
Index(1-15) in <u>Schedule</u> Setup:,,,,				
Note: Acti	on and Idle Timeout settings will be ignored.			
	OK Cancel			

Action

Specify the action for each protocol.

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

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

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

3.4.6 DoS Defense

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

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

🗹 Enable DoS Defense			
Enable SYN flood defense	Threshold	50 packets /	sec
	Timeout	10 sec	
Enable UDP flood defense	Threshold	150 packets /	sec
	Timeout	10 sec	
Enable ICMP flood defense	Threshold	50 packets /	sec
	Timeout	10 sec	
Enable Port Scan detection	Threshold	150 packets /	sec
Block IP options	📃 Block TCP f	lag scan	
🔲 Block Land	📃 Block Tear	Drop	
🔲 Block Smurf	📃 Block Ping (of Death	
🔲 Block trace route	📃 Block ICMP	fragment	
🔲 Block SYN fragment	📃 Block Unkno	ownProtocol	
📃 Block Fraggle Attack			
Enable DoS defense function to crackers.	prevent the attacks	from hacker or	

Cincural		DeC	defense	Cature
Firewall	~~	005	defense	Setup

Enable Dos Defense	Check the box to activate the DoS Defense Functionality.
Enable SYN flood defense	Check the box to activate the SYN flood defense function. Once detecting the Threshold of the TCP SYN packets from the Internet has exceeded the defined value, the Vigor router will start to randomly discard the subsequent TCP SYN packets for a period defined in Timeout. The goal for this is prevent the TCP SYN packets' attempt to exhaust the limited-resource of Vigor router. By default, the threshold and timeout values are set to 50 packets per second and 10 seconds, respectively.
Enable UDP flood defense	Check the box to activate the UDP flood defense function. Once detecting the Threshold of the UDP packets from the Internet has exceeded the defined value, the Vigor router will start to randomly discard the subsequent UDP packets for a period defined in Timeout. The default setting for threshold and timeout are 150 packets per second and 10 seconds, respectively.
Enable ICMP flood defense	Check the box to activate the ICMP flood defense function. Similar to the UDP flood defense function, once if the Threshold of ICMP packets from Internet has exceeded the defined value, the router will discard the ICMP echo requests coming from the Internet. The default setting for threshold and timeout are 50 packets per second and 10 seconds, respectively.
Enable PortScan detection	Port Scan attacks the Vigor router by sending lots of packets to many ports in an attempt to find ignorant services would respond. Check the box to activate the Port Scan detection. Whenever detecting this malicious exploration behavior by monitoring the

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

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

Warning 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. (Refer to System
Maintenance >> Syslog/Mail Alert for detail information.)

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

Enable					
	Server IP /	Address	192.168.1.115		
	Destinatior	n Port	514		
DrayTek Syslog	ę.				
Controls	31	192.168.1.1 Vigor 3100 series Dmt RX Packets 1182	WAN Status Getway IP (Fixed) WAN IP (Fixed) WAN IP (Fixed)	TX Packets	RX Rate 0 TX Rate 0
Time Jan 1 00:00:42 Jan 1 00:00:34	Host Messe Vigor DoS s Vigor DoS is		168 1.115,10605 -> 192.168 1.1 2.168 1.115 -> 192.168 1.1 PR 1	,23 PR 6(top) len 20 4 (icmp) len 20 60 icmp	0 -\$ 3943751 0/8

3.4.7 URL Content Filter

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

State

HANDSHAKE

Up Speed

Down Spe

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

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

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

ADSL Status

SNR Margin

Loop Atl

Firewall >> URL Content Filter

Content Filter Setup									
Enable URL Access Contro Black List (block those ma									
 White List (pass those ma 	- , ,								
	yword		ACT		Ke	yword			
1 V sex		5							
2		6							
3		7							
4 🗌 Note that multiple keywords	are allowed to specify	8 /int	he hla	nk. Eor ex	ample:	hotmail v	ahoo m	sn l	
Prevent web access from									
 ✓ Enable Restrict Web Feat ✓ Java ✓ ActiveX Cookie Proxy 	ure] Exec	utable file	s [] Multime	edia files		
Enable Excepting Subnets	5								
	IP Address				Subn	et Mask			
1 🗹 🗌 .			~	L]	_		
2			~				_		
3			~						
4			~						
Time Schedule									
Index(1-15) in <u>Schedule</u> Setu			_, [
Note: Action and Idle Timeout	settings will be ignored	Ι.							
	OK Clear	All	C	ancel					
Enable URL Access Control	Check the box to	o act	tivate	URL A	Access	Contro	ol.		
Black List (block those matching keyword)	Click this button webpage with the				•		-	ondi	ng
White List (pass those matching keyword)	Click this button webpage with the				-		-	onding	ğ
Keyword	The Vigor router each frame support noun, a partial not within a frame and addition, the max After specifying connection request user-defined key the blocking key perform.	orts oun re so xim key est t wor	mult , or a epara al ler word o the rd. It	iple key comple ted by s ngth of e ls, the V website should	yword ete UR space, each fi /igor i e whos be not	s. The l L strin comma rame is couter v se URL iced th	keywor g. Mult a, or ser 32-cha vill dec string at the n	d cou iple l nicol racte line t matc nore s	Id be a ceywords on. In r long. he hed to any simplified
Prevent web access from IP address	Check the box to such as http://202 dodges the URL	2.6.	3.2.7	The reas	son fo	-		-	
	You must clear y filtering facility obefore.								

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

3.4.8 Web Content Filter

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

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

3.5 Bandwidth Management

3.5.1 Sessions Limit

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

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

Bandwidth Management >> Sessions Limit

Sessions Limit	
🛇 Enable 💿 Disable	
Default Max Sessions: 100	
Limitation List	
Index Start IP End IP Max Sessions	
Specific Limitation Start IP: End IP: Maximum Sessions:	
Add Edit Remove	
Time Schedule	
Index(1-15) in <u>Schedule</u> Setup:,,,	
Note: Action and Idle Timeout settings will be ignored.	

OK

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

Enable	Click this button to activate the function of limit session.
Disable	Click this button to close the function of limit session.
Default session limit	Define the default session number used for each computer in LAN.
Limitation List	Display a list of specific limitations that you set on this web page.
Start IP	Define the start IP address for limit session.
End IP	Define the end IP address for limit session.
Maximum Sessions	Define the available session number for specific range of IP addresses. If you do not set the session number in this field, the system will use the default session limit for the specific limitation you set for each index.
Add	Add the specific session limitation onto the list above.
Edit	Allows you to edit the settings for the selected limitation.
Remove	Remove the selected settings existing on the limitation list.
Index (1-15) in Schedule Setup	You can type in four sets of time schedule for your request. All the schedules can be set previously in Application – Schedule web page and you can use the number that you have set in that web page.

3.5.2 Bandwidth Limit

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

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

🔘 Enat	ole 💿 Disable			
Default 1	ΓX Limit: 200	Kbps Default R	× Limit: 800	Кbps
Limitati	on List			
Index	Start IP	End IP	TX limit	RX limit
Specific	Limitation			
Start IP:		End IP:		
TX Limit:	Kbps	RX Limit: Add Edit	Kbps Remove	
Schedule				
ndex(1-15) in	n <u>Schedule</u> Setup			

Bandwidth Management >> Bandwidth Limit

OK

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

Enable	Click this button to activate the function of limit bandwidth.		
Disable	Click this button to close the function of limit bandwidth.		
Default TX limit	Define the default speed of the upstream for each computer in LAN.		
Default RX limit	Define the default speed of the downstream for each computer in LAN.		
Limitation List	Display a list of specific limitations that you set on this web page.		
Start IP	Define the start IP address for limit bandwidth.		
End IP	Define the end IP address for limit bandwidth.		
TX limit	Define the limitation for the speed of the upstream. If you do not set the limit in this field, the system will use the default speed for the specific limitation you set for each index.		
RX limit	Define the limitation for the speed of the downstream. If you do not set the limit in this field, the system will use the default speed for the specific limitation you set for each index.		

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

3.5.3 Quality of Service

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

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

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

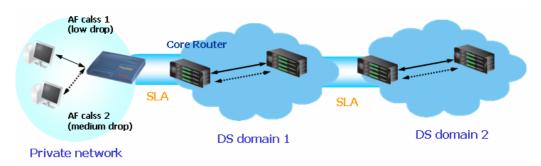
There are two components within Primary configuration of QoS deployment:

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

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

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

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



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

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

Quality of Service				Set to Fac	<u>ctory Default</u>
🗹 Enable t	he QoS Control				
Direction [OUT 💌				
Index	Class Name	Reserved_ba	ndwidth Ratio	S	etup
1.		25	%	Basic	Advanced
2.		25	%	Basic	Advanced
з.		25	%	Basic	Advanced
4.	Others	25	%		
🗌 Enable U	JDP Bandwidth Control	Limit	ed_bandwidth Rati	o 25	94
🔲 Outbour	nd TCP ACK Prioritize			<u>(</u>	Online Statistic

Bandwidth Management >> Quality of Service

OK Clear All

Enable the QoS Control	The factory default for this setting is checked.
Direction	Define which traffic the QoS Control settings apply to. IN- apply to incoming traffic only. OUT-apply to outgoing traffic only. BOTH- apply to both incoming and outgoing traffic.
Index	The group index number of QoS Control settings. There are total 4 groups.
Class Name	Define the name for the group index.
Reserved Bandwidth Ratio	It is reserved for the group index in the form of ratio of reserved bandwidth to upstream speed and reserved bandwidth to downstream speed .
Setup	There are two-level of settings: Basic - setup Reserved Bandwidth Ratio according to the traffic service type. We provide a list of common service types. Advance - custom setting of Reserved Bandwidth Ratio based on the source address, destination address, DiffServ CodePoint, and service type.

Enable UDP Bandwidth Control	Check this and set the limited bandwidth ratio on the right field. This is a protection of TCP application traffic since UDP application traffic such as streaming video will exhaust lots of bandwidth.				
Outbound TCP ACK Prioritize	Check to ena	ble this	function.		
Limited_bandwidth Ratio	The ratio typ application.	ed here	is reserved for l	imited bandwidth of UDP	
On Line Statistics	Display an online statistics for quality of service for your reference. Bandwidth Management >> Quality of Service Online Statistics				
	Indeu Direction	Class Name	Reserved-bandwidth Ratio	Outbound Throughput (Bytes/sec)	
	1 OUT	Class Name	25%	Outbound Inrodgipat (Bytes/sec)	
	2 OUT	<u> </u>	25%	0	
	3 OUT		25%	0	
	4 OUT	Others	25%	0	
		Refresh Interv	al : 30 💌 seconds	Reload	
		Ou	tbound Status ers 0 5	10 (Bps)	

Basic Settings for QoS

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

lass Index #1		
ANY AUTH(TCP:113) BGP(TCP:179) BOOTPCLIENT(UDP:68) BOOTPSERVER(UDP:67) CU-SEEME-HI(TCP/UDP:24032) CU-SEEME-LO(TCP/UDP:7648) DNS(TCP/UDP:53) FINGER(TCP:79)	ADD »	
	guration, we only care about the service type. ess will be replaced with any when you press "OK Clear All Cancel	

Choose one of the items from the left box and click **ADD**>>. The selected one will be shown on the right box. To remove the selected on from the right box, simply choose the one again and click **<<Remove.**

Enable UDP Bandwidth Control	Check this and set the limited bandwidth ratio on the right field. This is a protection of TCP application traffic since UDP application traffic such as streaming video will exhaust lots of bandwidth.				
Outbound TCP ACK Prioritize	Check to ena	ble this	function.		
Limited_bandwidth Ratio	The ratio typ application.	ed here	is reserved for l	imited bandwidth of UDP	
On Line Statistics	Display an online statistics for quality of service for your reference. Bandwidth Management >> Quality of Service Online Statistics				
	Indeu Direction	Class Name	Reserved-bandwidth Ratio	Outbound Throughput (Bytes/sec)	
	1 OUT	Class Name	25%	Outbound Inrodgipat (Bytes/sec)	
	2 OUT	<u> </u>	25%	0	
	3 OUT		25%	0	
	4 OUT	Others	25%	0	
		Refresh Interv	al : 30 💌 seconds	Reload	
		Ou	tbound Status ers 0 5	10 (Bps)	

Basic Settings for QoS

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

lass Index #1		
ANY AUTH(TCP:113) BGP(TCP:179) BOOTPCLIENT(UDP:68) BOOTPSERVER(UDP:67) CU-SEEME-HI(TCP/UDP:24032) CU-SEEME-LO(TCP/UDP:7648) DNS(TCP/UDP:53) FINGER(TCP:79)	ADD »	
	guration, we only care about the service type. ess will be replaced with any when you press "OK Clear All Cancel	

Choose one of the items from the left box and click **ADD**>>. The selected one will be shown on the right box. To remove the selected on from the right box, simply choose the one again and click **<<Remove.**

Advanced Settings for QoS

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

Bandwidth Management >> Quality of Service

Class Index #1 NO Status Source Address Destination Address DiffServ CodePoint Service Type 1. • Empty - - - - Insert new Rule before 1 (Rule Number). - - Move selected Rule (select an Index Number) to 1 (Rule Number).	Quality of Service							
NO Status Source Address Address DiffServ CodePoint Service Type 1. O Empty - - - - Insert new Rule before 1 (Rule Number).								
Insert new Rule before 1 (Rule Number).	э							
Edit selected Rule Delete selected Rule								

Cancel

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

0	Qual	ity of Service				
	АСТ	Source Address	Destination Address	DiffServ CodePoint	Service Type	
		Any SrcEdit	Any DestEdit	ANY	ANY Add Edit Delete	*

Note: Please choose/setup the Service Type first.

OK Cancel

SrcEdit/DestEdit

It allows you to edit source address information.

Address	Type	Any Address	
Address	Type		
Start IP	Address	Any Address Single Address	
End IP 4	\ddrocc	Range Address	
End IP A	Ruuress	Subnet Address	
Subnet	Mask	0.0.0.0	

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.

Bandwidth Management >> Quality of Service

Service Name	
Service Type	TCP 💌
Port Configuration	
Туре	💿 Single 🛛 Range
Port Number	0 – 0

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

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

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

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

3.6 Applications

3.6.1 Dynamic DNS

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

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

Enable the Function and Add a Dynamic DNS Account

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

Applications >> Dynamic DNS Setup

Enable Dynamic DNS Setu	ιþ	View Log	Force Update
Accounts :			
Index	Domain Name		Active
<u>1.</u>			х
<u>2.</u>			х
<u>3.</u>			х

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

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

Index : 1	
🗹 Enable Dynamic DNS /	Account
Service Provider	dyndns.org (www.dyndns.org)
Service Type	Dynamic 💌
Domain Name	chrono01 . dyndns.org 💌
Login Name	chrono6853 (max. 23 characters)
Password	•••••••• (max. 23 characters)
🔲 Wildcards	
🔲 Backup MX	
Mail Extender	
	OK Clear Cancel

Service Provider	Select the service provider for the DDNS account.
Service Type	Select a service type (Dynamic, Custom, Static).
Domain Name	Type in a domain name that you applied previously.
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

Applications >> Schedule

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

3.6.2 Schedule

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

You have to set your time before set schedule. In **System Maintenance>> Time Setup** 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>	×	<u>9.</u>	×
<u>2.</u>	х	<u>10.</u>	×
<u>3.</u>	х	<u>11.</u>	×
<u>4.</u>	х	<u>12.</u>	×
<u>5.</u>	х	<u>13.</u>	×
<u>6.</u>	х	<u>14.</u>	×
<u>7.</u>	×	<u>15.</u>	×
<u>8.</u>	×		

Clear All

You can set up to 15 schedules. Then you can apply them to your Internet Access.

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

Applications >> Schedule

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

OK Clear Cancel

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

Example

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



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

4. Assign these two profiles to the PPPoE Internet access profile. Now, the PPPoE Internet connection will follow the schedule order to perform **Force On** or **Force Down** action according to the time plan that has been pre-defined in the schedule profiles.

3.6.3 RADIUS

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

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

RADIUS Setup	
🗹 Enable	
Server IP 4	Address
Destination	n Port 1812
Shared Sec	cret
Re-type Sł	hared 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 mu be configured to use the same shared secret.
Re-type Shared Secret	Re-type the Shared Secret for confirmation.

Applications >> RADIUS

3.6.4 UPnP

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

Applications >> UPnP

110-0	
UPnP	
Enable UPnP Service	
Enable Connection control Service	
Enable Connection Status Service	

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

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

Enable UPNP Service

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

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

dress 🔇 Network Connections		😻 IP Broadband Connection on R	outer Status 🔽
Network Tasks	Broadband		
 Create a new connection Set up a home or small office network 	hinet Disconnected WAN Miniport (PPPOE)	General Internet Gateway Status:	Connected
0	Dial-up	Duration:	00:19:06
See Also	- test	Speed:	100.0 Mbps
Network Troubleshooter Other Places	Disconnected DrayTek.ISDN PPP	Activity Internet Internet Gateway	My Computer
Control Panel My Network Places	IP Broadband Connection on Router Enabled	Packets: Sent: 404	734
My Computer	LAN or High-Speed Internet	Received: 1,115	666
Details (*) Network Connections System Folder	Local Area Connection Enabled Realterk RTL8139/810x Family	Properties Disable	

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.

neral	Services
ionnect to the Internet using:	Select the services running on your network that Internet users car access.
🧐 IP Broadband Connection on Router	Services
	 ☐ Ftp Example ✓ msnmsgr (192.168.29.11:13135) 60654 UDP ✓ msnmsgr (192.168.29.11:7824) 13251 UDP
his connection allows you to connect to the Internet through a nared connection on another computer.	msnmsgr (192.168.29.11:8789) 63231 TCP
Settings	
Show icon in notification area when connected	Add Edit Delete

The reminder as regards concern about Firewall and UPnP:

Can't work with Firewall Software

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

Security Considerations

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

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

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

3.6.5 IGMP

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

Applications >> IGMP

2.

з.

239.255.255.250

225.0.0.1

IGMP					
Enable IGM	P Proxy				
	is to act as a multicast proxy f any multicast group. But this fu				
🗹 Enable IGM	P Snooping				
	Snooping, multicast traffic is snooping, multicast traffic is				
	C	K Cano	cel		
					<u>Refresh</u>
Working Multic	ast Groups				
Index	Group ID	P1	P2	P3	P4

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

v

٧

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

Applications >> IGMP

IGMP ✓ Enable IGMP Proxy IGMP Proxy is to act as a multicast proxy for hosts on the LAN side. Enable IGMP Proxy, if you will access any multicast group. But this function take no affect when Bridge Mode is enabled. ■ Enable IGMP Snooping Enable IGMP Snooping, multicast traffic is only forwarded to ports that have members of that group. Disable IGMP snooping, multicast traffic is treated in the same manner as broadcast traffic.



					<u>Refresh</u>
Working Multi	cast Groups				
Index	Group ID	P1	P2	P3	P4
1.	224.0.0.9	v	v	v	v
2.	239.255.255.250	v	v	v	v
З.	225.0.0.1	v	v	v	v

If you check Enable IGMP Snooping only, you will get the following page. Though all the multicast groups are listed, yet all the LAN ports (P1 to P4) are not available for use.

Applications >> IGMP

IGMP
Enable IGMP Proxy
IGMP Proxy is to act as a multicast proxy for hosts on the LAN side. Enable IGMP Proxy, if you will access any multicast group. But this function take no affect when Bridge Mode is enabled .
Enable IGMP Snooping
Enable IGMP Snooping, multicast traffic is only forwarded to ports that have members of that group. Disable IGMP snooping, multicast traffic is treated in the same manner as broadcast traffic.
OK Cancel

					<u>Refresh</u>
Working Multi	cast Groups				
Index	Group ID	P1	P2	P3	P4
1.	224.0.0.9				
2.	239.255.255.250				
З.	225.0.0.1				

3.6.6 Wake on LAN

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

Applicatio	on >> Wake on I	_AN	
Wake on	LAN		
	Note: Wake on can wake up th		IP to MAC function, only binded PCs
	Wake by:	MAC Address 👻	
	IP Address:	💌	
	MAC Address:		: Wake Up!
	Result		
Wake by		choose Wake by	de for you to wake up the binded IP. If you MAC Address, you have to type the correct f the host in MAC Address boxes. If you choose
			lress, you have to choose the correct IP address
		•	should be binded with MAC address configured
		in Bind IP to M	0
		Wake by:	MAC Address
			MAC Address
			IP Address

IP AddressThe IP addresses that have been configured in Firewall>>Bind
IP to MAC will be shown in this drop down list. Choose the IP
address from the drop down list that you want to wake up.MAC AddressType any one of the MAC address of the binded PCs.Wake Up!Click this button to wake up the selected IP. See the following
figure. The result will be shown on the box.

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

Application >> Wake on LAN

3.7 VPN and Remote Access

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

In addition, ISDN Internet access settings, LAN to LAN for ISDN and remote dial-in with ISDN also will be explained in this section.

3.7.1 Remote Access Control

Enable the necessary VPN service as you need. If you intend to run a VPN server inside your LAN, you should disable the VPN service of Vigor Router to allow VPN tunnel pass through, as well as the appropriate NAT settings, such as DMZ or open port. And, if you want to enable ISDN dial-in function, please check "Enable ISDN Dial-In" in this page.

VPN and Remote Access >> Remote Access Control Setup

Remote Access Control Setup

v	Enable PPTP VPN Service
	Enable IPSec VPN Service
	Enable L2TP VPN Service
	Enable ISDN Dial-In

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

ОК	Clear	Cancel
OK	Cicai	Cancer

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

3.7.2 PPP General Setup

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

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

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

Dial-In PPP Authentication PAP Only	Select this option to force the router to authenticate dial-in users with the PAP protocol.
PAP or CHAP	Selecting this option means the router will attempt to authenticate dial-in users with the CHAP protocol first. If the dial-in user does not support this protocol, it will fall back to use the PAP protocol for authentication.
Dial-In PPP Encryption (MPPE Optional MPPE	This option represents that the MPPE encryption method will be optionally employed in the router for the remote dial-in user. If the remote dial-in user does not support the MPPE encryption algorithm, the router will transmit "no MPPE encrypted packets". Otherwise, the MPPE encryption scheme will be used to encrypt the data. Optional MPPE Require MPPE(40/128 bit) Maximum MPPE(128 bit) Maximum MPPE(128 bit) Require MPPE (40/128bits) - Selecting this option will force the router to encrypt packets by using the MPPE encryption algorithm. In addition, the remote dial-in user will use 128-bit to perform encryption prior to using 40-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 only use the MPPE encryption scheme with maximum bits (128 bits) 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.

3.7.3 IPSec General Setup

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

There are two phases of IPSec.

- \triangleright 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.
- \triangleright Phase 2: negotiation IPSec security methods including Authentication Header (AH) or Encapsulating Security Payload (ESP) for the following IKE exchange and mutual examination of the secure tunnel establishment.

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

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

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

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

IKE Authentication Method This usually applies to those are remote dial-in user or node (LAN-to-LAN) which uses dynamic IP address and IPSec-related VPN connections such as L2TP over IPSec and IPSec tunnel.

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

3.7.4 IPSec Peer Identity

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

VPN and Remote Access >> IPSec Peer Identity

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

Set to Factory Default	Click it to clear all indexes.	
Index	Click the number below Index to access into the setting page of IPSec Peer Identity.	
Name	Display the profile name of that index.	
Next	Click this link to access into next page for setting more accounts.	

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

VPN and Remote Access >> IPSec Peer Identity

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

3.7.5 Remote Dial-In User

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

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

VPN and Remote Access >> Remote Dial-in User

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

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

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.
Next	Click this link to access into next page for setting more accounts.

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

User account and Authentication		
Enable this account	Username	David
Idle Timeout 300 second(s)	Password	••••
Allowed Dial-In Type	IKE Authentication	Method
ISDN	🛛 🗹 Pre-Shared Key	
₽РТР	IKE Pre-Shared Key	
🗹 IPSec Tunnel	📃 🔲 Digital Signature (X	(.509)
L2TP with IPSec Policy None	??? 💙	
Specify Remote Node Remote Client IP or Peer ISDN Number	IPSec Security Meth Medium (AH) High (ESP) DES 3DES Local ID Callback Function Check to enable Ca Specify the call Callback Number Callback to enable Callback Budget	✓ AES (optional)

Enable this account	Check the box to enable this function. Idle Timeout- If the dial-in user is idle over the limitation of the time, 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.
РРТР	Allow the remote dial-in user to make a PPTP VPN connection through the Internet. You should set the User Name and Password of remote dial-in user below
IPSec Tunnel	Allow the remote dial-in user to trigger 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 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 PPTP or L2TP with or without IPSec policy above.
Password	This field is applicable when you select 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 router owner will be charged the connection fee by the telecom. Check to enable Callback function-Enables the callback function. Specify the callback number-The option is for extra security. Once enabled, the router will ONLY call back to the specified Callback Number. Check to enable callback budget control-By default, the callback function has a time restriction. Once the callback budget has been exhausted, the callback mechanism will be disabled automatically. Callback Budget (Unit: minutes)- Specify the time budget for the dial-in user. The budget will be decreased automatically per callback connection.

3.7.6 LAN to LAN

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

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

Besides, you can connect two networks through ISDN connection (for *i* model only). The way to set profile (for dial-in and dial-out) for ISDN connection is the same as VPN tunnel setting profile.

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

VPN and Remote Access >> LAN to LAN

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

Set to Factory Default	Click to clear all indexes.
Name	Indicate the name of the LAN-to-LAN profile. The symbol ??? represents that the profile is empty.
Status	Indicate the status of individual profiles. The symbol V and X represent the profile to be active and inactive, respectively.

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

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

VPN and Remote Access >> LAN to LAN

Profile Index : 1

Common Settings	
Profile Name draytek	Call Direction 💿 Both 🔿 Dial-Out 🔿 Dial-In
🔲 Enable this profile	Always on
	Idle Timeout 300 second(s)
	Enable PING to keep alive
	PING to the IP
Dial-Out Settings	
Type of Server I am calling	Link Type 64k bps 👻
O ISDN	Username ???
○ РРТР	Password
O IPSec Tunnel	PPP Authentication PAP/CHAP 🛩
	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) 172.16.3.229	IKE Authentication Method

Profile Name	Specify a name for the profile of the LAN-to-LAN connection.
Enable this profile	Check here to activate this profile.
Call Direction	Specify the allowed call direction of this LAN-to-LAN profile: Both - initiator/responder Dial-Out - initiator only Dial-In - responder only
Always On or Idle Timeout	Always On-Check to enable router always keep VPN connection.Idle Timeout: The default value is 300 seconds. If the connection has been idled over the value, the router will drop the connection.
Enable PING to keep alive	This function is to help the router to determine the status of IPSec VPN connection, especially useful in the case of abnormal VPN IPSec tunnel disruption. For details, please refer to the note below. Check to enable the transmission of PING packets to a specified IP address.
PING to the IP	Enter the IP address of the remote host that located at the other-end of the VPN tunnel.

	 Enable PING to Keep Alive is used to handle abnormal IPSec VPN connection disruption. It will help to provide the state of a VPN connection for router's judgment of redial. Normally, if any one of VPN peers wants to disconnect the connection, it should follow a serial of packet exchange procedure to inform each other. However, if the remote peer disconnect without notice, Vigor router will by no where to know this situation. To resolve this dilemma, by continuously sending PING packets to the remote host, the Vigor router can know the true existence of this VPN connection and react accordingly. This is independent of DPD (dead peer detection).
ISDN	If you want to connect two networks with ISDN connection, please select ISDN radio button to build ISDN dial-out connection to the server. You should set up Link Type and identity like User Name and Password for the authentication of remote server. You can further set up Callback (CBCP) function below. This feature is useful for <i>i</i> model only.
PPTP	Build a PPTP VPN connection to the server through the Internet. You should set the identity like User Name and Password below for the authentication of remote server.
IPSec Tunnel	Build a 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 PPTP or L2TP with or without IPSec policy above.
Password	This field is applicable when you select PPTP or L2TP with or without IPSec policy above.
PPP Authentication	This field is applicable when you select PPTP or L2TP with or without IPSec policy above. PAP/CHAP is the most common selection due to wild compatibility.
VJ compression	This field is applicable when you select PPTP or L2TP with or without IPSec policy above. VJ Compression is used for TCP/IP protocol header compression. Normally set to Yes to improve bandwidth utilization.
IKE Authentication Method	This group of fields is applicable for IPSec Tunnels and L2TP with IPSec Policy. Pre-Shared Key -Input 1-63 characters as pre-shared key. Digital Signature (X.509) - Select one predefined Profiles set in the VPN and Remote Access >> IPSec Peer Identity .

IPSec Security Method	This group of fields is a must for IPSec Tunnels and L2TP with IPSec Policy.
Medium	Authentication Header (AH)- means data will be authenticated, but not be encrypted. By default, this option is active.
	 High (ESP-Encapsulating Security Payload)- means payload (data) will be encrypted and authenticated. Select from below: DES without Authentication -Use DES encryption algorithm and not apply any authentication scheme. DES with Authentication-Use DES encryption algorithm and apply MD5 or SHA-1 authentication algorithm. 3DES without Authentication-Use triple DES encryption algorithm and not apply any authentication scheme. 3DES with Authentication-Use triple DES encryption algorithm and not apply any authentication scheme. 3DES with Authentication-Use triple DES encryption algorithm. AES without Authentication-Use triple DES encryption algorithm. AES without Authentication-Use AES encryption algorithm and not apply any authentication scheme. AES with Authentication-Use AES encryption algorithm and apply MD5 or SHA-1 authentication algorithm and paply any authentication scheme.
Advanced	Specify mode, proposal and key life of each IKE phase, Gateway etc. The window of advance setup is shown as below:
	IKE advanced settings - Microsoft Internet Explorer IKE advanced settings IKE phase 1 mode Main mode Aggressive mode IKE phase 1 proposal DES_MD5_G1 Image: Compose in the image: Com

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

Callback Function (for I models only) The length of the ID is limited to 47 characters. 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.

address while identity authenticating with remote VPN server.

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.**

Dial-In Settings				
Allowed Dial-In Type				
ISDN			Username	???
PPTP			Password	
🗹 IPSec Tunnel			VJ Compression	💿 On 🔘 Off
L2TP with IPSec Poli	icy Must 💌		IKE Authentication	Method
	or Remote VPN Gatew		🗹 Pre-Shared Key	
Peer ISDN Number or P		ay	IKE Pre-Shared Key	
			🔲 Digital Signature(X	.509)
or Peer ID			??? 🗸	
			IPSec Security Met	nod
			🗹 Medium (AH)	
			High (ESP)	
			🗹 DES 🗹 3D	DES 🗹 AES
			Callback Function (CBCP)
			🗌 Enable Callback F	unction
			🔲 Use the Following	Number to Callback
			Callback Number	
			Callback Budget	0 minute(s)
TCP/IP Network Setting	ļs			
My WAN IP	0.0.0.0		RIP Direction	TX/RX Both 💌
Remote Gateway IP	0.0.0.0		RIP Version	Ver. 2 💌
Remote Network IP	0.0.0.0		For NAT operation, tr	eat remote sub-net as
Remote Network Mask	255.255.255.0			Private IP 💌
	More		Change default ro	ute to this VPN tunnel
	OK	Cle	ear Cancel	

Allowed Dial-In Type	Determine the dial-in connection with different types.
ISDN	Allow the remote ISDN dial-in connection. You can further set up Callback function below. You should set the User Name and Password of remote dial-in user below. This feature is useful for <i>i</i> model only.
РРТР	Allow the remote dial-in user to make a PPTP VPN connection through the Internet. You should set the User Name and Password of remote dial-in user below.
IPSec Tunnel	Allow the remote dial-in user to trigger a IPSec VPN connection through Internet.
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 ISDN CLID or Remote VPN Gateway Peer ISDN Number or Peer VPN Server IP	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 model only.). Also, you should further specify the corresponding security methods on the right side.
	If you uncheck the checkbox, the connection type you select above will apply the authentication methods and security methods in the general settings.
User Name	This field is applicable when you select PPTP or L2TP with or without IPSec policy above.
Password	This field is applicable when you select 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 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 ISDN CLID (for <i>i</i> model only) or Remote VPN Gateway Peer ISDN Number (for <i>i</i> model only) or Peer VPN Server IP. The only exception is Digital Signature (X.509) can be set when you select IPSec tunnel either with or without specify the CLID or IP address of the remote node.
	Pre-Shared Key - Input 1-63 characters as 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 (2DES), and AES
Callback Function	 Triple DES (3DES), and AES. The callback function provides a callback service only for the ISDN dial-in user (this feature is useful for <i>i</i> model only). The router owner will be charged the connection fee by the telecom. Check to enable Callback function-Enables the callback function. Callback number-The option is for extra security. Once enabled, the router will ONLY call back to the specified Callback Number. Callback budget- By default, the callback function has limitation of callback period. Once the callback budget is exhausted, the function will be disabled automatically. Callback Budget (Unit: minutes)- Specify the time budget for

	the dial-in user. The budget will be decreased automatically per callback connection. The default value 0 means no limitation of callback period.
My WAN IP	This field is only applicable when you select PPTP or L2TP with or without IPSec policy above. The default value is 0.0.0.0, which means the Vigor router will get a 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.
Remote Gateway IP	This field is only applicable when you select PPTP or L2TP with or without IPSec policy above. The default value is 0.0.0.0, which means the Vigor router will get a remote Gateway 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.
Remote Network IP/ Remote Network Mask	Add a static router to direct all traffic destined to this Remote Network IP Address/ Remote Network Mask through the VPN connection. For IPSec, this is the destination clients IDs of phase 2 quick mode.
More	Add a static router to direct all traffic destined to more Remote Network IP Addresses/ Remote Network Mask through the VPN connection. This is usually used when you find there are several subnets behind the remote VPN router.
RIP Direction	The option specifies the direction of RIP (Routing Information Protocol) packets. You can enable/disable one of direction here. Herein, we provide four options: TX/RX Both, TX Only, RX Only, and Disable.
RIP Version	Select the RIP protocol version. Specify Ver. 2 for greatest compatibility.
For NAT operation, treat remote sub-net as	While communicating with remote subnet, the router can treat it as private subnet by sending packets with the router's private IP address, or treat it as public subnet by sending packets with the router's public IP address.
Change default route to this VPN tunnel	Check this box to change the default route with this VPN tunnel. Be aware that this setting is available only for one WAN interface is enabled. It is not available when both WAN

interfaces are enabled.

3.7.7 Connection Management

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

VPN and Remote Access >> Connection Management

Dial-out Tool				Refres	h Seconds	s : 10 🔽	Refresh
			~	Dial			
VPN Connection Status Current Page: 1							Next
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 execu	te dial o	ut functi	on.	
Refresh Seconds	Choose th and 30.	ne time f	for refres	h the di	al inform	nation am	ong 5, 10
Refresh	Click this	button	to refres	h the wł	nole conr	nection st	atus.
Note: The status of L	AN to LAN for I	SDN is	shown o	n the pa	ge of O r	nline Stat	tus.
							-

System Statu	5						S	ystem U	ptime: 0:27:54
LAN Status		Р	rimary DN	IS: 194.109	9.6.66	S	econd	ary DNS:	194.98.0.1
IP Address		TX Pac	kets	RX Pack	ets				
192.168.1.1		653		599					
WAN Status			GW I	P Addr: 17	2.16.3.1				
Mode	IP Addr	ess	TX Pac	kets TX	Rate F	X Packet	ts F	RX Rate	Up Time
Static IP	172,16.3	3.229	0	0	C)	0)	0:01:03
ADSL Informa	tion	(ADSL Fir	mware Ver	sion: 1211	202_B)				
ATM Statisti	cs TX B	locks	RX E	Blocks	Co	rrected E	locks	Uncor	rected Blocks
	0		0		0			0	
ADSL Status	Mode	State	U	p Speed	Down	Speed	SNR N	/largin	Loop Att.
		READY	0		0	-	0	_	0
ISDN Status									
Channel Act	ive Conn	ection	TX Pkts	TX Rate	RX Pkt	s RX I	Rate	Up Time	AOC
B1 Idle	[]		0	0	0	0		0:0:0	0
B2 Idle	[]		0	0	0	0		0:0:0	0
D DOV	VN								
							>>	Drop B:	L >> Drop B2

3.8 Certificate Management

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

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

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

3.8.1 Local Certificate

Certificate Management >> Local Certificate

Name	Subject	Status	Modify
Local			View Delete
ENERATE	IMPORT REFRESH		
X509 Local C	ertificate		
			<u>~</u>

Generate Click this button to open Generate Certificate Request window. Certificate Management >> Local Certificate Generate Certificate Request Subject Alternative Name Туре IP Address ΙP 172.16.3.229 Subject Name Country (C) TW State (ST) Location (L) Orginization (O) Draytek RD Department Orginization Unit (OU) Common Name (CN) Email (E) service@draytek.com Кеу Туре Key Size 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.

Click this button to view the detailed settings for certificate request.

After clicking Generate, the generated information will be displayed on the window below: Certificate Management >> Local Certificate

Name	Subject	Status	Modify
Local	/C=TW/O=Draytek/OU=RD Depart	Requesting	View Delete
GENERATE X509 L	IMPORT REFRESH		
MIIBv7 BgNVBA eXRlay P101ME B1u43G 11v3+p A1UdEC 1AwSL7 kc2yc2 JH1AH4	EGIN CERTIFICATE REQUEST CCASYCAQAwWZELMAKGA1UEBhMCVFcxEDAOI STDVJEIERLcGFydG1lbnQxIjAgBgkqhkiG SjD20wgZ8wDQYJKoZlbncNAQEBQADgYOAI zTbUKPQp190PefEvoE1WCN6Vv1MZejLOhff EYSO7NdY6YrsEFgRWbjSVJeYNMeFfZs1cR- SS2U+61WtFpLnskQ8tz3BAgMBAAGgIjAgI QIMAAHBKwQA+UwDQYJKoZlhvcNAQEFBQADg 'xyM4XHd5la2haRQjDYGf43Cd1Vz+glsMXV4 U1SDS9T+JRxi/cff+vQRC1wWK2J7pX5M0wJ PwDmyck8AiEFHSoxE= ND CERTIFICATE REOUEST	WOBCQEWE3N1c MIGJAoGBAOyCa DMzjzqzWsXcQk HDMGfc12f6WdS SgkqhkiG9wOBC gYEABgtWjFrL5 łh2G/FdlxfexQ	nZpY2VAZHJh 1K2vcBeeO+M C54zDhJUv6r UUpTnwlaXqu Q4xEzARNA86 XECxE4CV9pq 2E027BHJB11K

3.8.2 Trusted CA Certificate

Trusted CA certificate lists three sets of trusted CA certificate.

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

X509 Trusted CA Certificate Configuration

Trusted CA-1 Trusted CA-2	View Delete
Trusted CA-2	
	View Delete
Trusted CA-3	View Delete

IMPORT REFRESH

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

Certificate Management >> Trusted CA Certificate				
Import X509 Trusted CA Certific	ate			
Select a tru	sted 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.

View

🕘 Cer	tificate Information - Microsoft Inter	net Explorer	
			<u>~</u>
	Certific	ate Detail Information	
	Certificate Name:	Trusted CA-1	
	Issuer:		
	Subject:		
	Subject Alternative Name:		
	Valid From:		
	Valid To:		
		Close	-
			~

3.9 VoIP

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

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

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

sip: user:password @ host: port

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

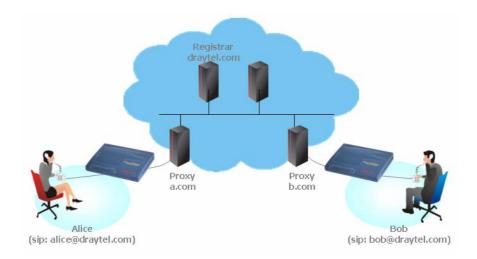
After a call is setup, the voice streams transmit via RTP (Real-Time Transport Protocol). Different codecs (methods to compress and encode the voice) can be embedded into RTP packets. Vigor V models provide various codecs, including G.711 A/ μ -law, G.723, G.726 and G.729 A & B. Each codec uses a different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

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

• Calling via SIP Servers

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

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



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

Peer-to-Peer

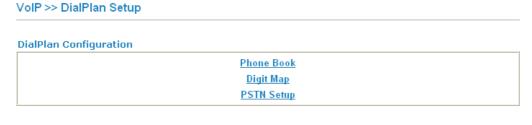
Before calling, you have to know your friend's IP Address. The Vigor VoIP Routers will build connection between each other. Please refer to the **Example 3 in the Calling Scenario.**



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

3.9.1 DialPlan

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



Note: The PSTN Setup link is available for Vigor2700V(MODULE: 2S1L) and Vigor2700VG(MODULE: 2S1L) only.

Phone Book

In this section, you can set your VoIP contacts in the "phonebook", called DialPlan. It can help you to make calls quickly and easily by using "speed-dial" **Phone Number**. There are total 60 index entries in the DialPlan for you to store all your friends and family members' SIP addresses.

For the models of Vigor 2700VGi/2700V (MODULE: 2S1L)/2700VG (MODULE: 2S1L), the phone book settings should be the same as the following:

VoIP >> DialPlan Setup

Index	Phone number	Display Name	SIP URL	Loop through	Backup Phone Number	Status
<u>1.</u>				None		×
<u>2.</u>				None		×
<u>3.</u>				None		×
<u>4.</u>				None		×
<u>5.</u>				None		×
<u>6.</u>				None		×
<u>7.</u>				None		×
<u>8.</u>				None		х
<u>9.</u>				None		×
<u>10.</u>				None		×
<u>11.</u>				None		×
<u>12.</u>				None		×
<u>13.</u>				None		х
<u>14.</u>				None		×
<u>15.</u>				None		×
<u>16.</u>				None		×
<u>17.</u>				None		×
<u>18.</u>				None		×
<u>19.</u>				None		х
<u>20.</u>				None		х

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

For the models of Vigor2700V (MODULE: 2S)/ 2700VG (MODULE: 2S), the phone book settings should be the same as the following:

VoIP >> DialPlan Setu	p
-----------------------	---

Index	Phone number	Display Name	SIP URL	Status
<u>1.</u>				×
<u>2.</u>				×
3.				×

Click any index number to display the dial plan setup page. Below is a sample page obtained from Vigor 2700V(MODUEL:2S)/2700VG(MODUEL:2S).

VolP:	>> Dia	IPlan	Setup

🗹 Enable			
	Phone Number	1	
	Display Name	Polly	
	SIP URL	1112	@ fwd.pulver.com

Enable	Click this to enable this entry.
Phone Number	The speed-dial number of this index. This can be any number you choose, using digits 0-9 and * .
Display Name	The Caller-ID that you want to be displayed on your friend's screen. This let your friend can easily know who's calling without memorizing lots of SIP URL Address.
SIP URL	Enter your friend's SIP Address

This page will differ for different models. Below is a sample page obtained from Vigor 2700VGi. The selection for **Loop through** differs slightly in Vigor 2700VGi and Vigor 2700V(MODULE: 2S1L)/ 2700VG (MODULE: 2S1L).

VoIP >>	DialP	lan Setur	С
---------	-------	-----------	---

Phone Book I	ndex No. 1		
	Phone Number	1]
	Display Name	Polly]
	SIP URL	1112	@ fwd. pulver. com
	Loop through	None 🚩	
	Backup Phone Number		
	OK	Clear	Cancel

Enable

Click this to enable this entry.

Phone Number

The speed-dial number of this index. This can be any number you choose, using digits **0-9** and *****.

Display Name	The Caller-ID that you want to be displayed on your friend's screen. This let your friend can easily know who's calling without memorizing lots of SIP URL Address.			
SIP URL	Enter your friend's SIF	Address		
Loop through	•	2700V (MODULE: 2S1L)/ Vigor 2S1L), the selection should be as the		
	Loop through	None 🕶 None PSTN		
	For the model of Vigor 2700VGi, the selection should be as the following:			
	Loop through	None V None ISDN		
Backup Phone Number	USDN When the VoIP phone is obstructs or the Internet breaks down for some reasons, the backup phone will be dialed out to replace the VoIP phone number. At this time, the phone call will be changed from VoIP phone into PSTN call according to the loo through direction chosen. Note that, during the phone switch, the blare of phone will appear for a short time. And when the VoIP phone is switched into the PSTN phone, the telecom co. might charge you for the connection fee. Please type in backup phone number (PSTN number) for this VoIP phone setting.			

Digit Map

VoIP >> DialPlan Setup

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.

nable	Prefix Number	Mod		OP Number	Min Len	Max Len	Interface
 Image: A start of the start of	03	Replac	e 💙	8863	7	9	VolP1 🔽
~	886	Strip	~	886	7	9	VolP4 🔽
~		None	~		0	0	PSTN 🔽
		None	\sim		0	0	PSTN 🔽
		None	\sim		0	0	PSTN 🔽
		None	~		0	0	PSTN 🔽
		None	~		0	0	PSTN 🗠
		None	\sim		0	0	PSTN 🗸
		None	~		0	0	PSTN 🗸
		None	~		0	0	PSTN 🗸
		None	~		0	0	PSTN 🗸
		None	\sim		0	0	PSTN 🗸
		None	\sim		0	0	PSTN 🗸
		None	~		0	0	PSTN V
		None	~		0	0	PSTN 🗸
		None	\sim		0	0	PSTN 🗸
		None	\sim		0	0	PSTN 🗸
		None	~		0	0	PSTN 🗸
		None	~		0	0	PSTN 🗸
		None	~		0	0	PSTN 🗸

Enable	Check this box to invoke this setting.
Prefix Number	The phone number set here is used to add, strip, or replace the OP number.
Mode	None - No action. Add - When you choose this mode, the OP number will be added with the prefix number for calling out through the specific VoIP interface. Strip - When you choose this mode, the OP number will be deleted by the prefix number for calling out through the specific VoIP interface. Take the above picture (Prefix Table Setup web page) as an example, the OP number of 886 will be deleted completely for the prefix number is set with 886. Replace - When you choose this mode, the OP number will be replaced by the prefix number for calling out through the specific VoIP interface. Take the above picture (Prefix Table Setup web page) as an example, the prefix number of 03 will be replaced by 8863. For example: dial number of "031111111" will be changed to "88631111111" and sent to SIP server. Mode Replace None Add Strip Replace
OP Number	The front number you type here is the first part of the account number that you want to execute special function (according to the chosen mode) by using the prefix number.
Min Len	Set the minimal length of the dial number for applying the prefix number settings. Take the above picture (Prefix Table Setup web page) as an example, if the dial number is between 7 and 9, that number can apply the prefix number settings here.
Max Len	Set the maximum length of the dial number for applying the prefix number settings.
Interface	Choose the one that you want to enable the prefix number settings from the seven pre-saved SIP accounts (including PSTN). The PSTN interface is available for 2700V (MODULE: 2S1L)/ Vigor 2700VG (MODULE: 2S1L) only.

PSTN Setup

Some emergency phone (e.g., 911) or special phone cannot be dialed out by using VoIP and can be called out through PSTN line only. To solve this problem, this page allows you to set five sets of PSTN number for dialing without passing through Internet. Please type the number in the field of **phone number for PSTN relay**.

Enable	phone number for PSTN relay
v	911

Then, check the Enable box to make the PSTN number available for dial whenever you need.

Note: This function is available for Vigor2700V/2700VG (MODULE 2S1L) only.

3.9.2 SIP Accounts

VoIP >> SIP Accounts

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

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

					_	
SIP Acc	ounts Lis	t				Refresh
Index	Profile	Domain/Realm	Proxy	Account Name	Ring Port	Status
1				change_me	VoIP1 VoIP2 ISDN	-
2				change_me	VoIP1 VoIP2 ISDN	-
<u>3</u>				change_me	VoIP1 VoIP2 ISDN	-
4				change_me	VoIP1 VoIP2 ISDN	-
<u>5</u>				change_me	VoIP1 VoIP2 ISDN	-
<u>6</u>			change_me		VoIP1 VoIP2 ISDN	-
NAT Tra	i <mark>versal Se</mark> STUN s					
External IP:				\neg		
SIP PING interval:		150	sec			
				ОК		
ndex		Cli	ck this linl	k to access into	o next page for setting SII	P accou
Profile Display the profile name of the account.						
rofile			splay the p	forme name of	the account.	
	ı/Realm	Dis			r IP address of the SIP reg	gistrar
	n/Realm	Disser	splay the d ver.	omain name o		
)omain Proxy	n/Realm t Name	Dis ser Dis	splay the d ver. splay the d	omain name o omain name o	r IP address of the SIP reg	

STUN Server Type in the IP address of the STUN server.

External IP	Type in the gateway IP address.
SIP PING interval	The default value is 150 (sec). It is useful for a Nortel server NAT Traversal Support.
Status	Show the status for the corresponding SIP account. \mathbf{R} means such account is registered on SIP server successfully. – means the account is failed to register on SIP server.

VoIP >> SIP Accounts

Profile Name	(11 char max	.)
Register via	None 💌 🗌 make call without	t register
SIP Port	5060	
Domain/Realm		(63 char max.)
Proxy		(63 char max.)
🗌 Act as outbound	огоху	
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 💌	
Ring Port	VoIP1 VoIP2	
Ring Pattern	1 💌	

Profile Name	Assign a name for this profile for identifying. You can type similar name with the domain. For example, if the domain name is <i>draytel.org</i> , then you might set <i>draytel-1</i> in this field.		
Register via	If you do not want to register for VoIP phone, please choose None. In addition, some SIP server allows users to use VoIP function without registering. For such server, please check the box of make call without register . Choosing Auto is recommended. The system will select a proper way for your VoIP call. Register via None Auto WAN LAN/VPN		
SIP Port	Set the port number for sending/receiving SIP message for building a session. The default value is 5060. Your peer must set the same value in his/her Registrar.		
Domain/Realm	Set the domain name or IP address of the SIP Registrar server.		
Proxy	Set domain name or IP address of SIP proxy server. By the time you can type :port number after the domain name to specify that port as the destination of data transmission (e.g., nat.draytel.org :5065)		
Act as Outbound Proxy	Check this box to make the proxy acting as outbound proxy.		
Display Name	The caller-ID that you want to be displayed on your friend's screen.		

Account Number/Name	Enter your account name of SIP Address, e.g. every text before @.		
Authentication ID	Check the box to invoke this function and enter the name or number used for SIP Authorization with SIP Registrar. If this setting value is the same as Account Name, it is not necessary for you to check the box and set any value in this field.		
Password	The password provided to you when you registered with a SIP service.		
Expiry Time	The time duration that your SIP Registrar server keeps your registration record. Before the time expires, the router will send another register request to SIP Registrar again.		
NAT Traversal Support	If the router (e.g., broadband router) you use connects to internet by other device, you have to set this function for your necessity. NAT Traversal Support None Stun manual nortel None – Disable this function. Stun – Choose this option if there is Stun server provided for your router. Manual – Choose this option if you want to specify an external IP address as the NAT transversal support. Nortel – If the soft-switch that you use supports Nortel solution, you can choose this option.		
Ring Port	Set VoIP 1 or VoIP 2 as the default ring port.		
Ring Pattern	Choose a ring tone type for the VoIP phone call. Ring Pattern 1 2 3 4 5 6		

Below shows successful SIP accounts for your reference.

VoIP >> SIP Accounts

SIP Acc	ounts List					Refresh
Index	Profile	Domain/Realm	Proxy	Account Name	Ring Port	Status
1	draytel_1	draytel.org	draytel.org	813177	VoIP1 VoIP2	-
2	draytel_2	draytel.org	draytel.org	812862	🗌 VoIP1 🗹 VoIP2	R
<u>3</u>	draytel_3	draytel.org	draytel.org	811997	VoIP1 VoIP2	-
<u>4</u>	IPTEL	iptel.org	iptel.org	kevinyu	🗌 VoIP1 🗹 VoIP2	R
5	FWD	fwd.pulver.com	fwd.pulver.com	56984	VoIP1 VoIP2	-
<u>6</u>	SeedNet	seed.net.tw	139.175.232.13	070901002	✓ VoIP1 ✓ VoIP2	R

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

NAT Traversal Setting

STUN server:			
External IP:]
SIP PING interval:	150	sec	

OK

3.9.3 Phone Settings

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

VoIP >>	Phone	Settings
---------	-------	----------

Index	Port	Call feature	Codec	Tone	Gain (Mic/Speaker)	Default SIP Account	DTMF Relay
1	VoIP1		G.729A/B	User Defined	5/5		InBand
2	VoIP2		G.729A/B	User Defined	5/5		InBand
<u>3</u>	ISDN		G.729A/B	User Defined	5/5		InBand
ктр							
		Symmetric RT	P				
	Dyr	namic RTP port	t start	10	050		
Dynamic RTP port end 15000							
RTP TOS IP precedence 5 🔽 10100000							

RTP

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

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

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

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					
IP precedence 5	~				

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

RTP TOS

VoIP >> Phone Settings

Phone Index No.1					
Call feature		Codecs			
🔲 Hotline		Prefer Codec	G.729A/B (8Kbps) 🔽		
🔲 Session Timer	3600 sec		🔲 Single Codec		
🔲 T.38 Fax Function		Packet Size	20ms 💌		
		Voice Active Detector	Off 🕶		
Call Forwarding	disable 🔽				
SIP URL		Default SIP Account	1-??? 🐱		
Time Out	30 sec	Play dial tone only v	vhen account registered		
🔲 DND(Do Not Disturb) I		Default Call Route	Default Call Route		
Index(1-15) in <u>Sche</u>	edule Setup:	🔘 To ISDN: Dial 🔭	for VoIP		
		⊙ To VoIP: Dial #	for ISDN		
Note: Action and I be ignored.	dle Timeout settings wi]		
🔲 CLIR (hide caller ID)					
🔲 Call Waiting					
🔲 Call Transfer					
	Гок Г	Cancel Advanced			

Hotline Check the box to enable it. Type in the SIP URL in the field for dialing automatically when you pick up the phone set. Session Timer Check the box to enable the function. In the limited time that you set in this field, if there is no response, the connecting call will be closed automatically. T.38 Fax function If the remote end also supports FAX function, you can check this box to enable this function. **Call Forwarding** There are four options for you to choose. Disable is to close call forwarding function. Always means all the incoming calls will be forwarded into SIP URL without any reason. Busy means the incoming calls will be forwarded into SIP URL only when the local system is busy. No answer means if the incoming calls do not receive any response, they will be forwarded to the SIP URL by the time out. Call Forwarding disable alwavs 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)** Set a period of peace time without disturbing by VoIP phone mode call. During the period, the one who dial in will listen busy tone, yet the local user will not listen any ring tone. 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.

CLIR (hide caller ID)	Check this box to hide the caller ID on the display panel of the phone set for the remote side.					
Call Waiting	Check this box to invoke this function. A notice sound will appear to tell the user new phone call is waiting for your response. Click hook flash to pick up the waiting phone call.					
Call Transfer	Check this box to invoke this function. Click hook flash to initiate another phone call. When the phone call connection succeeds, hang up the phone. The other two sides can communicate, then.					
Prefer Codec	Select one of five codecs as the default for your VoIP call codec used for each call will be negotiated with the peer p before each session, and so many not be your default choi The default codec is G.729A/B; it occupies little bandwidt while maintaining good voice quality. If your upstream speed is only 64Kbps, do not use G.711 of It is better for you to have at least 256Kbps upstream if you would like to use G.711.					
	Prefer Codec	G.729A/B (8Kbps) G.711MU (64Kbps) G.711A (64Kbps) G.729A/B (8Kbps) G.723 (6.4kbps)				

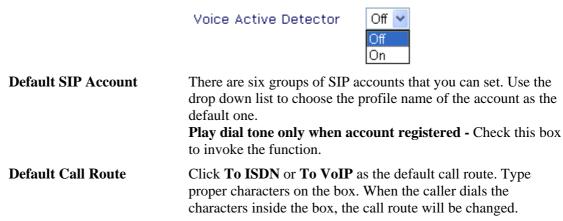
Single Codec – If the box is checked, only the selected Codec will be applied.

G.726_32 (32kbps)

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

20ms	1
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.



Packet Size

To ISDN: Current used phone is connected through ISDN network. If the caller dials the characters listed in this box, then the ISDN phone will be switched into VoIP phone on Internet. **To VoIP:** Current used phone is VoIP phone. If the caller dials the characters listed in this box, then the VoIP phone will be switched into phone through ISDN connection on Internet.

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 Set	tings						
Region	User Defined	*		Cal	ler ID Type	FSK_ETSI	~
		Low Freq (Hz)	High Freq (Hz)	T on 1 (msec)	T off 1 (msec)	T on 2 (msec)	T off 2 (msec)
Dial tone		350 440		0) 0		0
Ringing tone		400 450		400	200	400	2000
Busy tone		400	0	375	375	0	0
Conges	stion tone	0	0	0	0	0	0
Volume	Gain			DTMF			
Mic Gain(1-10)	5		DTMF mode		InBand	*
Speaker (Gain(1-10)	5		Payload Ty	ype(rfc2833)	101	
MISC							
Dial Tone Power Level		27	7				
Ring Frequency		25	5				

Region

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

Tone Settings					
Region	User Defined 💌				
	User Defined				
	UK (
Dia	US Denmark 0				
Ringi	ltaly D				
	Germany Netherlands 0				
Conges	Portugal Sweden				
Volume	Australia				
Mic Gain(Slovenia Czech				
Speaker (

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. DTMP **DTMF mode** – There are four selections provided here: InBand: Choose this one then the Vigor will send the DTMF tone as audio directly when you press the keypad on the phone **OutBand:** Choose this one then the Vigor will capture the keypad number you pressed and transform it to digital form then send to the other side; the receiver will generate the tone according to the digital form it receive. This function is very useful when the network traffic congestion occurs and it still can remain the accuracy of DTMF tone. **SIP INFO:** Choose this one then the Vigor will capture the DTMF tone and transfer it into SIP form. Then it will be sent to the remote end with SIP message. DTMF mode InBand InBand OutBand (RFC2833) SIP INFO (cisco format) SIP INFO (nortel format)

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

3.9.4 Status

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

```
VoIP >> Status
```

Status								Refresh S	econds:	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
VoIP1	IDLE			00:00:00	0	0	0	0	0	0	5
VoIP2	IDLE			00:00:00	0	0	0	0	0	0	5
ISDN1	IDLE			00:00:00	0	0	0	0	0	0	5
ISDN2	IDLE			00:00:00	0	0	0	0	0	0	5
Log Date		Tim		Duratio		n/Out	Pee	er ID			
(mm-do 00-00-	1–9999) - O		:mm:ss) 00:00	(hh:mm: 00:00:0							
00-00-	-		00:00	00:00:0	-						
00-00-	-		00:00	00:00:0	-						
00-00-	-		00:00	00:00:0	-	-					
00-00-	-		00:00	00:00:0	-						
00-00-	-		00:00	00:00:0	-						
00-00-	-		00:00	00:00:0	-						
00-00-	-		00:00 00:00	00:00:0 00:00:0							
00-00-	-		00:00	00:00:0							
00-00-	0	00.	00.00	30.00.0							

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.

> . 10 🗸 Refresh Seconds

4	10	~
	5	
	10	
	30	

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

Out Calls	The accumulating times of out-call.
Speaker Gain	The volume of present call.
Log	Display logs of VoIP calls.

3.10 ISDN

ISDN stands for Integrated Services Digital Network. It is an international communications standard for sending voice, video, and data over digital telephone lines.

Note: The feature is available for *i* models only.

3.10.1 General Setup

ISDN >> General Setup

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

	OK
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 from the drop down list.
Own Number	Enter your ISDN number. Every outgoing call will carry the number to the receiver.
MSN Numbers for the Router	MSN Numbers mean that the router is able to accept only number-matched incoming calls. In addition, MSN services should be supported by local ISDN network

number.

provider. The router provides three fields for MSN numbers. Note that MSN services must be acquired from your local telecommunication operators. By default, MSN function is disabled. If you leave the fields blank, all incoming calls will be accepted without number matching.

Blocked MSN Numbers for the router Enter the specified MSN number into the fields to prevent the router from dialing the specific MSN

Vigor2700 Series User's Guide

3.10.2 Dialing to a Single ISP

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

ISDN >>	Dialing	to a S	ingle	ISP
---------	---------	--------	-------	-----

Single ISP			
ISP Access Setup		PPP/MP Setup	
ISP Name	dlin	Link Type	Dialup BOD 🛛 🔽
Dial Number	30	PPP Authentication	PAP or CHAP 💌
		Idle Timeout	180 second(s)
Username	dlin	IP Address Assignm	ent Method (IPCP)
Password	••••	Fixed IP	🔘 Yes 💿 No (Dynamic IP)
🔲 Require ISP callback	(CBCP)	Fixed IP Address	
Index(1-15) in <u>Schedul</u>	<u>e</u> Setup:		
=>,	,,		
		OK	

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

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

Fixed IP Address Type the IP address.

3.10.3 Dialing to Dual ISPs

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

ISDN >> Dialing to Dual ISPs

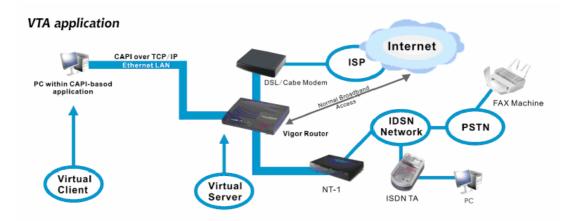
Dual ISP			
Common Settings		PPP/MP Setup	
1. 🗹 Enable Dual I	ISPs Function	Link Type	Dialup BOD 🛛 👻
2. 🔲 Require ISP o	callback (CBCP)	PPP Authentication	PAP or CHAP 🔽
		Idle Timeout	180 second(s)
Primary ISP Setup)	Secondary ISP Set	up
ISP Name	dlin	ISP Name	prima
Dial Number	30	Dial Number	66
Username	dlin	Username	prima
Password	••••	Password	••••
IP Address Assign	ment 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	
		ж	

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

3.10.4 Virtual TA

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

- The Virtual TA client only supports MicrosoftTM Windows 95 OSR2.1/98/98SE/Me/2000 platforms.
- The Virtual TA client only supports the CAPI 2.0 protocol and has no built-in FAX engine.
- One ISDN BRI interface has two B channels. The maximum number of active clients is also two.
- Before you configure the Virtual TA, you must set the correct country code.



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

Before you configure the Virtual TA (Remote CAPI) Setup, please install the virtual TA client first. Simply insert the CD bundled with your Vigor router, or directly double-click one of the installer files. In which **Vsetup95.exe** is for Windows 95 OSR2.1 or higher; **Vsetup98.exe** is for Windows 98, 98SE and Me; and **Vsetup2k.exe** is for Windows 2000. Follow the on-screen instructions of the installer. The last step will ask you to restart your computer. Click **OK** to restart your computer.

After the computer restarts, you will see a VT icon in the taskbar (usually in the bottom-right of the screen, near the clock) as shown below.



When the icon text is GREEN, the Virtual TA client is connected to the Virtual TA server and you can launch your CAPI-based software to use the client to access the router. Please read your software user guide for detailed configuration. If the icon text is RED, it means the client has lost the connection to the server. In such condition, please check the physical Ethernet connection.

™⊡∢({<mark>♥</mark>■ 2:51 PM

Next, click the **Virtual TA** (**Remote CAPI**) **Setup** link in the **Quick Setup** group to configure the Virtual TA features.

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

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

ISDN >> Virtual TA

rtual TA Server	: 💿 Enabl	le 🔘 Disable			
irtual TA Users Prof	iles				
Username	Password	MSN1	MSN2	MSN3	Active
1.					
2.					
3.					
4.					
5.					

Virtual TA Server	Enable: Select it to activate the server. Disable: Select it to deactivate the server. All Virtual TA applications will be terminated.
Username	Enter the username of a specific client.
Password	Enter the password of a specific client.
MSN1/ MSN2/MSN3	MSN stands for Multiple Subscriber Number . It means you can apply to more than one ISDN lines number over a single subscribed line. Note that the service must be acquired from your telecom. Specify the MSN numbers for a specific client. If you have no MSN services, leave this field blank.
Active	Check it to enable the client to access the server.

User Profile

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

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

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

Virtual TA Users Prof	iles				
Username	Password	MSN1	MSN2	MSN3	Active
1. alan	••••				

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



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

Virtual TA Login	
User Name :	alan
Password :	****
OK S	Cancel

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

MSN Configuration

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

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

Virtual TA Users	Profiles				
Username	Password	MSN1	MSN2	MSN3	Active
1. alan	••••	123			

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

3.10.5 Call Control

Some applications require that the router (only for *i* models) be remotely activated, or be able to dial up to the ISP via the ISDN interface. Vigor routers provide this feature which allows you to make a phone call to the router and then ask it to dial up to the ISP.

Please set **Dialing to a Single ISP** first before configuring this web page.

ISDN >> Call Control			
Call Control Setup			
Dial Retry	0 times	Remote Activation	
Dial Delay Interval	0 second(s)		
PPP/MP Dial-Out Setup			
Basic Setup		Bandwidth On Demand	l (BOD) Setup
Link Type	Dialup BOD 🛛 👻	High Water Mark	7000 cps
PPP Authentication	PAP or CHAP 🔽	High Water Time	30 second(s)
TCP Header Compression	None 🖌	Low Water Mark	6000 cps
Idle Timeout	180 second(s)	Low Water Time	30 second(s)
Dial Retry	triggered packe local network. each triggered p		destination is outside the no dial retry. If set to 5, f dial 5 times until it is
Dial Delay Interval	It specifies the interval between dialup retries. By default, the interval is 0 second.		
Remote Activation	It specifies a phone number in the Remote Activation field to enable the remote activation function. If the router accepts a cal from the number 12345678, it will terminate the incoming call immediately and dial to the ISP.		
Link Type	Because ISDN has two B channels (64Kbps/per channel), you can specify whether you would like to have single B channel,		

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. VJ Compression - It is used for TCP/IP protocol header **TCP Header Compression** compression. Normally it is set to None to improve bandwidth

V

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

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

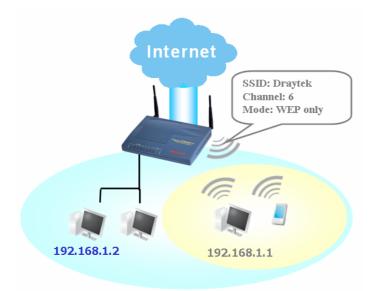
3.11 Wireless LAN

Note: This function is used for *G* models only.

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

3.11.1 Basic Concept

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 with other wired hosts via Vigor wireless router. The **General Settings** will set up the information of this wireless network, including its SSID as identification, located channel etc.



Security Overview

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

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

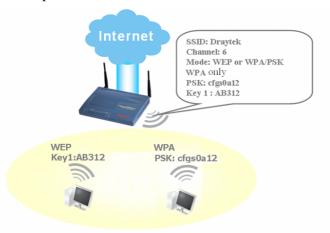
WEP (Wired Equivalent Privacy) is a legacy method to encrypt each frame transmitted via radio using either a 64-bit or 128-bit key. Usually access point will preset a set of four keys and it will communicate with each station using only one out of the four keys.

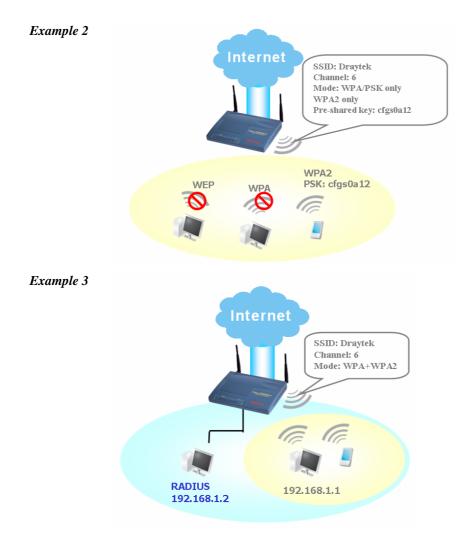
WPA (Wi-Fi Protected Access), the most dominating security mechanism in industry, is separated into two categories: WPA-personal or called WPA Pre-Share Key (WPA/PSK), and WPA-Enterprise or called WPA/802.1x.

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

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

Example 1





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 a filter of MAC address to isolate single user's access from wired LAN.

Manage Wireless Stations - Station List will display all the station in your wireless network and the status of their connection.

3.11.2 General Settings

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

E	nable Wireless LA	٩N								
	Mode:		٨	/lixed(11b+11g) 🔽						
	Index(1-15) in <u>Schedule</u>		Setup:	,,	,					
	Enable Hi	de SSID	:	SSID	Isolate	LAN	Member			
	1		default							
	2									
	3 🔲									
	4									
) from being scan	ned.						
	Isolate Memb Wireless client		s) with the same §	SSID cannot acc	cess for each o	ther.				
	Isolate LAN:) with the same (N.			
			.,							
	Channel: Chan	nel 6 💌	Lo	ong Preamble: [
	Long Preamble:	: necessar	y for some old 80:	2.11 b devices o	only(lower perf	ormano	ce)			
	Packet-OVERD	RIVETM								
	🔲 Tx Burst									
		ne technolo	ogy must also be :	supported in clie	ents to boost V	/LAN				
	performance.									
	Rate Control									
	0010 1	Enable	Upload		Downl					
	SSID 1		30000	kbps	30000		ps			
	SSID 2		30000	kbps	30000		ps			
	SSID 3		30000	kbps	30000		ps			
	SSID 4 Note: range 10		30000	kbps	30000	kł	ps			
	Note. Tange 1	00-00,000	Корз							
			ОК	Cancel						
Enal	ole Wireless	LAN	Check the bo	ox to enable	wireless fu	inctio	on.			
Mod	е		Select an app	oropriate wi	reless mod	e.				
			Mixed (11b+				ates wit	th star	ndard 802.	11b
			and standard							
			11g only-Th					rd 802	2.11b STA	s.
			11b only-Th							
			Mode :				1b+11g)			
			mode .			•				
						Only	1b+11g)			
						Only	r i i i i i i i i i i i i i i i i i i i			
						Oni,	y			
Inde	ndex(1-15)		Set the wirel	ess LAN to	work at ce	rtain	time in	terval	only. You	ı may
			choose up to	4 schedules	s out of the	15 s	chedule	s pre-	defined in	
			Application	s >> Sched	ule setup. 7	The d	lefault s	etting	of this file	ed is
			blank and the					0		
Enal	ale		Charle tha he	ov to anobla	the cottine					
rial	ле		Check the bo		the setting	•				

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 doing site survey.
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.
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 device only support long preamble. Check it to use Long Preamble if needed to communicate with this kind of devices.
Packet- OVERDRIVE TM	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: Vigor610 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 Vigor610 wireless utility window, check **TxBURST** on the tab of **Advanced**).

Profile Link Status Site Survey Statistics	Advanced QoS About
Wireless mode 802.11 B/G mix	Select Your Country Region Code
Ad hoc wireless mode C Only B C B/G Mixed C Only G C	,
B/G Protection Auto	- C CX20
Tx Rate Auto 💌	LEAP turn on CCKM
I x BURST	Enable Radio Measurement Non-Serving Channel Measurements
Enable TCP Window Size	Limit 250 milliseconds (0-2000)
Fast Roaming at -70 dBm	
Turn off RF	Apply

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

It controls the data transmission rate through wireless connection. **Upload** – Check Enable and type the transmitting rate for data

Rate Control

upload. Default value is 30,000 kbps. **Download** – Type the transmitting rate for data download. Default value is 30,000 kbps.

3.11.3 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.

ID 1	SSID 2	SSID 3	SSID 4		
	Mode:		Disable	*	
WPA	:				
	Pre-Shared Key(PSK):	*****		
	Type 8~63 ASCI "cfgs01a2" or '			igits leading by "0x",	for example
WEP:					
	Key Length		64-Bit 💙		
	◉Key 1 :		*****		
	○Кеу 2 : ○Кеу 3 :		*****		

	⊖Key 4 :		*****		
Туре	4 bit WEP key 5 ASCII character 42333132".	r or 10 Hexade	ecimal digits leadir	g by "Ox", for exampl	e "AB312" or
Туре	28 bit WEP key 13 ASCII characti 456789abc" or "0>			ng by "Ox", for examp "	ole

ΟK

Mode

Disable-Turn off the encryption mechanism. For the security of your router, please select any one of the encryption mode here.

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

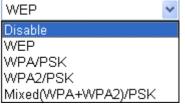
WPA/PSK-Accepts only WPA clients and the encryption key should be entered in PSK.

Cancel

WPA2/PSK-Accepts only WPA2 clients and the encryption key should be entered in PSK.

Mixed (WPA+ WPA2)/PSK - Accepts WPA and WPA2 clients simultaneously and the encryption key should be entered in PSK.

Mode:



The WPA encrypts each frame transmitted from the radio using the key, which either PSK (Pre-Shared Key) entered manually in this field below or automatically negotiated via 802.1x authentication. Either **8~63** ASCII characters, such as 012345678(or 64 Hexadecimal digits leading by 0x, such as "0x321253abcde...").

WPA

WEP
 For key length 64 bits - For 64 bits WEP key, either 5 ASCII characters, such as 12345 (or 10 hexadecimal digitals leading by 0x, such as 0x4142434445.)
 For key length 128 bits - For 128 bits WEP key, either 13 ASCII characters, such as ABCDEFGHIJKLM. (or 26 hexadecimal digits leading by 0x, such as 0x4142434445464748494A4B4C4D)
 All wireless devices must support the same WEP encryption bit size and have the same key. Four keys can be entered here, but only one key can be selected at a time. The keys can be entered in ASCII or Hexadecimal. Check the key you wish to use.

3.11.4 Access Control

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

cess Control	
E	nable Mac Address Filter
	SSID 1 SSID 2 SSID 3 SSID 4
	MAC Address Filter
	Index Attribute MAC Address
	Client's MAC Address : : : : : : : : : : :
	s: Isolate the station from LAN
	Add Remove Edit Cancel

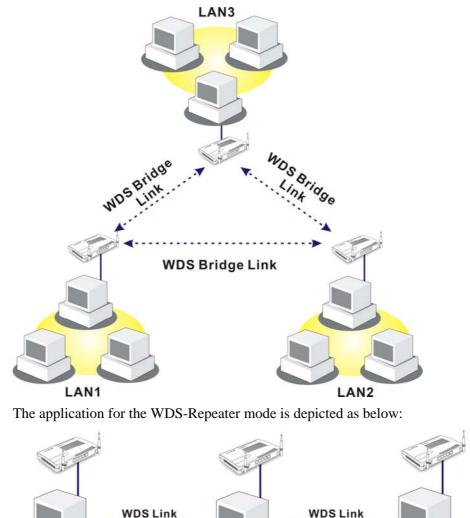
Enable Mac Access Filter	Select to enable the MAC Address filter for wireless LAN identified with SSID 1 to 4 respectively. All the clients (expressed by MAC addresses) listed in the box can be grouped under different wireless LAN. For example, they can be grouped under SSID 1 and SSID 2 at the same time if you check SSID 1 and SSID 2.
Client's MAC Address	Manually enter the MAC address of wireless client.
S	Check this box to isolate the stations from LAN.
Add	Add a new MAC address into the list.
Remove	Delete the selected MAC address in the list.
Edit	Edit the selected MAC address in the list.
Cancel	Give up the access control set up.
OK	Click it to save the access control list.
Clear All	Clean all entries in the MAC address list.

3.11.5 WDS

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

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

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



The 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.

Host with

repeater Interface

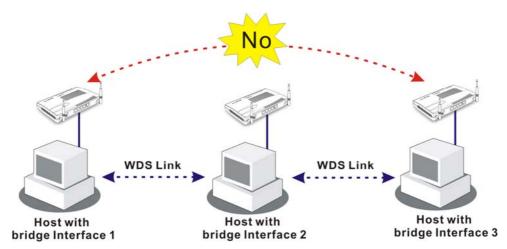
Host with

bridge Interface 2

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.

Host with

bridge Interface 1



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

Wireless LAN >> WDS Settings

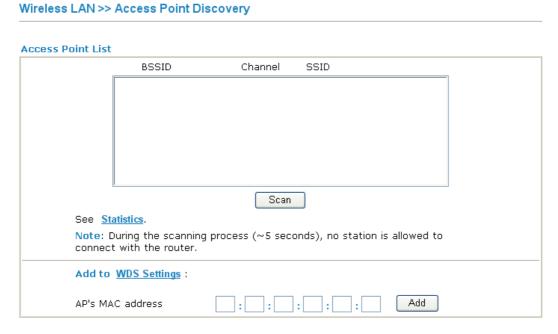
		Bridge		
Mode:	Disable 🔽	Enable Peer MAC Address		
Security:				
💿 Disable 🗌 W	'EP 🔵 Pre-shared Key			
	,			
WEP:				
Use the same WEP k	key set in <u>Security Settings</u> .	Note: Disable unused links to get better performance.		
Pre-shared Key:		 Repeater		
Туре	: TKIP	Enable Peer MAC Addess		
Кеу				
	haracters or 64 hexadecimal ", for example "cfgs01a2" or	r		
"0x655abcd".	, ioi onampio orgoorazini or	Access Point Function:		
		Enable Obisable		
Ande Choose the m invoke any W		Clear Cancel node for WDS setting. Disable mode will not WDS setting. Bridge mode is designed to fulfill to application. Repeater mode is for the second on		
	•• •			
	Mode:	Disable Disable Bridge Repeater		
Security There are thr		ee types for security, Disable , WEP and		
	Pre-shared k	key . The setting you choose here will make the EP or Pre-shared key field valid or not. Choose		
VEP Check this bo page. If you d		ox to use the same key set in Security Settings did not set any key in Security Settings page, th ill be dimmed.		

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

3.11.6 AP Discovery

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.

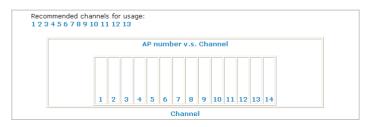




It is used to discover all the connected AP. The results will be shown on the box above this button.

Statistics

It displays the statistics for the channels used by APs. Wireless LAN>> Site Survey Statistics



Add

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

3.11.7 Station List

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

	Status MAC Address				
	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 successfuly, it may be				
	turnned off without notice. In that case, it will still be on the list until the				
	connection expires.				
	Add to Access Control :				
	Client's MAC address				
	Add				
efresh	Click this button to refresh the status of stat				
dd	Click this button to add aureant calcuted M				
u	Click this button to add current selected MA				

Wireless LAN >> Station List

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

3.12 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 and Date, Reboot System and Firmware Upgrade.

3.12.1 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

Firmware Version : 2. Build Date/Time : M		Vigor2700 series 2.7.2_RC4 Mar 2 2007 09:22:10 121201_A Annex B			
LAN MAC Address : 00-5 1st IP Address : 192. 1st Subnet Mask : 255. DHCP Server : Yes			WAN Link Status MAC Address Connection IP Address	: Disconnected : 00-50-7F-00-00-01 : :	
VoIP Port SIP registrar Account ID Register Codec In Calls	: 1 : : change_ : : : 0	2 me change_me O	Default Gateway DNS Wireless LAN MAC Address Frequency Domain Firmware Version	: : 194.109.6.66 : 00-50-7f-00-00-00 : Europe : 1.0.4.0	

Model Name	Displays the model name of the router.
Firmware Version	Displays the firmware version of the router.
Build Date/Time	Displays the date and time of the current firmware build.
MAC Address	Displays the MAC address of the LAN Interface.
1 st IP Address	Displays the IP address of the LAN interface.
1 st Subnet Mask	Displays the subnet mask address of the LAN interface.
DHCP Server	Displays the current status of DHCP server of the LAN interface.
MAC Address	Displays the MAC address of the WAN Interface.
IP Address	Displays the IP address of the WAN interface.
Default Gateway	Displays the assigned IP address of the default gateway.
DNS	Displays the assigned IP address of the primary DNS.
MAC Address	Displays the MAC address of the wireless Interface.
Frequency Domain	Displays the available channel supported by the wireless product. It varies in different country, Europe (13 usable channels), USA (11 usable channels).
Firmware Version	Displays information about equipped WLAN card driver.

3.12.2 Administrator Password

This page allows you to set new password.

Administrator Password		
Old Password		
New Password	••••	
Retype New Password	••••	
·		

ΟK

Old Password	Type in the old password.	The factory	default setting	for password is
	blank.			

New Password Type in new password in this filed.

Retype New Password Type in the new password again.

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

3.12.3 Configuration Backup

Backup the Configuration

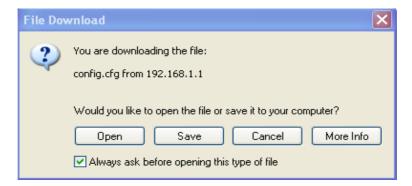
Follow the steps below to backup your configuration.

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.



3. In **Save As** dialog, the default filename is **config.cfg**. You could give it another name by yourself.

Save As						? 🗙
Save in:	🞯 Desktop		~	O Ø	• 🛄 🍤	
My Recent Documents Desktop My Documents	My Document My Computer My Network P My Network P My Network P My Network P MwSnap300 TeleDanmark Tools Config v2k2_232_coi v2k6_250_coi	laces nfia 1				
My Computer						
	File name:	config			~ (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.

Restore Configuration

System Maintenance >> Configuration Backup

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

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

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

3.12.4 Syslog/Mail Alert

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

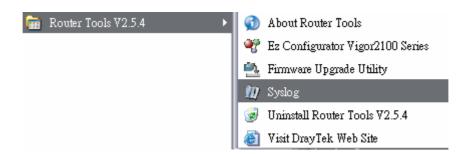
System Maintenance >> SysLog / Mail Alert Setup

	SysLog / Mail Alert Setup			
	SysLog Access Setup		Mail Alert Setup	
	🗹 Enable		🗹 Enable	
	Server IP Address		SMTP Server	
	Destination Port 514		Mail To	
	Enable syslog message:		Return-Path	
	🗹 Firewall Log		Authentication	
	VPN Log		User Name	
	✓ User Access Log ✓ Call Log		Password	
	WAN Log			
	Router/DSL information			
		ок С	Clear Cancel	
F	Enable	Check	« " Enable " to activat	te this function.
S	syslog Server IP	The I	P address of the Sysl	og server.
I	Destination Port	Assig	n a port for the Sysle	og protocol.
F	Enable syslog message	Check messa	•	or viewing its log on syslog
S	SMTP Server	The I	P address of the SMT	ΓP server.
N	Aail To	Assig	n a mail address for	sending mails out.
F	Return-Path	Assig	n a path for receiving	g the mail from outside.
A	Authentication	might	need user name and	this function. Some servers password for authentication. echanism is required.
ι	Jser Name	Туре	the user name for the	e authentication.
F	assword	Type	the password for the	authentication.

Click **OK** to save these settings.

For viewing the Syslog, please do the following:

- 1. Just set your monitor PC's IP address in the field of Server IP Address
- 2. Install the Router Tools in the **Utility** within provided CD. After installation, click on the **Router Tools>>Syslog** from program menu.



3. From the Syslog screen, select the router you want to monitor. Be reminded that in **Network Information**, select the network adapter used to connect to the router. Otherwise, you won't succeed in retrieving information from the router.

		192.168.1 Vigor serie		Gateway IP (Fixed	d) TX Packet	s RX Rate
AN Status		vigor serie	S DIIICIDIS		0	0
	ackets	RX Pack	iets	WAN IP (Fixed)	RX Packet	s TX Rate
9	61	759			0	0
ewall Log VP	N Log User Acces	ss Log Ca	ll Log WAN Lo	Network Infomation	n Net State	
On Line Router			Host Name:	niki-pc		
IP Address	Mask	MAC	NIC Descriptio	n: Realtek R TL813	9 Family PCI Fast E	themet NIC - : 🔽
192.168.1.1	255.255.255.0	00-50-`	-NIC Informati			
			MAC Address:	00-0E-A6-2A-D5-A1	Default Geteway:	192.168.1.1
			IP Address:	192.168.1.10	DHCP Server:	192.168.1.1
			Subnet Mask:	255.255.255.0	Lease Obtained:	Wed Apr 06 16:59:40 2005
<		>	DNS Servers:	168.95.1.1	Lease Expires:	Sat Apr 09
	R	efresh		192.168.1.1	воже вкриез.	16:59:40 2005

3.12.5 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	2000 Jan 2 Sun 18 : 0 : 59 Inquire Time
Time Setup	
💿 Use Browser Time	
🔘 Use Internet Time Client	
Time Protocol	NTP (RFC-1305)
Server IP Address	
Time Zone	(GMT) Greenwich Mean Time : Dublin 🛛 👻
Enable Daylight Saving	
Automatically Update Int	erval 30 sec 💌
	OK Cancel
Current System Time	OK Cancel Click Inquire Time to get the current time.
Use Browser Time	Click Inquire Time to get the current time. Select this option to use the browser time from the remot
Current System Time Use Browser Time Use Internet Time Client Time Protocol	Click Inquire Time to get the current time. Select this option to use the browser time from the remote administrator PC host as router's system time. Select to inquire time information from Time Server on
Use Browser Time Use Internet Time Client	Click Inquire Time to get the current time. Select this option to use the browser time from the remote administrator PC host as router's system time. Select to inquire time information from Time Server on the Internet using assigned protocol.
Use Browser Time Use Internet Time Client Time Protocol	Click Inquire Time to get the current time. Select this option to use the browser time from the remote administrator PC host as router's system time. Select to inquire time information from Time Server on the Internet using assigned protocol. Select a time protocol.

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

Click **OK** to save these settings.

3.12.6 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.

System Maintenance >> Management

Man	agement Setup					
Management Access Control			Management Port Setup			
 Enable remote firmware upgrade(FTP) Allow management from the Internet 			O Default Ports (Telnet: 23, HTTP: 80, HTTPS: 443, FTP: 21)			
Allow management non the Internet Disable PING from the Internet			⊙ User Define Ports			
<u> </u>			Telnet Port	23		
	ess List		HTTP Port	80		
List	IP 195.5.66.5	Subnet Mask 255.255.255.255 / 32 💙	HTTPS Port	443		
2	212.49.189.0	255.255.255.0 / 24	FTP Port	21		
3	80.25.157.230	255.255.255.255 / 32 💌	SNMP Setup			
			📃 Enable SNMP Agent			
			Get Community	public		
			Set Community	private		
			Manager Host IP			
			Trap Community	public		
			Notification Host IP			
			Trap Timeout	10 seconds		

OK

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

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

3.12.7 Reboot System

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

System Maintenance >> Reboot System

Do You want to reboot your router ?	
Do Tou Walk to report your router :	
Osing current configuration	
O Using factory default configuration	

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

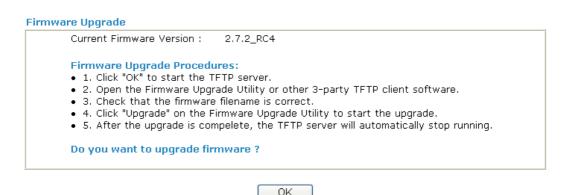
3.12.8 Firmware Upgrade

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



Click OK. The following screen will appear.

Firewall >> Firmware Upgrade



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

3.13 Diagnostics

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

3.13.1 WAN Connection

Click **Diagnostics** and click **WAN Connection** to open the web page. According to the model you have, the WAN connection page will differ slightly. For example, ISDN Link Status appears only for *i* model.

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

Diagnostics >> WAN Connection

Refresh	
Dial ISDN	

To obtain the latest information, click here to reload the page.

Click it to force the router to establish an ISDN connection. This function is available for i models only.

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

DropPPPoE or PPPoA Click it to force the router to cut off a PPPoE or PPPoA connection.

3.13.2 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 31 5D 39-00 0E A6 2A D5 A1-08 00
45 00 00 43 50 F6 00 00-7F 11 7F A1 CO A8 01 0A
A8 5F 01 01 05 5B 00 35-00 2F 14 C1 00 91 01 00
00 01 00 00 00 00 00 00-09 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 00 00 00 00 00-00 00 00 00 00 00 00 00
Decoded Format:
192.168.1.10,1371 -> 168.95.1.1,domain
Pr udp HLen 20 TLen 67

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.

3.13.3 Routing Table

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

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

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

Refresh

Click it to reload the page.

3.13.4 ARP Cache Table

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

```
      Diagnostics >> View ARP Cache Table

      Ethernet ARP Cache Table

      IP Address

      192.168.1.10

      OD-OE-A6-2A-D5-A1

      Refresh

      Click it to reload the page.
```

Click it to clear the whole table.

3.13.5 DHCP Table

Clear

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 se	erver: Running				^
Index	IP Address	MAC Address	Leased Time	HOST ID	
1 2	192.168.1.1 192.168.1.10	00-50-7F-31-5D-39 00-0E-A6-2A-D5-A1	ROUTER IP 0:00:06.760	ok-lccgjyiy075u	
					~
ndex		It displays the cor	nnection item nu	mber.	

IP Address	It displays the IP address assigned by this router for specified PC.
MAC Address	It displays the MAC address for the specified PC that DHCP assigned IP address for it.
Leased Time	It displays the leased time of the specified PC.
HOST ID	It displays the host ID name of the specified PC.

Refresh

Click it to reload the page.

3.13.6 NAT Sessions Table

Diagnostics >> NAT Sessions Table

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

NAT Active Sessions Table

Private IP:Port	It indicates the source IP address and port of local PC.	
#Pseudo Port	It indicates the temporary port of the router used for NAT.	
Peer IP:Port	It indicates the destination IP address and port of remote host.	
Ifno	It displays the representing number for different interface.0:LAN1~2:ISDN3:WAN4 or above:VPN	
Status	The status values are defined as follows:0:other TCP status1:TCP fin incoming2:TCP fin out3:TCP fin closing4:TCP syn5:TCP syn,ack6:TCP ack	
Refresh	Click it to reload the page.	

3.13.7 Ping Diagnosis

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

Diagnostics >>	Ping	Diagnos	is
Diagnostics	i ilig	Diagnos	10

Ping to: Host / IP V Host / IP GateWay	IP Address:
Result DNS	<u>Clear</u>
	<u>^</u>
	~

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

3.13.8 Data Flow Monitor

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

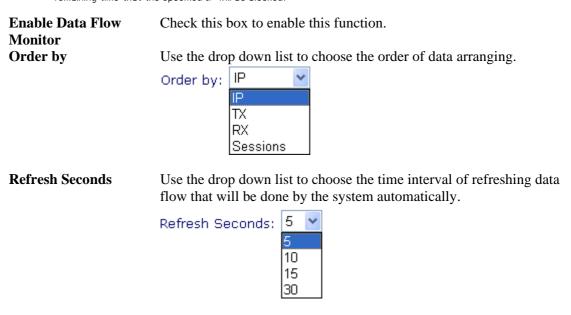
Limit Session	
💿 Enable 🛛 Disat	ole
Default Max Sessions:	100
Limitation List	

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

Diagnostics >> Data Flow Monitor

Image: Tenable Data Flow Monitor Order by: P Refresh Seconds: 5 Index IP Address TX rate(Kbps) RX rate(Kbps) Sessions Action Image: TX rate(Kbps) Image: TX rate(Kbps)</

Note: 1. Click "Block" to prevent specified PC from surfing Internet for 5 minutes.
 2. The IP blocked by the router will be shown in red, and the session column will display the remaining time that the specified IP will be blocked.



Refresh

Click this link to refresh this page manually.

Index	Display the number of the data flow.
IP Address	Display the IP address of the monitored device.
TX rate (kbps)	Display the transmission speed of the monitored device.
RX rate (kbps)	Display the receiving speed of the monitored device.
Sessions	Display the session number that you specified in Limit Session web page.
Action	Block - can prevent specified PC accessing into Internet within 5

Block - can prevent specified PC accessing into Internet within 5 minutes.



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



3.13.9 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	
Host / IP Address:	Run
Result	<u>Clear</u>
traceroute to 172.16.3.229, 30 hops ma 1 Request timed out. * 2 Request timed out. * Trace complete.	x

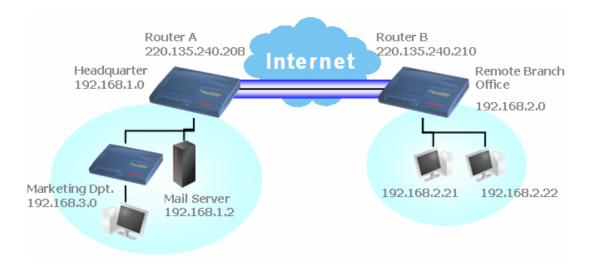
Host/IP Address	It indicates the IP address of the host.
Run	Click this button to start route tracing work.
Clear	Click this link to remove the result on the window.

This page is left blank.

4 Application and Examples

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

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



Settings in Router A in headquarter:

VPN and Remote Access >> PPP General Setup

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

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

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

ΟK

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

VPN and Remote Access >> IPSec General Setup		
VPN IKE/IPSec General Setup Dial-in Set up for Remote Dial-in	, users and Dynamic IP Client (LAN to LAN).	
IKE Authentication Met	· · · · ·	
Pre-Shared Key		
Re-type Pre-Shared Key		
IPSec Security Method		
Medium (AH)		
Data will be authenti	c, but will not be encrypted.	
High (ESP) 🗹 DES	SDES AES	
Data will be encrypte	ed and 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 draytek	Call Direction 🛛 💿 Both 🔿 Dial-Out 🔿 Dial-In
Enable this profile	🔲 Always on
	Idle Timeout 300 second(s)
	Enable PING to keep alive
	PING to the IP

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

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

2. Dial-Out Settings	
Type of Server I am calling	Link Type 64k bps 🛩
O ISDN	Username ???
○ РРТР	Password
IPSec Tunnel	PPP Authentication PAP/CHAP
O L2TP with IPSec Policy None	VJ Compression On O Off
Server IP/Host Name for VPN. (such as draytek.com or 123.45.67.89) 200.135.240.210	IKE Authentication Method Pre-Shared Key
	IKE Pre-Shared Key
	O Digital Signature(X.509)
	??? 🗸
	IPSec Security Method
	Medium(AH)
	O High(ESP) DES without Authentication
	Advanced
	Index(1-15) in <u>Schedule</u> Setup:
	,,,
	Callback Function (CBCP)
	Require Remote to Callback
	Provide ISDN Number to Remote

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

2. Dial-Out Settings		
Type of Server I am calling	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
Server IP/Host Name for VPN. (such as draytek.com or 123.45.67.89)	IKE Authentication M	ethod
(such as draytek.com or 123.45.67.89) 200.135.240.210	Pre-Shared Key	
200.133.240.210	IKE Pre-Shared Key	
	 Digital Signature(X.509) 	
	??? 🗸	
	IPSec Security Method	
	Medium(AH) High(ESP) DES without Authentication	
	Advanced	
	Index(1-15) in <u>Schedule</u> Setup:	
	,,, _	,
	Callback Function (C	BCD)
	Require Remote to	· · · · · · · · · · · · · · · · · · ·
	Provide ISDN Numb	

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

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

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

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

4. TCP/IP Network Sett	ings		
My WAN IP	0.0.0.0	RIP Direction	TX/RX Both 💌
Remote Gateway IP	0.0.0.0	RIP Version	Ver. 2 💌
Remote Network IP	192.168.2.0	For NAT operation, trea	
Remote Network Mask	255.255.255.0		Private IP 🚩
	More	🔲 Change default route	e to this VPN tunnel
OK Clear Cancel			

Settings in Router B in the remote office:

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

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

PPP General Setup		
PPP/MP Protocol	IP Address Assignment for D)ial-In Users
Dial-In PPP Authentication	Start IP Address	192.168.2.200
Dial-In PPP Encryption Optional MPPE		
Mutual Authentication (PAP) 🛛 🔘 Yes 💿 No		
Username		
Password		
	IK	

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

IKE Authentication Method		
Pre-Shared Key	••••	
Re-type 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.	

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

Profile Index : 1 1. Common Settings			
Profile Name	Branch 1	Call Direction	📀 Both 🔘 Dial-Out 🔘 Dial-In
🗹 Enable this profile		🔲 Always on	
		Idle Timeout	300 second(s)
		📃 Enable PING t	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	64k bps 🔒
O ISDN	Username	???
О РРТР	Password	
IPSec Tunnel	PPP Authentication	PAP/CHAP V
O L2TP with IPSec Policy None	VJ Compression	● On ○ Off
Server IP/Host Name for VPN.	IKE Authentication M	ethod
(such as draytek.com or 123.45.67.89) 220 135 240 208	Pre-Shared Key	
220.135.240.208	IKE Pre-Shared Key	•••••
	Digital Signature(X.5)	09)
	??? 🗸	,
	IPSec Security Method Medium(AH) High(ESP) DES without Authentication	
	Advanced	
	Index(1-15) in <u>Schedule</u> Setup:	
	Callback Function (C	BCP)
	Require Remote to	Callback
	Provide ISDN Numb	er te Remete

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

Type of Server I am calling	Link Type	64k bps 💉	
O ISDN	Username	draytek	
PPTP	Password	****	
🔘 IPSec Tunnel	PPP Authentication		
C L2TP with IPSec Policy None	VJ Compression	⊙ On ◯ Off	
Server IP/Host Name for VPN. (such as draytek.com or 123.45.67.89)	IKE Authentication M	lethod	
220.135.240.208	Pre-Shared Key	Pre-Shared Key	
220.133.240.200	IKE Pre-Shared Key		
	O Digital Signature(X.5	(09)	
	??? 🗸	,	
	IPSec Security Metho	od	
	Medium(AH)		
	O High(ESP) DES wi	thout Authentication 🛛 👻	
	Advanced		
	Index(1-15) in <u>Schedul</u>	e Setup:	
	Callback Function (C	BCP)	
	🗌 Require Remote to	Callback	
	Provide ISDN Numb	ier 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 ???
PPTP	Password
IPSec Tunnel	VJ Compression 💿 On 🔘 Off
L2TP with IPSec Policy None	IKE Authentication Method
Specify Remote VPN Gateway	🗹 Pre-Shared Key
Peer VPN Server IP	IKE Pre-Shared Key
220.135.240.208	Digital Signature(X.509)
or Peer ID	??? 👻
	IPSec Security Method
	Medium (AH)
	High (ESP)
	🗹 DES 🔽 3DES 🔽 AES
	Callback Function (CBCP)
	Enable Callback Function
	Use the Following Number to Callback
	Callback Number
	Callback Budget 0 minute(s)

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

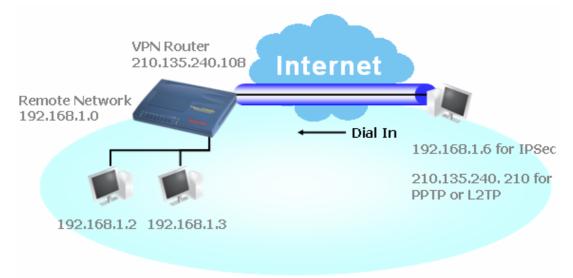
3. Dial-In Settings		
Allowed Dial-In Type		
ISDN	Username	draytek
PPTP	Password	
🔲 IPSec Tunnel	VJ Compression	💿 On 🔘 Off
L2TP with IPSec Policy None		
	IKE Authentication Method	
Specify Remote VPN Gateway	🗹 Pre-Shared Key	
Peer VPN Server IP	IKE Pre-Shared Key	
220.135.240.208	Digital Signature(X.509)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

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

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

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

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



Settings in VPN Router in the enterprise office:

VPN and Remote Access >> PPP General Setup

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

PPP/MP Protocol		IP Address Assignment for	Dial-In 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 **IKE/IPSec General Setup**, such as the pre-shared key that both parties have known.

IKE Authentication Method	
Pre-Shared Key	••••
Re-type Pre-Shared Key	•••••
IPSec Security Method	
🗹 Medium (AH)	
Data will be authentic, but v	will not be encrypted.
High (ESP) 🛛 🗹 DES 📝 3(DES 🗹 AES
Data will be encrypted and a	authentic.

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

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

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

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.

2. Dial-Out Settings		
Type of Server I am calling	Link Type	64k bps 🔒
O ISDN	Username	draytek
• РРТР	Password	
O IPSec Tunnel	PPP Authentication	
O L2TP with IPSec Policy None	VJ Compression	💿 On 🔘 Off
Server IP/Host Name for VPN. (such as draytek.com or 123.45.67.89) 200.135.240.210	IKE Authentication M • Pre-Shared Key	lethod
200.100.210.210	IKE Pre-Shared Key	•••••
	O Digital Signature(X.5	509)
	??? 🗸	
	IPSec Security Meth	
	 Medium(AH) 	ba
		thout Authentication 🔽
	Advanced	
	Index(1-15) in <u>Schedul</u>	e Setup:
	Callback Function (C	BCP)
	🗌 Require Remote to	Callback
	🗌 Provide ISDN Numb	er to Remote

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 <u>www.draytek.com</u> download center. Install as instructed.
- 2. After successful installation, for the first time user, you should click on the **Step 0. Configure** button. Reboot the host.

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

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

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

Dial To VPN					
Session Name:	Office				
VPN Server IP/HOST	Name(such as 123.45.67.89 or draytek.com)				
192,168,1,1					
192,100,1,1					
User Name :	draytek_user1				
Password :	*****				
Type of VPN					
○ РРТР	○L2TP				
IPSec Tunnel	OL2TP over IPSec				
PPTP Encryption -					
No encryption	n				
O Require encr					
Maximum strength encryption					
Use default gateway on remote network					
OK Cancel					

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

IPSec Policy Setti	ng	×
My IP :	172.16.3.100) 🗸
Type of IPSec		
Standard IPS	iec Tunnel	
Remote Su	bnet :	0.0.0.0
Remote Su	bnet Mask :	255 . 255 . 255 . 0
💽 Virture IP	DrayT	ek Virture Interface 🗸
💿 Obtain a	n IP address a	utomatically (DHCP over IPSec)
🔘 Specify a	an IP address	
IP Addr	ess:	192 . 168 . 1 . 201
Subnet	Mask:	255 . 255 . 255 . 0
Security Method -		
O Medium(AH)	0	High(ESP)
MD5	~	DES 💌
Authority Method		
• Pre-shared K	ey: *****	
 Certification 	Authority:	
		Browse
0	ĸ	Cancel

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

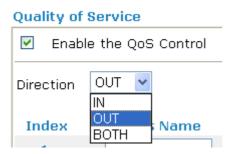
Dial To YPN	X			
Session Name:	office			
VPN Server IP/HOST	Name(such as 123.45.67.89 or draytek.com)			
192.168.1.1				
User Name :	draytek_user1			
Password :	****			
Type of VPN				
O IPSec Tunnel O L2TP over IPSec				
PPTP Encryption -				
🔘 No encryptio	n			
Require encr	yption			
O Maximum strength encryption				
Use default gateway on remote network				
OK Cancel				

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

4.3 QoS Setting Example

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

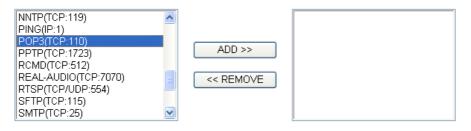
1. Click on Application >>QoS Control. Make sure you have checked the box of Enable the QoS Control. And select BOTH in Direction.



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

Index	Class Name	Reserved_bandwidtl	h Ratio	Setup
1.	E-mail	25	96	Basic Advanced
2.		25	%	Basic Advanced

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



4. Enter the Class Name of Index 2. In this index, she will set reserve bandwidth for HTTP. And click **Basic** on the right.

I	ndex	Class Name	Reserved_bar	ndwidth Ratio	Setup
	1.	E-mail	25	%	Basic Advanced
	2.	HTTP	25	%	Basic Advanced

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

~	HTTPS(TCP:443)
ADD >>	
<< REMOVE	
~	
	ADD >>

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

Quality of	Quality of Service Set to Factory Default						
🗹 Enab	Enable the QoS Control						
Direction	BOTH 💌						
Index	Class Name	Reserved_ba	ndwidth Ratio	Setup			
1.	E-mail	25	%	Basic Advanced]		
2.	HTTP	25	%	Basic Advanced]		
з.		25	96	Basic Advanced]		
4.	Others	25	%				
Enable UDP Bandwidth Control Limited_bandwidth Ratio 25 9 Outbound TCP ACK Prioritize Online Statistice					% atistics		
		ОК	Clear All				

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

And click Advanced button on the right.



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

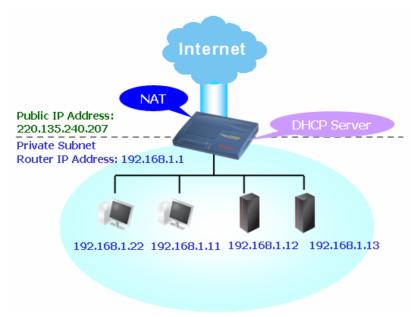
ACT	ity of Service Source Address	Destination Address	DiffServ CodePoint	Service Type
•	192.168.1.0 SrcEdit	192.168.2.0 DestEdit	ANY	ANY Add Edit Delete
Note	:: Please choose/se	tup the Service Typ	e first.	

Cancel

OK

4.4 LAN - Created by Using NAT

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

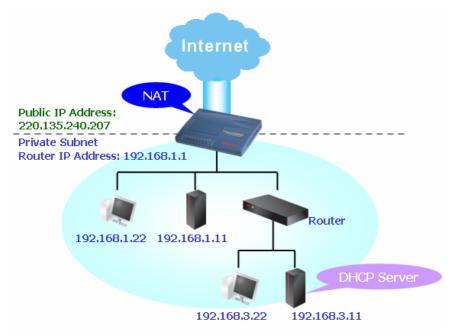


You can just set the settings wrapped inside the red rectangles to fit the request of NAT usage.

LAN >> General Setup

LAN IP Network Confi	guration	DHCP Server Configur	DHCP Server Configuration		
Eor NAT Usage		⊙Enable Server ○Disable Server			
1st IP Address	192.168.1.1	Relay Agent: 🔘 1st Sub	net O2nd Subnet		
1st Subnet Mask	255.255.255.0	Start IP Address	192.168.1.10		
For IP Routing Usage (🕽 Enable 💿 Disable	IP Pool Counts	50		
2nd IP Address	192.168.2.1	Gateway IP Address	192.168.1.1		
2nd Subnet Mask	255.255.255.0	DHCP Server IP Address			
	2nd Subnet DHCP Server	for Relay Agent			
		DNS Server IP Address	5		
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 shown below.



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

Ethernet TCP / IP and D	HCP Setup			
LAN IP Network Configu	ration	DHCP Server Configuration		
For NAT Usage		◯Enable Server ⊙Disa	ble Server	
1st IP Address 192.168.1.1		Relay Agent: 🔘 1st Su	bnet 🔾 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 for Relay Agent	192.168.3.11	
2nd Subnet DHCP Server		1 - 2		
		DNS Server IP Address	5	
RIP Protocol Control	Disable 🗸	Primary IP Address		
		Secondary IP Address		
		DK		

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

Phone Book	Index No. 1			
🗹 Enable				
	Phone Number	1111		
	Display Name	David		
	SIP URL	4321	@ iptel.org	

(11 char max.)

make call without register

(23 char max.)

sec

(63 char max.)

draytel 1

Auto

draytel.org

draytel.org

5060

Johr

1234

....

None

1 🕶

1 hour 🔽 3600

VoIP1 VoIP2

SIP Accounts Settings ----

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

CODEC/RTP/DTMF ---

(Use default value)

John calls David ---

Profile Name

Register via

Domain/Realm

Display Name

Password

Expiry Time

Ring Port

Ring Pattern

Account Number/Name

Authentication ID

NAT Traversal Support

Act as outbound proxy

SID Port

Proxy

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

OK Cancel

Settings for David	VoIP >> DialPlan Setup			
DialPlan index 1	Phone Book Index No. 1			
Phone Number:2222	V Enable			
Display Name: John SIP URL:1234@draytel.org	Phone Number 2222 Display Name John SIP URL 1234 @draytel.org			
	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)

VoIP >> SIP Accounts

Profile Name	iptel 1 (11 char ma	ах.)
Register via	Auto 🕑 🗌 make call witho	ut register
SIP Port	5060	
Domain/Realm	iptel.org	(63 char max.)
Proxy	iptel.org	(63 char max.)
🗌 Act as outbound p	roxy	
Display Name	David (23 char ma	ых.)
Account Number/Name	4321	(63 char max.)
🔲 Authentication ID		(63 char max.)
Password	••••	(63 char max.)
Expiry Time	1 hour 💌 3600 sec	
NAT Traversal Support	None 🖌	
Ring Port	VoIP1 VoIP2	
Ring Pattern	1 🛩	

OK Cancel

David calls John

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

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

VolP >> DialPlan Setup

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)

Enable		12		
Phone I	Number	1111		
Display	Name	David		
SIP URI		4321	@ drayte	Lorg
P Account Index No.				
P Account Index No. Profile Name	draytel 1		(11 char max.	
P Account Index No. Profile Name Register via	draytel 1 Auto		(11 char max. e call without	
P Account Index No. Profile Name Register via SIP Port	draytel 1 Auto 5060	Mak	e call without	register
P Account Index No. Profile Name Register via	draytel 1 Auto	Mak	e call without	
P Account Index No. Profile Name Register via SIP Port	draytel 1 Auto 5060	Mak Data	e call without	register
P Account Index No. Profile Name Register via SIP Port Domain/Realm Proxy	draytel 1 Auto 5060 draytel.org	Mak Data	e call without	(63 char max.)



John calls David

VoIP >> DialPlan Setup

hone Book Index No. 1

VoIP >> SIP Accounts

SIP Account Index No. 1

Profile Name

Register via

Domain/Realm

Display Name

Password

Expiry Time

Ring Port

Ring Pattern

Act as out

Account Number/Name

Authentication ID

NAT Traversal Support

SIP Port

Proxv

Phone Number

Display Name

SIP URL

🗹 Enable

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)

2222

John

1234

draytel 1

Auto

draytel.org

draytel.org

1 hour 💌 [3600

VoIP1 VoIP2

5060

N X COL

4321

None

1 *

OK Clear Cancel

@ draytel.org

(63 char max.)

(11 char max.)

(23 char max.)

make call without register

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)

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)

OK Cancel

4.5.2 Peer-to-Peer Calling

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

Arnor's SIP URL: 1234@214.61.172.53

Settings for Arnor

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

SIP Accounts Settings ----

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

CODEC/RTP/DTMF---

(Use default value)

Paulin's SIP URL: 4321@ 203.69.175.24

ne Book Index No. 1	
Enable	
Phone Number	1111
Display Name	paulin
SIP URL	4321 @ 203.69.175.24
[OK Clear Cancel
IP Account Index No. 1	
Profile Name	Paulin (11 char max.)
Register via	Auto 💌 🗌 make call without register
Register via SIP Port	Auto Auto
-	
SIP Port	5060
SIP Port Domain/Realm	5050 (63 char max.) (63 char max.) (63 char max.)
SIP Port Domain/Realm Proxy	5050 (63 char max.) (63 char max.) (63 char max.)
SIP Port Domain/Realm Proxy Act as outbound ;	5050
SIP Port Domain/Realm Proxy Act as outbound p Display Name	5050 (63 char max.) proxy (63 char max.)
SIP Port Domain/Realm Proxy □ Act as outbound µ Display Name Account Number/Name	6050 (63 char max.) proxy (63 char max.) [1234 (63 char max.)
SIP Port Domain/Realm Proxy Display Name Account Number/Name Account Number/Name	6050 (63 char max.) proxy (63 char max.) 1234 (63 char max.) (63 char max.) (63 char max.)
SIP Port Domain/Realm Proxy Act as outbound y Display Name Account Number/Name Atthentication ID Password	0060 (63 char max.) proxy (63 char max.) 1234 (63 char max.) (63 char max.) (63 char max.)
SIP Port Domain/Realm Proxy Act as outbound p Display Name Account Number/Name Account Number/Name Authentication ID Password Expiry Time	Sobo (63 char max.) proxy (63 char max.) 1234 (63 char max.) (63 char max.) (63 char max.) 1 hour (63 char max.)

OK Cancel

Arnor calls Paulin

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

Settings for Paulin

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

SIP Accounts Settings ----

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

CODEC/RTP/DTMF---

(Use default value)

VoIP >> DialPlan Setup Phone Book Index No. 1 ✓ Enable Phone Number 2222 Display Name Anor SIP URL 1234 @214.61 172.53 OK Clear Cancel

VoIP >> SIP Accounts

Profile Name	Amor (11 char max.)
Register via	Auto 💌 🗌 make call without register
SIP Port	5060
Domain/Realm	(63 char max.)
Proxy	(63 char max.)
🗌 Act as outbound p	roxy
Display Name	Paulin (23 char max.)
Account Number/Name	4321 (63 char max.)
🔲 Authentication ID	(63 char max.)
Password	(63 char max.)
Expiry Time	1 hour 🖌 3600 sec
NAT Traversal Support	None 🖌
Ring Port	VoIP1 VoIP2
Ring Pattern	1 💌

Paulin calls Arnor

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

4.6 Upgrade Firmware for Your Router

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

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

Please remember to set as follows in your DrayTek Router :

- Server IP Address : IP address of the PC that runs the Syslog
- Port Number : Default value 514

Install Now!

- 4. The file **RTSxxx.exe** will be asked to copy onto your computer. Remember the place of storing the execution file.
- 5. Go to **www.draytek.com** to find out the newly update firmware for your router.
- 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.

 Note : Brief introduction for Tools

Tools of Vigor						
Name	Version	Language	Release Date	OS	File	Size
Router Tools	4.0	English	04/12/2003	MacOS9	<u>hqx</u>	6.13 MB
Router Tools	2.4.5	English	04/12/2003	MacOSX	<u>hqx</u>	4.48 MB
Router Tools	2.5.3	English	04/12/2003	Windows	zip	0.93 MB
Smart VPN Client	3.2.2	English	21/03/2005	Windows	zip	0.54 MB
VTA	2.8	English	20/06/2005	Windows2000/XP	<u>zip</u>	0.65 MB
LPR	1.0	English	20/06/2005	Windows	<u>zip</u>	0.54 MB
TOP						

- 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**.

🛳 DrayTek Firmware Upgrade Utility 📃 🗖 🔁				
Operation Mode Opgrade Backup Setting Time Out(Sec.) 5	Router IP: Firmware file: Password:			
Port 69	Abort Send			

12. Type in your router IP, usually **192.168.1.1**.

R TS2

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.

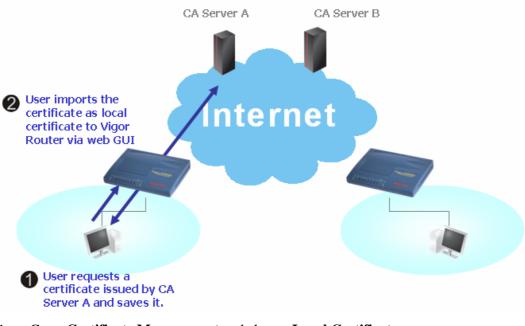
🖄 DrayTek Firmware I	Ipgrade Utility 📃 🗖 🔀
Operation Mode Oupgrade Backup Setting Time Out(Sec.) S Port	Router IP: 192.168.1.1 Firmware file: C:\Documents and Settings\Carrie Password:
69	Abort Send

14. Click Send.

៉ DrayTek Firmware	Opgrade Utility 📃 🗖 🔀
Operation Mode Upgrade Backup Setting	Router IP: 192.168.1.1
Time Out(Sec.)	C:\Documents and Settings\Carrie
Port	
69 Sending	Abort Send

15. Now the firmware update is finished.

4.7 Request a Certificate from a CA Server on Windows CA Server



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

Certificate Management >> Local Certificate

X509 Local Certifi	cate Configuration		
Name	Subject	Status	Modify
Local			View Delete
GENERATE	IMPORT REFRESH		
X509 Loca	al Certificate		
			~
			~
-			

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

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

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

Generate

	2		
Name	Subject	Status	Modify
Local	/C=TW/O=Draytek/emailAddress	Requesting	View Delete
GENERATE	IMPORT REFRESH		
X509	Local Certificate Request		
MIIBe Bgkqh A4GNA oyzoZ 2bNXE oCkwJ hkiGG OE1LV g54BY	BEGIN CERTIFICATE REQUEST jCCARMCAQAwQTELMAkGA1UEBhMCVFcxEDAO kiG9w0BCQEWEXByZXNzQGRyYX10ZWsuY29t DCBiQKBgQDsgmtStr3AXnjvjD9TtTPM021C 2ZM486s1rF3EJAueMw4SVL+qwdbuNxhGOTu fgzBn3Ndn+1nU1FKU58JW16rt2b9/qUkt1P wYJKoZIhvcNAQkOMRowGDAWBgNVHREEDzAN w0BAQUFAA0BgQA6vTERvfyqvAyCyLZCrKru 1R+huvCdf/qK71/3SkQqwvyckIzAt2IM+bX RQxi0SthkX4gcryq1FEVvC44zjtsU9UqyYV END CERTIFICATE REOUEST	MIGfMAOGCSqGS jOKZfTj3nxL6B zXWOmK7BBYEVm un9VrRaS57JEP ggtkcmF5dGVrL dH1mx7w97C3kG vfy2b/NpFr/1P	Ib3DQEBAQUA NVgjelb9TGX 4401SXmDTHhX Lc9wQIDAQAB mNvbTANBgkq +N77X4NFV42 SruiobBgIdJ
	EMD CERTIFICATE REQUEST		~

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

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

Select Advanced request.

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

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

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

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

Microsoft Certifica	te Services vigor		<u>Home</u>
Submit A Save	d Request		
		request or PKCS #7 renewal request generated by an external a t to the certification authority (CA).	pplication (such as a web
Saved Request:			
Certificate Request	BEGIN CERTIFICATE REQUI HIBGJCCARMCAQAwGTELMAKGAlU BgkghkiG90BCC9EEXByZXN2QCR, A4GNADCB1QKBgQDQYB7wm2FfFhNS hX4bp99cUF9dloACGG1M/cBOCk X/G0A7CTv0/fQ2pxroCw1JTJLSJS	EBhRCVFcxEDAO YYX102WsuY29t J/IeQnG03Xk++ dc2dFFv1XcP3	
	<u>Browse</u> for a file to insert.		
Certificate Templa	ate:		
	Administrator 🗸		
Additional Attribut	Administrator Authenticated Session Basic EFS EFS Recovery Agent User		
	IPSEC (Offline request) Router (Offline request)		
	Subordinate Certification Authority Web Server		Submit >

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

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

you will find the below window showing "-----BEGIN CERTIFICATE-----"

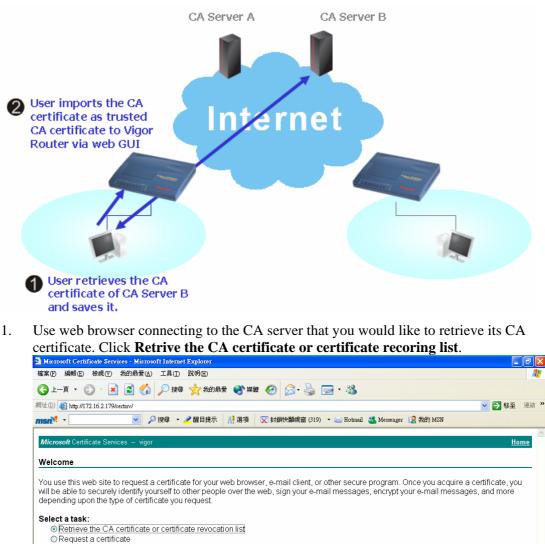
X509 Local Certificate Configuration

Name	Subject	Status	Modify
Local	/C=TW/O=Draytek/emailAddress	Requesting	View Delete
GENERATE	IMPORT REFRESH		
X509 Loc	cal Certificate Request		
BE(GIN CERTIFICATE REQUEST		^
MIIBqjC	CARMCAQAwQTELMAkGA1UEBhMCVFcxEDAO	BgNVBAoTBORyY	X10ZWsxIDAe
	G9w0BCQEWEXByZXNzQGRyYX10ZWsuY29t1	-	
	BiQKBgQDsgmtStr3AXnjvjD9TtTPMO21C		
	M486s1rF3EJAueMw4SVL+qwdbuNxhGOTu:		
	zBn3Ndn+1nU1FKU58JW16rtZb9/qUkt1P		
	JKoZIhvcNAQkOMRowGDAWBgNVHREEDzAN(
	BAQUFAAOBgQA6vTERvfyqvAyCyLZCrKruo		
	+huvCdf/qK71/3SkQqwvyckIzAt2IM+bXv		-
g54BYRQ	xiOSthkX4gcryq1FEVvC44zjtsU9UqyYV	E8NF8b/Tf1ar	Xm2GSMiJA==
EN	D CERTIFICATE REQUEST		
			*

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

🕘 Cer	tificate Request Information -	Microsoft Internet Explorer	
	C	ertificate Request Information	
	Name :	Local	
	Issuer :		
	Subject :	/C=TW/O=Draytek/emailAddress=press@draytek.com	
	Subject Alternative Name :	DNS:draytek.com	
	Valid From :		
	Valid To :		
	<u>-</u>	Close	

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



O Check on a pending certificate

Next >

- 2. In Choose file to download, click CA Certificate Current and Base 64 encoded, and Download CA certificate to save the .cer. file.
 - Microsoft Certificate Services Microsoft Internet Explorer ③ 上-頁 * ◎ · 図 ② ☆ / 2 搜尋 ☆ 我的最爱 ④ 媒體 Ø ◎ - ◎ 三 · ◎ 網址 (D) 🕘 http://172.16.2.179/certsrv/certcarc.asp ✓ → 移至 連結 msn 🔨 -🗸 🔎 搜尋 🝷 🛹 醒目提示 🛛 👖 選項 🛛 🔀 封鎖快顯視窗 (319) 🔹 🔤 Hotmail 🔉 Messenger [2 我的 MSN Mic Retrieve The CA Certificate Or Certificate Revocation List Install this CA certification path to allow your computer to trust certificates issued from this certification authority. It is not necessary to manually install the CA certification path if you request and install a certificate from this certification authority, because the CA certification path will be installed for you automatically. Choose file to download: CA Certificate: Current [vigor(1)] Previous [vigor] ○DER encoded or ●Base 64 encoded Download CA certificate Download CA certification path Download latest certificate revocation list
- 3. Back to Vigor router, go to **Trusted CA Certificate**. Click **IMPORT** button and browse the file to import the certificate (.cer file) into Vigor router. When finished, click **REFRESH** and you will find the below illustration.

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

IMPORT REFRESH

>> Time and Date to reset current time of the router first.

Certificate Management >> Trusted CA Certificate

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

Ce	rtificate Detail Information
Certificate Name:	Trusted CA-1
Issuer:	/C=US/CN=vigor
Subject:	/C=US/CN=vigor
Subject Alternative Name	e:
Valid From:	Aug 30 23:16:53 2005 GMT
Valid To:	Aug 30 23:16:53 2007 GMT
	Close

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.

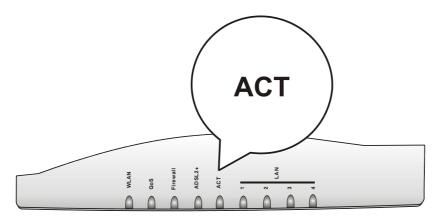
- Checking if the hardware status is OK or not.
- Checking if the network connection settings on your computer are OK or not.
- Pinging the router from your computer.
- Checking if the ISP settings are OK or not.
- Backing to factory default setting if necessary.

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**.

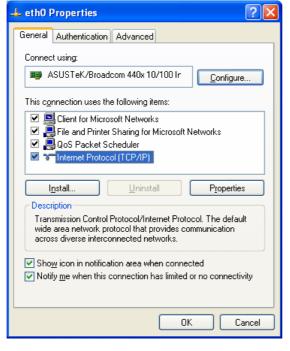
1. Go to Control Panel and then double-click on Network Connections.



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



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



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

Internet Protocol (TCP/IP)Properties 🛛 🛛 🔀	
General Alternate Configuration	
You can get IP settings assigned auto this capability. Otherwise, you need to the appropriate IP settings.	
⊙ <u>O</u> btain an IP address automatica	lly
Use the following IP address: —	
IP address:	
S <u>u</u> bnet mask:	
Default gateway:	
⊙ D <u>b</u> tain DNS server address auto	matically
OUse the following DNS server ad	dresses:
Preferred DNS server:	and the second sec
Alternate DNS server:	· · ·
	Ad <u>v</u> anced
	OK Cancel

For MacOs

- 1. Double click on the current used MacOs on the desktop.
- 2. Open the **Application** folder and get into **Network**.
- 3. On the **Network** screen, select **Using DHCP** from the drop down list of Configure IPv4.

) 🖯 🔿	Network	C
how All Displays Sou	A Network Startup Disk	
L	ocation: Automatic	
	Show: Built-in Ethernet	
ТСР	/IP PPPoE AppleTalk Proxies Ethernet	
Configure IPv4:	Using DHCP	
IP Address:	192.168.1.10 Renew DHC	P Lease
Subnet Mask:	255.255.255.0 DHCP Client ID: (If required)	
Router:		
DNS Servers:		(Optional)
Search Domains:		(Optional)
IPv6 Address:	fe80:0000:0000:0000:020a:95ff:fe8d:72e4	
	Configure IPv6	(?)

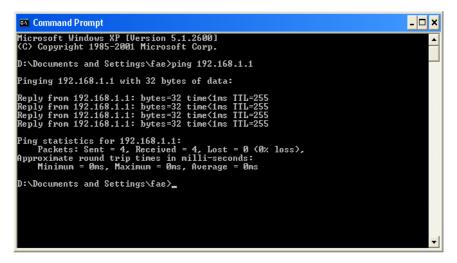
5.3 Pinging the Router from Your Computer

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.

😑 😑 💮 Terminal — bash — 80x24	
Last login: Sat Jan 3 02:24:18 on ttyp1 Welcome to Darwin! Vigor10:~ draytek\$ ping 192.168.1.1 PING 192.168.1.1 (192.168.1.1): 56 data bytes 64 bytes from 192.168.1.1: icmp_seq=0 ttl=255 time=0.755 ms 64 bytes from 192.168.1.1: icmp_seq=1 ttl=255 time=0.697 ms 64 bytes from 192.168.1.1: icmp_seq=2 ttl=255 time=0.716 ms	8
64 bytes from 192.168.1.1: icmp_seq=3 ttl=255 time=0.731 ms 64 bytes from 192.168.1.1: icmp_seq=4 ttl=255 time=0.72 ms ^C 192.168.1.1 ping statistics 5 packets transmitted, 5 packets received, 0% packet loss round-trip min/avg/max = 0.697/0.723/0.755 ms Vigor10:~ draytek\$	

5.4 Checking If the ISP Settings are OK or Not

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



For PPPoE/PPPoA Users

- 1. Check if the **Enable** option is selected.
- 2. Check if **Username** and **Password** are entered with correct values that you **got from** your **ISP**.

PPPoE / PPPoA Client Mode	
PPPoE/PPPoA Client Image: Client Image:	ISP Access Setup
DSL Modem Settings Multi-PVC channel Channel 1	Username
VPI 0 VCI 33 Encapsulating Type LLC/SNAP Protocol PPPoE Modulation Multimode	PPP Authentication PAP or CHAP Always On Idle Timeout IB0 second(s) IP Address From ISP WAN IP Alias Fixed IP Yes No (Dynamic IP)
PPPoE Pass-through For Wired LAN For Wireless LAN Note: If this box is checked while using the PPPoA protocol, the router will behave like a modem which only serves the PPPoE client on the LAN. ISDN Dial Backup Setup Dial Backup Mode None	Fixed IP Address • Default MAC Address • Specify a MAC Address MAC Address MAC Address MAC Address MAC Address MAC Address MAC Address MAC Address MAC Address MAC Address MAC Address MAC Address MAC Address MAC Address MAC Address MAC Address MAC Address
C	K

Internet Access >> PPPoE / PPPoA

For MPoA Users

1. Check if the **Enable** option for Broadband Access is selected.

Internet Access >> MPoA (RFC1483/2684)

MPoA (REC1493/2694) Mode	
MPoA (RFC1483/2684	🕨 🔿 Enable 💿 Disable	WAN IP Network Settings
DSL Modem Settings		Obtain an IP address automatically Router Name *
Multi-PVC channel	Channel 2 🔷	Domain Name *
Encapsulation 1483 E	Bridged IP LLC	Specify an IP address WAN IP Alias
VPI		IP Address 192.168.1.100
VCI	1	Subnet Mask 255.255.2
Modulation	Multimode 🗸	Gateway IP Address 192.168.1.1
RIP Protocol Enable RIP Bridge Mode Enable Bridge Mode		 * : Required for some ISPs Default MAC Address Specify a MAC Address MAC Address : 00 . 50 . 7F :31 . 5D . 3A DNS Server IP Address Primary IP Address Secondary IP Address
		ок

- 2. Check if all parameters of **DSL Modem Settings** are entered with correct value that provided by your ISP. Especially, check if the encapsulation is selected properly or not (it should be the same with the setting on **Quick Start Wizard**).
- 3. Check if **IP Address, Subnet Mask** and **Gateway** are set correctly (must identify with the values from your ISP) if you choose **Specify an IP address**.

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

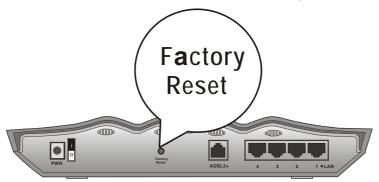
You can reset the router to factory default via Web page.

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.

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

Hardware Reset

While the router is running (ACT LED blinking), press the **Factory Reset** button and hold for more than 5 seconds. When you see the **ACT** LED blinks rapidly, please release the button. Then, the router will restart with the default configuration.



After restore the factory default setting, you can configure the settings for the router again to fit your personal request.

5.6 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.