

DrayTek

Vigor3300V+

Multi WAN Security Router



Your reliable networking solutions partner

User's Guide

V1.1

Vigor3300 V+ Multi-WAN Security Router User's Guide

Version: 1.1

Firmware Version: V2.6.3

Date: 23/08/2010

Copyright Information

Copyright Declarations

Copyright 2010 All rights reserved. This publication contains information that is protected by copyright. No part may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language without written permission from the copyright holders.

Trademarks

The following trademarks are used in this document:

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

Safety Instructions and Approval

Safety Instructions

- Read the installation guide thoroughly before you set up the router.
- The router is a complicated electronic unit that may be repaired only by authorized and qualified personnel. Do not try to open or repair the router yourself.
- Do not place the router in a damp or humid place, e.g. a bathroom.
- The router should be used in a sheltered area, within a temperature range of +5 to +40 Celsius.
- Do not expose the router to direct sunlight or other heat sources. The housing and electronic components may be damaged by direct sunlight or heat sources.
- Do not deploy the cable for LAN connection outdoor to prevent electronic shock hazards.
- Keep the package out of reach of children.
- When you want to dispose of the router, please follow local regulations on conservation of the environment.

Warranty

We warrant to the original end user (purchaser) that the router will be free from any defects in workmanship or materials for a period of two (2) years from the date of purchase from the dealer. Please keep your purchase receipt in a safe place as it serves as proof of date of purchase. During the warranty period, and upon proof of purchase, should the product have indications of failure due to faulty workmanship and/or materials, we will, at our discretion, repair or replace the defective products or components, without charge for either parts or labor, to whatever extent we deem necessary to restore the product to proper operating condition. Any replacement will consist of a new or re-manufactured functionally equivalent product of equal value, and will be offered solely at our discretion. This warranty will not apply if the product is modified, misused, tampered with, damaged by an act of God, or subjected to abnormal working conditions. The warranty does not cover the bundled or licensed software of other vendors. Defects which do not significantly affect the usability of the product will not be covered by the warranty. We reserve the right to revise the manual and online documentation and to make changes from time to time in the contents hereof without obligation to notify any person of such revision or changes.

Be a Registered Owner

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

Firmware & Tools Updates

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

<http://www.draytek.com>

European Community Declarations

Manufacturer: DrayTek Corp.

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

Product: Vigor3300V+

DrayTek Corp. declares that Vigor3300V+ of routers are in compliance with the following essential requirements and other relevant provisions of R&TTE Directive 1999/5/EEC.

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

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

Regulatory Information

Federal Communication Commission Interference Statement

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

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

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

- (1) This device may not cause harmful interference, and
- (2) This device may accept any interference received, including interference that may cause undesired operation.

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



This product is designed for the ISDN and POTS network throughout the EC region and Switzerland. Please see the user manual for the applicable networks on your product.

Table of Contents

Chapter 1: Preface	1
1.1 Web Configuration Buttons Explanation	1
1.2 LED Indicators and Connectors	2
1.2.1 For Vigor3300V+	3
1.3 Hardware Installation.....	6
1.3.1 Network Connection	6
1.3.2 ISDN Phone Adapter Installation.....	7
1.3.3 Rack-Mounted Installation	9
<hr/>	
Chapter 2: Configuring Basic Settings	11
2.1 Changing Password	11
2.2 Quick Setup.....	13
2.2.1 Static Mode.....	14
2.2.2 DHCP Mode.....	17
2.2.3 PPPoE	18
2.2.4 PPTP	21
<hr/>	
Chapter 3: Applications.....	23
3.1 Application for 802.1 VLAN	23
3.1.1 Block LAN-to-LAN Communication	23
3.1.2 How to Check/Edit VLAN ID on Your PC?	24
3.1.3 Four VLANs for Different Departments in A Company.....	30
3.1.4 Two VLANs for Different Departments in A Company	32
3.1.5 Example for the Companies in the Same Building	34
3.1.6 Example for A Company and Guest.....	36
3.1.7 Example for Trunk Usage	38
3.2 Application for VoIP	40
3.2.1 FXS and FXO	40
3.2.2 Practical Application of FXS card with PBX.....	42
3.2.3 Practical Application of FXO card with PBX	42
3.2.4 ISDN NT and TE.....	43
3.2.5 Practical Application of ISDN-NT with PBX	44
3.2.6 Practical Application of ISDN-TE with PBX	44
3.2.7 VoIP Basic	45
3.3 VoIP and ISDN Examples	51
3.3.1 Example 1 - Basic Configuration and Registration.....	51
3.3.2 Example 2 - Basic Configuration and Registration for ISDN	56
3.3.3 Example 3 - Basic Calling Method.....	61
3.3.4 Example 4 - VoIP over VPN	68
3.3.5 Example 5 - Practical Application of FXS.....	75
3.3.6 Example 6 - Practical Application of FXO.....	77
3.3.7 Example 7: Practical Application of ISDN-NT	80
3.3.8 Example 8: Practical Application of ISDN-TE.....	82
3.4 Application for mOTP	85
<hr/>	
Chapter 4: Reference - Advanced Web Configuration.....	91

4.1 System Setup	91
4.1.1 Status	91
4.1.2 Time	95
4.1.3 Syslog	96
4.1.4 Access Control.....	98
4.1.5 Configuration Setup.....	99
4.1.6 Firmware Upgrade Setup	100
4.1.7 Reboot	103
4.1.8 Diagnostic Tools	104
4.2 Network Setup.....	107
4.2.1 WAN	108
4.2.2 Load Balance Policy	115
4.2.3 Auto Load Balance	118
4.2.4 LAN	118
4.2.5 High Availability	121
4.2.6 RIP Configuration	123
4.2.6 Bandwidth Management.....	124
4.2.7 Limit Session	126
4.3 Advanced Setup	128
4.3.1 Static Route Setup.....	128
4.3.2 NAT Setup	130
4.3.3 RADIUS Setup.....	135
4.3.4 Port Block	136
4.3.5 DDNS Setup	136
4.3.6 Call Schedule Setup	139
4.3.7 WAN Port Mirroring Setup.....	140
4.3.8 LAN Port Mirroring Setup.....	142
4.3.9 LAN VLAN Setup	142
4.3.10 SNMP	145
4.3.11 SIP ALG.....	148
4.4 Firewall Setup.....	149
4.4.1 IP Filter	149
4.4.2 DoS	153
4.4.3 URL Filter.....	155
4.4.4 Bind IP to MAC	160
4.4.5 IM/P2P Blocking	161
4.5 Quality of Service Setup.....	162
4.5.1 Incoming/Outgoing Class Setup.....	163
4.5.2 Incoming/Outgoing Class Filter	164
4.6 VPN and Remote Access Setup	166
4.6.1 IPSec	167
4.6.2 PPTP & L2TP	185
4.7 VoIP Setup	190
4.7.1 Protocol	190
4.7.2 Port Settings	197
4.7.3 Speed Dial	205
4.7.4 Dial Plan	205
4.7.5 Miscellaneous.....	208
4.7.6 Tone Settings.....	209
4.7.7 QoS	211
4.7.8 NAT Traversal.....	212
4.7.9 Incoming Call Barring	213
4.7.10 Call History	215

4.7.11 Tone Upload	216
4.7.12 Status	217
4.7.13 Config Activate.....	218

Chapter 5: Trouble Shooting.....219

5.1 Checking If the Hardware Status Is OK or Not.....	219
5.2 Checking If the Network Connection Settings on Your Computer Is OK or Not	220
5.3 Pinging the Router from Your Computer	222
5.4 Checking If the ISP Settings are OK or Not	223
5.5 Backing to Factory Default Setting If Necessary.....	227
5.6 Contacting Your Dealer	227

Appendix: Hardware Specifications.....229

Chapter 1: Preface


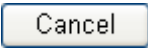
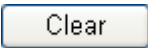
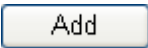

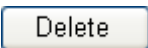
The Vigor3300V+ Series integrates a rich suite of functions, including NAT, firewall, VPN, load balance, bandwidth management, and VoIP capability. These products are very suitable for providing multi-integrated solutions to SME markets. An application scenario for the Vigor3300 Series is depicted in the following figure, which illustrates interconnections among branch offices through the Internet via the Vigor3300 Series routers. By combining with an existing PABX, an Internet phone from a remote branch can also access any extension number on a local PABX or a traditional phone via PSTN. In addition, by combining load balancing, data security, and Internet phone features, the company can benefit from reducing operation fees.

A Virtual Private Network (VPN) is an extension of a private network that encompasses links across shared or public networks like an Intranet. A VPN enables you to send data between two computers across a shared public Internet network in a manner that emulates the properties of a point-to-point private link. The DrayTek Vigor3300 Series VPN router supports Internet-industry standards technology to provide customers with open, interoperable VPN solutions such as X.509, DHCP over Internet Protocol Security (IPSec) up to 200 tunnels, and Point-to-Point Tunneling Protocol (PPTP).

Internet Telephony, also known as Voice over Internet Protocol (VoIP), is a technology that allows you to make telephone calls using a broadband Internet connection instead of a regular (analog) phone line. Combining a PABX with a V3300V allows you to call anyone who has an Internet phone or a traditional telephone number – including local, long distance, mobile, and international numbers. Internet Telephony offers features and services that are unavailable with a traditional phone at no additional cost. Because Internet Telephony requires strictly minimal packet delay and jitter (since voice quality is intolerant of packet loss), the Vigor3300V integrates VoIP feature with QoS and packet loss concealment mechanisms to effectively transport high priority voice traffic over IP with low latency. Another feature is T.38 fax relay. By enabling and configuring fax rate on a dial peer, the originating and the terminating V3300V can enter fax relay transfer mode. By using the T.38 function, customers can also save on fax expenses. Lastly, by enabling the load balance feature on multiple WAN ports, lease lines can be replaced to provide a cost-effective method for network infrastructure.

1.1 Web Configuration Buttons Explanation

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

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

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

1.2 LED Indicators and Connectors

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

Definitions for ISDN Ports

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

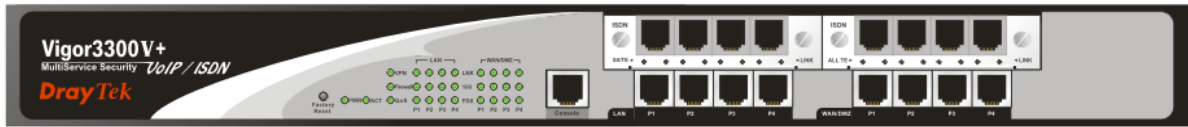
ISDN TE (Terminal Equipment) means an interface for transmitting analog signal through Internet between Switching and router. Such interface is also named with **ISDN S0 extern** in Germany.

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

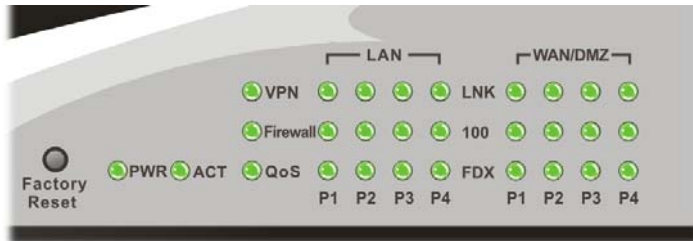
VoIP FXO (Foreign exchange office) is a port that used to connect to PSTN network.

VoIP FXS (Foreign exchange station) is a port that used to connect telephone set.

1.2.1 For Vigor3300V+

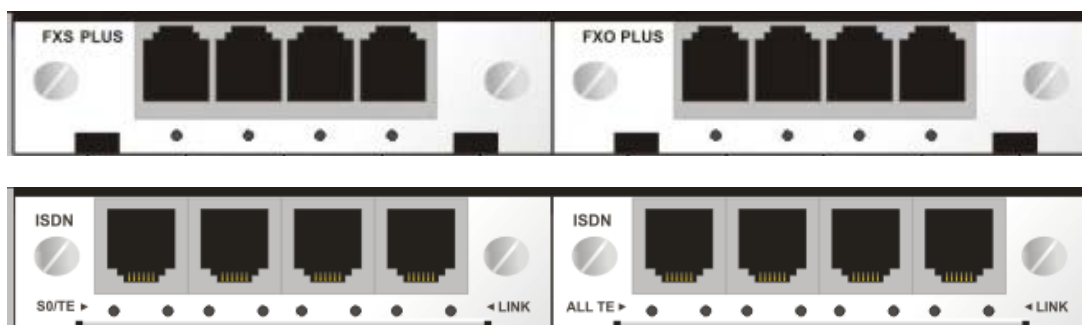


Description for LED



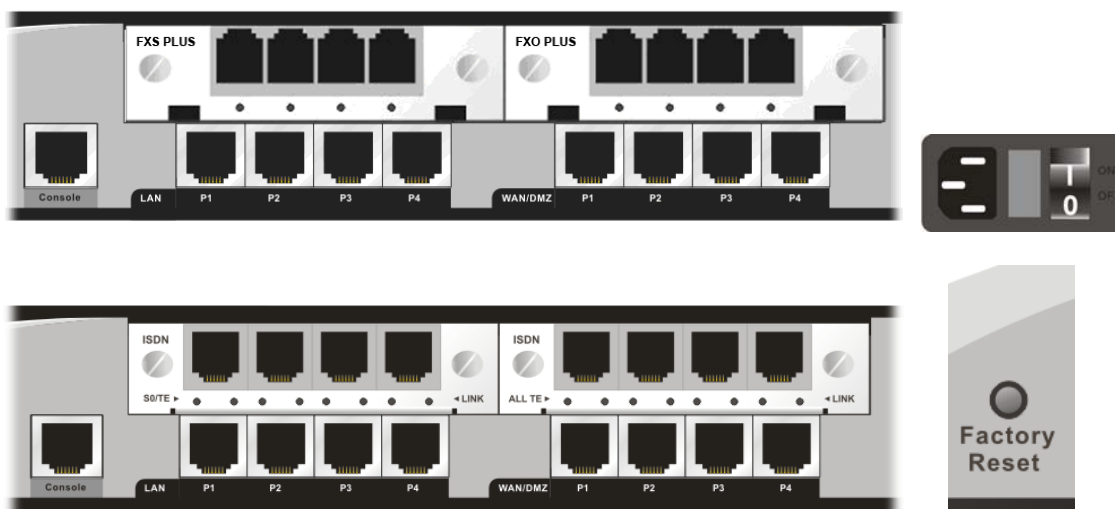
LED		Status	Explanation
PWR (Power)		On	The router is powered on.
		Off	The router is powered off.
ACT (Activity)		Blinking	The router is powered on and running normally.
		Off	The router is not ready or failed.
WAN		On	The WAN connection is ready.
		Blinking	It will blink while transmitting data.
VPN		On	VPN tunnel is up and down.
		Off	VPN tunnel is closed.
Firewall		On	The Firewall function is active.
		Off	The Firewall function is inactive.
QoS		On	The QoS function is active.
		Off	The QoS function is inactive.
LAN 1/2/3/4	LNK	On	The Ethernet link is established on corresponding port.
		Off	No Ethernet link is established.
	100	On	It means that a normal 100 Mbps connection is through its corresponding port.
		Off	It means that a normal 10 Mbps connection is through its corresponding port.
	FDX	On	It means a full duplex connection on corresponding port.
		Off	It means a half duplex connection on corresponding port.
WAN/DMZ (1, 2, 3, 4)	LNK	On	The Ethernet link is established.
		Blinking	The data transmission is done through the corresponding port.
		Off	No Ethernet link is established.
	100	On	It means that a normal 100Mbps connection is through its corresponding port.
		Off	It means that a normal 10Mbps connection is through its corresponding port.
	FDX	On	It means a full duplex connection on corresponding port.
Off		It means a half duplex connection on corresponding port.	

For the router supports functions of *FXS*, *FXO*, *ISDN S0/TE*, *ISDN ALL TE* modules that are optional, users can purchase them and installed them into the router according to the real requirement. The LED description for there four modules are different slightly. Please read the following for detailed explanation.



LED	Status	Explanation
FXS/FXO	On	It means VoIP port is connected and ready to use.
	Off	It means VoIP port is not connected.
	Blinking	It means a phone call is coming and the port is ringing.
S0/TE (Left LED)	On	It means S0 port is connected and S0 mode is ready.
	Off	It means TE port is connected and TE mode is ready.
	Blinking	No ISDN phone adapter connected.
S0/TE (Right LED)	On	It means ISDN link is established.
	Off	It means ISDN link is off.
	Blinking	It means the data and voice transmission is on-going.
ALL TE (Left LED)	On	It means TE port is connected and TE mode is ready.
ALL TE (Right LED)	On	It means ISDN link is established.
	Off	It means ISDN link is off.
	Blinking	It means the data and voice transmission is on-going.

Description for Connectors



Interface	Description
Console	Provided for technician use.
LAN (P1 ~ P4)	Connector for local networked devices.
WAN/DMZ (P1 ~ P4)	Connector for remote networked devices.
FXS	Connector for telephone set.
FXO	Connector for FXS interface of PABX.
ISDN S0/TE	Connector for ISDN phone/ISDN line.
ISDN ALL TE	Connector for ISDN line.
Factory Reset button	Used to restore the default settings. Turn on the router (ACT LED is blinking). Press the hole and keep for more than 5 seconds. When you see the ACT LED begins to blink rapidly than usual, release the button. Then the router will restart with the factory default configuration.
PWR	Connector for a power cord.
ON/OFF	Power switch.

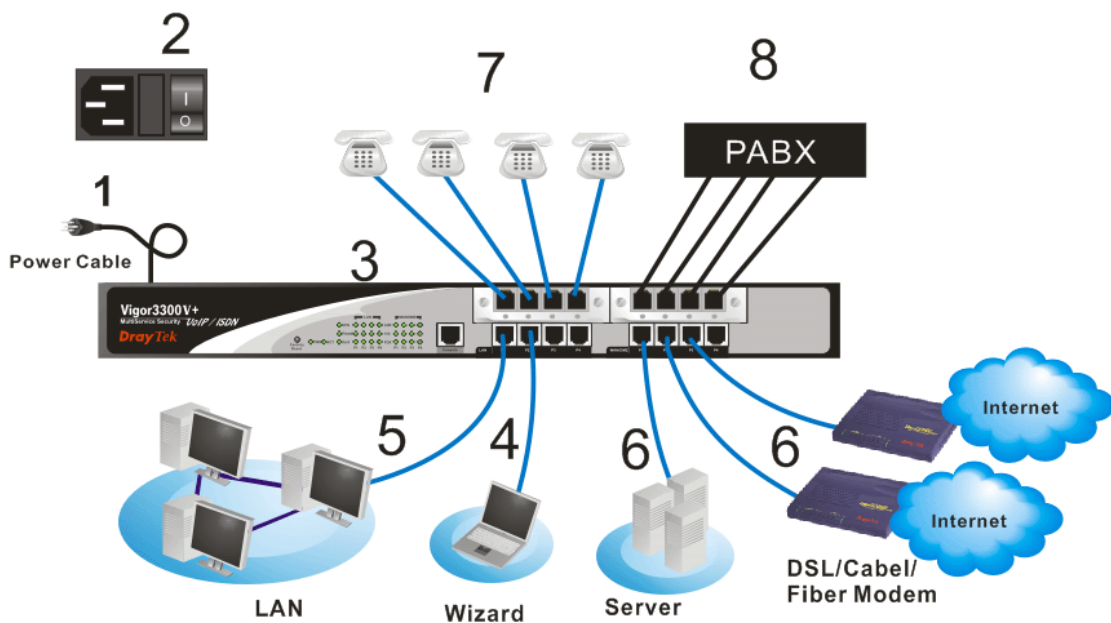
1.3 Hardware Installation

1.3.1 Network Connection

Before starting to configure the router, you have to connect your devices correctly. In this case, we suppose you have *FXS/FXO* module inserted into the router.

1. Connect the power cord to Vigor3300V+'s power port on the rear panel, and the other side into a wall outlet.
2. Power on the device by pressing down the power switch on the rear panel. The **PWR** LED should be **ON**.
3. The system starts to initiate. After completing the system test, the **ACT** LED will light up and start blinking.
4. Connect one end of an Ethernet cable (RJ-45) to one of the **LAN** ports of Vigor3300.
5. Connect the other end of the cable (RJ-45) to the Ethernet port on your computer (that device also can connect to other computers to form a small area network). The **LAN** LED for that port on the front panel will light up.
6. Connect a server/modem/router (depends on your requirement) to any WAN port of Vigor3300V+ with Ethernet cable (RJ-45). The **WAN1 (to WAN4)** LED will light up.
7. Connect telephone sets to the **FXS** ports of Vigor3300V+ with telephone lines (RJ-11 to RJ-11).
8. Connect the **FXO** ports to PABX with telephone lines (RJ-11 to RJ-11).

Below shows an outline of the hardware installation for your reference.



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

1.3.2 ISDN Phone Adapter Installation

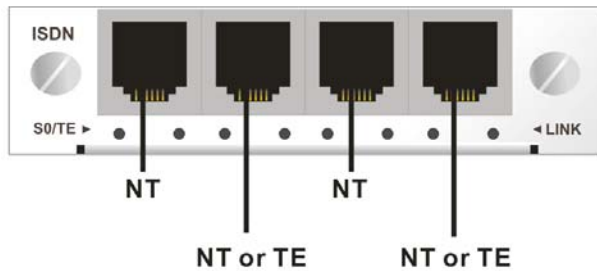
ISDN S0/TE Mode

ISDN NT is always fixed to connect ISDN phone. However, ISDN S0/TE is configurable as NT or TE mode. It can be adjusted in **VoIP>> Port Settings**.

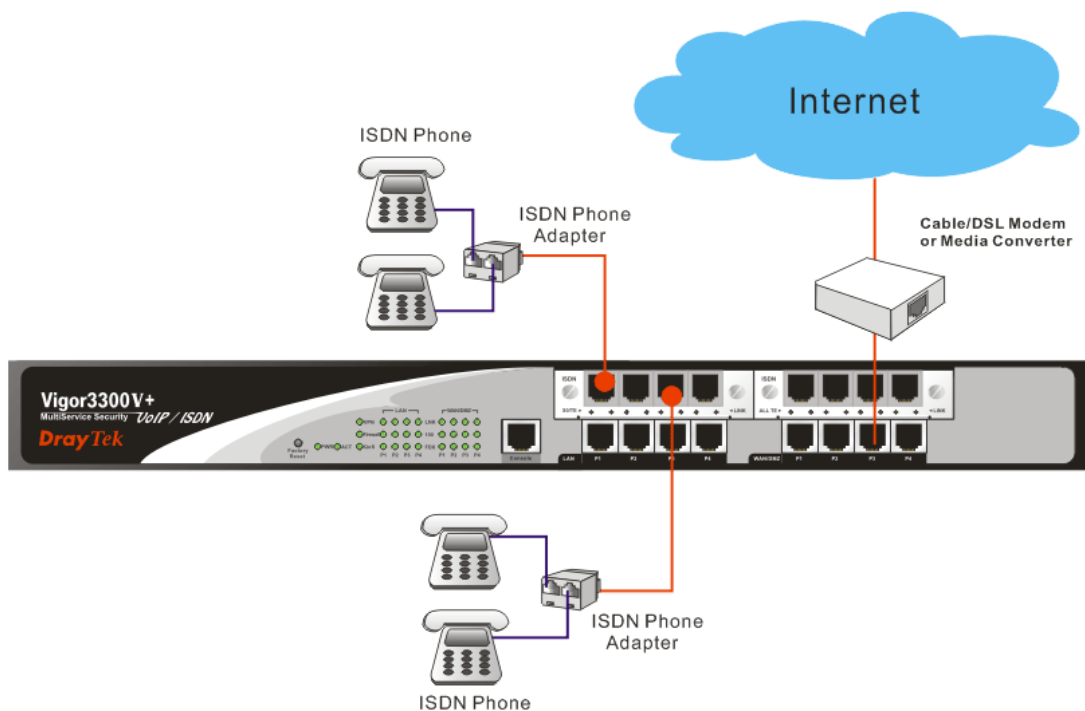
Note:

When NT or TE port is dedicated with TE mode, the Green LED will flash while data transmission.

However, if it is dedicated with NT mode, the Orange LED will light on when it connect to ISDN phone set.



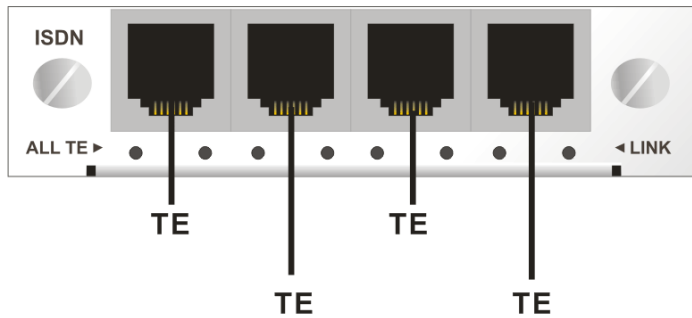
And by using ISDN phone adapters (coming from the router package), the user can connect several phones to the router for communication. Refer to the following figure for reference.



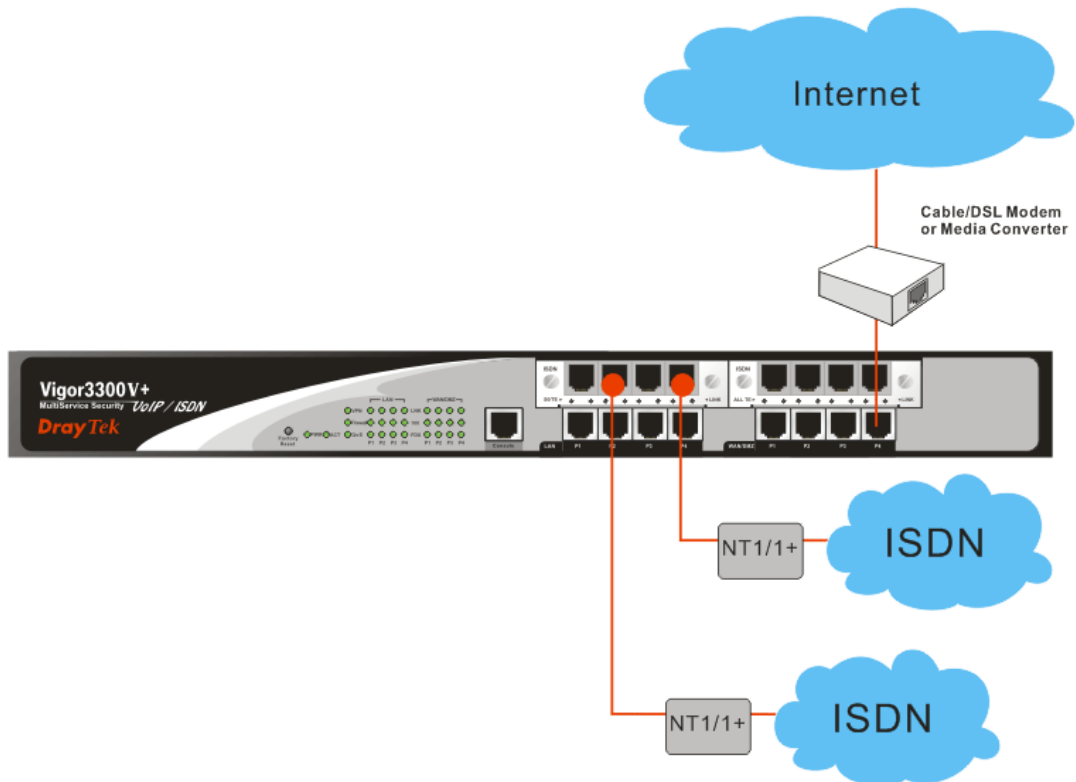
Note: When ISDN phone is connected, the Orange LED will light on.
When there is no ISDN phone connected, the Orange LED will flash.

ISDN ALL TE Mode

Such interface is used for connecting ISDN line. Each port is dedicated to TE mode only. Therefore, you cannot use such interface to connect to any ISDN phone.



For the connection, refer to the following figure for reference.



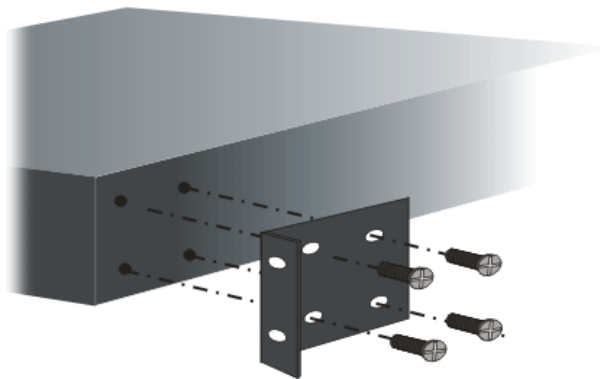
Note: When data transmission through this interface, the Green LED will flash.

1.3.3 Rack-Mounted Installation

The Vigor3300V+ Series can be mounted on a rack by using standard brackets in a 19-inch rack or optional larger brackets on 23-inch rack (not included). The bracket for 19- and 23-inch racks are shown below.



Attach the brackets to the chassis of a 19- or a 23-inch rack. The second bracket attaches the other side of the chassis as above procedure.



After the bracket installation, the Vigor3300 Series chassis can be installed in a rack by using four screws for each side of the rack.



Desktop Type Installation

Rubber pads are included with the Vigor3300V+ Series. These rubber pads improve the air circulation and decrease unnecessary rubbing on the desktop.

Chapter 2: Configuring Basic Settings

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

This chapter explains how to setup a password for an administrator 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 browser 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 on the window for the first time accessing. The default value for user name is **draytek** and the password is **1234**. Next, click **OK**.

Login to Vigor 3300

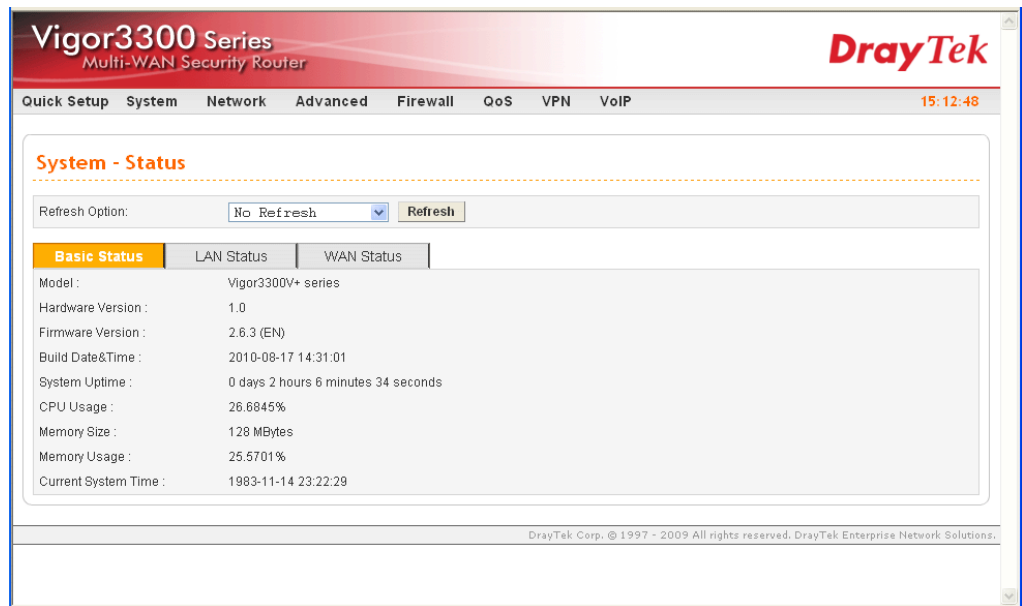
User name: draytek

Password:

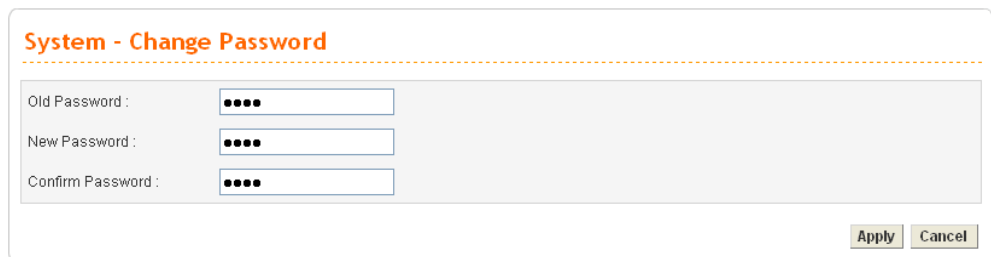
Remember my password

OK Cancel

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



4. Go to **System** page and choose **Change Password**.



5. Enter the login password (1234) on the field of Old Password. Type a new one in the field of New Password and retype it on the field of Confirm Password. Then click **Apply** to continue.
6. Now, the password has been changed. Next time, use the new password to access the Web Configurator for this router.



2.2 Quick Setup

Quick Setup is designed for configuring your broadband router accessing Internet with simply steps. There are two phases of quick setup, one is WAN configuration and the other is LAN configuration.

In the **Quick Setup** group, you can configure the router to access the Internet with different modes such as Static, DHCP, PPPoE, or PPTP modes. For most users, Internet access is the primary application. The router supports the Ethernet WAN interface for Internet access. The following sections will explain in more detail the various broadband access configurations. All the settings in this section will be used in the first WAN1 interface.

Quick Setup - WAN

MAC Address : Default MAC User Defined MAC
00:00:00:00:00:02

Downstream Rate : 102400 (kbps)

Upstream Rate : 102400 (kbps)

Type : Fast Ethernet

Physical Mode : Auto Negotiation

IP Mode : Static DHCP PPPoE PPTP

Static/DHCP Configuration | PPPoE/PPTP Configuration

IP Address : Host Name :

Subnet Mask : Domain Name :

Default Gateway : (Host Name and Domain Name are required for some ISPs.)

Primary DNS :

Secondary DNS :

IP Alias List

1.	<input type="text"/>	2.	<input type="text"/>
3.	<input type="text"/>	4.	<input type="text"/>
5.	<input type="text"/>	6.	<input type="text"/>
7.	<input type="text"/>	8.	<input type="text"/>

Next >>

MAC Address

Default MAC-

Use the default Mac address stored originally in router.

User Defined MAC-

Use a MAC address defined by the user.

Downstream Rate

Assign the downstream rate for this WAN interface. The default value is 102400 kbps (100 Megabit). This setting is very important for Vigor3300 Series incoming buffer adjustment. If you use a DSL subscriber service with a 2Mbps downstream, please set the downstream rate setting with 2Mbps.

Upstream Rate

Assign the transmission rate for this WAN interface. The default value is 102400 kbps (100 Megabit). This setting is very important for Vigor3300 Series outgoing buffer adjustment. If you use a DSL subscriber service with a 256Kbps downstream, please set the downstream rate setting with 256Kbps.

Type

Select a connection type for this WAN interface. Currently, there is only one setting offered for you to choose - Fast Ethernet.

Physical Mode

Select connection speed mode for this WAN interface. There are **auto negotiation**, **full duplex**, and **half duplex** of either 10M or 100M speed options for the WAN Interface.

IP Mode

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. Select an IP mode for this WAN interface. There are four available modes for Internet access, **Static**, **DHCP**, **PPPoE**, and **PPTP**. On this page you may configure the WAN interface to use **Static** (fixed IP), **DHCP** (dynamic IP address), **PPPoE** or **PPTP**. Most of the cable users will use the **DHCP** mode to get a globally reachable IP address from the cable host system.

2.2.1 Static Mode

You can manually assign a static IP address to the WAN interface and complete the configuration by applying the settings and rebooting your router. Choosing **Static** as the IP mode, you will see the following page.

The screenshot shows the WAN configuration interface for Static Mode. At the top, 'Physical Mode' is set to 'auto negotiation'. Below it, 'IP Mode' has radio buttons for 'Static' (selected), 'DHCP', 'PPPoE', and 'PPTP'. There are two tabs: 'Static/DHCP Configuration' (active) and 'PPPoE/PPTP Configuration'. The 'Static/DHCP Configuration' section contains the following fields:

- IP Address: 172.16.3.229
- Subnet Mask: 255.255.255.0
- Default Gateway: 172.16.3.1
- Primary DNS: 168.95.1.1
- Secondary DNS: 168.95.192.1
- Host Name: (empty)
- Domain Name: (empty)

A note below the Host Name and Domain Name fields states: '(Host Name and Domain Name are required for some ISPs.)'. Below this is an 'IP Alias List' table with 8 rows and 2 columns for IP addresses:

IP Alias List	
1.	10.1.1.100
2.	10.1.1.101
3.	10.1.1.102
4.	
5.	
6.	
7.	
8.	

A 'Next >>' button is located at the bottom right of the configuration area.

All the settings here are set by privately. Your ISP will not provide these settings.

IP Address

Type a private IP address to the WAN interface.

Subnet Mask

Type a subnet mask value to the WAN interface.

Default Gateway

Type a private IP address to the gateway.

Primary DNS

Type a private IP address to the primary DNS.

Secondary DNS

Type a private IP address to the secondary DNS.

IP Alias List

Type other IP addresses to be bound to this interface. This setting is optional. If you have typed addresses here, you can see and choose it in later web page settings (e.g., **Advanced >> NAT >> Port Redirection/DMZ Host**). Thirty-two IP addresses settings are allowed at one time.

After setting up the WAN interface, click **Next** to setup the LAN interface continuously.

Quick Setup - LAN

LAN IP/DHCP DHCP Relay Agent IP Routing

IP Configuration

IP Address :

Subnet Mask :

DHCP Server

Status : Enable Disable Relay Agent

Start IP :

End IP :

Primary DNS :

Secondary DNS :

Lease Time (Min) :

Gateway IP(Optional) :

- IP Address** Type an IP address for the LAN interface.
- Subnet Mask** Type the subnet mask for the LAN interface.
- Status** Click **Enable** to use DHCP server; click **Disable** to close DHCP server; click **Relay Agent** to activate relay agent function.
- Start IP** Type the start IP address of the IP pool that DHCP server can use for clients in LAN.
- End IP** Type the end IP address of the IP pool that DHCP sever can use for clients in LAN.
- Primary DNS** Type the IP address for primary DNS.
- Secondary DNS** Type a private IP address to the secondary DNS.
- Lease Time (Min)** Set a lease time for the DHCP server. The time unit is minute.
- Gateway IP (Optional)** Set a gateway IP address for the DHCP server.
- Next, click **DHCP Relay Agent** tab to set DHCP server if required.

Quick Setup - LAN

LAN IP/DHCP **DHCP Relay Agent** IP Routing

Relay Agent

WAN Interface :

DHCP Server IP Address :

- WAN Interface** Choose the WAN interface for such connection.
- DHCP Server IP Address** Type an IP address for the DHCP server.
- Next, click **IP Routing** tab to set routing path for each WAN interface if required.

Quick Setup - LAN

LAN IP/DHCP	DHCP Relay Agent	IP Routing
WAN1		
Status:	<input type="radio"/> Enable	<input checked="" type="radio"/> Disable
IP Address:	<input type="text"/>	
Subnet Mask:	<input type="text"/>	
WAN2		
Status:	<input type="radio"/> Enable	<input checked="" type="radio"/> Disable
IP Address:	<input type="text"/>	
Subnet Mask:	<input type="text"/>	
WAN3		
Status:	<input type="radio"/> Enable	<input checked="" type="radio"/> Disable
IP Address:	<input type="text"/>	
Subnet Mask:	<input type="text"/>	
WAN4		
Status:	<input type="radio"/> Enable	<input checked="" type="radio"/> Disable
IP Address:	<input type="text"/>	
Subnet Mask:	<input type="text"/>	

When you finished the above required settings, please click **Finish**. A system reboot page will appear. Click **Apply** to activate the static mode configuration.

2.2.2 DHCP Mode

DHCP allows a user to obtain an IP address automatically from a DHCP server on the Internet. If you choose **DHCP** mode, the DHCP server of your ISP will assign a dynamic IP address for Vigor3300 automatically. It is not necessary for you to assign any setting. (Host Name and Domain Name are required for some ISPs).

Simply click **Next** to setup LAN interface.

Quick Setup - LAN

LAN IP/DHCP | DHCP Relay Agent | IP Routing

IP Configuration

IP Address :

Subnet Mask :

DHCP Server

Status : Enable Disable Relay Agent

Start IP :

End IP :

Primary DNS :

Secondary DNS :

Lease Time (Min) :

Gateway IP(Optional) :

- IP Address** Type an IP address for the LAN interface.
- Subnet Mask** Type the subnet mask for the LAN interface.
- Status** Click **Enable** to use DHCP server; click **Disable** to close DHCP server; click **Relay Agent** to activate relay agent function.
- Start IP** Type the start IP address of the IP pool that DHCP server can use for clients in LAN.
- End IP** Type the end IP address of the IP pool that DHCP sever can use for clients in LAN.
- Primary DNS** Type the IP address for primary DNS.
- Secondary DNS** Type a private IP address to the secondary DNS.
- Lease Time (Min)** Set a lease time for the DHCP server. The time unit is minute.
- Gateway IP (Optional)** Set a gateway IP address for the DHCP server.
- Next, click **DHCP Relay Agent** tab to set DHCP server if required.

Quick Setup - LAN

LAN IP/DHCP | **DHCP Relay Agent** | IP Routing

Relay Agent

WAN Interface :

DHCP Server IP Address :

WAN Interface Choose the WAN interface for such connection.

DHCP Server IP Address Type an IP address for the DHCP server.

Next, click **IP Routing** tab to set routing path for each WAN interface if required.

Quick Setup - LAN

LAN IP/DHCP | DHCP Relay Agent | **IP Routing**

WAN1

Status: Enable Disable

IP Address:

Subnet Mask:

WAN2

Status: Enable Disable

IP Address:

Subnet Mask:

WAN3

Status: Enable Disable

IP Address:

Subnet Mask:

WAN4

Status: Enable Disable

IP Address:

Subnet Mask:

When you finished the above settings, please click **Finish**. A system reboot page will appear. Click **Apply** to activate the DHCP mode configuration.

2.2.3 PPPoE

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

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

If your ISP provides you the **PPPoE** (Point-to-Point Protocol over Ethernet) connection, please select **PPPoE** for this router to get the following page. Enter the **username** and **password** provided by your ISP on the web page.

Static/DHCP Configuration	PPPoE/PPTP Configuration		
User Name :	1234@hinet.net	PPTP Local Address :	<input type="text"/>
Password :	••••	PPTP Subnet Mask :	<input type="text"/>
Authentication :	PAP	PPTP Server Address :	<input type="text"/>
Service Name (Optional):	<input type="text"/>		

Next >>

- User Name** Type a specific valid user name provided by the ISP.
- Password** Type a valid password provided by the ISP.
- Authentication** Select **PAP**, **CHAP**, **MS-CHAP** or **MS-CHAP-V2** protocol for PPP authentication. The default value is **PAP**.

- Service Name** Type a service name required from ISP service.
- After setting up the **PPPoE**, click **Next** to setup the LAN interface continuously.

Quick Setup - LAN

LAN IP/DHCP	DHCP Relay Agent	IP Routing
IP Configuration		
IP Address :	192.168.1.1	
Subnet Mask :	255.255.255.0	
DHCP Server		
Status :	<input checked="" type="radio"/> Enable <input type="radio"/> Disable <input type="radio"/> Relay Agent	
Start IP :	192.168.1.10	
End IP :	192.168.1.254	
Primary DNS :	<input type="text"/>	
Secondary DNS :	<input type="text"/>	
Lease Time (Min) :	1440	
Gateway IP(Optional) :	<input type="text"/>	

- IP Address** Type an IP address for the LAN interface.
- Subnet Mask** Type the subnet mask for the LAN interface.
- Status** Click **Enable** to use DHCP server; click **Disable** to close DHCP server; click **Relay Agent** to activate relay agent function.
- Start IP** Type the start IP address of the IP pool that DHCP server can use for clients in LAN.
- End IP** Type the end IP address of the IP pool that DHCP sever can use for clients in LAN.

- Primary DNS** Type the IP address for primary DNS.
- Secondary DNS** Type a private IP address to the secondary DNS.
- Lease Time (Min)** Set a lease time for the DHCP server. The time unit is minute.
- Gateway IP (Optional)** Set a gateway IP address for the DHCP server.

Next, click **DHCP Relay Agent** tab to set DHCP server if required.

The screenshot shows the 'Quick Setup - LAN' configuration page with the 'DHCP Relay Agent' tab selected. The 'Relay Agent' section includes a 'WAN Interface' dropdown menu set to 'WAN1' and an empty 'DHCP Server IP Address' text box. At the bottom right, there are '<<Previous' and 'Finish' buttons.

WAN Interface Choose the WAN interface for such connection.

DHCP Server IP Address Type an IP address for the DHCP server.

Next, click **IP Routing** tab to set routing path for each WAN interface if required.

The screenshot shows the 'Quick Setup - LAN' configuration page with the 'IP Routing' tab selected. It displays four WAN interface sections (WAN1, WAN2, WAN3, WAN4). Each section has a 'Status' field with radio buttons for 'Enable' and 'Disable', and 'IP Address' and 'Subnet Mask' text boxes. The 'Finish' button at the bottom right is circled in red.

When you finished the above settings, please click **Finish**. A system reboot page will appear. Click **Apply** to activate the PPPoE mode configuration.

2.2.4 PPTP

This mode lets user get the IP group information by a DSL modem with PPTP service from ISP. Your service provider will give you user name, password, and authentication mode for a PPTP setting. Click **PPTP** as the protocol. Type in all the information that your ISP provides for this protocol.

If your ISP offers you **PPTP** (Point-to-Point Tunneling Protocol) mode, please select **PPTP** for this router. Next, enter the **PPTP Subnet Mask (e.g., 255.255.255.0)**, **PPTP Local Address (e.g., 10.66.99.88)** and **PPTP Server Address (e.g., 172.66.99.88)** provided by your ISP on the web page.

Static/DHCP Configuration	PPPoE/PPTP Configuration		
User Name :	1234@hinet.net	PPTP Local Address :	10.66.99.88
Password :	••••	PPTP Subnet Mask :	255.255.255.0
Authentication :	PAP	PPTP Server Address :	172.66.99.88
Service Name (Optional):			

Next >>

PPTP Local Address Assign a local IP address of PPTP.

PPTP Subnet Mask Assign a net mask value for IP address of PPTP.

PPTP Server Address Assign a remote IP address of PPTP server.

After setting up the **PPTP**, click **Next** to setup the LAN interface continuously.

Quick Setup - LAN

LAN IP/DHCP | DHCP Relay Agent | IP Routing

IP Configuration

IP Address : 192.168.1.1

Subnet Mask : 255.255.255.0

DHCP Server

Status : Enable Disable Relay Agent

Start IP : 192.168.1.10

End IP : 192.168.1.254

Primary DNS :

Secondary DNS :

Lease Time (Min) : 1440

Gateway IP(Optional) :

<<Previous **Finish**

IP Address Type an IP address for the LAN interface.

Subnet Mask Type the subnet mask for the LAN interface.

Status Click **Enable** to use DHCP server; click **Disable** to close DHCP server; click **Relay Agent** to activate relay agent function.

Start IP	Type the start IP address of the IP pool that DHCP server can use for clients in LAN.
End IP	Type the end IP address of the IP pool that DHCP sever can use for clients in LAN.
Primary DNS	Type the IP address for primary DNS.
Secondary DNS	Type a private IP address to the secondary DNS.
Lease Time (Min)	Set a lease time for the DHCP server. The time unit is minute.
Gateway IP (Optional)	Set a gateway IP address for the DHCP server.

Next, click **DHCP Relay Agent** tab to set DHCP server if required.

The screenshot shows the 'Quick Setup - LAN' configuration page with the 'DHCP Relay Agent' tab selected. The 'Relay Agent' section includes a 'WAN Interface' dropdown menu set to 'WAN1' and a 'DHCP Server IP Address' text input field. At the bottom right, there are '<<Previous' and 'Finish' buttons.

WAN Interface Choose the WAN interface for such connection.

DHCP Server IP Address Type an IP address for the DHCP server.

Next, click **IP Routing** tab to set routing path for each WAN interface if required.

The screenshot shows the 'Quick Setup - LAN' configuration page with the 'IP Routing' tab selected. It displays four WAN interface sections (WAN1, WAN2, WAN3, WAN4). Each section has a 'Status' field with radio buttons for 'Enable' and 'Disable' (where 'Disable' is selected for all), and 'IP Address' and 'Subnet Mask' text input fields. At the bottom right, the 'Finish' button is circled in red.

When you finished the above settings, please click **Finish**. A system reboot page will appear. Click **Apply** to activate the PPTP mode configuration.

Chapter 3: Applications

3.1 Application for 802.1 VLAN

3.1.1 Block LAN-to-LAN Communication

To control the communication of PCs among different network segments effectively, please adjust firewall setting to **deny** LAN to LAN communication from **Firewall > IP Filter Group Table**. Thus, PCs that belong to various LANs will not connect with each other through the router. To a company with several departments, such feature is useful for it to determine data sharing among different departments.

1. Open **Firewall > IP Filter > Group Table** to access into the following page. Click Index #2 radio button.

IP Filter Group Table			
Index	Group Name	Next Group	Comment
<input checked="" type="radio"/> 1	Pass	Block	Group for pass rules
<input type="radio"/> 2	Block	none	Group for block rules

2. In this page, click **Add Rule**. Choose **Block** as Next Group Name.

Group Name :

Next Group Name :

Comment :

3. In the following page, please set **Block immediately** as the action and click **Apply**.

Firewall - IP Filter - Add Filter Rule

Filter Condition

Active

Source : IP :
 Subnet Mask :
 Port : = -

Destination : IP :
 Subnet Mask :
 Port : = -

Group Name :

Protocol :

Direction :

Fragment :

Action

Block or Pass :

Next Group Name :

- Now you will get the following page.

Firewall - IP Filter Table

Group Name :

Next Group Name :

Comment :

IP Filter Table											
Index	Source IP	Subnet Mask	Port	Destination IP	Subnet Mask	Port	Protocol	Direction	Block	Active	
1	any	255.255.255.0		any			any protocol	LAN to LAN	Block immediately	<input checked="" type="checkbox"/>	

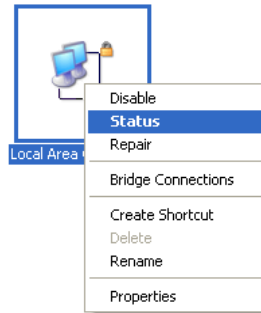
3.1.2 How to Check/Edit VLAN ID on Your PC?

Not all the network cards support VLAN features. If you cannot sure if the network card of your computer supports tagged VLAN or not, please do the following steps to check (or edit) VLAN ID on your PC.

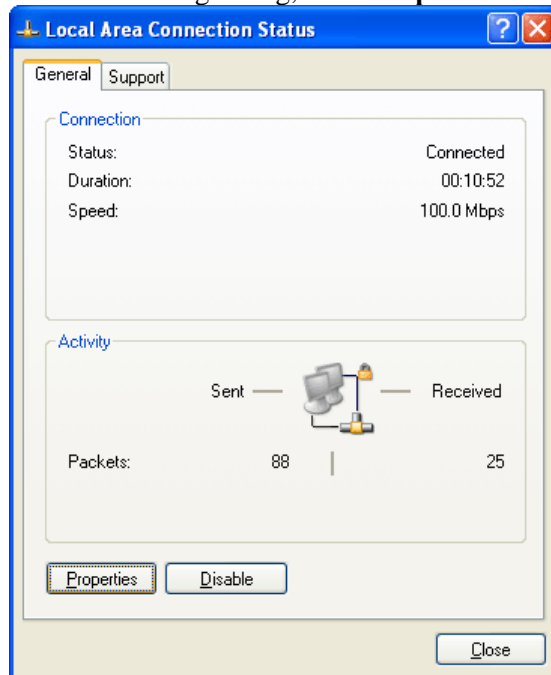
- Go to **Control Panel** and then double-click on **Network Connections**.



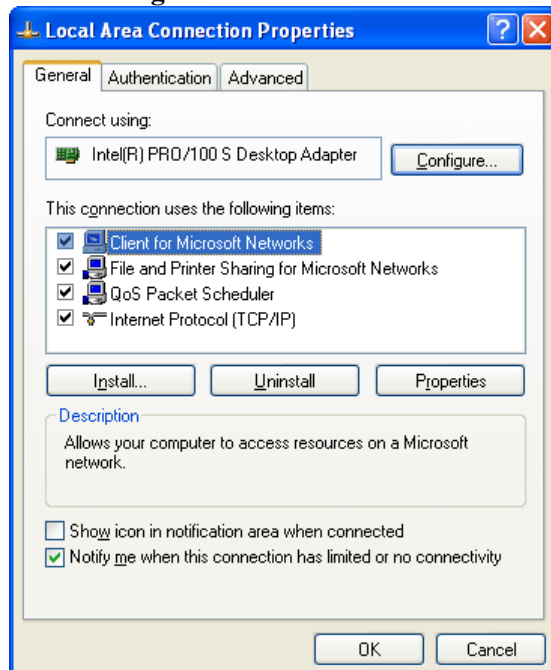
2. Right-click on **Local Area Connection** and click on **Status**.



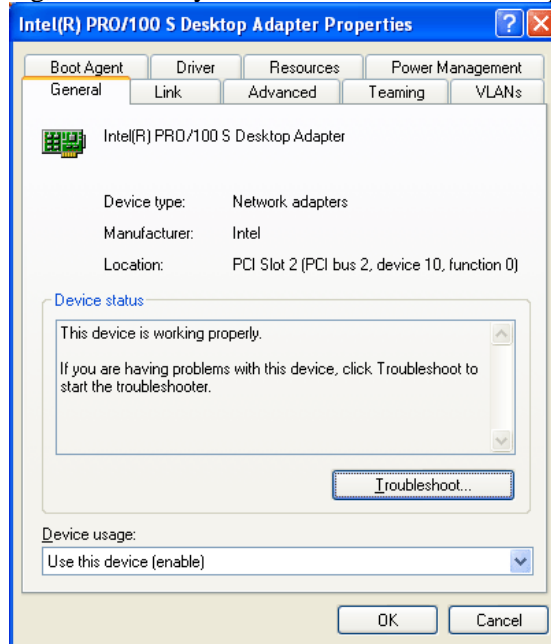
3. On the following dialog, click **Properties**.



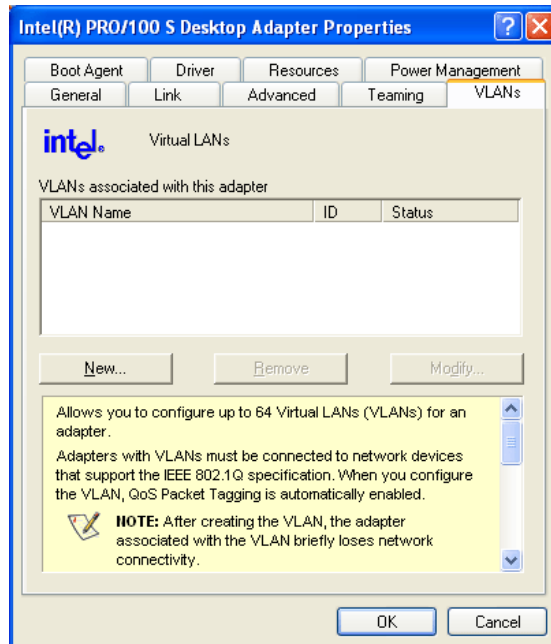
4. Click **Configure** to access into next screen.



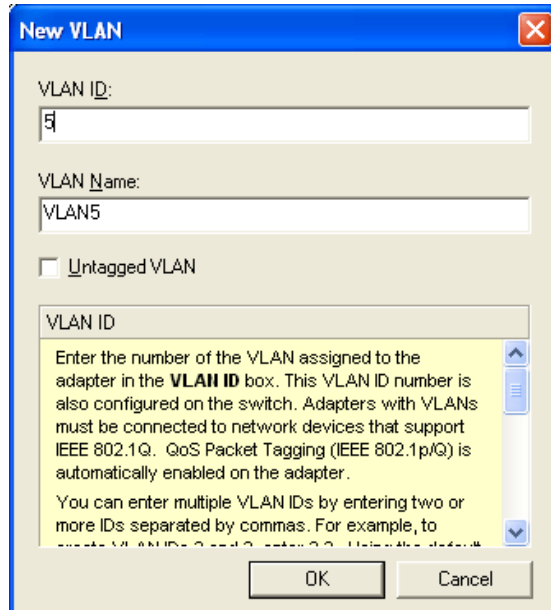
5. On this dialog box, locate **VLANs** tag and click on it. If you cannot find out VLANs tag, that means your network card does not support VLAN feature.



6. In this screen, there is no VALN existed. You can create a new one. Please click the **New...** button.



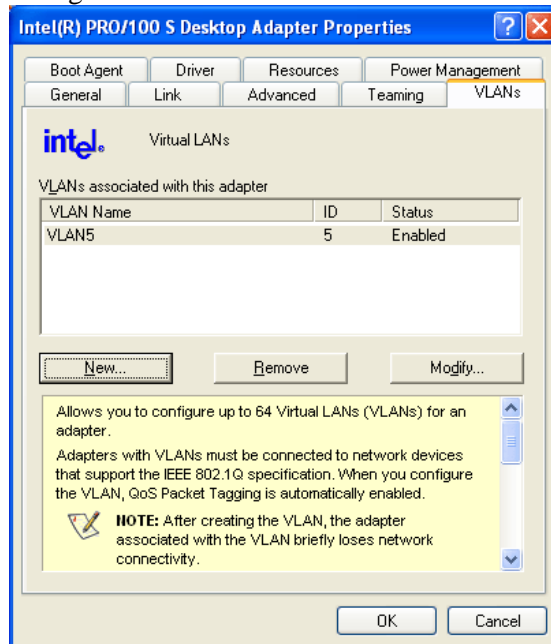
7. In **New VLAN** dialog, please type a number in the box of VLAN ID. Here, “5” is entered. The corresponding VLAN Name will appear automatically. Next, click **OK** to create it.



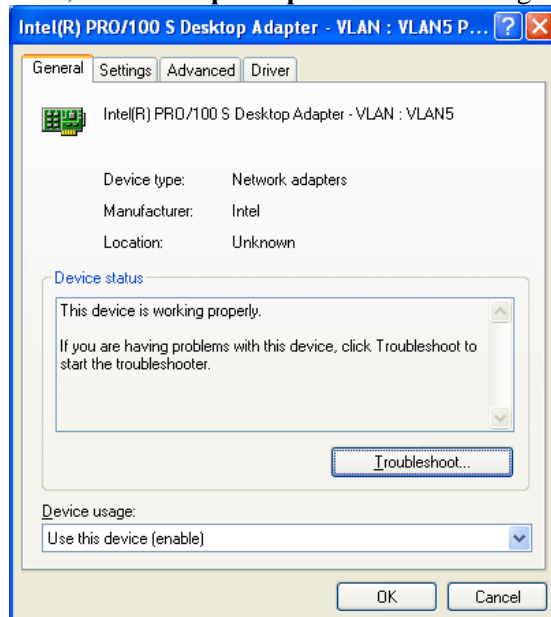
8. After you click OK, the system will configure for the VLAN settings. Please wait for several seconds.



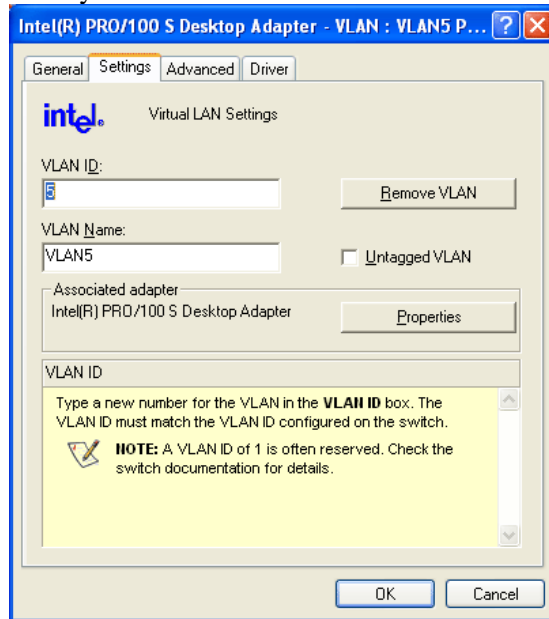
9. When the configuration is finished, the new VLAN settings with ID number and name will appear on previous dialog, **Desktop Adapter Properties**. Click **OK** to exit this dialog.



10. Now, the **Desktop Adapter – VLAN** dialog will appear as follows. Please click **OK**.

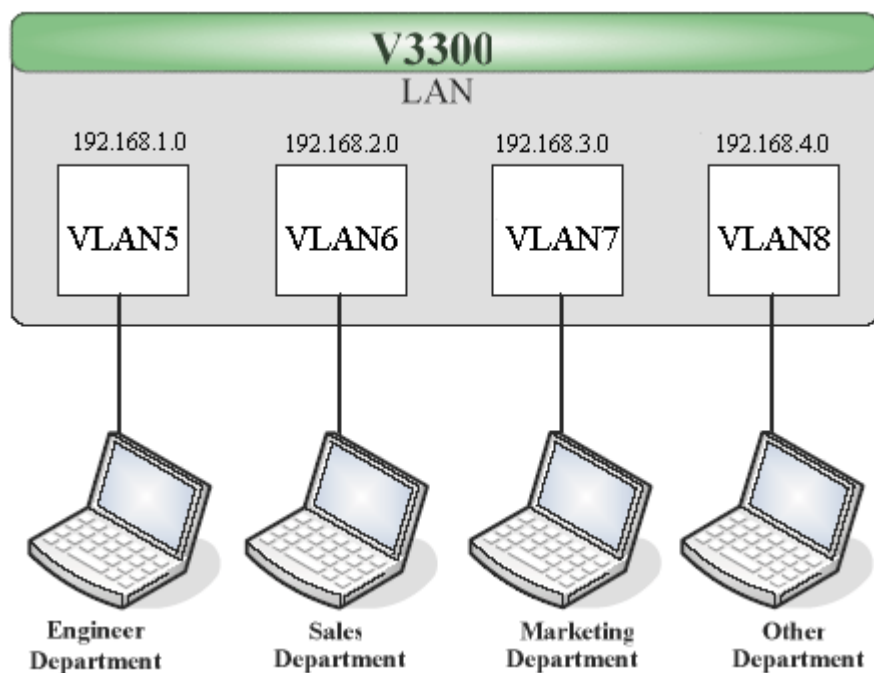


11. Next time, if you want to check VLAN setting again, please open **Settings** tag to modify it.



3.1.3 Four VLANs for Different Departments in A Company

A company wants to separate the Engineer Department, Sales Department, Marketing Department and Other Department to limit their communication with each other to ensure the security. In this case, we can define four VLANs that are VLAN5, VLAN6, VLAN7 and VLAN8. The subnet of VLAN5 is 192.168.1.0; the subnet of VLAN6 is 192.168.2.0; the subnet of VLAN7 is 192.168.3.0, and the subnet of VLAN8 is 192.168.4.0. However, each PC in the company does not support 802.1Q.



Procedure:

1. Refer to A.1 to block LAN-to-LAN communication.
2. Create VLAN5, VLAN6, VLAN7 and VLAN8 Groups.
3. In the VLAN5, input "5" to VLAN ID. In the Member field, choose p1. Then choose the "Untagged" for Frame Tag Operation in p1. Configure the PVID to "5" for the device does not support 802.1Q VLAN.
4. In the VLAN6, input "6" to VLAN ID. In the Member field, choose p2. Then choose the "Untagged" for Frame Tag Operation in p2. Configure the PVID to "6" for the device does not support 802.1Q VLAN.
5. In the VLAN7, input "7" to VLAN ID. In the Member field, choose p3. Then choose the "Untagged" for Frame Tag Operation in p3. Configure the PVID to "7" for the device does not support 802.1Q VLAN.
6. In the VLAN8, input "8" to VLAN ID. In the Member field, choose p4. Then choose the "Untagged" for Frame Tag Operation in p4. Configure the PVID to "8" for the device does not support 802.1Q VLAN.

Advanced - LAN VLAN Setting

Disable
 Port Base VLAN
 802.1Q VLAN

Port Base VLAN: **802.1Q VLAN**

Group

Index	Active	Name	VLAN ID	Member				Frame Tag Operation			
				P1	P2	P3	P4	P1	P2	P3	P4
1	<input checked="" type="checkbox"/>	VLAN5	5	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Untagged	Tagged	Tagged	Tagged
2	<input checked="" type="checkbox"/>	VLAN6	6	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Tagged	Untagged	Tagged	Tagged
3	<input checked="" type="checkbox"/>	VLAN7	7	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Tagged	Tagged	Untagged	Tagged
4	<input checked="" type="checkbox"/>	VLAN8	8	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Tagged	Tagged	Tagged	Untagged

Enable management port for P4

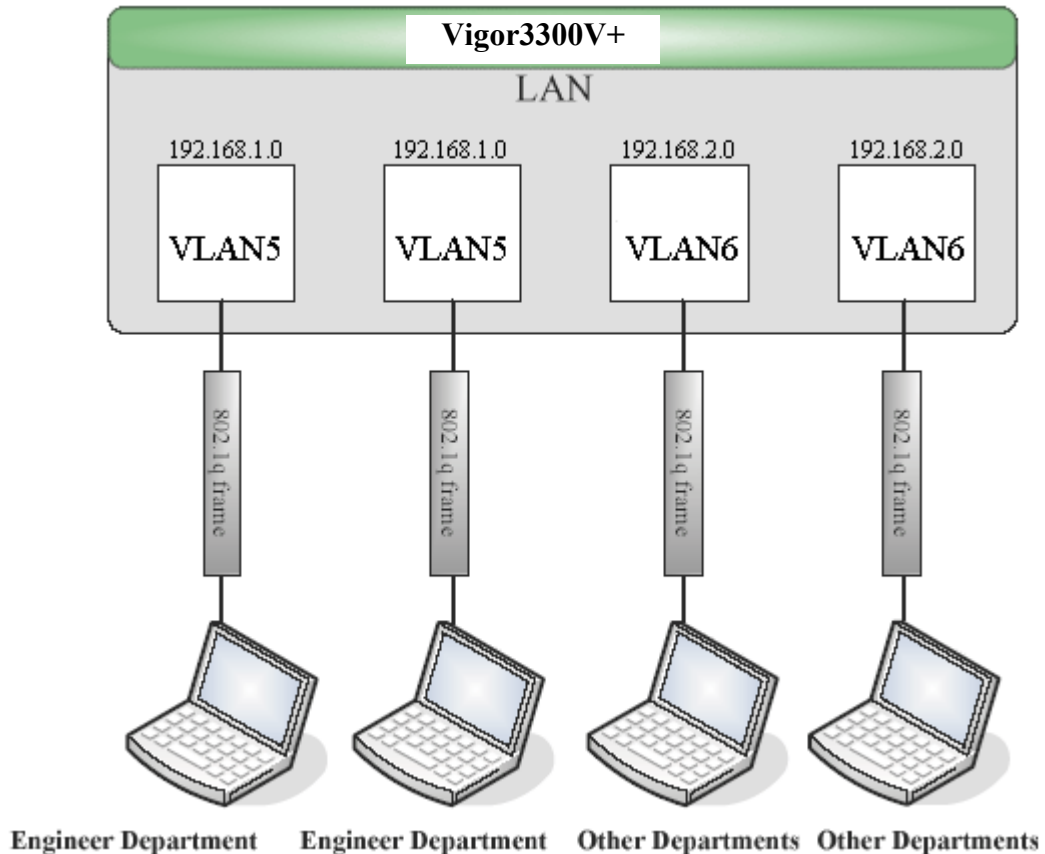
Port Setting

	P1	P2	P3	P4
Port VLAN ID	5	6	7	8

7. After applying the settings, the web page will be redirected to “reboot” web page. You can ignore it and continue to configure the Network setting. After finishing Network setting, you can execute the reboot procedure.
8. After rebooting, the tagged ports will communicate with 802.1Q tagged devices only.
9. In the Network setting, type the subnet 192.168.1.0 to LAN. For example, the VLAN5 LAN IP is 192.168.1.1 and the Subnet Mask is 255.255.255.0. Then, users in the Engineer Department can set IP address from 192.168.1.2 to 192.168.1.254.
10. In the Network setting, type the subnet 192.168.2.0 to LAN2. For example, the VLAN6 LAN IP is 192.168.2.1 and the Subnet Mask is 255.255.255.0. Then, users in the Engineer Department can set IP address from 192.168.2.2 to 192.168.2.254.
11. In the Network setting, type the subnet 192.168.3.0 to LAN3. For example, the VLAN7 LAN IP is 192.168.3.1 and the Subnet Mask is 255.255.255.0. Then, users in the Engineer Department can set IP address from 192.168.3.2 to 192.168.3.254.
12. In the Network setting, type the subnet 192.168.4.0 to LAN4. For example, the VLAN8 LAN IP is 192.168.4.1 and the Subnet Mask is 255.255.255.0. Then, users in the Engineer Department can set IP address from 192.168.4.2 to 192.168.4.254.

3.1.4 Two VLANs for Different Departments in A Company

A company wants to separate the Engineer Department and Other Departments to limit their communication to protect the engineering data. In this case, we can define two VLANs that are VLAN5 and VLAN6. The subnet of VLAN5 is 192.168.1.0, and the subnet of VLAN6 is 192.168.2.0.



Procedure:

1. Refer to A.1 to block LAN-to-LAN communication.
2. Create VLAN5 and VLAN6 Groups.
3. In the VLAN5, type “5” to VLAN ID. In the Member field, choose p1 and p2. Then choose “Tagged” for Frame Tag Operation in p1 and p2. We can ignore the PVID (Port VLAN because 802.1q tag will be inserted to the frame from the PC of Engineer Department.
4. In the VLAN6, type “6” to VLAN ID. In the Member field, choose p3 and p4. Then choose “Tagged” for Frame Tag Operation in p3 and p4. We can ignore the PVID (Port VLAN because 802.1q tag will be inserted to the frame from other departments.

Advanced - LAN VLAN Setting

Disable
 Port Base VLAN
 802.1Q VLAN

Port Base VLAN: 802.1Q VLAN

Group

Index	Active	Name	VLAN ID	Member				Frame Tag Operation			
				P1	P2	P3	P4	P1	P2	P3	P4
1	<input checked="" type="checkbox"/>	VLAN5	5	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Tagged	Tagged	Tagged	Tagged
2	<input checked="" type="checkbox"/>	VLAN6	6	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Tagged	Tagged	Tagged	Tagged
3	<input checked="" type="checkbox"/>	VLAN7	7	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Tagged	Tagged	Untagged	Tagged
4	<input checked="" type="checkbox"/>	VLAN8	8	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Tagged	Tagged	Tagged	Untagged

Enable management port for P4

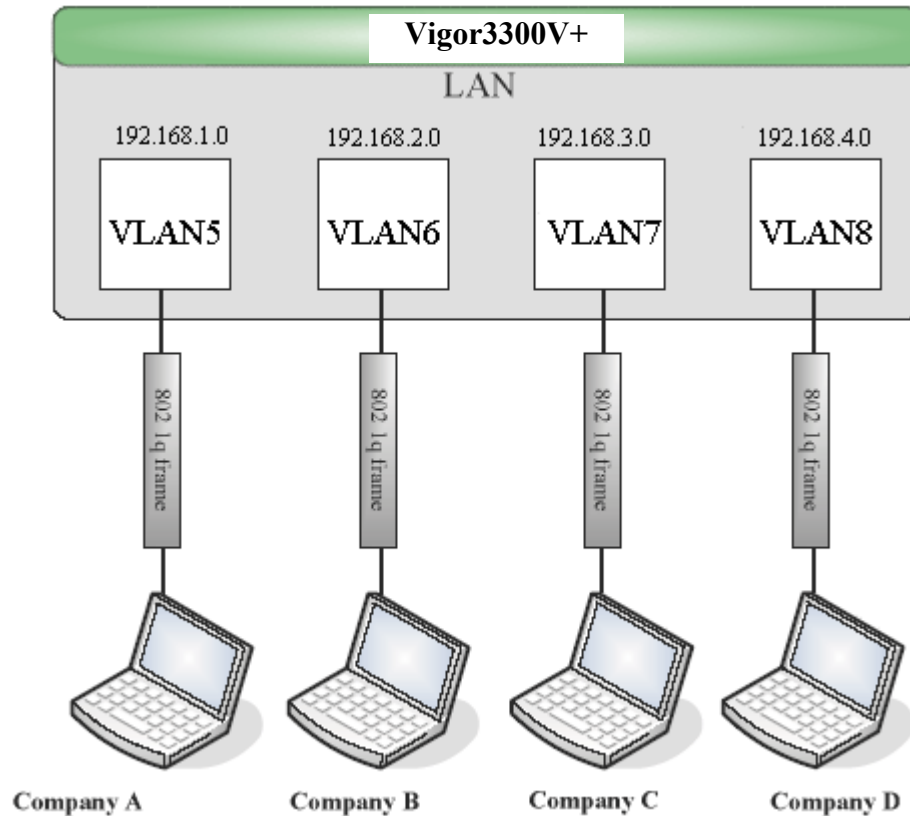
Port Setting

	P1	P2	P3	P4
Port VLAN ID	5	6	7	8

5. After applying the settings, the web page will be redirected to “reboot” web page. User can it and continue to configure the Network setting. After finishing Network setting, you can execute the reboot procedure.
6. After rebooting, the tagged ports will communicate with 802.1Q tagged devices only.
7. In the Network setting, type the subnet 192.168.1.0 to LAN. For example, the VLAN5 LAN IP is 192.168.1.1 and the Subnet Mask is 255.255.255.0. Then, users in the Engineer Department can set IP address from 192.168.1.2 to 192.168.1.254.
8. In the Network setting, type the subnet 192.168.2.0 to LAN2. For example, the VLAN6 LAN IP is 192.168.2.1 and the Subnet Mask is 255.255.255.0. Then, users in the other departments can set IP address from 192.168.2.2 to 192.168.2.254.

3.1.5 Example for the Companies in the Same Building

There are four companies in the same building. They share the broadband network and use the Vigor3300V+ router to achieve the load balance, security, and VoIP features. In this case, we can define four VLANs including VLAN5, VLAN6, VLAN7 and VLAN8. The subnet of VLAN5 is 192.168.1.0; the subnet of VLAN6 is 192.168.2.0; the subnet of VLAN7 is 192.168.3.0; and the subnet of VLAN8 is 192.168.4.0.



Procedure:

1. Refer to A.1 to block LAN-to-LAN communication.
2. Create VLAN5, VLAN6, VLAN7 and VLAN8 Groups.
3. In the VLAN5, type “5” to VLAN ID. In the Member field, choose p1. Then choose the “Tagged” for Frame Tag Operation in p1. We can ignore the PVID (Port VLAN ID), because 802.1q tag will be inserted to the frame from the PC of company A.
4. In the VLAN6, type “6” to VLAN ID. In the Member field, choose p2. Then choose the “Tagged” for Frame Tag Operation in p2. We can ignore the PVID (Port VLAN ID), because 802.1q tag will be inserted to the frame from company B.
5. In the VLAN7, type “7” to VLAN ID. In the Member field, choose p3. Then choose the “Tagged” for Frame Tag Operation in p3. We can ignore the PVID (Port VLAN ID), because 802.1q tag will be inserted to the frame from the PC of company C.

- In the VLAN8, type “8” to VLAN ID. In the Member field, choose p4. Then choose the “Tagged” for Frame Tag Operation in p4. We can ignore the PVID (Port VLAN ID), because 802.1q tag will be inserted to the frame from company D.

Advanced - LAN VLAN Setting

Disable
 Port Base VLAN
 802.1Q VLAN

Port Base VLAN: 802.1Q VLAN

Group

Index	Active	Name	VLAN ID	Member				Frame Tag Operation			
				P1	P2	P3	P4	P1	P2	P3	P4
1	<input checked="" type="checkbox"/>	VLAN5	5	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Tagged	Tagged	Tagged	Tagged
2	<input checked="" type="checkbox"/>	VLAN6	6	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Tagged	Tagged	Tagged	Tagged
3	<input checked="" type="checkbox"/>	VLAN7	7	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Tagged	Tagged	Tagged	Tagged
4	<input checked="" type="checkbox"/>	VLAN8	8	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Tagged	Tagged	Tagged	Tagged

Enable management port for P4

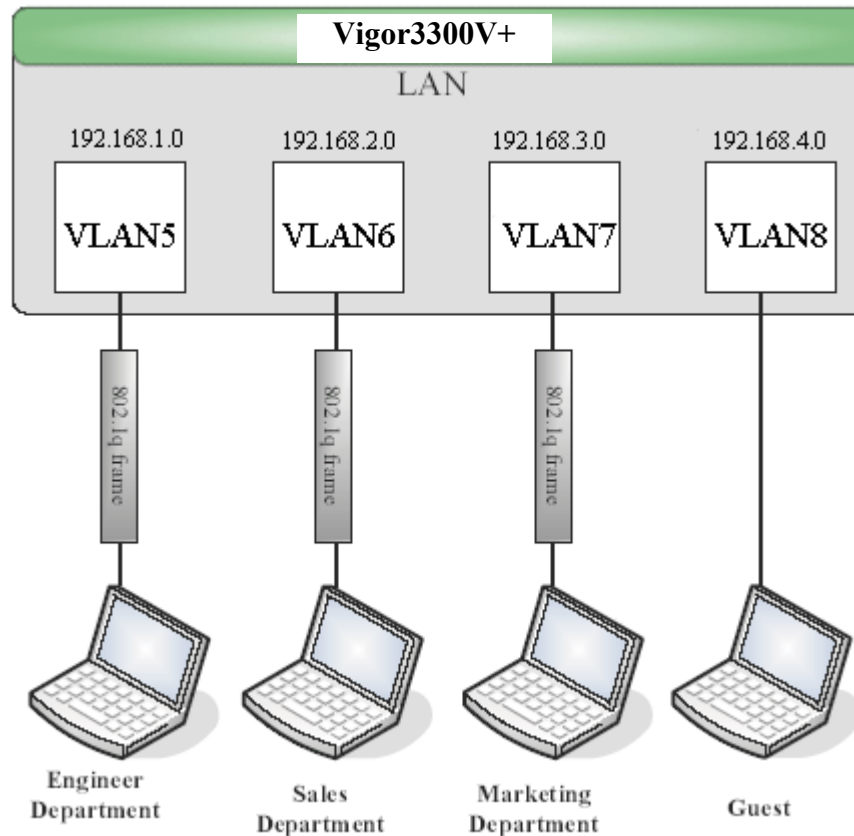
Port Setting

	P1	P2	P3	P4
Port VLAN ID	5	6	7	8

- After applying the settings, the web page will be redirect to “reboot” web page. User can ignore it and continue to configure the Network setting. After finishing Network setting, you can execute the reboot procedure.
- After rebooting, the tagged ports will communicate with 802.1Q tagged devices only.
- The network configuration is the same with A.2.1. Please refer to A.2.1.

3.1.6 Example for A Company and Guest

A company wants to separate the Engineer Department, Sales Department, Marketing Department and guest to limit their communication with any department to ensure the security. In this case, we can define four VLANs that are VLAN5, VLAN6, VLAN7 and VLAN8. The subnet of VLAN5 is 192.168.1.0; the subnet of VLAN6 is 192.168.2.0; the subnet of VLAN7 is 192.168.3.0; and the subnet of VLAN8 is 192.168.4.0. However, the notebook of guest does not support 802.1Q.



Procedure:

1. Refer to A.1 to block LAN-to-LAN communication.
2. Create VLAN5, VLAN6, VLAN7 and VLAN8 Groups.
3. In the VLAN5, type "5" to VLAN ID. In the Member field, choose p1. Then choose the "Tagged" for Frame Tag Operation in p1. We can ignore the PVID (Port VLAN ID), because 802.1q tag will be inserted to the frame from the PC of Engineer Department.
4. In the VLAN6, type "6" to VLAN ID. In the Member field, choose p2. Then choose the "Tagged" for Frame Tag Operation in p2. We can ignore the PVID (Port VLAN ID), because 802.1q tag will be inserted to the frame from Engineer Department.
5. In the VLAN7, type "7" to VLAN ID. In the Member field, choose p3. Then choose the "Tagged" for Frame Tag Operation in p3. We can ignore the PVID (Port VLAN ID), because 802.1q tag will be inserted to the frame from the PC of Engineer Department.

- In the VLAN8, type “8” to VLAN ID. In the Member field, choose p4. Then choose the “Untagged” for Frame Tag Operation in p4. We should configure the PVID to “8”, because the device does not support 802.1Q VLAN.

Advanced - LAN VLAN Setting

Disable
 Port Base VLAN
 802.1Q VLAN

Port Base VLAN: **802.1Q VLAN**

Group

Index	Active	Name	VLAN ID	Member				Frame Tag Operation			
				P1	P2	P3	P4	P1	P2	P3	P4
1	<input checked="" type="checkbox"/>	VLAN5	5	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Tagged	Tagged	Tagged	Tagged
2	<input checked="" type="checkbox"/>	VLAN6	6	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Tagged	Tagged	Tagged	Tagged
3	<input checked="" type="checkbox"/>	VLAN7	7	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Tagged	Tagged	Tagged	Tagged
4	<input checked="" type="checkbox"/>	VLAN8	8	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Tagged	Tagged	Tagged	Untagged

Enable management port for P4

Port Setting

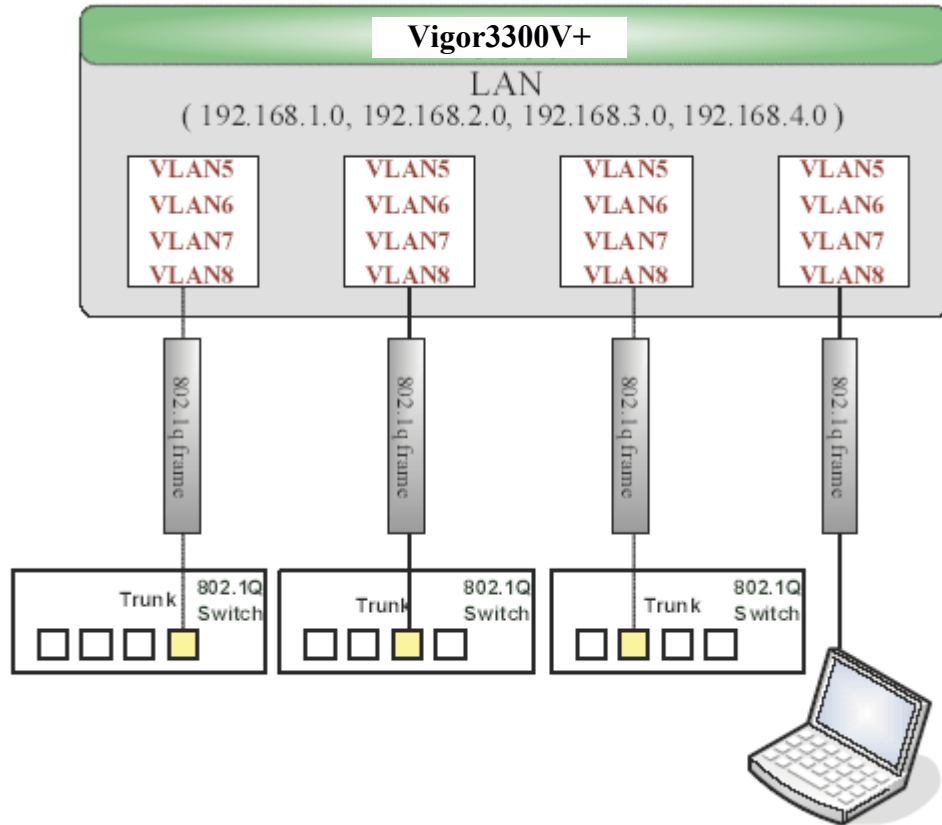
	P1	P2	P3	P4
Port VLAN ID	5	6	7	8

Apply Reset Cancel

- After applying the settings, the web page will be redirected to “reboot” web page. User can ignore it and continue to configure the Network setting. After finishing Network setting, you can execute the reboot procedure.
- After rebooting, the tagged ports will communicate with 802.1Q tagged devices only.
- The network configuration is the same with A.2.1. Please refer to A.2.1 part.

3.1.7 Example for Trunk Usage

A company wants to separate the Engineer Department, Sales Department, Marketing Department and other departments to limit their communication with each other to ensure the security. Many employees of the company use some switches supported 802.1Q VLAN to expand the network. In this case, we can define four VLANs that are VLAN5, VLAN6, VLAN7 and VLAN8. Each LAN port is Trunk port which supports multiple VLAN. The subnet of VLAN5 is 192.168.1.0; the subnet of VLAN6 is 192.168.2.0; the subnet of VLAN7 is 192.168.3.0 and the subnet of VLAN8 is 192.168.4.0.



Procedure:

1. Refer to A.1 to block LAN-to-LAN communication.
2. Create VLAN5, VLAN6, VLAN7 and VLAN8 Groups.
3. In the VLAN5, input “5” to VLAN ID. In the Member field, choose p1, p2, p3 and p4. Then choose the “Tagged” for Frame Tag Operation in p1, p2, p3 and p4. We can ignore the PVID (Port VLAN ID), because 802.1q tag will be inserted to the frame from the switch.
4. In the VLAN6, type “6” to VLAN ID. In the Member field, choose p1, p2, p3 and p4. Then choose the “Tagged” for Frame Tag Operation in p1, p2, p3 and p4. We can ignore the PVID (Port VLAN ID), because 802.1q tag will be inserted to the frame from switch.
5. In the VLAN7, type “7” to VLAN ID. In the Member field, choose p1, p2, p3 and p4. Then choose the “Tagged” for Frame Tag Operation in p1, p2, p3 and p4. We can

ignore the PVID (Port VLAN ID), because 802.1q tag will be inserted to the frame from the switch.

- In the VLAN8, type “8” to VLAN ID. In the Member field, choose p1, p2, p3 and p4. Then choose the “Tagged” for Frame Tag Operation in p1, p2, p3 and p4. We can ignore the PVID (Port VLAN ID), because 802.1q tag will be inserted to the frame from some users.

Advanced - LAN VLAN Setting

Disable
 Port Base VLAN
 802.1Q VLAN

Port Base VLAN: **802.1Q VLAN**

Group

Index	Active	Name	VLAN ID	Member				Frame Tag Operation			
				P1	P2	P3	P4	P1	P2	P3	P4
1	<input checked="" type="checkbox"/>	VLAN5	5	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Tagged	Tagged	Tagged	Tagged
2	<input checked="" type="checkbox"/>	VLAN6	6	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Tagged	Tagged	Tagged	Tagged
3	<input checked="" type="checkbox"/>	VLAN7	7	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Tagged	Tagged	Tagged	Tagged
4	<input checked="" type="checkbox"/>	VLAN8	8	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Tagged	Tagged	Tagged	Tagged

Enable management port for P4

Port Setting

	P1	P2	P3	P4
Port VLAN ID	5	6	7	8

Apply Reset Cancel

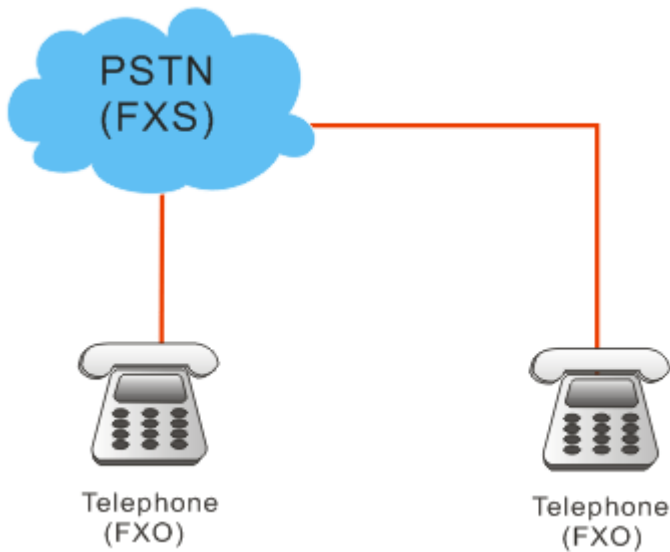
- After applying the settings, the web page will be redirected to “reboot” web page. User can ignore it and continue to configure the Network setting. After finishing Network setting, you can execute the reboot procedure.
- After rebooting, the tagged ports will communicate with 802.1Q tagged devices only.
- The network configuration is the same with A.2.1. Please refer to A.2.1 part.

3.2 Application for VoIP

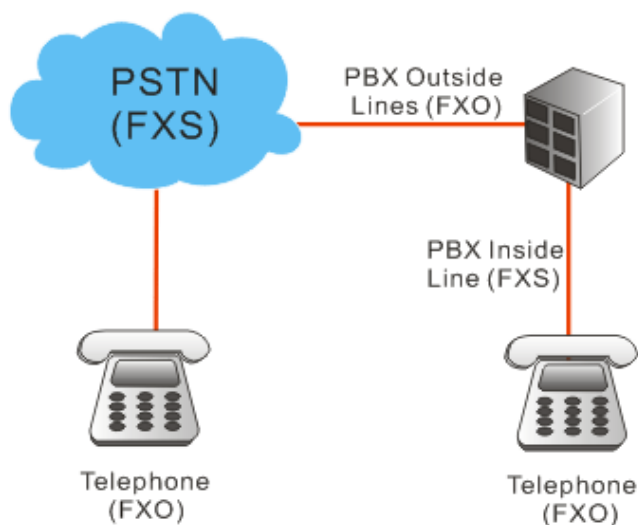
3300V+ has two expansion slots; each slot can be plugged into 4-port VoIP card, ISDN-NTTE or ISDN-TE card. The VoIP card involves two kinds of interface: FXS and FXO. The ISDN-NTTE card involves two kinds of interface: NT for port 1 and 3; TE or NT (user configurable) for port 2 and 4. And ISDN-TE card involves 4-port TE mode. You can deploy different VoIP/ISDN applications according to the requirements.

3.2.1 FXS and FXO

FXS (Foreign eXchange Station) and FXO (Foreign eXchange Office) are assembled with a pair. A telecommunications line from an FXO device must be connected to an FXS device. Similarly, an FXS device must be connected to an FXO device. For example, PSTN is FXS equipment, and a telephone is FXO equipment.



As for the Private Branch Exchange (PBX), it is more special because it has both FXS and FXO devices at the same time. Outside lines of the PBX are usually connected to the phone line, at this case, the PBX acts as FXO equipment; inside lines of the PBX are usually connected to telephones, so the PBX acts as FXS equipment.



FXS equipment

PSTN or inside lines of PBX

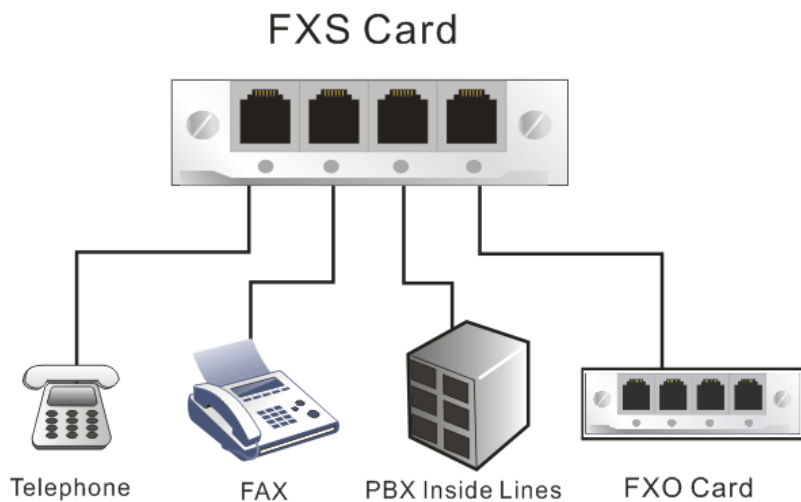
FXO equipment

Telephones, FAX machines and outside lines of PBX.

Based on the characteristics described above that the FXS equipment and the FXO equipment must connect with each other, please pay special attention when you use FXS card and FXO card.

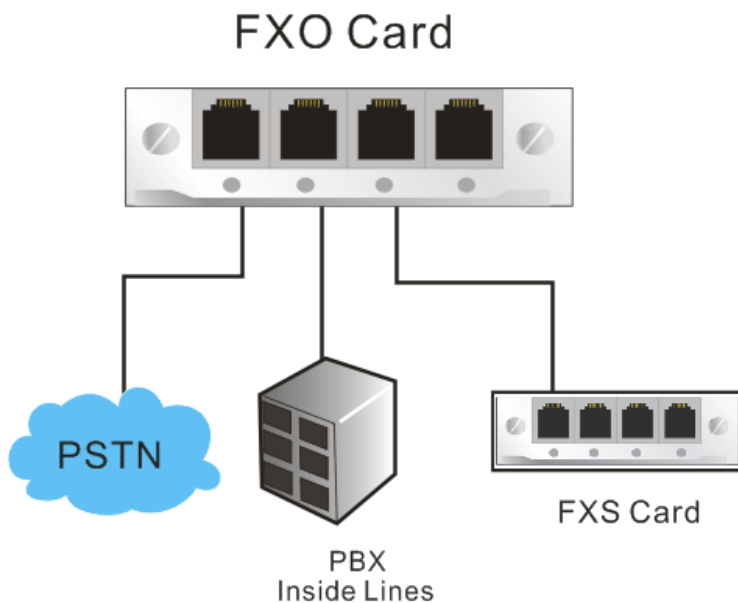
FXS card

This card can connect to the telephone, FAX machine, outside lines of PBX and FXO port on FXO card.



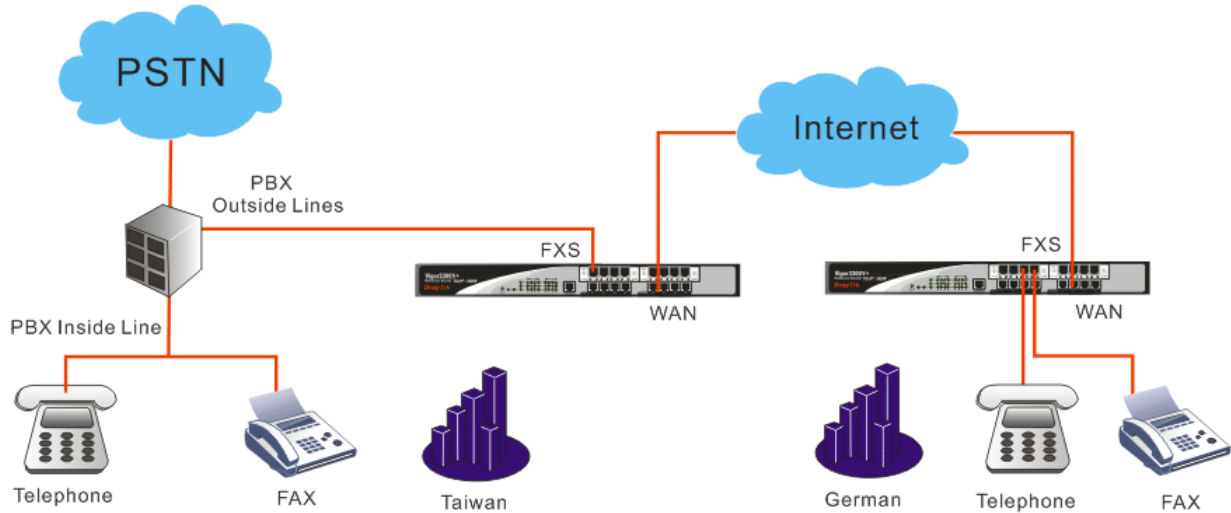
FXO card

This card can connect to PSTN, inside lines of PBX and FXS port on FXS cards.



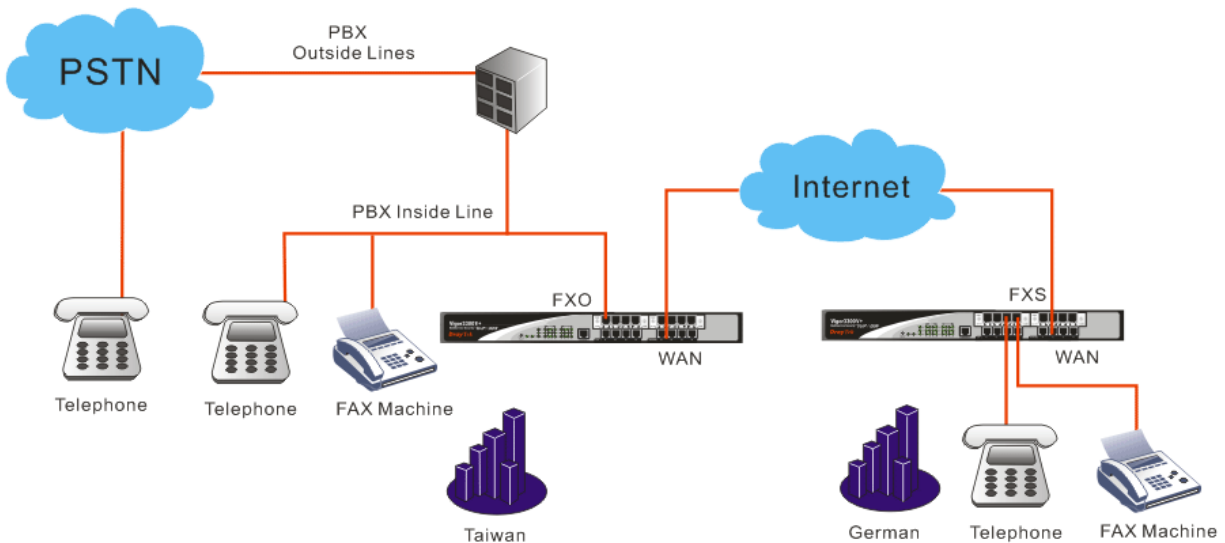
3.2.2 Practical Application of FXS card with PBX

By combining the FXS with headquarters' PBX, it allows the internal telephones in headquarters to communicate with branch's telephones through the Internet. (For detailed configuration, please refer to VoIP and ISDN examples.)



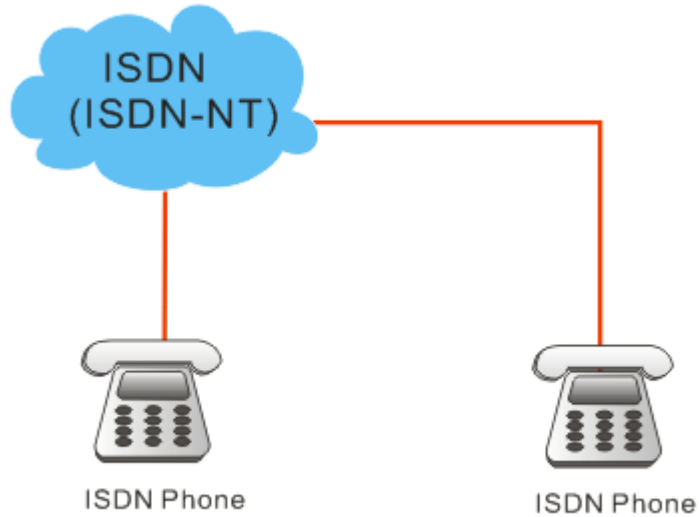
3.2.3 Practical Application of FXO card with PBX

By combining the FXO with headquarters' PBX, it allows the branch's telephones to connect to Headquarters' PBX via the Internet, and communicate with the customers via the PBX. Another application is that you can call back to the Headquarters from outside, and communicate with the branch via the Internet. (For detailed configuration, please refer to VoIP and ISDN examples.)

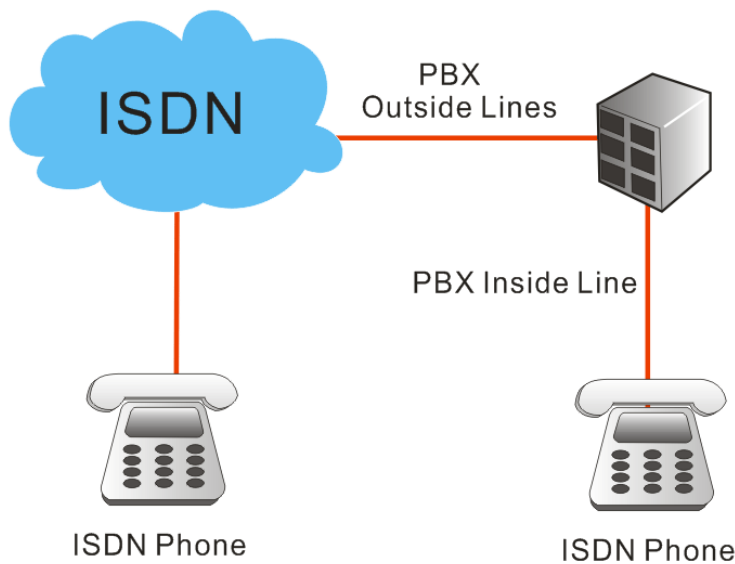


3.2.4 ISDN NT and TE

NT means Network Terminal. The ISDN port in NT mode is a port that used to connect general ISDN phones. And TE means Terminal Equipment. The ISDN port in TE mode is a port that used to connect ISDN line or ISDN PBX.



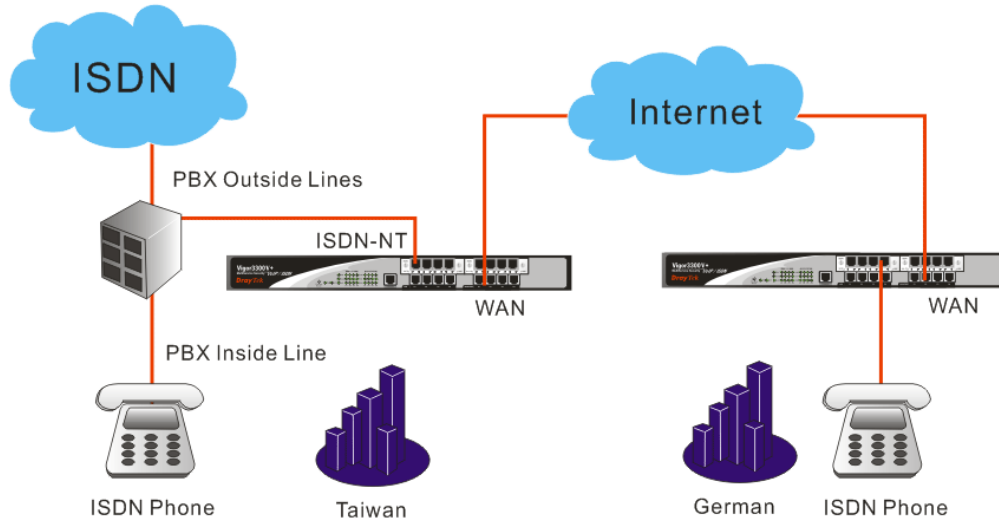
As for the Private Branch Exchange (PBX), it is more special because it has both ISDN-NT and ISDN-TE devices at the same time. Outside lines of the PBX are usually connected to the ISDN line, at this case, the PBX acts as ISDN-TE equipment; inside lines of the PBX are usually connected to telephones, so the PBX acts as ISDN-NT equipment.



Based on the characteristics described above that the ISDN-NT equipment and the ISDN-TE equipment must connect with each other, please pay special attention when you use ISDN-NT card and ISDN-TE card.

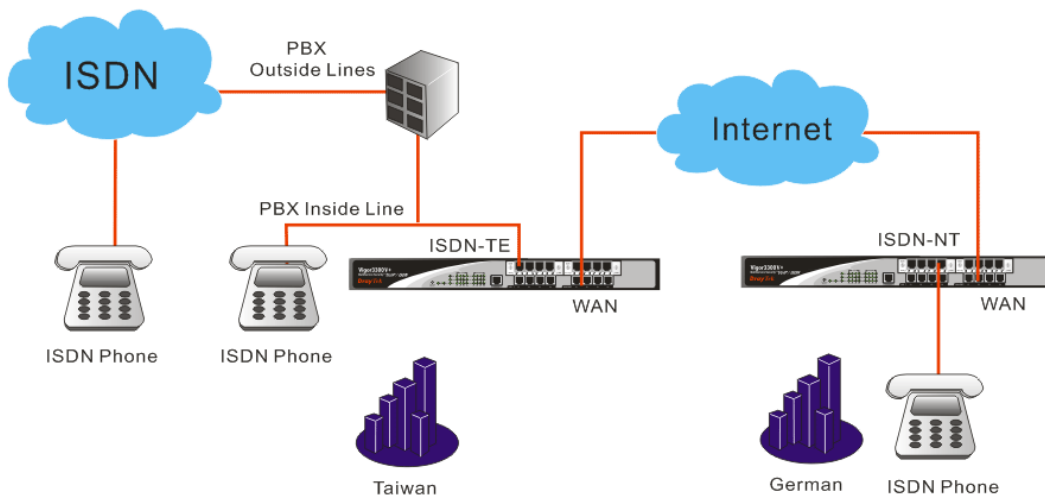
3.2.5 Practical Application of ISDN-NT with PBX

By combining the ISDN-NT with headquarters' PBX, it allows the internal telephones in headquarters to communicate with branch's telephones through the Internet. (For detailed configuration, please refer to VoIP and ISDN examples.)



3.2.6 Practical Application of ISDN-TE with PBX

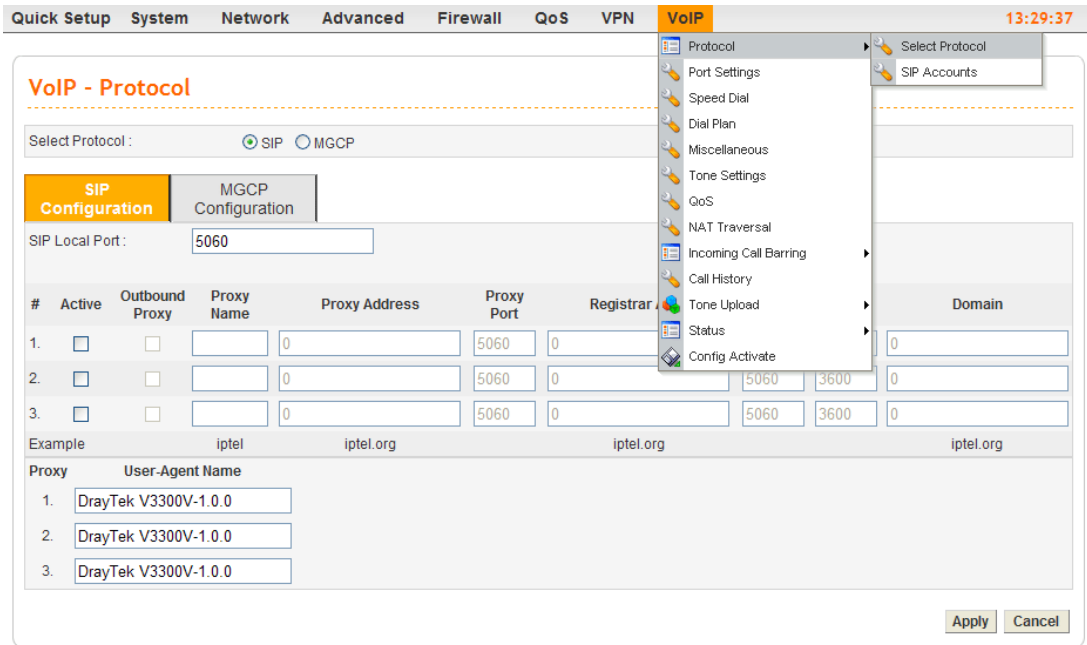
By combining the ISDN-TE with headquarters' PBX, it allows the branch's telephones to connect to Headquarters' PBX via the Internet, and communicate with the customers via the PBX. Another application is that you can call back to the Headquarters from outside, and communicate with the branch via the Internet. (For detailed configuration, please refer to VoIP and ISDN examples.)



3.2.7 VoIP Basic

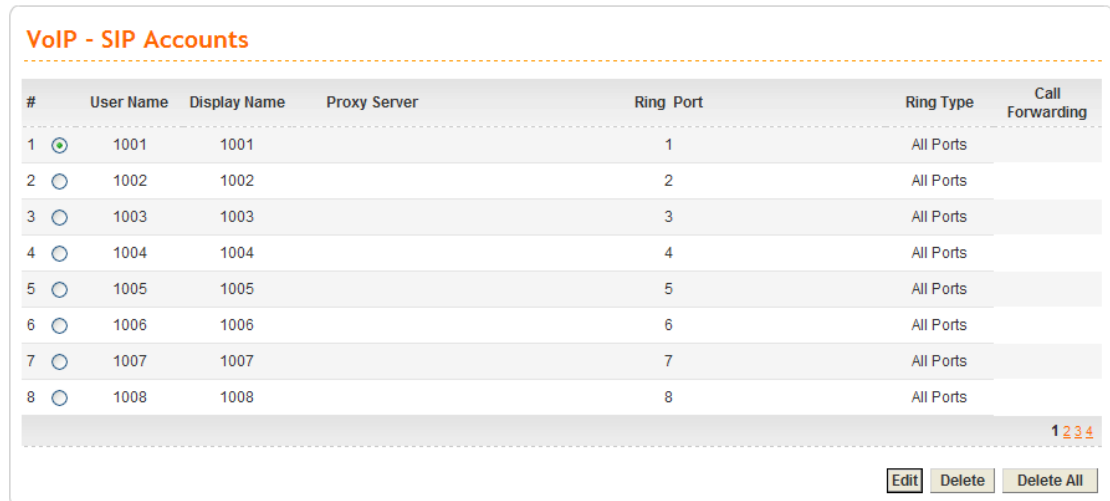
Protocol – Select Protocol

Select the communication protocol (SIP or MGCP) and the IP Address (WAN or LAN/VPN) used by VoIP. You need to configure relative settings at first. Please refer to the figure below as an example of Vigor 3300V+.



Protocol – SIP Accounts

Router provides default configuration for SIP accounts. You can click any one of the radio buttons and click Edit to modify the SIP account for your necessity.



Port Settings

This page displays the basic settings for each port. Click the **Edit** icon in the **Phone Number** page to enter the **Edit** page. Then you can configure this port.

VoIP - Port Settings

#	Edit	Type	Active	SIP Account	Supplemental Service	Hotline	Mic/Spk Gain	FAX	Codec	DTMF
1		ISDN-NT	V	1 - 1001			0 / 0	Transparent	G.729A	RFC2833
2		ISDN-TE	V	2 - 1002			0 / 0	Transparent	G.729A	RFC2833
3		ISDN-NT	V	3 - 1003			0 / 0	Transparent	G.729A	RFC2833
4		ISDN-TE	V	4 - 1004			0 / 0	Transparent	G.729A	RFC2833
5										
6										
7										
8										

OR

VoIP - Port Settings

#	Edit	Type	Active	SIP Account	Supplemental Service	Hotline	Mic/Spk Gain	FAX	Codec	DTMF
1		FXS	V	1 - 1001			0 / 0	Transparent	G.729A	RFC2833
2		FXS	V	2 - 1002			0 / 0	Transparent	G.729A	RFC2833
3		FXS	V	3 - 1003			0 / 0	Transparent	G.729A	RFC2833
4		FXS	V	4 - 1004			0 / 0	Transparent	G.729A	RFC2833
5		FXO	V	5 - 1005			0 / 0	Transparent	G.729A	RFC2833
6		FXO	V	6 - 1006			0 / 0	Transparent	G.729A	RFC2833
7		FXO	V	7 - 1007			0 / 0	Transparent	G.729A	RFC2833
8		FXO	V	8 - 1008			0 / 0	Transparent	G.729A	RFC2833

Port Settings - Port – Edit

Configure related VoIP settings for each port respectively.

VoIP - Port Settings - Port1 - Edit

Port 1 (FXS)

Disable Enable

Default SIP Accounts:

VoIP IP Address:

Hotline

Hotline Number to Internet:

Hotline Number to PBX: (p:delay 1.8sec)

FXO

Manual Disconnection:

Codec

Preferred Codec:

Single Codec:

Codec Rate: (ms)

Codec VAD: Disable Enable

CAS

Microphone Gain: (Range: -14 ~ 6)

Speaker Gain: (Range: -14 ~ 6)

FAX

FAX Mode:

FAX Bypass Codec:

FAX Bypass Codec Rate: (ms)

DTMF

DTMF Mode: InBand OutBand(RFC2833) SIP INFO

DTMF Volume: (Range: 0 ~ 31)

Supplemental Service

Disable Enable

Speed Dial

Setup the Speed Dial Phone numbers, this function is more convenient to dial extension number or IP address. There are 150 entries available at most.

Quick Setup System Network Advanced Firewall QoS VPN **VoIP** 13:27:50

VoIP - Speed Dial

#	Speed Dial Phone Number	Speed Dial Destination	Memo
1	<input type="text"/>	<input type="text"/>	<input type="text"/>
2	<input type="text"/>	<input type="text"/>	<input type="text"/>
3	<input type="text"/>	<input type="text"/>	<input type="text"/>
4	<input type="text"/>	<input type="text"/>	<input type="text"/>
5	<input type="text"/>	<input type="text"/>	<input type="text"/>

Example 101 101@iptel.org

1 2 3 4 5 6 7 8 9 10 >

Apply Cancel Clear This Page

Dial Plan

It can simplify the dial process. There are 60 dial plan entries available at most.

Quick Setup System Network Advanced Firewall QoS VPN **VoIP** 10:49:31

VoIP - Dial Plan

#	Match String	Min Length	Max Length	Prefix Strip	Prefix Add	Time Out	Memo
1	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
2	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
3	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
4	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
5	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
6	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
7	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
8	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
9	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
10	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>

1

Edit Delete Delete All

Miscellaneous

Other related VoIP settings.

Quick Setup System Network Advanced Firewall QoS VPN **VoIP** 13:25:49

VoIP - Miscellaneous

RTP Starting Port:

T.38 Starting Port:

T.38 Redundancy number: (Range: 0~4)

Dialing Completion Timeout: sec (Range: 1~60)

VoIP ToS:

Line Polarity Reversal: as Callee on-hook as Callee Answer

FXO auto disconnection if no packet is received in seconds. (Range: 5~3600, 0: no auto disconnection)

FXS On-hook Tip/Ring Voltage:

FXS Ringing

Ringing Frequency: (HZ)

Ringing Cadence - On: (msec)

Ringing Cadence - Off: (msec)

Apply Cancel

Tone Settings

There are optional built-in 15 groups of tone for different regions, and a group of tone (User Defined) can be configured by users.

Quick Setup System Network Advanced Firewall QoS VPN **VoIP** 13:24:36

VoIP - Tone Settings

Region: Caller ID Type:

Tone Classification	Low Frequency(Hz)	High Frequency(Hz)	On2 (msec)	Toff2 (10msec)
Dial tone	<input type="text" value="350"/>	<input type="text" value="440"/>	<input type="text" value="5"/>	<input type="text" value="0"/>
Ringing tone	<input type="text" value="440"/>	<input type="text" value="480"/>	<input type="text" value="0"/>	<input type="text" value="400"/>
Busy tone	<input type="text" value="480"/>	<input type="text" value="620"/>	<input type="text" value="0"/>	<input type="text" value="50"/>
Congestion tone	<input type="text" value="480"/>	<input type="text" value="620"/>	<input type="text" value="0"/>	<input type="text" value="25"/>

Tone Timer

Dial Tone: Busy Tone: Howler Tone: Ringing Tone:

Special Dial Tone: Call Waiting Tone: Congestion Tone: Reorder Tone:

Apply Cancel

QoS

Enable this function to ensure the quality of VoIP conversation. The default value is **Enable**.

Quick Setup System Network Advanced Firewall QoS VPN VoIP 13:23:28

VoIP - QoS

Disable (non-guaranteed voice quality, higher data throughput)

Enable (guaranteed voice quality, normal data throughput)

Advanced QoS

Link Fragmentation and Interleaving: (For uplink bandwidth < 768 kbps)

Apply Cancel

DrayTek Corp. © 1997 Enterprise Network Solutions.

NAT Traversal

When the WAN interface of Vigor3300+ is a private IP address, the VoIP traffics must pass through the upper-layer NAT router. User can enable STUN function in order to make VoIP function can work smoothly.

Quick Setup System Network Advanced Firewall QoS VPN VoIP 13:22:32

VoIP - NAT Traversal

NAT Traversal

Disable

Manually Input NAT IP Address

NAT IP Address :

Auto Discover NAT IP Address

Semi-auto, need to config NAT

STUN Local Port :

STUN Server Address :

STUN Server Port :

Symmetric Media

Disable symmetric RTP and T.38 Enable symmetric RTP and T.38

NAT Status

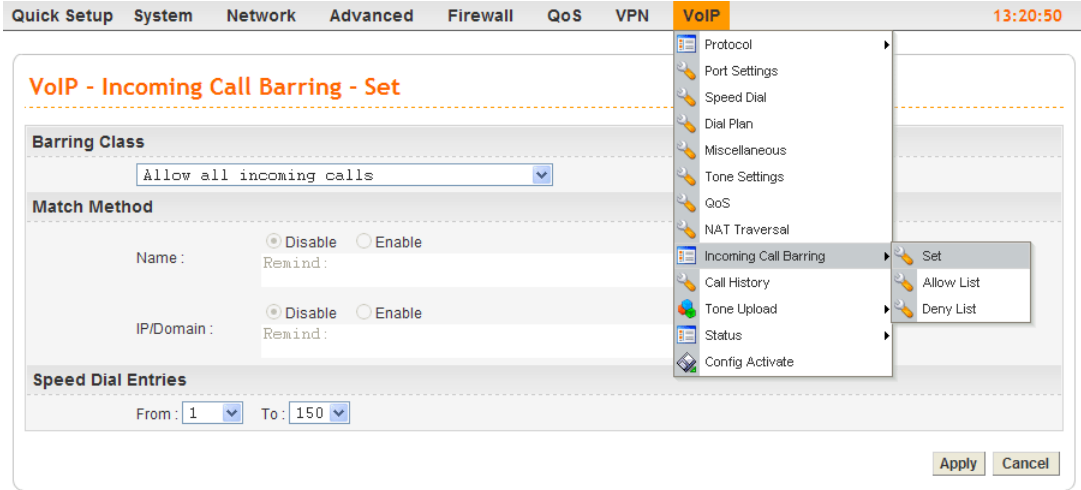
NAT Type: N/A, Local IP Address: 127.0.0.1, WAN IP Address: 127.0.0.1

Apply Cancel

Note: The upper-layer router must forward the UDP packets with port number 5060 (for SIP protocol), 13456~13486 (for RTP) and 49170~49200 (for T.38) to the WAN IP address of Vigor3300V+. Users can define the port number(s) for their necessity.

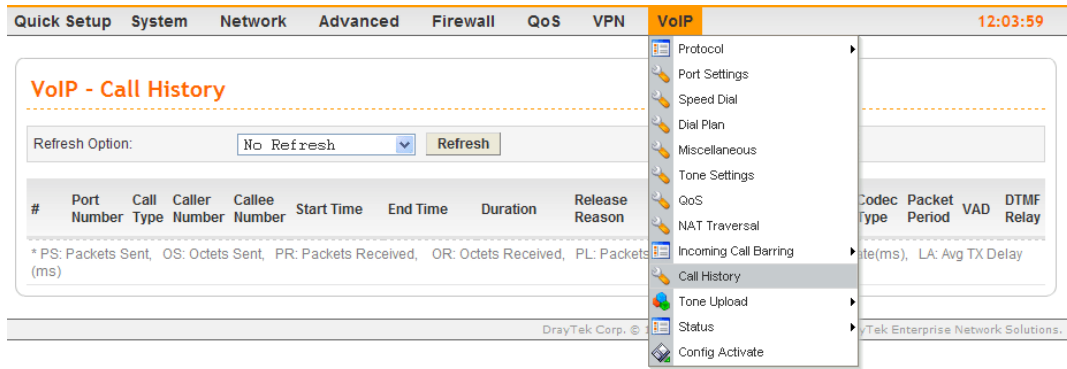
Incoming Call Barring – Set

This function can receive or reject the specific VoIP calling via Internet. The rules are based on the speed dial number or IP/Domain.



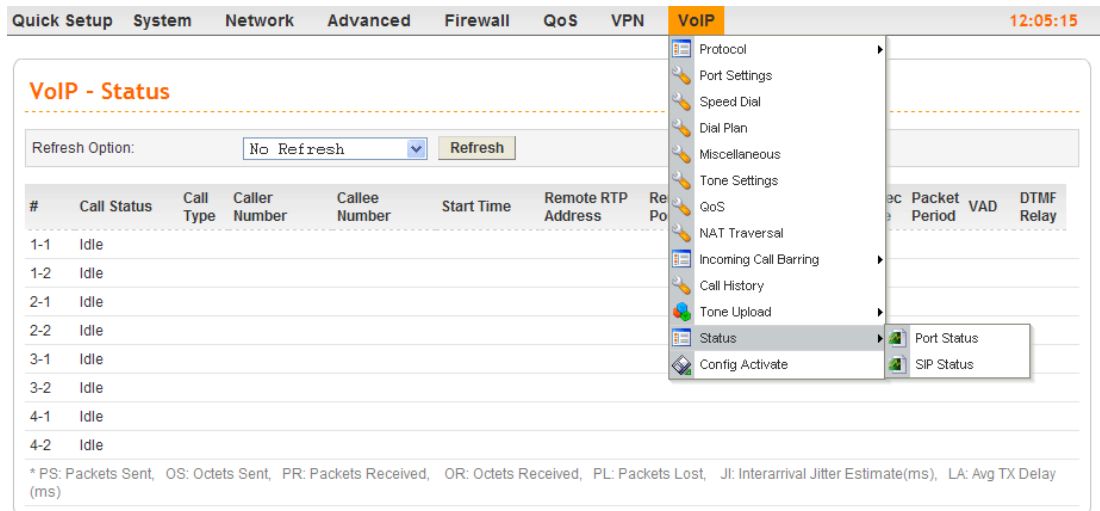
Call History

It can display 50 groups of calling information.



Status

Display current VoIP registering status and calling status.



3.3 VoIP and ISDN Examples

There are many different kinds of applications about VoIP function. Most of VoIP callings must be via a VoIP Server by registering, except we can dial VoIP number by the IP address directly. We will set up a basic configuration and registration as an example 1. The other examples might be revised based on this example.

The VoIP function mainly depends on the requirement and application. All the examples are based on example 1 to revise configuration in accordance with the usage requirement and application.

Example 1: Basic Configuration and Registration

Example 2: Basic Configuration and Registration for ISDN

Example 3: Basic Calling Method

Example 4: VoIP over VPN

Example 5: Practical Application of FXS

Example 6: Practical Application of FXO

Example 7: Practical Application of ISDN-NT

Example 8: Practical Application of ISDN-TE

3.3.1 Example 1 - Basic Configuration and Registration

In this case, Vigor3300V+ uses a FXS card and a FXO card with four groups of “iptel” numbers and “fwd” numbers respectively. The Codec is G.729A. WAN IP address is 220.135.240.207. 2910V has two VoIP Ports with an iptel number and the fwd number respectively. The Codec is G.729A, and the WAN IP is 61.31.167.135.

Basic settings in Vigor 3300V+ and 2910V

	WAN IP	Port Number	Phone Number	Proxy	Codec
3300V+	220.135.240.207	Port1(FXS)	888833	iptel	G.729A
		Port2(FXS)	888834	iptel	G.729A
		Port3(FXS)	660533	fwd	G.729A
		Port4(FXS)	660534	fwd	G.729A
		Port5(FXO)	888835	iptel	G.729A
		Port6(FXO)	888836	iptel	G.729A
		Port7(FXO)	660525	fwd	G.729A
		Port8(FXO)	660526	fwd	G.729A
2910V	61.31.167.135	Port1(FXS)	888829	iptel	G.729A
		Port2(FXS)	660529	fwd	G.729A

	Proxy	Domain	Port
iptel	iptel.org	iptel.org	5060
fwd	fwd.pulver.com	fwd.pulver.com	5060

Configuration Example for Vigor3300V+

1. Enter **VoIP - Protocol** page and configure related settings on SIP Configuration.

#	Active	Outbound Proxy	Proxy Name	Proxy Address	Proxy Port	Registrar Addr	Registrar Port	Expires (sec)	Domain
1	<input checked="" type="checkbox"/>	<input type="checkbox"/>	iptel	iptel.org	5060	iptel.org	5060	300	iptel.org
2	<input checked="" type="checkbox"/>	<input type="checkbox"/>	fwd	fwd.puheer.com	5060	fwd.puheer.com	5060	300	fwd.puheer.com
3	<input type="checkbox"/>	<input type="checkbox"/>			5060		5060	300	

2. Set SIP accounts (e.g., username and proxy server) by referring to the table “Basic settings in Vigor 3300V+ and 2910V” on last page.

3. Enter **VoIP - Port Settings** page, click the **Edit** icon of port 1.

#	Edit	Type	Active	SIP Account	Supplemental Service	Hotline	Mic/Spk Gain	FAX	Codec	DTMF
1		FXS	V	1 - 888833			0 / 0	Transparent	G.729A	RFC2833
2		FXS	V	2 - 888834			0 / 0	Transparent	G.729A	RFC2833
3		FXS	V	3 - 660533			0 / 0	Transparent	G.729A	RFC2833
4		FXS	V	4 - 660534			0 / 0	Transparent	G.729A	RFC2833
5		FXO	V	5 - 888835			0 / 0	Transparent	G.729A	RFC2833
6		FXO	V	6 - 888836			0 / 0	Transparent	G.729A	RFC2833
7		FXO	V	7 - 660525			0 / 0	Transparent	G.729A	RFC2833
8		FXO	V	8 - 660526			0 / 0	Transparent	G.729A	RFC2833

4. Enter the **Port 1** page. This page falls into six sections.
Port1 (FXS) Display the port type, **enable** or **disable** the port, choose the SIP account, and etc.

5. Set Port 2 ~ Port 8 one by one in turn.
Type: Port 1 ~Port 4 are **FXS**, Port 5 ~Port 8 are **FXO**.
Active: Port 1 ~Port 8 are all **active** (v=Enable).
SIP Account: Accounts of Port 1 ~ Port 8.
Codec: Port 1 ~Port 8 all prior use **G.729A - 8kbps**.

VoIP - Port Settings

#	Edit	Type	Active	SIP Account	Supplemental Service	Hotline	Mic/Spk Gain	FAX	Codec	DTMF
1		FXS	V	1 - 1001			0 / 0	Transparent	G.729A	RFC2833
2		FXS	V	2 - 1002			0 / 0	Transparent	G.729A	RFC2833
3		FXS	V	3 - 1003			0 / 0	Transparent	G.729A	RFC2833
4		FXS	V	4 - 1004			0 / 0	Transparent	G.729A	RFC2833
5		FXO	V	5 - 1005			0 / 0	Transparent	G.729A	RFC2833
6		FXO	V	6 - 1006			0 / 0	Transparent	G.729A	RFC2833
7		FXO	V	7 - 1007			0 / 0	Transparent	G.729A	RFC2833
8		FXO	V	8 - 1008			0 / 0	Transparent	G.729A	RFC2833

6. Check the VoIP Status. Please enter the **VoIP – Status - SIP Status** page first and wait one or two minutes (The time depends on SIP Server's response speed and the network condition). **OK** means the registration is successful; **Failed** means the registration is failed.

VoIP -SIP Status

Refresh Option:

#	Register Status	#	Register Status	#	Register Status	#	Register Status
1		9		17		25	
2		10		18		26	
3		11		19		27	
4		12		20		28	
5		13		21		29	
6		14		22		30	
7		15		23		31	
8		16		24		32	

Next, please enter **VoIP – Status - Port Status**. This page will display calling information from Port 1 ~ Port 8. **Idle** means there is no conversations on Port 1 ~ Port 8.

VoIP - Status

Refresh Option:

#	Call Status	Call Type	Caller Number	Callee Number	Start Time	Remote RTP Address	Remote RTP Port	RTP Statistic	Codec Type	Packet Period	VAD	DTMF Relay
1-1	Idle											
2-1	Idle											
3-1	Idle											
4-1	Idle											
5-1	Idle											
6-1	Idle											
7-1	Idle											
8-1	Idle											

* PS: Packets Sent, OS: Octets Sent, PR: Packets Received, OR: Octets Received, PL: Packets Lost, JI: Interarrival Jitter Estimate(ms), LA: Avg TX Delay(ms)

Note: This page will automatically refresh based on the setting configured in **Refresh Option**. You may click **Refresh** button to renew immediately.

Configuration Example for Vigor2910V

1. Open the Web interface of the router and open **VoIP** menu.

The screenshot shows the web interface of a Vigor2910 Series Dual-WAN Security Router. The left sidebar contains navigation options: Quick Start Wizard, Online Status, WAN, LAN, NAT, Firewall, Objects Setting, CSM, Bandwidth Management, Applications, VPN and Remote Access, Certificate Management, VoIP, ISDN, Wireless LAN, VLAN, USB Application, System Maintenance, and Diagnostics. The main content area displays the System Status page with the following information:

System Status

Model Name : DrayTek Vigor2910
 Firmware Version : 3.2.1_RC2
 Build Date/Time : Tue Jul 29 18:35:51.48 2008

System	
CPU Usage	: 2 %
Total Memory	: 16M
Memory usage	: 61 %

LAN	
MAC Address	: 00-50-7F-DD-15-18
1st IP Address	: 192.168.1.1
1st Subnet Mask	: 255.255.255.0
DHCP Server	: Yes
Primary DNS	:
Secondary DNS	:

VoIP	
Port	: 1 2
SIP registrar	:
Account ID	: change_me change_me
Register	:
Codec	:
In Calls	: 0 0
Out Calls	: 0 0

WAN 1	
Link Status	: Connected
MAC Address	: 00-50-7F-DD-15-19
Connection	: Static IP
IP Address	: 172.16.3.229
Default Gateway	: 172.16.3.4
Primary DNS	:
Secondary DNS	:

WAN 2	
Link Status	: Disconnected
MAC Address	: 00-50-7F-DD-15-1A
Connection	: ---
IP Address	: ---
Default Gateway	: ---
Primary DNS	:
Secondary DNS	:

Wireless LAN	
Register	:
MAC Address	: 00-14-85-08-69-19
Frequency Domain	: Europe
Firmware Version	: v2.01.10.10.5.4

Click **SIP Account**.

The screenshot shows the VoIP menu with the following options:

- VoIP
 - ▶ DialPlan
 - ▶ SIP Accounts
 - ▶ Phone Settings
 - ▶ Status

Configure Port1 and Port2 by clicking Index number 1 and 2.

VoIP >> SIP Accounts

SIP Accounts List Refresh

Index	Profile	Domain/Realm	Proxy	Account Name	Ring Port	Status
<u>1</u>				change_me	<input type="checkbox"/> VoIP1 <input type="checkbox"/> VoIP2 <input type="checkbox"/> ISDN	-
<u>2</u>				change_me	<input type="checkbox"/> VoIP1 <input type="checkbox"/> VoIP2 <input type="checkbox"/> ISDN	-
<u>3</u>				change_me	<input type="checkbox"/> VoIP1 <input type="checkbox"/> VoIP2 <input type="checkbox"/> ISDN	-
<u>4</u>				change_me	<input type="checkbox"/> VoIP1 <input type="checkbox"/> VoIP2 <input type="checkbox"/> ISDN	-
<u>5</u>				change_me	<input type="checkbox"/> VoIP1 <input type="checkbox"/> VoIP2 <input type="checkbox"/> ISDN	-
<u>6</u>				change_me	<input type="checkbox"/> VoIP1 <input type="checkbox"/> VoIP2 <input type="checkbox"/> ISDN	-

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

NAT Traversal Setting

STUN server:	<input type="text" value="stun.fwdnet.net"/>
External IP:	<input type="text"/>
SIP PING interval:	<input type="text" value="150"/> sec

OK

Type relevant SIP Servers used for registration respectively.

VoIP >> SIP Accounts

SIP Account Index No. 1

Profile Name	<input type="text" value="test"/> (11 char max.)
Register via	WAN <input type="checkbox"/> make call without register
SIP Port	<input type="text" value="5060"/>
Domain/Realm	<input type="text" value="iptel.org"/> (63 char max.)
Proxy	<input type="text" value="iptel.org"/> (63 char max.)
<input type="checkbox"/> Act as outbound proxy	
Display Name	<input type="text" value="2910V_Port1_iptel"/> (23 char max.)
Account Number/Name	<input type="text" value="888829"/> (63 char max.)
<input type="checkbox"/> Authentication ID	<input type="text" value="888829"/> (63 char max.)
Password	<input type="text" value="****"/> (63 char max.)
Expiry Time	1 hour <input type="text" value="3600"/> sec
NAT Traversal Support	None
Ring Port	<input checked="" type="checkbox"/> VoIP1 <input type="checkbox"/> VoIP2 <input type="checkbox"/> ISDN
Ring Pattern	1

After configuration, please click **OK** to save the settings. 2910 series will go to **VoIP >>SIP Account** page automatically.

1. Open **VoIP>>Status**.



2. Wait one or two minutes (The time depends on SIP Server's response speed and the network condition).

Channel: **R** means Port 1 and Port 2 register successfully.

Status: **IDLE** means there is no conversations on Port 1~ Port 8.

VoIP >> Status

Status Refresh Seconds:

Port	Status	Codec	PeerID	Elapse (hh:mm:ss)	Tx Pkts	Rx Pkts	Rx Losts	Rx Jitter (ms)	In Calls	Out Calls	Speaker Gain
FXO	R			00:00:00	0	0	0	0	0	0	5
FXO	R			00:00:00	0	0	0	0	0	0	5

Now the configuration is completed.

3.3.2 Example 2 - Basic Configuration and Registration for ISDN

In this case, Vigor3300V+ uses an ISDN-NT card and an ISDN-TE card with four groups of “iptel” numbers and “fwd” numbers respectively. The Codec is G.729A. WAN IP address is 220.135.240.207. 2910V has two VoIP Ports with an iptel number and the fwd number respectively. The Codec is G.729A, and the WAN IP is 61.31.167.135.

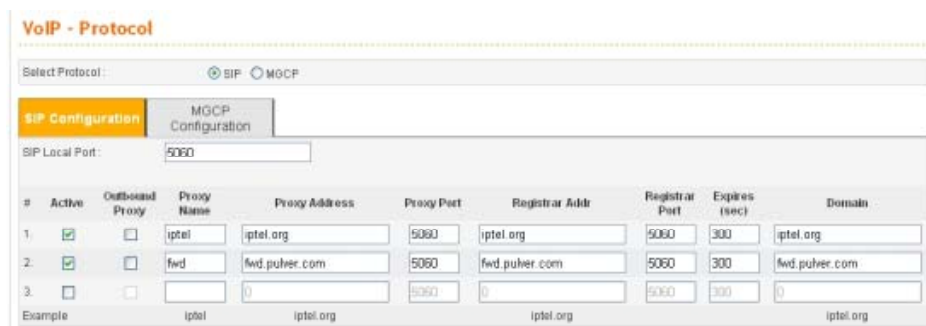
Basic settings in Vigor 3300V+ and 2910V

	WAN IP	Port Number	Phone Number	Proxy	Codec
3300V+	220.135.240.207	Port1(ISDN-NT)	888833	iptel	G.729A
		Port2(ISDN-NT)	888834	iptel	G.729A
		Port3(ISDN-NT)	660533	fwd	G.729A
		Port4(ISDN-NT)	660534	fwd	G.729A
		Port5(ISDN-TE)	888835	iptel	G.729A
		Port6 ISDN-TE)	888836	iptel	G.729A
		Port7(ISDN-TE)	660525	fwd	G.729A
		Port8(ISDN-TE)	660526	fwd	G.729A
2910V	61.31.167.135	Port1(ISDN-NT)	888829	iptel	G.729A
		Port2(ISDN-NT)	660529	fwd	G.729A

	Proxy	Domain	Port
iptel	iptel.org	iptel.org	5060
fwd	fwd.pulver.com	fwd.pulver.com	5060

Configuration Example for Vigor3300V+

1. Enter **VoIP - Protocol** page and configure related settings on SIP Configuration.



- Set SIP accounts (e.g., username and proxy server) by referring to the table “Basic settings in Vigor 3300V+ and 2910V” on last page.

VoIP - SIP Accounts - Edit

1

Disable Enable

Username:

Password:

Display Name:

Authentication ID:

Proxy Server:

Call without Registration: Disable Enable

VoIP IP Address:

- Enter **VoIP - Port Settings** page, click the **Edit** icon of port 1.

VoIP - Port Settings

#	Edit	Type	Active	SIP Account	Supplemental Service	Hotline	Mic/Spk Gain	FAX	Codec	DTMF
1		ISDN-NT	V	1 - 888833			0 / 0	Transparent	G.729A	RFC2833
2		ISDN-NT	V	2 - 888834			0 / 0	Transparent	G.729A	RFC2833
3		ISDN-NT	V	3 - 660533			0 / 0	Transparent	G.729A	RFC2833
4		ISDN-NT	V	4 - 660534			0 / 0	Transparent	G.729A	RFC2833
5		ISDN-TE	V	5 - 888835			0 / 0	Transparent	G.729A	RFC2833
6		ISDN-TE	V	6 - 888836			0 / 0	Transparent	G.729A	RFC2833
7		ISDN-TE	V	7 - 660525			0 / 0	Transparent	G.729A	RFC2833
8		ISDN-TE	V	8 - 660526			0 / 0	Transparent	G.729A	RFC2833

- Enter the **Port 1** page. This page falls into six sections.
Port1 (ISDN-NT) Display the port type, **enable** or **disable** the port, choose the SIP account, and etc.

VoIP - Port Settings - Port1 - Edit

Port 1 (ISDN-NT)

Disable Enable

Default SIP Accounts:

VoIP IP Address:

- Set Port 2 ~ Port 8 one by one in turn.
Type: Port 1 ~Port 4 are **ISDN-NT**, Port 5 ~Port 8 are **ISDN-TE**.
Active: Port 1 ~Port 8 are all **active** (v=Enable).
SIP Account: Accounts of Port 1 ~ Port 8.
Codec: Port 1 ~Port 8 all prior use **G.729A - 8kbps**.

VoIP - Port Settings

#	Edit	Type	Active	SIP Account	Supplemental Service	Hotline	Mic/Spk Gain	FAX	Codec	DTMF
1		ISDN-NT	V	1 - 1001			0 / 0	Transparent	G.729A	RFC2833
2		ISDN-NT	V	2 - 1002			0 / 0	Transparent	G.729A	RFC2833
3		ISDN-NT	V	3 - 1003			0 / 0	Transparent	G.729A	RFC2833
4		ISDN-NT	V	4 - 1004			0 / 0	Transparent	G.729A	RFC2833
5		ISDN-TE	V	5 - 1005			0 / 0	Transparent	G.729A	RFC2833
6		ISDN-TE	V	6 - 1006			0 / 0	Transparent	G.729A	RFC2833
7		ISDN-TE	V	7 - 1007			0 / 0	Transparent	G.729A	RFC2833
8		ISDN-TE	V	8 - 1008			0 / 0	Transparent	G.729A	RFC2833

6. Check the VoIP Status. Please enter the **VoIP – Status - SIP Status** page first and wait one or two minutes (The time depends on SIP Server's response speed and the network condition). **OK** means the registration is successful; **Failed** means the registration is failed.

VoIP - SIP Status

Refresh Option:

#	Register Status	#	Register Status	#	Register Status	#	Register Status
1		9		17		25	
2		10		18		26	
3		11		19		27	
4		12		20		28	
5		13		21		29	
6		14		22		30	
7		15		23		31	
8		16		24		32	

Next, please enter **VoIP – Status - Port Status**. This page will display calling information from Port 1 ~ Port 8. **Idle** means there is no conversations on Port 1 ~ Port 8.

VoIP - Status

Refresh Option:

#	Call Status	Call Type	Caller Number	Callee Number	Start Time	Remote RTP Address	Remote RTP Port	RTP Statistic	Codec Type	Packet Period	VAD	DTMF Relay
1-1	Idle											
2-1	Idle											
3-1	Idle											
4-1	Idle											
5-1	Idle											
6-1	Idle											
7-1	Idle											
8-1	Idle											

* PS: Packets Sent, OS: Octets Sent, PR: Packets Received, OR: Octets Received, PL: Packets Lost, JI: Interarrival Jitter Estimate(ms), LA: Avg TX Delay(ms)

Note: This page will automatically refresh based on the setting configured in **Refresh Option**. You may click **Refresh** button to renew immediately.

Configuration Example for Vigor2910V series

1. Open the Web interface of the router and open **VoIP** menu.

Vigor2910 Series
Dual-WAN Security Router

DrayTek
www.draytek.com

Quick Start Wizard
Online Status

WAN
LAN
NAT
Firewall
Objects Setting
CSM
Bandwidth Management
Applications
VPN and Remote Access
Certificate Management
VoIP
ISDN
Wireless LAN
VLAN
USB Application
System Maintenance
Diagnostics

All Rights Reserved.

System Status

Model Name : DrayTek Vigor2910
Firmware Version : 3.2.1_RC2
Build Date/Time : Tue Jul 29 18:35:51.48 2008

System	
CPU Usage	: 2 %
Total Memory	: 16M
Memory usage	: 61 %

LAN	
MAC Address	: 00-50-7F-DD-15-18
1st IP Address	: 192.168.1.1
1st Subnet Mask	: 255.255.255.0
DHCP Server	: Yes
Primary DNS	:
Secondary DNS	:

VoIP	
Port	: 1 2
SIP registrar	:
Account ID	: change_me change_me
Register	:
Codec	:
In Calls	: 0 0
Out Calls	: 0 0

WAN 1	
Link Status	: Connected
MAC Address	: 00-50-7F-DD-15-19
Connection	: Static IP
IP Address	: 172.16.3.229
Default Gateway	: 172.16.3.4
Primary DNS	:
Secondary DNS	:

WAN 2	
Link Status	: Disconnected
MAC Address	: 00-50-7F-DD-15-1A
Connection	: ---
IP Address	: ---
Default Gateway	: ---
Primary DNS	:
Secondary DNS	:

Wireless LAN	
MAC Address	: 00-14-85-08-69-19
Frequency Domain	: Europe
Firmware Version	: v2.01.10.10.5.4

Click **SIP Account**.

VoIP

- ▶ DialPlan
- ▶ SIP Accounts
- ▶ Phone Settings
- ▶ Status

Configure Port1 and Port2 by clicking Index number 1 and 2.

VoIP >> SIP Accounts

SIP Accounts List Refresh

Index	Profile	Domain/Realm	Proxy	Account Name	Ring Port	Status
<u>1</u>				change_me	<input type="checkbox"/> VoIP1 <input type="checkbox"/> VoIP2 <input type="checkbox"/> ISDN	-
<u>2</u>				change_me	<input type="checkbox"/> VoIP1 <input type="checkbox"/> VoIP2 <input type="checkbox"/> ISDN	-
<u>3</u>				change_me	<input type="checkbox"/> VoIP1 <input type="checkbox"/> VoIP2 <input type="checkbox"/> ISDN	-
<u>4</u>				change_me	<input type="checkbox"/> VoIP1 <input type="checkbox"/> VoIP2 <input type="checkbox"/> ISDN	-
<u>5</u>				change_me	<input type="checkbox"/> VoIP1 <input type="checkbox"/> VoIP2 <input type="checkbox"/> ISDN	-
<u>6</u>				change_me	<input type="checkbox"/> VoIP1 <input type="checkbox"/> VoIP2 <input type="checkbox"/> ISDN	-

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

NAT Traversal Setting

STUN server:	<input type="text" value="stun.fwdnet.net"/>
External IP:	<input type="text"/>
SIP PING interval:	<input type="text" value="150"/> sec

OK

Type relevant SIP Servers used for registration respectively.

VoIP >> SIP Accounts

SIP Account Index No. 1

Profile Name	test	(11 char max.)
Register via	WAN	<input type="checkbox"/> make call without register
SIP Port	5060	
Domain/Realm	iptel.org	(63 char max.)
Proxy	iptel.org	(63 char max.)
	<input type="checkbox"/> Act as outbound proxy	
Display Name	2910V_Port1_ipitel	(23 char max.)
Account Number/Name	888829	(63 char max.)
<input type="checkbox"/> Authentication ID	888829	(63 char max.)
Password	(63 char max.)
Expiry Time	1 hour	3600 sec
NAT Traversal Support	None	
Ring Port	<input checked="" type="checkbox"/> VoIP1	<input type="checkbox"/> VoIP2 <input type="checkbox"/> ISDN
Ring Pattern	1	

OK Cancel

After configuration, please click **OK** to save the settings. 2910 series will go to **VoIP >>SIP Account** page automatically.

2. Open **VoIP>>Status**.



3. Wait one or two minutes (The time depends on SIP Server's response speed and the network condition).

Channel: **R** means Port 1 and Port 2 register successfully.

Status: **IDLE** means there is no conversations on Port 1~ Port 8.

VoIP >> Status

Status Refresh Seconds: 10

Port	Status	Codec	PeerID	Elapse (hh:mm:ss)	Tx Pkts	Rx Pkts	Rx Losses	Rx Jitter (ms)	In Calls	Out Calls	Speaker Gain
ISDN1	R			00:00:00	0	0	0	0	0	0	5
ISDN2	R			00:00:00	0	0	0	0	0	0	5

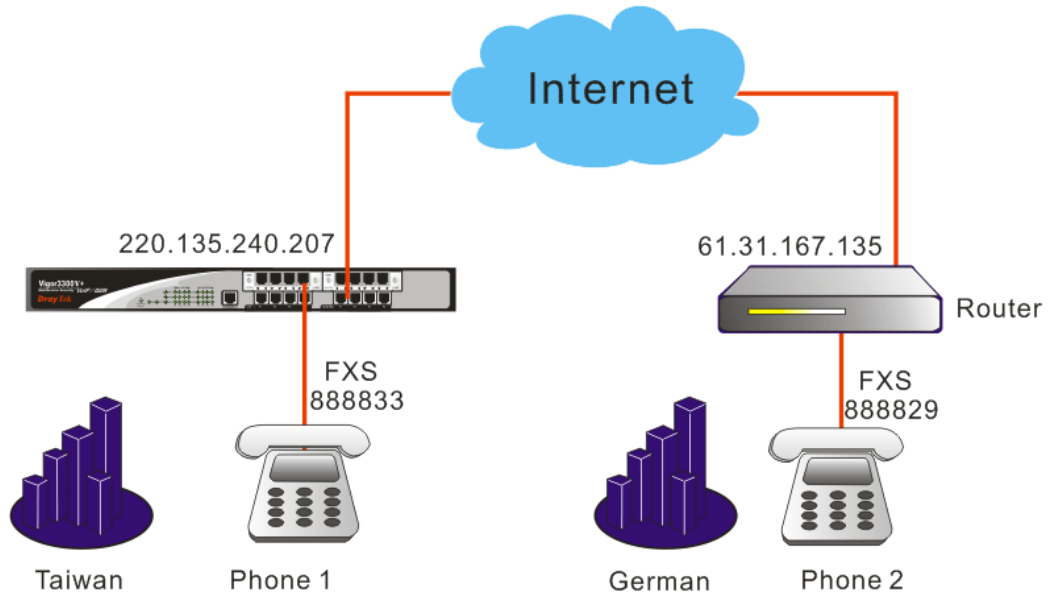
Now the configuration is completed.

3.3.3 Example 3 - Basic Calling Method

We will introduce three basic VoIP calling methods, involving Direct IP Call, Intercommunication with one SIP Proxy Server and Intercommunication with different SIP Proxy Servers. All the settings are based on the VoIP Example 1(Basic Configuration and Registration).

Direct IP Call (Call with each other without registration)

Connect a telephone into 3300V+'s Port 1 and 2910V's Port 1 respectively. They can call with each other directly with IP addresses if only 3300V+ and 2910V both have public IP addresses and have set up the Phone Numbers. Below shows a scenario architecture graph:



Configuration table

	WAN IP	Port Number	Phone Number	Proxy	Codec
3300V+	220.135.240.207	Port1(FXS)	888833	iptel	G.729A
2910V	61.31.167.135	Port1(FXS)	888829	iptel	G.729A

Furthermore, do **NOT** enable the **Outbound Proxy** feature when you set up 3300V+ and 2910V to use Direct IP Call. (It is not **active** in the Example 1; please see Figure 30-2 shown below) Otherwise, even if you dial the IP address, the call will be sent to the SIP Proxy Server still. Besides, if the SIP Proxy Server doesn't forward the call to remote VoIP user's WAN IP, you can't do this action.

VoIP - Protocol

Select Protocol : SIP MGCP

SIP Configuration | MGCP Configuration

SIP Local Port :

#	Active	Outbound Proxy	Proxy Name	Proxy Address
1.	<input checked="" type="checkbox"/>	<input type="checkbox"/>	iptel	iptel.org
2.	<input checked="" type="checkbox"/>	<input type="checkbox"/>	fwd	fwd.pulver.com
3.	<input type="checkbox"/>	<input type="checkbox"/>		

Example iptel iptel.org

VoIP >> SIP Accounts

SIP Account Index No. 1

Profile Name :

Register via : mal

SIP Port :

Domain/Realm :

Proxy :

Act as outbound proxy

Display Name :

Account Number/Name :

Authentication ID :

Configuration Example for Vigor3300V+

Enter VoIP - Speed Dial page, configure relevant settings for 2910V's Port1.

Speed Dial Phone Number: type 2901.

Speed Dial Destination: Cal lee's **Number@IP**, type 888829@61.31.167.135.

Memo: To facilitate ease differentiation please type 2910V_Port1_IP.

Click **Apply** to save the settings and finish the configuration.

VoIP - Speed Dial

#	Speed Dial Phone Number	Speed Dial Destination	Memo
1	<input type="text" value="2901"/>	<input type="text" value="888829@61.31.167.135"/>	<input type="text" value="2910V_Part1_IP"/>
2	<input type="text"/>	<input type="text"/>	<input type="text"/>
3	<input type="text"/>	<input type="text"/>	<input type="text"/>
4	<input type="text"/>	<input type="text"/>	<input type="text"/>
5	<input type="text"/>	<input type="text"/>	<input type="text"/>

Example 101 101@iptel.org

1 2 3 4 5 6 7 8 9 10 >

Configuration Example for Vigor2910V

1. Open the Web interface of the router and open **VoIP** menu.

Vigor2910 Series
Dual-WAN Security Router

DrayTek
www.draytek.com

Quick Start Wizard
Online Status

WAN
LAN
NAT
Firewall
Objects Setting
CSM
Bandwidth Management
Applications
VPN and Remote Access
Certificate Management
VoIP
ISDN
Wireless LAN
VLAN
USB Application
System Maintenance
Diagnostics

All Rights Reserved.

System Status

Model Name : DrayTek Vigor2910
Firmware Version : 3.2.1_RC2
Build Date/Time : Tue Jul 29 18:35:51.48 2008

System	
CPU Usage	: 2 %
Total Memory	: 16M
Memory usage	: 61 %

LAN	
MAC Address	: 00-50-7F-DD-15-18
1st IP Address	: 192.168.1.1
1st Subnet Mask	: 255.255.255.0
DHCP Server	: Yes
Primary DNS	:
Secondary DNS	:

VoIP	
Port	: 1 2
SIP registrar	:
Account ID	: change_me change_me
Register	:
Codec	:
In Calls	: 0 0
Out Calls	: 0 0

WAN 1	
Link Status	: Connected
MAC Address	: 00-50-7F-DD-15-19
Connection	: Static IP
IP Address	: 172.16.3.229
Default Gateway	: 172.16.3.4
Primary DNS	:
Secondary DNS	:

WAN 2	
Link Status	: Disconnected
MAC Address	: 00-50-7F-DD-15-1A
Connection	: ---
IP Address	: ---
Default Gateway	: ---
Primary DNS	:
Secondary DNS	:

Wireless LAN	
MAC Address	: 00-14-85-08-69-19
Frequency Domain	: Europe
Firmware Version	: v2.01.10.10.5.4

2. Open **VoIP>>DialPlan** and click **Phone Book**

VoIP

- ▶ DialPlan
- ▶ SIP Accounts
- ▶ Phone Settings
- ▶ Status

3. Click Index 1.

VoIP >> DialPlan Setup

Phone Book

Index	Phone number	Display Name	SIP URL	Dial Out Account	Loop through
1.					
2.					
3.					
4.					

4. Enter relevant settings for 3300V+'s Port 1. Click **OK** to save the settings.

Enable: click (√) to activate the entry.

Phone Number: type **3301**.

Display Name: To facilitate ease differentiation please type **3300V_Port1_IP**.

SIP URL: Callee's Number@IP, please type **888833@220.135.240.207**.

VoIP >> DialPlan Setup

Phone Book Index No. 1

<input checked="" type="checkbox"/> Enable	
Phone Number	<input type="text" value="3301"/>
Display Name	<input type="text" value="3300V+_Port1_IP"/>
SIP URL	<input type="text" value="888833"/> @ <input type="text" value="220.135.240.207"/>
Dial Out Account	<input type="text" value="Default"/>
Loop through	<input type="text" value="None"/>
Backup Phone Number	<input type="text"/>

5. Confirm the settings are correct, and then finish the configuration.

VoIP >> DialPlan Setup

Phone Book

Index	Phone number	Display Name	SIP URL	Dial Out Account	Loop through
1.	3301	3300V+_Port1_IP	888833@220.135.240.207	Default	None
2.				Default	None
3.				Default	None
4.				Default	None

Start to dial by using telephones.

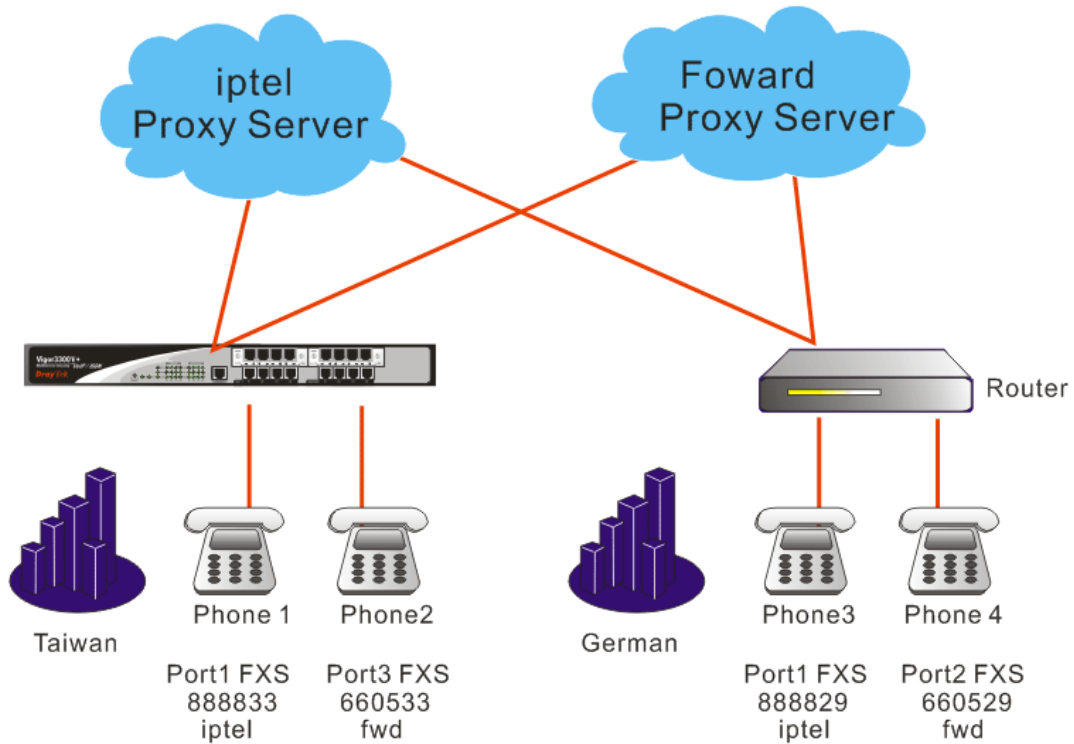
Phone 1 calls Phone 2 --->Press 2901# or 888829*61*31*167*135#.

Phone 2 calls Phone 1--->Press **3301#**.

Note: # indicates termination of the phone number. After pressing #, VoIP is immediately called out. Or you may wait 3 seconds if you do not press #. With 2910V you can't only dial alphanumeric addresses or @ symbols. To dial an IP address, start and end it with a # (hash) replace the dots with * (star). In this example you have to press #220*135*240*207#. But 3300V+ can only receive the format of Number@IP. So it is required to setup 3300V+'s number (**888833@220.135.240.207**) in the DialPlan entry.

Intercommunication with one SIP Proxy Server (registration)

Connect telephones into 3300V+'s Port 1 & Port 3 and 2910V's Port 1 & Port 2 respectively. Each port needs to register in the SIP Server. Below shows a scenario architecture graph:



Configurations between Vigor 3300V+ and 2910V

	WAN IP	Port Number	Phone Number	Proxy	Codec
3300V+	220.135.240.207	Port1(FXS)	888833	iptel	G.729A
		Port3(FXS)	660533	fwd	G.729A
2910V	61.31.167.135	Port1(FXS)	888829	iptel	G.729A
		Port2(FXS)	660529	fwd	G.729A

You can also add Speed Dial numbers in **Speed Dial** to speed up the dialing, or to accommodate the setup of company's extension numbers.

Configuration Example for Vigor3300V+

Enter the **VoIP - Speed Dial** page and add the second and third group of Speed Dial number. Then click **Apply** to save the settings and finish the configuration.

#	Speed Dial Phone Number	Speed Dial Destination	Memo
1	2901	888829@61.31.167.135	2900V_Port1_IP
2	291	888829	2900V_Port1
3	292	660529	2900V_Port2
4			
5			

Example 101 101@p01.org

1 2 3 4 5

Apply Cancel Clear This Page

Start to dial by using telephones.

Phone 1 call Phone 3---> Press **888829#** or **291#**.

Phone 2 call Phone 4--->Press 660529# or 292#.

Phone 3 call Phone 1--->Press 888833#.

Phone 4 call Phone 2--->Press 660533#.

Note: # indicates termination of the phone number. After pressing #, VoIP is immediately called out. Or you may wait 3 seconds if you do not press #.

Intercommunication with different SIP Proxy Servers

Connect telephones into 3300V+'s Port 1 & Port 3 and 2910V's Port 1 & Port 2 respectively. Each phone registers to the SIP Server. The settings and scenario are the same as the above example. But they must be set up in conjunction with the Speed Dial.

Configuration Example for Vigor3300+

Enter the **VoIP - Speed Dial** page and add the **4th** and **5th** group of Speed Dial number. Then press **Apply** to save the settings and finish the configuration.

VoIP - Speed Dial

#	Speed Dial Phone Number	Speed Dial Destination	Memo
1	2901	888829@192.168.29.1	2910V_Part1_VPN
2	291	888829	2910_Port1
3	292	660529	2910_Port2
4	2911	888829@iptel.org	2910V_Part1_iptel
5	2912	660529@fwd.pulver.com	2910V_Part2_fwd
Example 101	101	101@iptel.org	

1 2345678910 >

Configuration Example for Vigor2910V

Open **VoIP >>DialPlan** and click **Phone Book**. Then add the second and third group of Speed Dial number.

VoIP >> DialPlan Setup

Phone Book

Index	Phone number	Display Name	SIP URL	Dial Out Account	Loop through
1.	3301	3300V+_Port1_IP	888833@220.135.240.207	Default	None
2.	3311	3300V_Port_iptel	888833@iptel.org	Default	None
3.	3312	3300V+_Port2_fwd	660533@fwd.pulver.vom	Default	None
4.				Default	None

Start to dial by using telephone.

Phone 1 call Phone 4--->Press **2912#**.

Phone 2 call Phone 3--->Press **2911#**.

Phone 3 call Phone 1--->Press **3312#**.

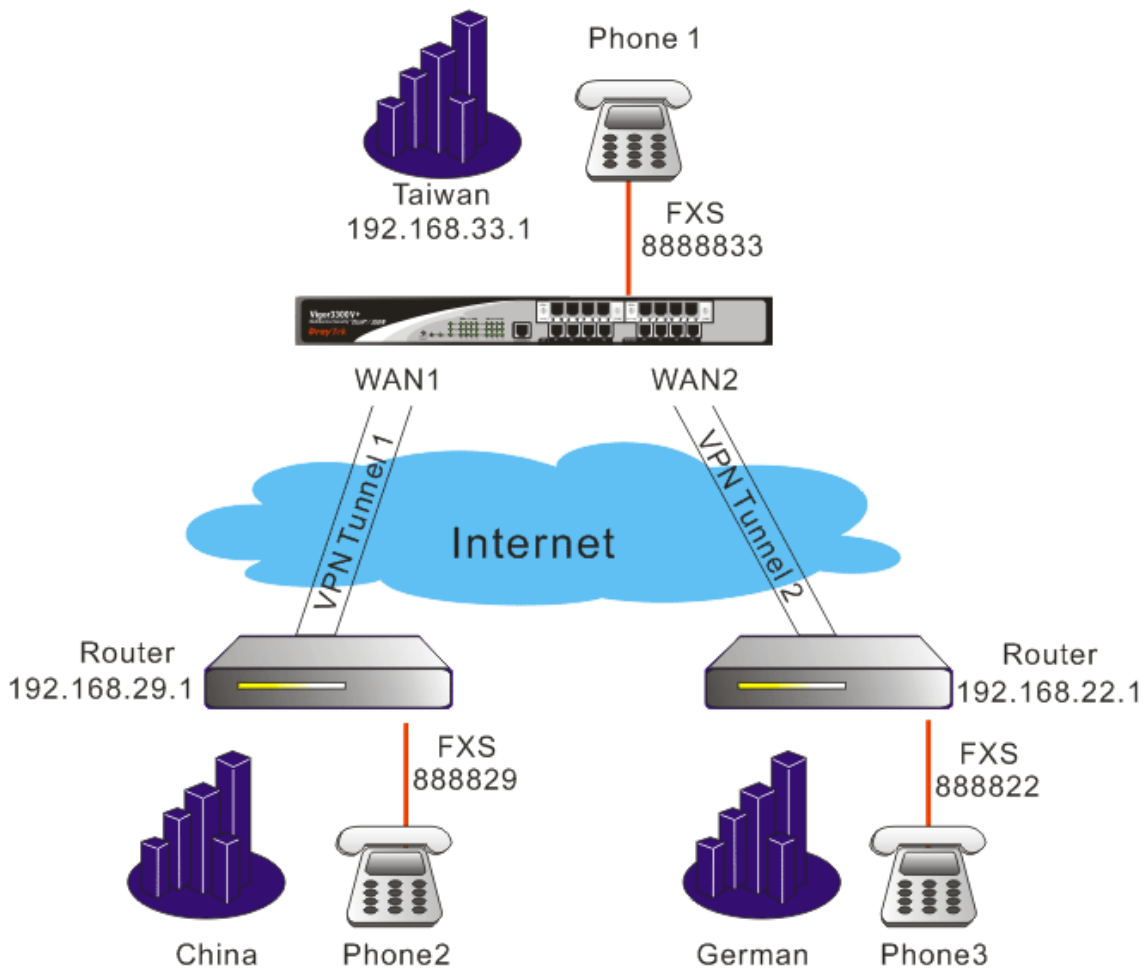
Phone 4 call Phone 2--->Press **3311#**.

Note: # indicates termination of the phone number. After pressing #, VoIP is immediately called out. Or you may wait 3 seconds if you do not press #.

3.3.4 Example 4 - VoIP over VPN

Based on the **VoIP Example 1(Basic Configuration and Registration)**, we will introduce how to dial the VoIP call through an encrypted VPN tunnel.

In this example Vigor3300V+ acts as a bridge accepting incoming VPN connections from the other two routers (Vigor2910V and Vigor2200V). The VPN traffic between Vigor2910V and Vigor2200V are all passed through Vigor3300V+. These three sites internal networks must be within the same subnet (192.168.X.X). Either site can ping the other two routers. Then you can make a VoIP call through the encrypted VPN tunnel by directly dialing remote router's LAN IP. Below shows the architecture graph:



Configuration table

	3300V+ Headquarters	2910V Branch Offices	2200V Teleworker
WAN IP	220.135.240.207 PPPoE, fixed IP	61.31.167.135 PPPoE, dynamic IP	
	219.81.160.206 PPPoE, fixed IP		61.230.207.146 PPPoE, dynamic IP
LAN IP	192.168.33.1	192.168.29.1	192.168.22.1
Internal network	192.168.33.X	192.168.29.X	192.168.22.X
Encryption method	DES-SHA1		
Preshared Key	3300		
	1234		1234

	WAN IP	Port Number	Phone Number	Proxy	Codec
3300V+	220.135.240.207	Port1(FXS)	888833		G.729A
2910V	61.31.167.135	Port1(FXS)	888829		G.729A
2200V	61.230.207.146	Port1(FXS)	888822		G.729A

About the VPN configurations please refer to **VPN Example 3(three part communication)**.
 About VoIP basic configuration please refer to **VoIP Example 1(Basic Configuration and Registration)**.

The following examples are modified which based on these two examples.

Configuration Example for Vigor3300V+

1. Enter the **VoIP>> Protocol>>Select Protocol** page. Disable all the **Active** entries by removing the (√) box. After configuration, please click **Apply** to save the settings.

VoIP - Protocol

Select Protocol: SIP MGCP

SIP Configuration | MGCP Configuration

SIP Local Port: 5060

#	Active	Outbound Proxy	Proxy Name	Proxy Address	Proxy Port	Registrar Addr	Registrar Port	Expires (sec)	Domain
1.	<input type="checkbox"/>	<input type="checkbox"/>		0	5060	0	5060	3600	0
2.	<input type="checkbox"/>	<input type="checkbox"/>		0	5060	0	5060	3600	0
3.	<input type="checkbox"/>	<input type="checkbox"/>		0	5060	0	5060	3600	0

Example: iptel iptel.org iptel.org iptel.org

Proxy: User-Agent Name

1. DrayTek V3300V-1.0.0

2. DrayTek V3300V-1.0.0

3. DrayTek V3300V-1.0.0

Apply Cancel

Or, open **VoIP>>SIP Accounts** and click radio button 1. Click **Edit**.

VoIP - SIP Accounts

#	User Name	Display Name	Proxy Server	Ring Port	Ring Type	Call Forwarding
1	1001	1001		1	All Ports	
2	1002	1002		2	All Ports	
3	1003	1003		3	All Ports	
4	1004	1004		4	All Ports	
5	1005	1005		5	All Ports	
6	1006	1006		6	All Ports	
7	1007	1007		7	All Ports	
8	1008	1008		8	All Ports	

1 2 3 4

Set **LAN/VPN** as VoIP IP Address.

VoIP - SIP Accounts - Edit

1

Disable Enable

Username:

Password:

Display Name:

Authentication ID:

Proxy Server:

Call without Registration:

VoIP IP Address:

Call Forwarding

Disable

Callforwarding all calls

Callforwarding busy

Callforwarding no answer after rings (Range:1~10)

SIP URL: (Example:8001@iptel.org)

2. Enter the **VoIP - Speed Dial** page and input the first and second group of Speed Dial Phone Number. Click **Apply** to save the settings.

VoIP - Speed Dial

#	Speed Dial Phone Number	Speed Dial Destination	Memo
1	<input type="text" value="2901"/>	<input type="text" value="888829@192.168.29.1"/>	<input type="text" value="2910V_Part1_VPN"/>
2	<input type="text" value="2201"/>	<input type="text" value="888822@192.168.22.1"/>	<input type="text" value="2200V_Part1_VPN"/>
3	<input type="text"/>	<input type="text"/>	<input type="text"/>
4	<input type="text"/>	<input type="text"/>	<input type="text"/>
5	<input type="text"/>	<input type="text"/>	<input type="text"/>

Example 101 101@iptel.org

1 2 3 4 5 6 7 8 9 10 >

Configuration Example for Vigor2910V series

1. Open the Web interface of the router and open **VoIP** menu.

Vigor2910 Series
Dual-WAN Security Router

DrayTek
www.draytek.com

Quick Start Wizard
Online Status

WAN
LAN
NAT
Firewall
Objects Setting
CSM
Bandwidth Management
Applications
VPN and Remote Access
Certificate Management
VoIP
ISDN
Wireless LAN
VLAN
USB Application
System Maintenance
Diagnostics

All Rights Reserved.

System Status

Model Name : DrayTek Vigor2910
Firmware Version : 3.2.1_RC2
Build Date/Time : Tue Jul 29 18:35:51.48 2008

System	
CPU Usage	: 2 %
Total Memory	: 16M
Memory usage	: 61 %

LAN	
MAC Address	: 00-50-7F-DD-15-18
1st IP Address	: 192.168.1.1
1st Subnet Mask	: 255.255.255.0
DHCP Server	: Yes
Primary DNS	:
Secondary DNS	:

VoIP	
Port	: 1 2
SIP registrar	:
Account ID	: change_me change_me
Register	:
Codec	:
In Calls	: 0 0
Out Calls	: 0 0

WAN 1	
Link Status	: Connected
MAC Address	: 00-50-7F-DD-15-19
Connection	: Static IP
IP Address	: 172.16.3.229
Default Gateway	: 172.16.3.4
Primary DNS	:
Secondary DNS	:

WAN 2	
Link Status	: Disconnected
MAC Address	: 00-50-7F-DD-15-1A
Connection	: ---
IP Address	: ---
Default Gateway	: ---
Primary DNS	:
Secondary DNS	:

Wireless LAN	
MAC Address	: 00-14-85-08-69-19
Frequency Domain	: Europe
Firmware Version	: v2.01.10.10.5.4

Click **SIP Account**.

VoIP

- ▶ DialPlan
- ▶ SIP Accounts
- ▶ Phone Settings
- ▶ Status

Configure Port1 and Port2 by clicking Index number 1 and 2.

VoIP >> SIP Accounts

SIP Accounts List Refresh

Index	Profile	Domain/Realm	Proxy	Account Name	Ring Port			Status
<u>1</u>				change_me	<input type="checkbox"/> VoIP1	<input type="checkbox"/> VoIP2	<input type="checkbox"/> ISDN	-
<u>2</u>				change_me	<input type="checkbox"/> VoIP1	<input type="checkbox"/> VoIP2	<input type="checkbox"/> ISDN	-
<u>3</u>				change_me	<input type="checkbox"/> VoIP1	<input type="checkbox"/> VoIP2	<input type="checkbox"/> ISDN	-
<u>4</u>				change_me	<input type="checkbox"/> VoIP1	<input type="checkbox"/> VoIP2	<input type="checkbox"/> ISDN	-
<u>5</u>				change_me	<input type="checkbox"/> VoIP1	<input type="checkbox"/> VoIP2	<input type="checkbox"/> ISDN	-
<u>6</u>				change_me	<input type="checkbox"/> VoIP1	<input type="checkbox"/> VoIP2	<input type="checkbox"/> ISDN	-

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

NAT Traversal Setting

STUN server:	<input type="text" value="stun.fwdnet.net"/>
External IP:	<input type="text"/>
SIP PING interval:	<input type="text" value="150"/> sec

OK

Note: Do not set Stun Server when calling through VPN.

Type relevant SIP Servers used for registration respectively. Set **LAN/VPN** as **Register via** for Port1 and Port2.

VoIP >> SIP Accounts

SIP Account Index No. 1

Profile Name	test (11 char max.)
Register via	LAN/VPN <input type="checkbox"/> make call without register
SIP Port	5060
Domain/Realm	iptel.org (63 char max.)
Proxy	iptel.org (63 char max.)
<input type="checkbox"/> Act as outbound proxy	
Display Name	2910V_Port1_iptel (23 char max.)
Account Number/Name	888829 (63 char max.)
<input type="checkbox"/> Authentication ID	888829 (63 char max.)
Password	**** (63 char max.)
Expiry Time	1 hour 3600 sec
NAT Traversal Support	None
Ring Port	<input checked="" type="checkbox"/> VoIP1 <input type="checkbox"/> VoIP2 <input type="checkbox"/> ISDN
Ring Pattern	1

OK Cancel

After configuration, please click **OK** to save the settings. Vigor2910 series will go to **VoIP >>SIP Account** page automatically.

- Open **VoIP>>DialPlan** and click **Phone Book**. Add the first and second group of Speed Dial Phone Number.

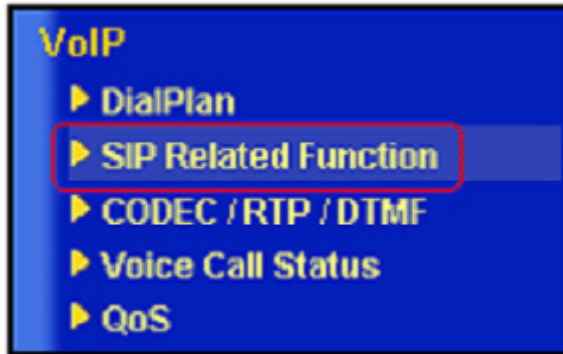
VoIP >> DialPlan Setup

Phone Book

Index	Phone number	Display Name	SIP URL	Dial Out Account	Loop through	Backup Phone Number	Status
1.	3301		888833@19	Default	None		x
2.	2201		888822@19	Default	None		x
3.				Default	None		x
4.				Default	None		x

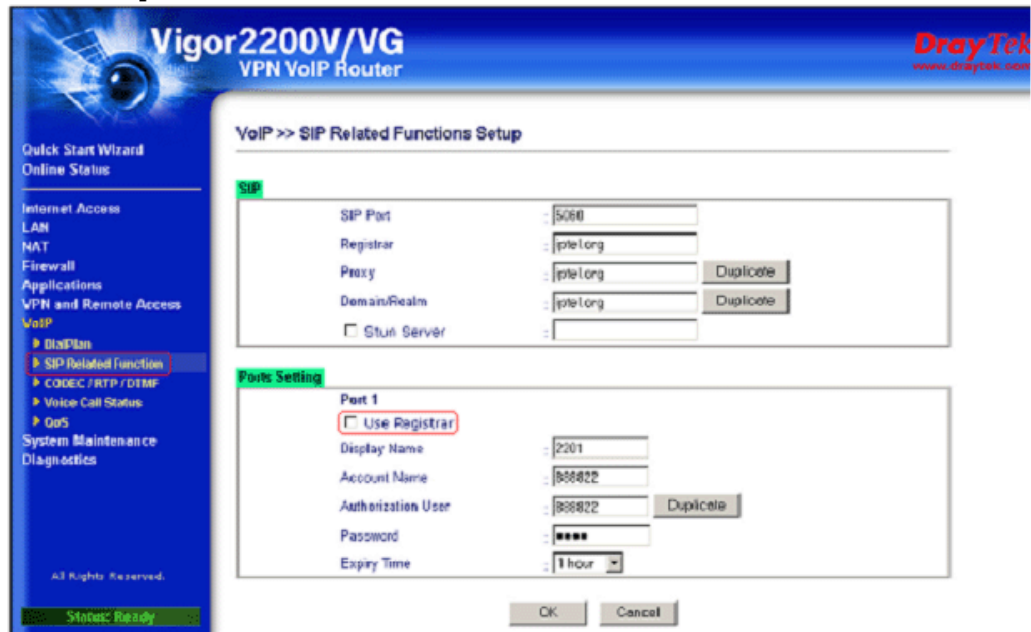
Configuration Example for Vigor2200V

1. Enter 2200V's Web and click **VoIP - SIP Related Function** page.



SIP related function of 2200V

2. Setup Port 1. This page falls into two sections, SIP: Set up the SIP Server used for registration. Ports: Set up the account details.



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

Note: Do not set up the Proxy and Stun Server when calling through VPN. While in 2200V firmware v2.5.5.4, the Proxy will be active if Use Registrar is enabled. So make sure not click Use Registrar.

3. Enter **VoIP - DialPlan** page and the first and second group of Speed Dial Phone Number.



After configuration, please confirm that the VPNs are established and they can communicate with each other. (Please refer to VPN - IPSec - LAN to LAN Usage Example 2).

Start to dial by using telephones.

Phone 1 call Phone 2---->Press 2901# or 888829*192*168*29*1#.

Phone 1 call Phone 3---->Press 2201# or 888822*192*168*22*1#.

Phone 2 call Phone 1---->Press **3301#**.

Phone 2 call Phone 3---->Press 2201# or #192*168*22*1#.

Phone 3 call Phone 1---->Press **3301#**.

Phone 3 call Phone 2---->Press 2901# or #192*168*29*1#.

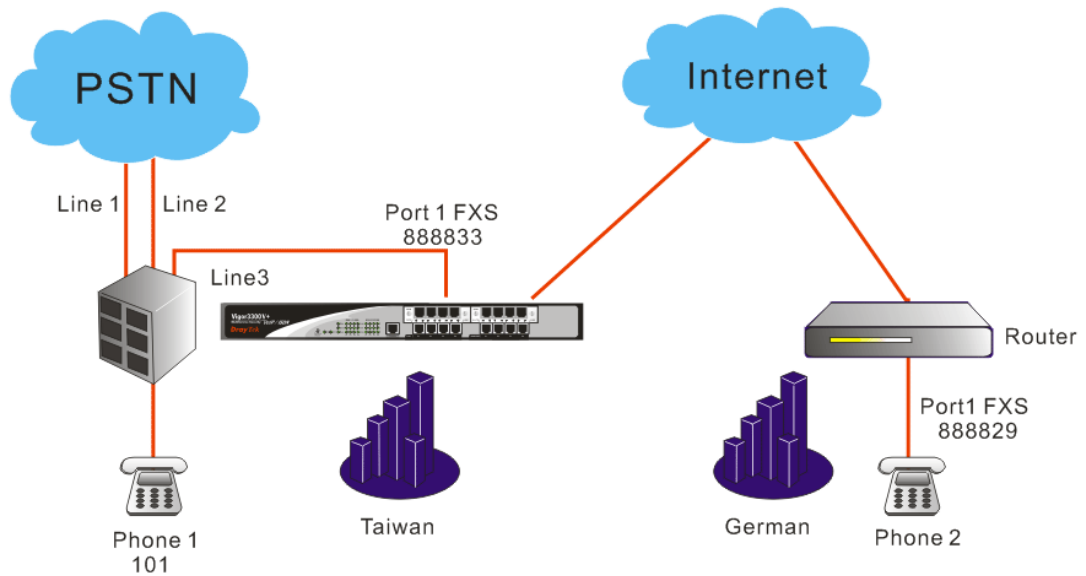
Note: # indicates termination of the phone number. After pressing #, VoIP is immediately called out. Or you may wait 3 seconds if you do not press #.

3.3.5 Example 5 - Practical Application of FXS

Based on the **VoIP Example 1(Basic Configuration and Registration)**, we will introduce the practical application of FXS.

Generally, the practical application of FXS falls into the following two sections.

- Connect the telephones (Please refer to VoIP Example 1). Two VoIP equipments call with each other.
- Connect PBX's Outside Lines. The usage is the same as that of PSTN line. Different PBX has its own settings and required configuration by you. Below shows a scenario architecture graph:



Configuration table between 3300V+and 2910V

	WAN IP	Port Number	Phone Number	Proxy	Codec
3300V+	220.135.240.207	Port1(FXS)	888833	iptel	G.729A
2910V	61.31.167.135	Port1(FXS)	888829	iptel	G.729A

Suppose there are two PSTN lines connected to PBX's Outside Lines. The third Outside Line is connected to 3300V+'s FXS Port1. The Inside Line is connected to a telephone with the extension 101. If the extension wants to dial VoIP using Line 3, you must firstly press 3, and then dial the phone number.

Example of lines connections

	PBX	Phone Number
Line3(3)	Outside Lines	888833
Phone1	Inside Lines	101

Start to dial by using telephones.

Phone 1 calls Phone 2---->Press **3**, after hearing the dial tone press VoIP number **888829#**.

Phone 2 calls Phone 1---->Press **888833#**, after getting through you will hear the auto reply from the PBX. Then press the extension **101**.

Note: # indicates termination of the phone number. After pressing #, VoIP is immediately called out. Or you may wait 3 seconds if you do not press #.

This example is the intercommunication with one SIP Proxy Server. For the applications of Direct IP Call and Intercommunication with different SIP Proxy Servers please refer to **3.3.3 Example 3(Basic Calling Method)**. The VoIP call can also work with VPN, please refer to **3.3.4 Example 4(VoIP over VPN)**.

Also you can set up the Speed Dial entry. To accommodate the extension please set up 888829 to **291**, 888833 to **331**. You may refer to the figures shown below and **3.3.3 Example 3(Basic Calling Method)**.

VoIP - Speed Dial

#	Speed Dial Phone Number	Speed Dial Destination	Memo
1	<input type="text" value="291"/>	<input type="text" value="888829"/>	<input type="text" value="2900V_Port1"/>
2	<input type="text"/>	<input type="text"/>	<input type="text"/>
3	<input type="text"/>	<input type="text"/>	<input type="text"/>
4	<input type="text"/>	<input type="text"/>	<input type="text"/>
5	<input type="text"/>	<input type="text"/>	<input type="text"/>

Example 101 101@iptel.org

1 2 3 4 5 6 7 8 9 10 >

VoIP >> DialPlan Setup

Phone Book Index No. 1

Enable

Phone Number

Display Name

SIP URL @

Dial Out Account ▾

Loop through ▾

Backup Phone Number

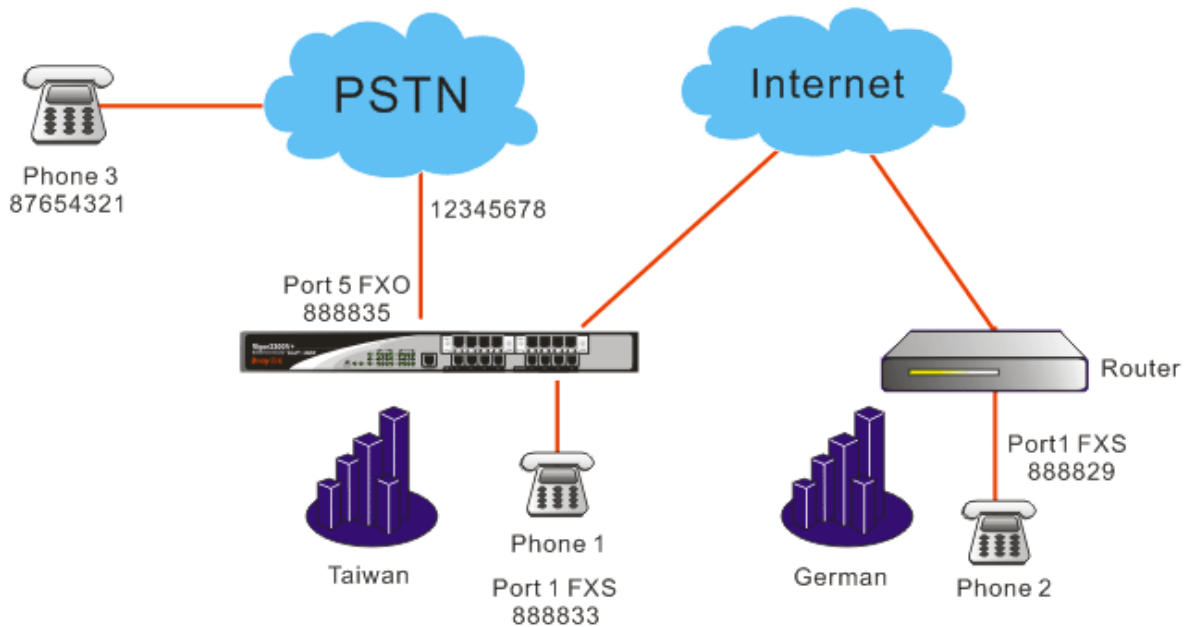
3.3.6 Example 6 - Practical Application of FXO

Based on the **VoIP Example 1(Basic Configuration and Registration)**, we will introduce the practical application of FXO.

Generally the practical application of FXO falls into the following two sections:

- Connect to PSTN line

By connecting 3300V+'s FXO Port 5 to a PSTN line, VoIP is seamlessly integrated to PSTN line and allows you to call not only the remote VoIP user, but also the remote PSTN user. Also the PSTN user can call the VoIP user. Below shows a scenario architecture graph:



Configuration table between 3300V+ and 2910V

	WAN IP	Port Number	Phone Number	Proxy	Codec
3300V+	220.135.240.207	Port1(FXS)	888833	iptel	G.729A
		Port5(FXO)	888835	iptel	G.729A
2100V	61.31.167.135	Port1(FXS)	888829	iptel	G.729A

The number of the PSTN line connected into the FXO Port 5 on the 3300V+ is 12345678. The number of another PSTN line is 87654321.

About VoIP basic settings please refer to VoIP Example 1(Basic configuration and registration)

Start to dial by using telephones.

Phone 1 calls Phone 3---->Press **888835#**. After getting through you will hear the dial tone, then press the PSTN number **87654321#**.

Phone 2 calls Phone 3---->Press **888835#**. After getting through you will hear the Dial tone, then press the PSTN number **87654321#**.

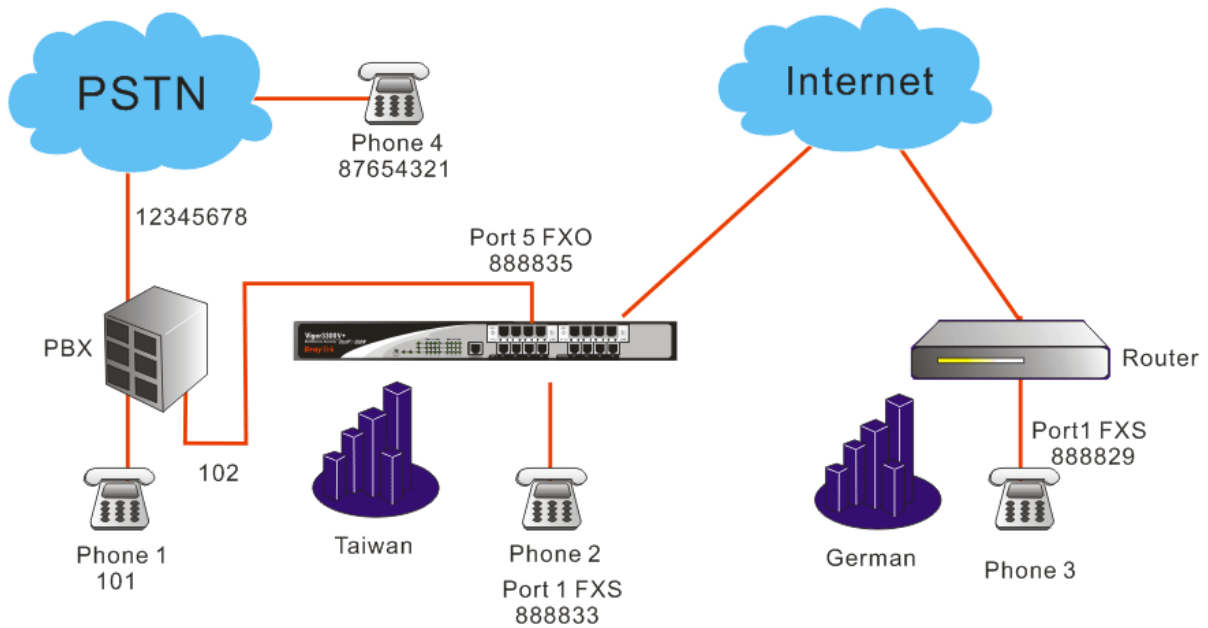
Phone 3 calls Phone 2---->Press **12345678**. After getting through you will hear the Dial tone, then press the VoIP number **888829#**.

Phone 3 calls Phone 1---->Press **12345678**. After getting through you will hear the Dial tone, then press the VoIP number **888833#**.

Note: # indicates termination of the phone number. After pressing #, VoIP is immediately called out. Or, you may wait 3 seconds if you do not press #.

- Connect PBX's Inside Lines. The usage is the same as that of common extension.
Different PBX has its own settings and required configuration by you.

By connecting 3300V+'s FXO Port5 to PBX's Inside Line, VoIP is seamlessly integrated to PBX's inside lines and allows you to call not only the VoIP, but also the PSTN line and PBX's extension. Also the remote user can call you from the PSTN line and PBX's extension.



Configuration table between 3300V+ and 2910V

	WAN IP	Port Number	Phone Number	Proxy	Codec
3300V+	220.135.240.207	Port1(FXS)	888833	iptel	G.729A
		Port5(FXO)	888835	iptel	G.729A
2910V	61.31.167.135	Port1(FXS)	888829	iptel	G.729A

Suppose the number of PBX's Outside Line is 12345678. One Inside Line is connected to a telephone with the extension 101. If you want to use PSTN from the extension, you must firstly press 0, and then dial the phone number.

The FXO Port5 on the 3300V+ is connected to PBX's Inside Line with the number 102. The number of another PSTN line is 87654321.

About VoIP basic settings please refer to VoIP Example 1. (Basic configuration and registration)

Start to dial by using telephones.

Phone 1 calls Phone 2---->Press extension **102**. After getting through you will hear the dial tone, then press the VoIP number **888833#**.

Phone 1 calls Phone 3---->Press extension **102**. After getting through you will hear the Dial tone, then press the VoIP number **888829#**.

Phone 2 calls Phone 1---->Press **888835#**. After getting through you will hear the Dial tone, then press the extension **101**.

Phone 2 calls Phone 4---->Press **888835#**. After getting through you will hear the Dial tone. Press outside line **0**, then press **87654321**.

Phone 3 calls Phone 1---->Press **888835#**. After getting through you will hear the Dial tone, then press the extension **101**.

Phone 3 call Phone 4---->Press **888835#**. After getting through you will hear the Dial tone. Press outside line **0**, then press **87654321**.

Phone 4 calls Phone 2---->Press **12345678**. After getting through you will hear the auto reply from the PBX, then press the extension **102**. After getting through you will hear the Dial tone, then press the VoIP number **888833#**.

Phone 4 calls Phone 3---->Press **12345678**. After getting through you will hear the auto reply from the PBX, then press the extension **102**. After getting through you will hear the Dial tone, then press the VoIP number **888829#**.

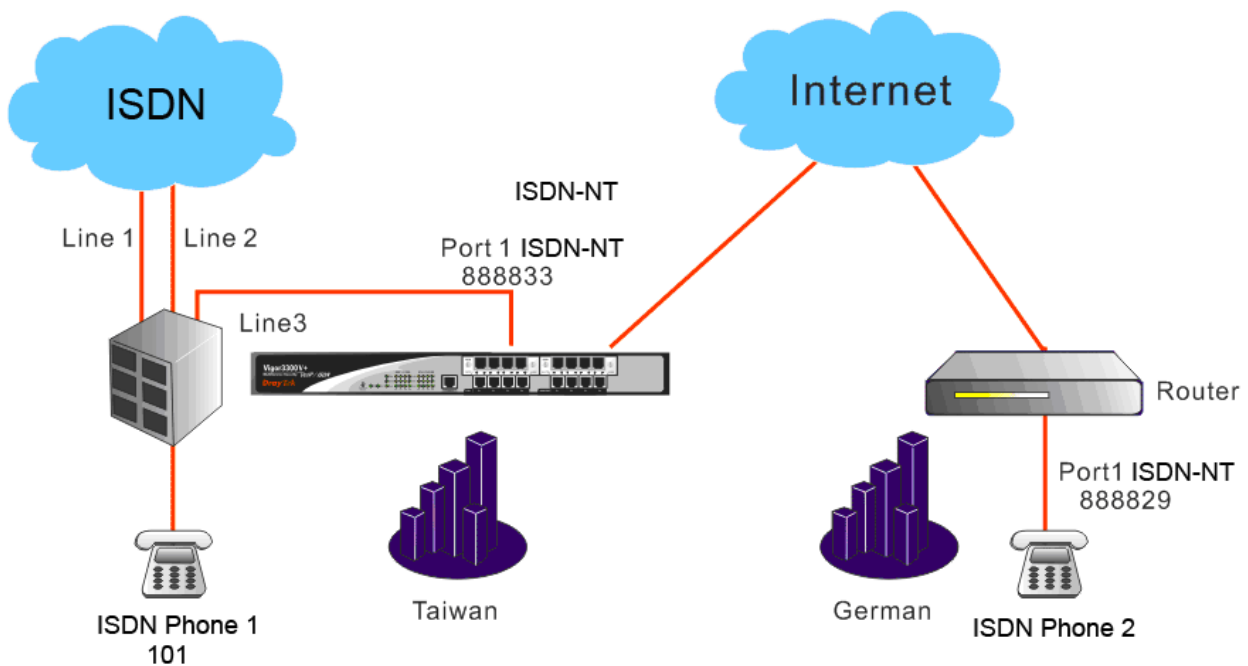
Note: # indicates termination of the phone number. After pressing #, VoIP is called out immediately. Or, you may wait 3 seconds if you do not press #. This example is intercommunication with one SIP Proxy Server. For the applications of Direct IP Call and Intercommunication with different SIP Proxy Servers please refer to **3.3.3 Example 3(Basic Calling Method)**. The VoIP call can also wok with VPN, please refer to **3.3.4 Example 4(VoIP over VPN)**.

3.3.7 Example 7: Practical Application of ISDN-NT

Based on **Example 2 - Basic Configuration and Registration for ISDN**, we will introduce the practical application of ISDN-NT.

Generally, the practical application of ISDN-NT falls into the following two sections.

- Connect the telephones (Please refer to VoIP Example 1). Two VoIP equipments call with each other.
- Connect PBX's Outside Lines. The usage is the same as that of ISDN line. Different PBX has its own settings and required configuration by you. Below shows a scenario architecture graph:



Configuration table between 3300V+ and 2910V

	WAN IP	Port Number	Phone Number	Proxy	Codec
3300V+	220.135.240.207	Port1(ISDN-NT)	888833	iptel	G.729A
2910V	61.31.167.135	Port1(ISDN-NT)	888829	iptel	G.729A

Suppose there are two ISDN lines connected to PBX's Outside Lines. The third Outside Line is connected to 3300V+'s ISDN-NT Port1. The Inside Line is connected to a telephone with the extension 101. If the extension wants to dial VoIP using Line 3, you must firstly press 3, and then dial the phone number.

Example of lines connections

	PBX	Phone Number
Line3(3)	Outside Lines	888833
Phone1	Inside Lines	101

Start to dial by using telephones.

Phone 1 calls Phone 2---->Press **3**, after hearing the dial tone press VoIP number **888829#**.

Phone 2 calls Phone 1---->Press **888833#**, after getting through you will hear the auto reply from the PBX. Then press the extension **101**.

Note: # indicates termination of the phone number. After pressing #, VoIP is immediately called out. Or you may wait 3 seconds if you do not press #.

This example is the intercommunication with one SIP Proxy Server. For the applications of Direct IP Call and Intercommunication with different SIP Proxy Servers please refer to **3.3.3 Example 3(Basic Calling Method)**. The VoIP call can also work with VPN, please refer to **3.3.4 Example 4(VoIP over VPN)**.

Also you can set up the Speed Dial entry. To accommodate the extension please set up 888829 to **291**, 888833 to **331**. You may refer to the figures shown below and **VoIP Example 2(Basic Calling Method)**.

VoIP - Speed Dial

#	Speed Dial Phone Number	Speed Dial Destination	Memo
1	291	888829	2900V_Port1
2			
3			
4			
5			

Example 101 101@iptel.org

1 2 3 4 5 6 7 8 9 10 >

VoIP >> DialPlan Setup

Phone Book Index No. 1

Enable

Phone Number

Display Name

SIP URL @

Dial Out Account ▾

Loop through ▾

Backup Phone Number

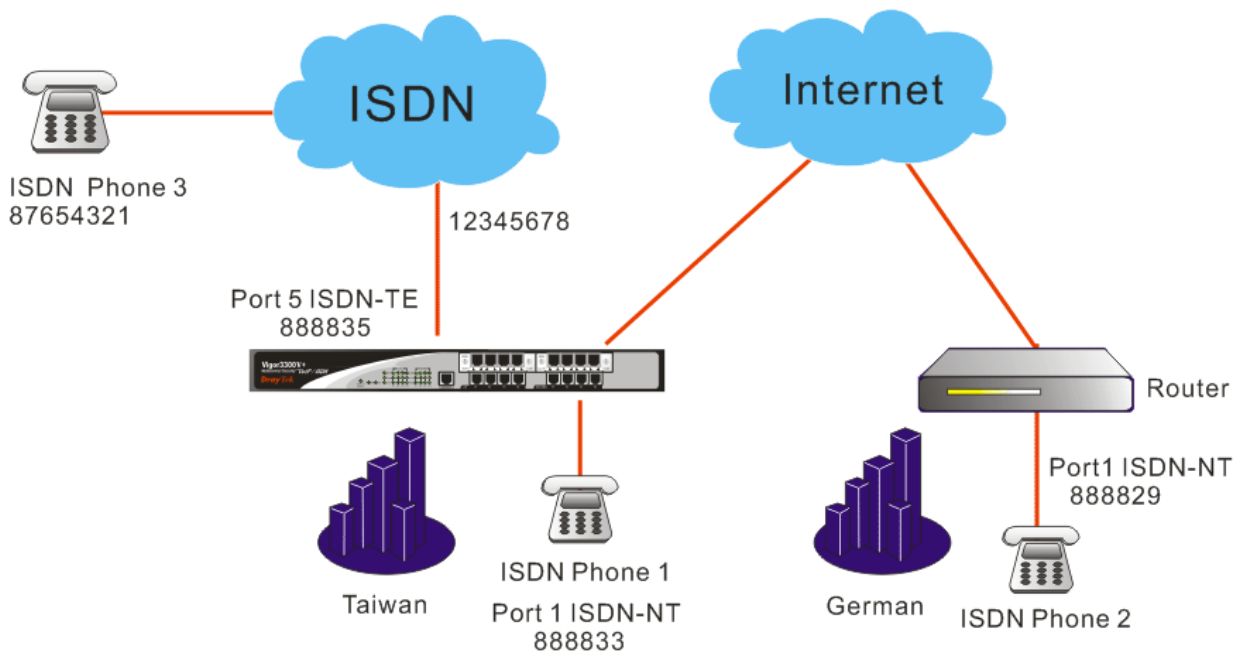
3.3.8 Example 8: Practical Application of ISDN-TE

Based on the **Example 2 - Basic Configuration and Registration for ISDN**, we will introduce the practical application of ISDN-TE.

Generally the practical application of ISDN-TE falls into the following two sections:

- Connect to ISDN line

By connecting 3300V+'s ISDN-TE Port 5 to a ISDN line, VoIP is seamlessly integrated to ISDN line and allows you to call not only the remote VoIP user, but also the remote ISDN user. Also the ISDN user can call the VoIP user. Below shows a scenario architecture graph:



Configuration table between 3300V+ and 2910V

	WAN IP	Port Number	Phone Number	Proxy	Codec
3300V+	220.135.240.207	Port1(ISDN-NT)	888833	iptel	G.729A
		Port5(ISDN-TE)	888835	iptel	G.729A
2910V	61.31.167.135	Port1(ISDN-NT)	888829	iptel	G.729A

The number of the PSTN line connected into the ISDN-TE Port 5 on the 3300V+ is 12345678. The number of another ISDN line is 87654321.

About VoIP basic settings please refer to **VoIP Example 2(Basic configuration and registration for ISDN)**.

Start to dial by using telephones.

Phone 1 calls Phone 3---->Press **888835#**. After getting through you will hear the dial tone, then press the PSTN number **87654321#**.

Phone 2 calls Phone 3---->Press **888835#**. After getting through you will hear the Dial tone, then press the PSTN number **87654321#**.

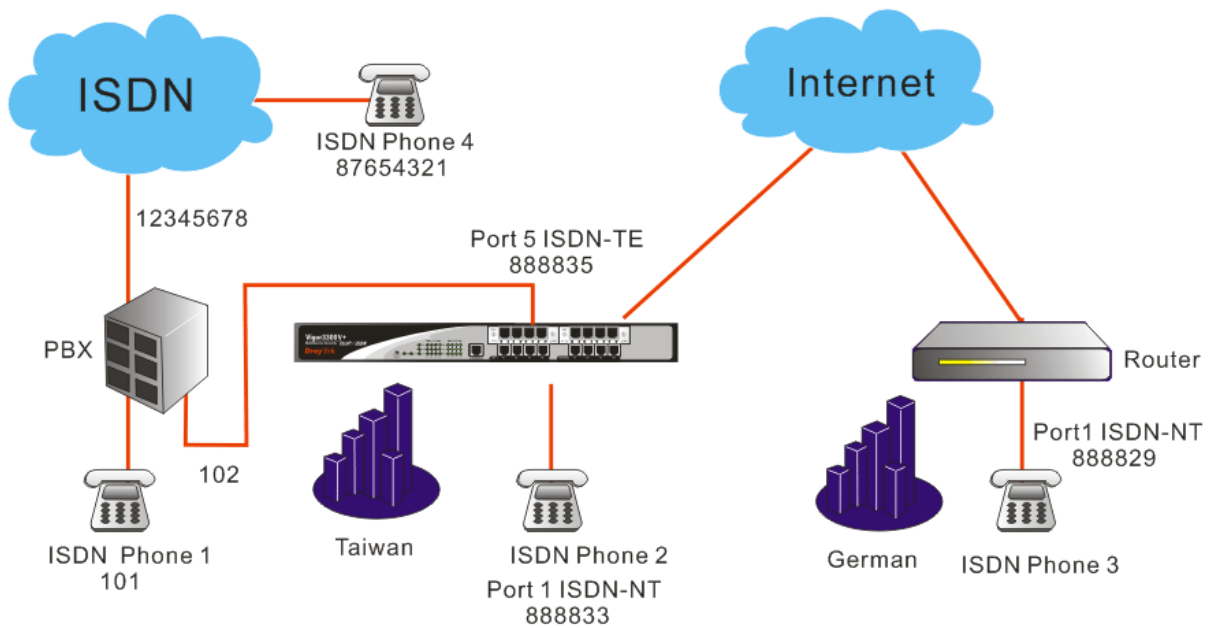
Phone 3 calls Phone 2---->Press **12345678**. After getting through you will hear the Dial tone, then press the VoIP number **888829#**.

Phone 3 calls Phone 1---->Press **12345678**. After getting through you will hear the Dial tone, then press the VoIP number **888833#**.

Note: # indicates termination of the phone number. After pressing #, VoIP is immediately called out. Or, you may wait 3 seconds if you do not press #.

- Connect PBX's Inside Lines. The usage is the same as that of common extension. Different PBX has its own settings and required configuration by you.

By connecting 3300V+'s ISDN-TE Port5 to PBX's Inside Line, VoIP is seamlessly integrated to PBX's inside lines and allows you to call not only the VoIP, but also the ISDN line and PBX's extension. Also the remote user can call you from the ISDN line and PBX's extension.



Configuration table between 3300V+ and 2910V

	WAN IP	Port Number	Phone Number	Proxy	Codec
3300V+	220.135.240.207	Port1(ISDN-NT)	888833	iptel	G.729A
		Port5(ISDN-TE)	888835	iptel	G.729A
2910V	61.31.167.135	Port1(ISDN-NT)	888829	iptel	G.729A

Suppose the number of PBX's Outside Line is 12345678. One Inside Line is connected to a telephone with the extension 101. If you want to use PSTN from the extension, you must firstly press 0, and then dial the phone number.

The ISDN-TE Port5 on the 3300V+ is connected to PBX's Inside Line with the number 102. The number of another PSTN line is 87654321.

About VoIP basic settings please refer to **VoIP Example 2 (Basic configuration and registration for ISDN)**

Start to dial by using telephones.

Phone 1 calls Phone 2---->Press extension **102**. After getting through you will hear the dial tone, then press the VoIP number **888833#**.

Phone 1 calls Phone 3---->Press extension **102**. After getting through you will hear the Dial tone, then press the VoIP number **888829#**.

Phone 2 calls Phone 1---->Press **888835#**. After getting through you will hear the Dial tone, then press the extension **101**.

Phone 2 calls Phone 4---->Press **888835#**. After getting through you will hear the Dial tone. Press outside line **0**, then press **87654321**.

Phone 3 calls Phone 1---->Press **888835#**. After getting through you will hear the Dial tone, then press the extension **101**.

Phone 3 call Phone 4---->Press **888835#**. After getting through you will hear the Dial tone. Press outside line **0**, then press **87654321**.

Phone 4 calls Phone 2---->Press **12345678**. After getting through you will hear the auto reply from the PBX, then press the extension **102**. After getting through you will hear the Dial tone, then press the VoIP number **888833#**.

Phone 4 calls Phone 3---->Press **12345678**. After getting through you will hear the auto reply from the PBX, then press the extension **102**. After getting through you will hear the Dial tone, then press the VoIP number **888829#**.

Note: # indicates termination of the phone number. After pressing #, VoIP is called out immediately. Or, you may wait 3 seconds if you do not press #. This example is intercommunication with one SIP Proxy Server. For the applications of Direct IP Call and Intercommunication with different SIP Proxy Servers please refer to **3.3.3 Example 3(Basic Calling Method)**. The VoIP call can also wok with VPN, please refer to **3.3.4 P Example 4(VoIP over VPN)**.

3.4 Application for mOTP

What is OTP and mobile-OTP

OTP (One-Time Password) is also named dynamic password with the feature of non-repeatability and validness just for one time. It uses more secure way to authenticate the data, named Two-factors. For the password will be changed all the time, it can avoid hackers or someone who interests to steal the account and password and then result in severe information security issue.

mobile-OTP is a free-charge resolution with **Strong Authentication**. It can generate OTP by using the mobile device (e.g., cell phone or PDA), USB disk, card or Token. Such resolution can visit router, firewall, network server or build VPN Tunnel based on time synchronization and one-time password. Refer to the following graphic for overall information.

How to apply mOTP to VPN Tunnel

First of all, load OTP program into the mobile device as mOTP token. Take Smart VPN Client as an example. The application can be shown as the following figure.



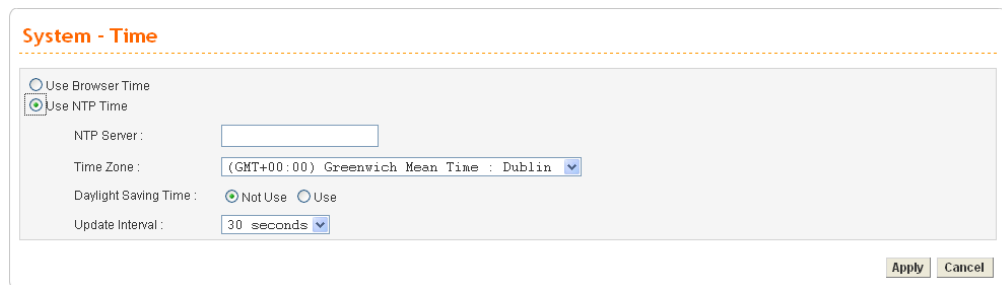
- VPN client must type username, pin code and secret number for authentication made by Vigor router.
- Use Smart VPN Client to finish relational dial-in settings for remote dial-in profile. Later, proceed to carry out remote VPN dial-in procedure.
- Vigor router will carry out the VPN dialing authentication. When it passes the authentication, it means that Remote Dial-in VPN is established successfully.

Example

In accordance to the above method, below shows an example. The user proceeds Smart VPN Client connection by using Smart VPN Client as mOTP token.

A. System Configuration in Vigor Router

1. Log in the web configurator of Vigor router and choose **System >> Time**.
2. Choose to use **Browse Time** or use **NTP Time** by specifying NTP server. Make sure **Current System** time. Click **Apply** to save it.



System - Time

Use Browser Time
 Use NTP Time

NTP Server:

Time Zone: (GMT+00:00) Greenwich Mean Time : Dublin

Daylight Saving Time: Not Use Use

Update Interval: 30 seconds

Apply Cancel

B. mOTP Operation in Smart VPN Client

1. Run Draytek Smart VPN Client. Click **Insert** to add a new VPN profile.



2. You can see the following screen.

Dial To VPN

Profile Name : mOTP

Auto re-dial after disconnect.

Auto run when system start up.

VPN Server IP/HOST Name(such as 123.45.67.89 or draytek.com)

114.37.161.182

User Name : draytek

Password :

Enable mobile One Time Password (mOTP)

Configure Secret for mOTP

Type of VPN

PPTP L2TP

IPsec Tunnel L2TP over IPsec

SSL VPN Tunnel

PPTP Encryption

No encryption

Require encryption

Maximum strength encryption

Authentication method MS-CHAP v2

Use default gateway on remote network More

OK Cancel

3. Type the profile name for such VPN (in this case, it is **mOTP**) and the VPN server IP address (in this case, it is **114.37.161.182**) .
4. Type the User Name (in this case, it is **draytek**) and check **Enable Mobile one time password (mOTP)**.
5. Press the button of **Configure Secret for mOTP** to generate the secrete number. In this case, **Automatically generate secret** is selected. It will generate a 32-digit secret number automatically. Next, click **Generate**.

Configure Secret for mOTP

Automatically generate secret

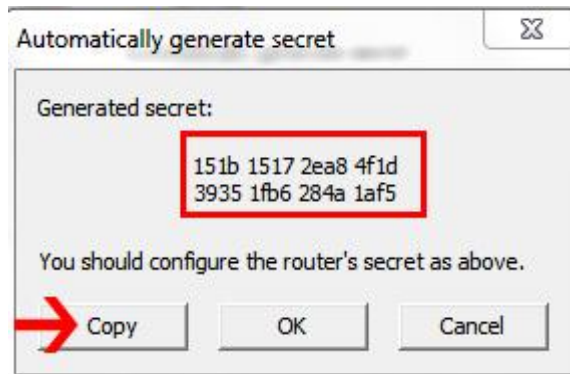
Manually type and store secret

Secret:

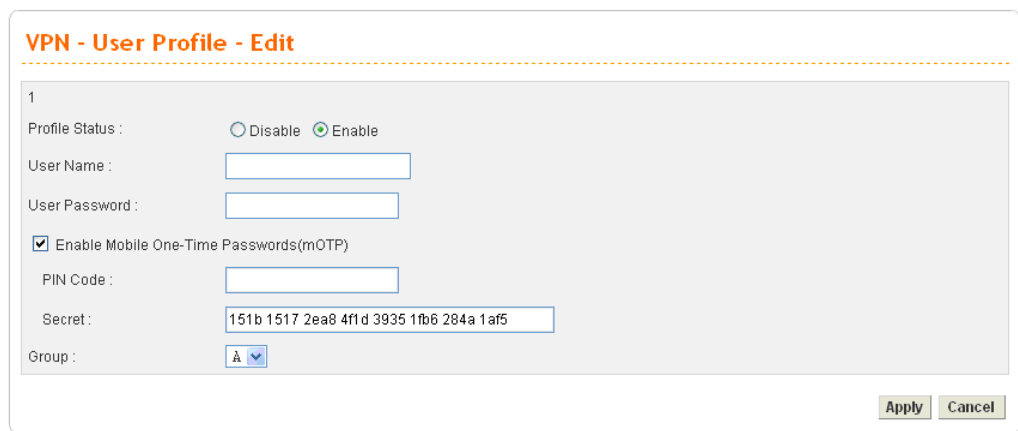
Note: To obtain fully secured authentication, you'd better use a Mobile device to generate or save the secret, instead. Such feature is used to experience Vigor mOTP function only.

Generate Cancel

6. A 32-digit secret number is generated randomly. Please click **Copy**.



7. Fill this number in the field of **Secret** in **VPN – User Profile – Edit** of Vigor 3300V+ web page. Then, click **Apply**.



8. In the field of **Type of VPN**, choose the type of VPN (in this case, it is **PPTP**) and click **Require Encryption**.
9. Choose **MS-CHAP v2** as **Authentication method**. Next, click **OK** to return to previous page.
10. After finishing Smart VPN Client configuration, click **Connect** to proceed the remote-dial in connection.



11. Type Username and pin code, e.g, draytek and 1234.

Dial To VPN

Type of VPN	PPTP (mOTP)
Remote IP Address	114.37.161.182
User Name :	draytek
Password :	
PIN Code:	****

OK Cancel

This page is left blank.

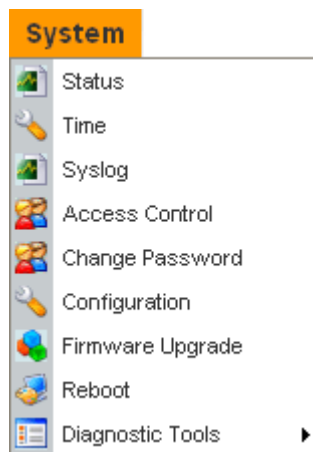
Chapter 4: Reference - Advanced Web Configuration

After finished basic configuration of the router, you can access Internet with ease. For the people who want to adjust more setting for suiting his/her request, please refer to this chapter for getting detailed information about the advanced configuration of this router. As for other examples of application, please refer to chapter 3.

4.1 System Setup

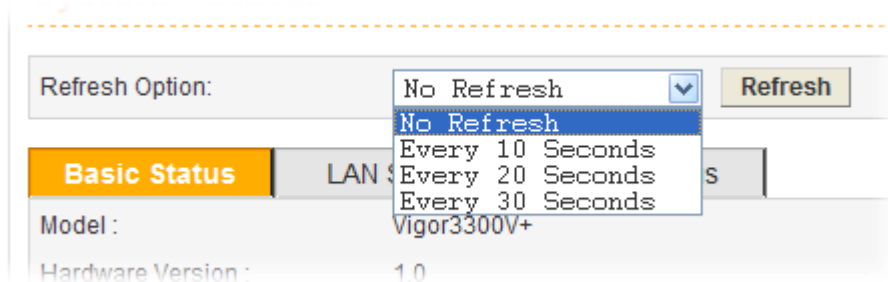
For the system setup, there are several items provided for you to configure ---- Status, Time Setup, Syslog Setup, Access Control Setup, Reboot and Firmware Upgrade Setup, Diagnostic Tools and Configuration Setup.

Below shows the menu items for System.



4.1.1 Status

The online **Status** function provides some useful system information on the current status of the Vigor3300V+ Series. A user can observe the system status on this Web page and determine which setting needed to be changed in corresponding web pages. Open **System >>Status**. The online **Status** Web page contains three parts: **Basic Status**, **LAN Status**, and **WAN Status**.



Refresh Option You can choose to refresh the Web page information automatically. There are four options given as shown below.

No Refresh: Static information page.

Every 10 Seconds: Refreshes the page every 10 seconds.

Every 20 Seconds: Refreshes the page every 20 seconds.

Every 30 Seconds: Refreshes the page every 30 seconds.

Basic Status

General status of this router will be displayed in this page.

System - Status

Refresh Option:

Basic Status	LAN Status	WAN Status
Model :	Vigor3300V+ series	
Hardware Version :	1.0	
Firmware Version :	2.6.3 (EN)	
Build Date&Time :	2010-08-17 14:31:01	
System Uptime :	0 days 2 hours 54 minutes 14 seconds	
CPU Usage :	8.1173%	
Memory Size :	128 MBytes	
Memory Usage :	25.6968%	
Current System Time :	1983-11-15 00:10:09	

Model	Display the model name of the router.
Hardware Version	Display the hardware version of the router.
Firmware Version	Display the firmware version of the router.
Build Date&Time	Display the date and time of the current firmware build.
System Uptime	Display the amount of time that the router has been online.
CPU Usage	Display the average percentage of the CPU used.
Memory Size	Display the size of the memory of this router.
Memory Usage	Display the percentage of memory used.
Current System Time	Display the current local system time.

LAN Status

The status of LAN connection will be displayed in this page. Simply click **LAN Status** tag to get the detailed.

System - Status

Refresh Option:

Basic Status	LAN Status	WAN Status
--------------	-------------------	------------

LAN1 :

IP Address :	192.168.1.1
MAC Address :	00:50:7F:2F:C4:C5
High Availability Status :	
RX Packets :	771
TX Packets :	551

IP Address

Display the IP address of the LAN interface.

MAC Address

Display the MAC address of the LAN Interface.

High Availability Status

The High Availability Status is shown when it is enabled in **Network>> High Availability**. When there are two Vigor3300V+ devices in the same LAN, one can be set as Master device and the other can be set as Slave device.
Master - It means that Vigor3300V+ plays the Master role in high availability feature.
Slave - It means that Vigor3300V+ plays the Slave role in high availability feature.
If there is only one Vigor3300V+ used in LAN, this line will be blank.

RX Packets

Display the total number of received packets at the LAN interface.

TX Packets

Display the total transmitted packets at the LAN interface.

WAN Status

The status of WAN interface (Static, DHCP, PPPoE, PPTP or DMZ) is shown in this page. Simply click **WAN Status** tag to get the detailed. There are four sets of WAN status can be shown in this page at one time. The sample below just lists one set of WAN status for only WAN1 interface is used.

System - Status

Refresh Option:

Basic Status	LAN Status	WAN Status
WAN1 :		WAN2 :
IP Address :	172.16.3.102	IP Address :
MAC Address :	00:50:7f:2f:c4:c6	MAC Address : 00:50:7f:2f:c4:c7
Primary DNS :	168.95.1.1	Primary DNS :
Secondary DNS :	168.95.192.1	Secondary DNS :
Gateway :	172.16.1.1	Gateway :
RX Packets :	9867	RX Packets :
TX Packets :	684	TX Packets :
Connection Status :	connected	Connection Status :
Up Time :	0 days 0 hours 3 minutes 47 seconds	Up Time :
WAN3 :		WAN4 :
IP Address :		IP Address :
MAC Address :	00:50:7f:2f:c4:c8	MAC Address : 00:50:7f:2f:c4:c9
Primary DNS :		Primary DNS :
Secondary DNS :		Secondary DNS :
Gateway :		Gateway :
RX Packets :		RX Packets :
TX Packets :		TX Packets :
Connection Status :		Connection Status :
Up Time :		Up Time :

IP Address

Display the IP address of the WAN interface.

MAC Address

Display the MAC address of the WAN Interface.

Primary DNS

Display the IP address of the primary DNS.

Secondary DNS

Display the IP address of the secondary DNS.

Gateway

Display the IP address of the default gateway.

RX Packets

Display the total received packets for each WAN interface.

TX Packets

Display the total transmitted packets for each WAN interface.

Connection Status

Display the connection status of the WAN interface.

Up Time

Display the total system uptime of the interface.

Connect

Click this button to make a connection manually.

4.1.2 Time

As an NTP (Network Time Protocol) client, the router gets standard time from the time server. Some time-based functions, such as **Call Schedule** and **URL Content filtering**, cannot work properly until the system time functions run successfully. Typically, NTP achieves high accuracy and reliability with multiple redundant servers and diverse network paths.

The Vigor3300 Series supports synchronization with a specific NTP server or the remote PC host of the administrator. In the **System** group, click the **Time** option. The Time page is shown below:

System - Time

Use Browser Time
 Use NTP Time

NTP Server :

Time Zone : (GMT+00:00) Greenwich Mean Time : Dublin ▼

Daylight Saving Time : Not Use Use

Update Interval : 30 seconds ▼

Apply Cancel

- | | |
|------------------------------|--|
| Use Browser Time | Click this option to use the browser time from the remote administrator PC host as router's system time. |
| Use NTP Time | Click this option to use the time from an NTP server as router's system time. |
| NTP Server | Type a public IP address or domain name of the NTP time server. |
| Time Zone | Select the time zone where the router is located. |
| Daylight Savings Time | Select Use to activate this function. This function is useful for some areas. |
| Update Interval | Select a time interval for updating from the NTP server. |
| Apply | Click Apply to save these settings. |

4.1.3 Syslog

The Vigor3300V+ Series supports a Syslog function to keep a record of abnormal conditions. The router will send Syslog packets to a Syslog server on the remote site. The administrator can observe any abnormal events from the router. Open **System**>> **Syslog**. The Syslog web page is shown below:

System - Syslog

Disable Enable

Syslog Server IP :

Syslog Server Port :

Firewall Log :

VPN Log :

User Access Log :

Call Log :

WAN Log :

VoIP syslog option

Syslog Facility :

Syslog Severity :

Apply Cancel

Disable/Enable Click **Enable** to activate this function. The router will send system log message for your reference. If you click **Disable**, the router will not send out any message about system log.

Syslog Server IP The IP address of the Syslog server. If a user assigns an IP address of “0.0.0.0”, the Syslog function will be disabled. Then, the router will not send Syslog packets to the Syslog server.

Syslog Server Port Type a port for the Syslog protocol.

Firewall Log Check this box to record the firewall log.

VPN Log Check this box to record the VPN application log.

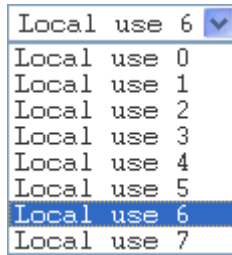
User Access Log Check this box to record the user access log. Such information will be seen in Syslog server.

Call Log Check this box to record the VoIP/ISDN phone log.

WAN Log Check this box to record the connection status log for WAN interface.

Syslog Facility When Vigor3300V+ runs VoIP program for dialing VoIP phone calls, information about VoIP starting, restarting, registered, crashed, and etc., will be created at the same time. Such information will be useful for the administrator to understand the running status of VoIP function and will be helpful for the administrator to solve the problems encountered.

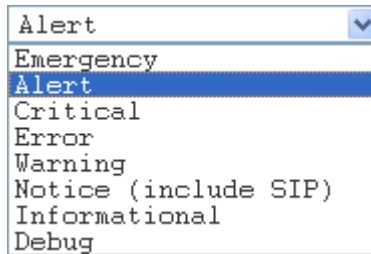
Syslog protocol usually will classify messages into several levels (facilities) based on the service types. Each facility (Local use0 ~ Local use7) possesses items and services used generally. The administrator can specify any one of the facilities used for VoIP function. Such function can assist the administrator to identify which log containing VoIP information.



Syslog Severity

Such feature is used to determine which types of error logs recorded under different conditions.

There are eight levels representing different severities. For example, if you choose Debug as the severity, the VoIP syslog will record log including Debug, Informational, Notice, Warning, Error, Critical, Alert and Emergency. And, if you choose Critical, the situation of Critical, Alert and Emergency will be recorded. That is, Debug owns the lowest severity and Emergency owns the highest severity.



Apply

Click **Apply** to save these settings.

Note: VoIP Syslog option is useful for the trouble(s) happened while using VoIP feature of Vigor router. It is optional and will be asked to be configured by the maintenance engineers when Vigor users meet the problem of VoIP and need help.

4.1.4 Access Control

This page allows you to determine which services (HTTP/Telnet/SSH) is used for the user to access Vigor router. In addition, you can also limit some hosts to access router Series with specified IP address.

Open **System>> Access Control**. You will get the following page:

Management Method

There are several servers provided by the system to allow you managing the router from Internet. Check the box(es) to specify.

Allow Management from the WAN

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.

Disable - Disable the management from the WAN interface.

Enable All - Enable all management (through HTTP/Telnet/SSH) from the WAN interface.

Enable User Defined WAN IP - System can be managed by these three IP addresses via WAN.

Allowed IP1 ~ IP3 – The former box indicates an IP address allowed to login to the router, and the later box indicates a subnet mask allowed to login to the router.

Management Port

Default Ports - Use the default ports for HTTP and Telnet if you choose HTTP and Telnet as management methods.

User Defined Ports - Or you can assign new port numbers for HTTP, Telnet and SSH respectively.

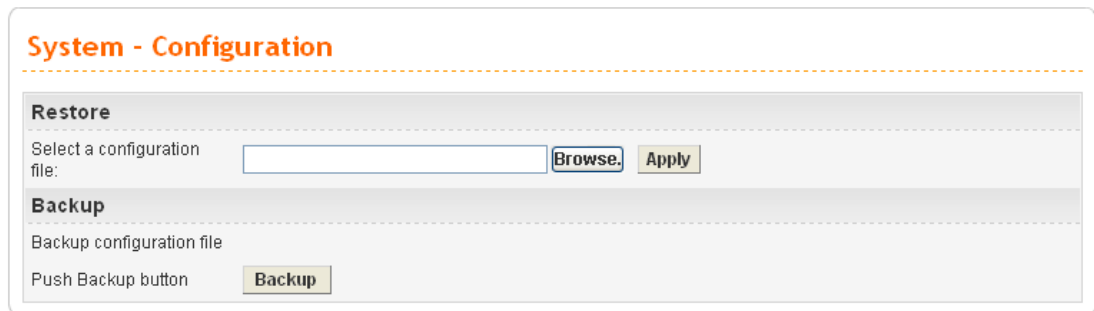
PING Restriction

Disable PING from the LAN -Choose this function to reject all ICMP packets from LAN side.

Disable PING from the WAN - Choose this function to reject all ICMP packets from WAN side.

4.1.5 Configuration Setup

Most of the settings can be saved locally as a configuration file, and can be applied to another router. The Vigor3300V+ Series supports the restore and upload functions of the **configuration files**. Open **System>>Configuration**. You can see the following page.



The screenshot shows a web interface titled "System - Configuration". It is divided into two main sections: "Restore" and "Backup".

- Restore Section:** Contains the text "Select a configuration file:" followed by an empty text input field, a "Browse..." button, and an "Apply" button.
- Backup Section:** Contains the text "Backup configuration file" and "Push Backup button" followed by a "Backup" button.

Select a Configuration File Please click the **Browse...** button to find out the location of the configuration file to be uploaded to the router and click **Apply**.

Backup Configuration File Push Backup Button Download the configuration file to a local host. The default file name is "v3300.cfg".

4.1.6 Firmware Upgrade Setup

Vigor3300V+ Series allows users to upgrade firmware through a Web interface. Click **System>>Firmware Upgrade**. You can see the following page. Before you execute the firmware upgrade, please download the **newest firmware** from Draytek's website (www.draytek.com) or FTP site ([ftp.draytek.com](ftp://ftp.draytek.com)) on the computer first.

System - Firmware Upgrade

Caution : After an upgrade procedure a reboot is required.

Current Version : Vigor3300V+ series 2.6.3 (EN)

Location : Local Remote

Firmware : **Browse...**

TFTP Server IP

Remote File Name

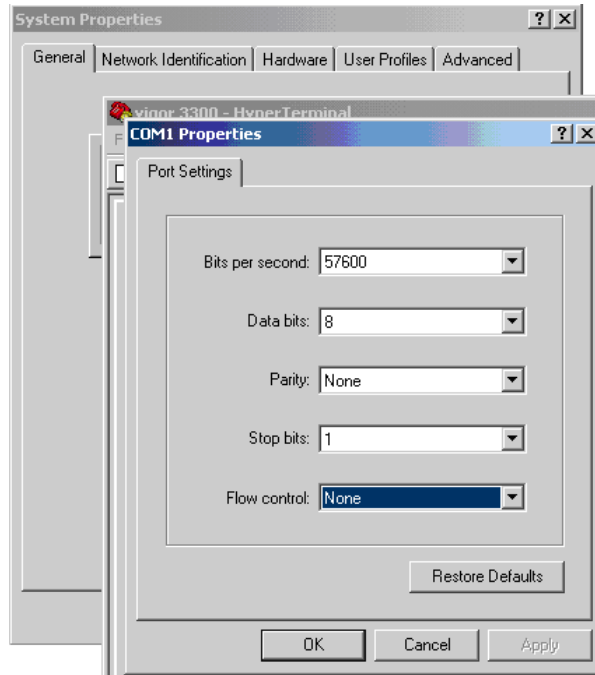
Apply **Cancel**

Caution	Display a caution for your reference.
Current Version	Display current firmware version that you are using.
Location	<i>Local</i> means upgrade firmware from browser. <i>Remote</i> means upgrade firmware from a remote TFTP server.
Firmware	Specify the location of the firmware file if you want to upgrade the firmware locally
TFTP Server IP	If you want to upgrade the firmware of this router from remote side, please type the IP address of the TFTP server.
Remote File Name	The default filename will be shown here. If you have use another name to save the firmware file, please type the new name in this field.
Apply	After finished your selection, please click Apply to execute the firmware upgrade.

Firmware Upgrade from a Console Port

Firmware upgrade can be done from a console port, too. The following example was run on a Windows environment.

1. Download the newest firmware from the DrayTek Website (www.draytek.com.tw) or FTP site ([ftp.draytek.com](ftp://ftp.draytek.com)) on your computer first.
2. Connect the RJ45 connector of console cable to the console port on Vigor3300 and the DB9 connector of the console cable to the RS232 port on the PC.



The default setting of the console port is “baud rate 57600, no parity, and 8 bit with 1 stop bit.”

3. Power on Vigor3300V+, then press **ENTER** before the system reboots completely.
4. Open Hyper Terminal on the PC. Now, Vigor3300V+ can accept a TFTP download and will display the following message:

```

*****
* DrayTek V3300 Bootloader *
*****

Press [ENTER] key within 5 sec. to download image...2
Current LAN IP is 192.168.1.1
New IP:
Prepare downloading.
  
```

5. Type the path name of the firmware image and activate the **TFTP Client** from the PC to download the image. The corresponding message is shown as follows:

```
TFTP -i 192.168.1.1 PUT [Vigor3300 image file name]
```



```

3300 - HyperTerminal
File Edit View Call Transfer Help
slot = 0 sector size = 65536
slot = 0 sector size = 65536
slot = 0 sector size = 65536
slot = 0 sector size = 65536
slot = 0 sector size = 65536
Updating flash block at bfd30000
set ethaddr0 00:50:7f:28:80:e3
set ethaddr1 00:50:7f:28:80:e4
set ethaddr2 00:50:7f:28:80:e4
set #default_nif_wan1_mac 00:50:7f:28:80:e4
set #default_nif_wan2_mac 00:50:7f:28:80:e5
set #default_nif_wan3_mac 00:50:7f:28:80:e6
set #default_nif_wan4_mac 00:50:7f:28:80:e7
set flash0_0 "780000:80000:general"

DrayTek Corporation Vigor 3300
Firmware version: V2.5.7
Hardware version: 0
V3 board, for V3 GPIO config
have voip card

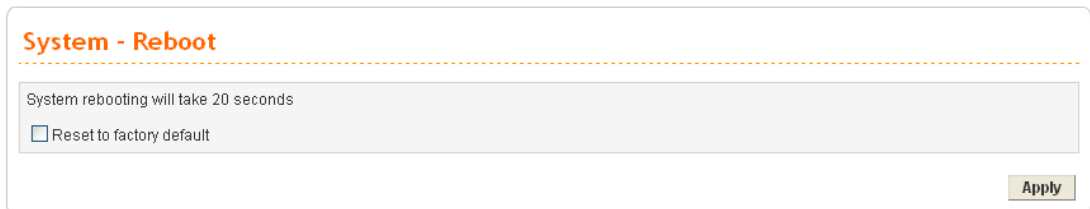
Draytek login: 3300 series

```

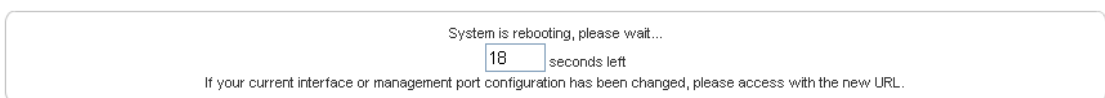
4.1.7 Reboot

The Vigor router system can be restarted from a Web browser. **Reboot** screen can appear after you finish the changing of WAN and LAN settings. You have to reboot the router to invoke the configured settings that you made before. Besides, you can select **Reset to factory default** to reboot the device and retrieve the default settings.

Click **System>>Reboot**. If you want to reboot the router using the current configuration, click **Apply**. To reset the router settings to default values, check **Reset to factory default** and click **Apply**.



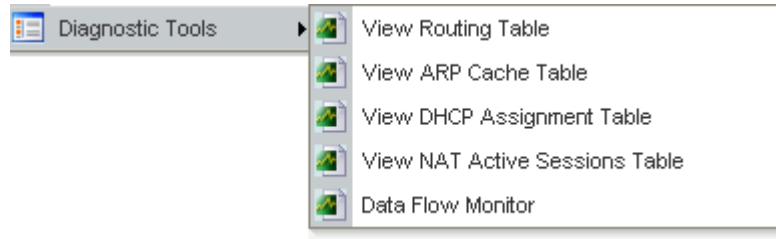
Click **Apply** to reboot the whole system. The rebooting procedure usually takes 20 or more seconds.



4.1.8 Diagnostic Tools

In some cases, a user may need to know some information about the router, such as static or dynamic databases, or other routing information. The Vigor3300V+ supports five functions, **Routing Table**, **ARP Cache Table**, **DHCP Assignment Table**, **NAT Active Sessions Table** and **Data Flow Monitor** for the user to review such information.

In the **System** group, click the **Diagnostic Tools** option



- Select **View Routing Table** to get the following page:

System - Diagnostic Tools - View Routing Table

Destination	Gateway	Subnet Mask	Flags	Interface
172.16.2.0	*	255.255.255.0	U	eth0
1.1.1.0	*	255.255.255.0	U	vlan10
1.1.1.0	*	255.255.255.0	U	ipsec0
127.0.0.0	*	255.0.0.0	U	lo

Refresh

Destination	Display the destination IP address for various routings.
Gateway	Display the default gateway.
Subnet Mask	Display the subnet mask for various routings.
Flags	Display the status of the routing entries.
Interface	Denoted by eth0 if it is a LAN interface and eth1 if it is a WAN interface.
Refresh	Click Refresh to re-display this web page for getting newest routing information.

- Select **View ARP Cache Table** to get the following page:

System - Diagnostic Tools - View ARP Cache Table

Index	IP Address	MAC Address	Interface
1	192.168.1.1	00:50:7F:00:00:00	eth0
2	192.168.1.10	00:0E:A6:2A:D5:A1	eth0

- IP Address** Display the IP address for different ARP cache.
- MAC Address** Display the MAC address for different ARP cache.
- Interface** Denoted by **eth0** if it is a LAN interface and **eth1** if it is a WAN interface.
- Refresh** Click **Refresh** to re-display this web page for getting newest ARP information.

- Select **View DHCP Assignment Table** to get the following page:

System - Diagnostic Tools - View DHCP Assignment Table

Index	Assigned IP	MAC Address	Time Left
1	192.168.1.10	00:00:00:00:00:00	expired
2	192.168.1.11	00:0E:A6:2A:D5:A1	expired

- Assigned IP** Display the IP address of the static DHCP server.
- MAC Address** Display the MAC address of the static DHCP server.
- Time Left** Display the remaining time for this IP address assigned by DHCP server. When the time expired, such IP address would not be kept for this client and might be assigned to other client.
- Refresh** Click **Refresh** to re-display this web page for getting newest routing information.

- Select **View NAT Active Sessions Table** to get the following page. This table can display about 30000 sessions with 20 pages.

System - Diagnostic Tools - View NAT Active Sessions Table

Type	Expire in	State	Source IP	Dest IP	sPort	dPort	Rep Source IP	Rep Dest IP	sPort	dPort
tcp	591	ESTABLISHED	192.168.1.222	207.46.6.24	3435	1863	207.46.6.24	172.16.2.225	1863	34682
tcp	598	ESTABLISHED	192.168.1.222	207.46.6.153	3476	1863	207.46.6.153	172.16.2.225	1863	34723

Page Index : 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20

Type	Display the protocol used for the active session.
Expire in	Display the remaining time (second) of this session.
State	Display the condition of this session.
Source IP	Display the source IP address of the packet transmitted.
Dest IP	Display the destination IP address of the packet transmitted.
sPort	Display the source port of the packet transmitted.
dPort	Display the destination port of the packet transmitted.
Rep Source IP	Display the source IP address of the packet replied.
Rep Dest IP	Display the destination IP address of the packet replied.
sPort	Display the source port of the packet replied.
dPort	Display the destination port of the packet replied.

- Select **Data Flow Monitor** to get the following page. This page displays the running procedure for the IP address monitored and refreshes the data in an interval of several seconds.

System - Diagnostic Tools - Data Flow Monitor

Disable Enable Refresh Seconds: 10

Index	IP Address	TX rate(kbps)	RX rate(kbps)	NAT sessions	Action
Page Index : 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20					

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 Action column will display the expire time left.

Refresh

Disable/Enable	Click Enable to invoke this function.
Index	Display the number of the data flow.
IP Address	Display the IP address of the monitored device.
TX rate (kbps)	Display the transmission speed of the monitored device.
RX rate (kbps)	Display the receiving speed of the monitored device.

Sessions	Display the session number that you specified in Limit Session web page.
Action	Block - can prevent specified PC accessing into Internet within 5 minutes. Unblock – the device with the IP address will be blocked in five minutes. The remaining time will be shown on the session column.
Refresh Seconds	Use the drop down list to choose the time interval of refreshing data flow that will be done by the system automatically.
Refresh	Click Refresh to re-display this web page for getting newest routing information.

4.2 Network Setup

Quick Setup offers user an easy method to quick setup the connection mode for the router. Moreover, if you want to adjust more settings for different WAN modes, please go to **Network**.

Basic of Internet Protocol (IP) Network

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

From 10.0.0.0 to 10.255.255.255

From 172.16.0.0 to 172.31.255.255

From 192.168.0.0 to 192.168.255.255

What are Public IP Address and Private IP Address

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

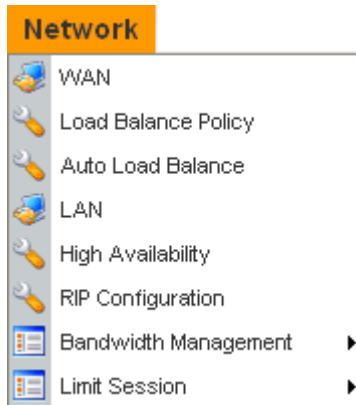
Get Your Public IP Address from ISP

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

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

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

Below shows the menu items for **Network**.



4.2.1 WAN

The Vigor3300V+ Series supports four WAN interfaces (Static, DHCP, PPPoE and PPTP), which share the same setting page. Click **Network >>WAN**. The following page will be shown.

Network - WAN

Load Balance : Disable Enable (Auto Weight)

Backup : Disable Enable

#	Edit	IP Mode	Active	Default Route	Load Balance	Weight	Backup-Master	Backup-Slave	VoIP
WAN1		Static	<input checked="" type="checkbox"/>	<input checked="" type="radio"/>	<input type="checkbox"/>	10%	<input checked="" type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
WAN2		Not Set	<input type="checkbox"/>	<input type="radio"/>	<input type="checkbox"/>	10%	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
WAN3		Not Set	<input type="checkbox"/>	<input type="radio"/>	<input type="checkbox"/>	10%	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
WAN4		Not Set	<input type="checkbox"/>	<input type="radio"/>	<input type="checkbox"/>	10%	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

- Load Balance** Enables or disables the WAN load balance function. The **Auto Weight** option becomes available if **Enable** mode is selected. Load Balance allows the router distributing data in and out of the Internet by using different WAN interfaces at the same time.
- Backup** Enables or disables backup function for WAN interfaces. If you enable this function, the backup-master/backup-slave will execute the job of master/slave device when the master/slave device fails to work.
- Edit** Open the configuration page of this WAN interface.
- IP Mode** Display current mode of this WAN interface. There are five options: Static, DHCP, PPPoE, PPTP and DHCP.
- Active** Activates/closes this WAN interface.
- Default Route** Set this WAN interface as default route interface.
- Load Balance** Adds this WAN interface to the load balance group.

- Weight** Set the weight load (10-90%) for this WAN interface for load balance. This selection is available only when Auto Weight is unchecked.
- Backup-Master** Set this WAN interface as a master interface. WAN1 must be assigned as Master interface if Backup function is enabled.
- Backup-Slave** Set this WAN interface as a slave interface.
- VoIP** Set this WAN interface for VoIP phone call. Such item is available only when a FXO / FXS module has been installed onto the router.

Most users will use their routers primarily for Internet access. The Vigor3300V+ Series supports broadband Internet access and provides multiple WAN interfaces. The following sections will give a detailed illustration to broadband access methods.

Configuring WAN Settings

Click the “Edit” icon from **Network >>WAN** page to bring up the WAN configuration page for the corresponding interface.

Network - WAN - WAN1 - Fast Ethernet

The screenshot shows the WAN configuration interface for WAN1 - Fast Ethernet. It includes the following fields and options:

- MAC Address:** Radio buttons for **Default MAC** (selected) and **User Defined MAC**. A text box contains the value `00:00:00:00:00:02`.
- Downstream Rate:** Text box with value `102400` and unit `(kbps)`.
- Upstream Rate:** Text box with value `102400` and unit `(kbps)`.
- Type:** Dropdown menu showing `Fast Ethernet`.
- Physical Mode:** Dropdown menu showing `Auto Negotiation`.
- IP Mode:** Radio buttons for **Static** (selected), **DHCP**, **PPPoE**, **PPTP**, and **DMZ**.

- MAC Address** **Default MAC** - Uses the default Mac address.
User Defined MAC - Uses a MAC address defined by users. If you select this item, you have to type the MAC address in the box below.
- Downstream Rate** Set downstream rate for this WAN interface. The default value is 102400 kbps (100 Megabit).
- Upstream Rate** Set transmission rate for this WAN interface. The default value is 102400 kbps (100 Megabit).
- Type** Set connection type for this WAN interface.
- Physical Mode** Set connection speed mode. There are five options including **Auto negotiation, full duplex, half duplex, 10M and 100M**.
- IP Mode** Set an IP Mode with **Static (fixed IP), DHCP (dynamic IP address), PPPoE, PPTP or DMZ** and creates the IP group information. Most cable modem users will use DHCP to get a globally reachable IP address from the cable head-end system. Different mode will lead different configuration and will be explained in later section.

Before you connect a broadband access device e.g. a DSL/Cable modem to Vigor3300V+, you need to know what kind of Internet access your ISP provides. The following sections introduce several widely used broadband access services: **Static, PPPoE, PPTP** for DSL, **DHCP** for Cable modem and **DMZ**. In most cases, you will get a DSL or cable modem from the broadband access service provider. Vigor3300V+ is connected behind the broadband device i.e. DSL/cable modem and works as a NAT or IP router for broadband connections.

Next, we will introduce each WAN mode in detailed.

Static IP Setup

It means that the IP group information for WAN interface is manually assigned by the user.

Static/DHCP Configuration	PPPoE/PPTP Configuration	DMZ Configuration
IP Address :	<input type="text" value="172.16.3.229"/>	Host Name : <input type="text"/>
Subnet Mask :	<input type="text" value="255.255.255.0"/>	Domain Name : <input type="text"/>
Default Gateway :	<input type="text" value="172.16.3.1"/>	(Host Name and Domain Name are required for some ISPs.)
Primary DNS :	<input type="text" value="168.95.1.1"/>	
Secondary DNS :	<input type="text" value="168.95.192.1"/>	
MTU :	<input type="text" value="1500"/>	
Connection Detection		
Detect Type :	<input type="text" value="Send ARP to Gateway"/>	
Detect Interval(sec) :	<input type="text" value="10"/>	
No-Reply Count :	<input type="text" value="2"/>	
Detect Destination Host : (IP or Domain Name)	<input type="text"/>	
IP Alias List		
1.	<input type="text" value="10.1.1.100"/>	2. <input type="text" value="10.1.1.101"/>
3.	<input type="text" value="10.1.1.102"/>	4. <input type="text"/>
5.	<input type="text"/>	6. <input type="text"/>
7.	<input type="text"/>	8. <input type="text"/>
9-32		
<input type="button" value="Apply"/> <input type="button" value="Reset"/> <input type="button" value="Cancel"/>		

IP Address

Set the private IP address of WAN interface.

Subnet Mask

Set the subnet mask value of WAN interface.

Default Gateway

Set the private IP address of gateway.

Primary DNS

Set the private IP address of primary DNS.

Secondary DNS

Set the private IP address of secondary DNS.

MTU

Mean maximum transmission unit of one packet. The default value is 1500.

Host Name

Some ISP may ask you to type your host name. Please type in if necessary.

Domain Name

Some ISP may ask you to type your domain name. Please type in if necessary.

Detect Type

Select a detecting type for this WAN interface. There are three ways **Send ARP to Gateway**, **Send PING** and **Send HTTP Request** supported in 3300.

Send Http Request	▼
Send ARP to Gateway	
Send PING	
Send Http Request	

Detect Interval (sec)

Assign an interval period of time for each detecting. The minimum value is 3 and no limit for maximum value.

No-Reply Count

Assign detecting times to ensure the connection of the WAN. After passing the times you set in this field and no reply

received by the router, the connection of WAN interface will be regarded as breaking down.

Detect Destination Host (IP or Domain Name)

Assign an IP address or Domain name as a destination to be detected whether the host is active (sending reply to the router) or not. If not, the connection of WAN interface will be regarded as breaking down. This function is available when **Detect Type** is set with **Send PING** or **Send Http Request**.

IP Alias List

Set other IP addresses binding in this interface. You can set up to 32 sets of IP alias settings. If you have typed addresses here, you can see and choose it in later web page settings (e.g., **Advanced >> NAT>>Port Redirection/DMZ Host**).

Apply

Click **Apply** to go back to the WAN Interface Configuration page. To apply all settings, click **Apply** on the WAN Interface Configuration page and reboot your router.

Reset

Click this button to clear all the configurations for this page.

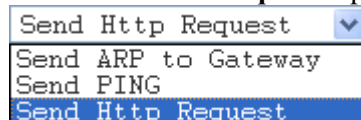
DHCP Client Setup

If the WAN interface is set as a DHCP client, the Vigor3300 Series will ask for IP network settings from the DHCP server or DSL modem automatically. In general, it is not necessary for users to manually configure the router. However, users can modify **Connection Detection** if required.

Static/DHCP Configuration	PPPoE/PPTP Configuration	DMZ Configuration
IP Address :	<input type="text" value="172.16.3.229"/>	Host Name : <input type="text"/>
Subnet Mask :	<input type="text" value="255.255.255.0"/>	Domain Name : <input type="text"/>
Default Gateway :	<input type="text" value="172.16.3.1"/>	(Host Name and Domain Name are required for some ISPs.)
Primary DNS :	<input type="text" value="168.95.1.1"/>	
Secondary DNS :	<input type="text" value="168.95.192.1"/>	
MTU :	<input type="text" value="1500"/>	
Connection Detection		
Detect Type :	<input type="text" value="Send ARP to Gateway"/>	
Detect Interval(sec) :	<input type="text" value="10"/>	
No-Reply Count :	<input type="text" value="2"/>	
Detect Destination Host : (IP or Domain Name)	<input type="text"/>	
<input type="button" value="Apply"/> <input type="button" value="Reset"/> <input type="button" value="Cancel"/>		

Connection Detection

Detect Type - Select a detecting type for this WAN interface. There are three ways **Send ARP to Gateway**, **Send PING** and **Send HTTP Request** supported in the router.



Detect Interval (sec) - Assign an interval period of time for each detecting. The minimum value is 3 and no limit for maximum value.

No-Reply Count - Assign detecting times to ensure the

connection of the WAN. After passing the times you set in this field and no reply received by the router, the connection of WAN interface will be regarded as breaking down.

Detect Destination Host (IP or Domain Name) - Assign an IP address or Domain name as a destination to be detected whether the host is active (sending reply to the router) or not. If not, the connection of WAN interface will be regarded as breaking down. This function is available when **Detect Type** is set with **Send PING** or **Send Http Request**.

Apply

Click **Apply** to go back to the WAN Interface Configuration page. To apply all settings, click **Apply** on the WAN Interface Configuration page and reboot your router.

Reset

Click this button to clear all the configurations for this page.

PPPoE with a DSL Modem Setup

Most DSL modem users will use this mode. All the local users can share one PPPoE connection to access the Internet.

User Name

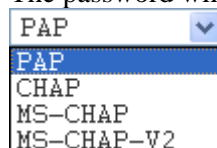
Assign a specific valid user name provided by local ISP.

Password

Assign a valid password provided by local ISP.

Authentication

Select **PAP**, **CHAP**, **MS-CHAP** or **MS-CHAP-V2** protocol for PPP authentication according to the feature that your ISP provided for widest compatibility. The default value is **PAP**. The password will be encrypted in CHAP but not in PAP.



Service Name

Assign a service name required for some ISP services.

PPPoE IP Alias

Set other IP addresses binding in this interface. You can set up to 32 sets of IP alias settings. If you have typed addresses here, you can see and choose it in later web page settings (e.g., **Advanced >> NAT>>Port Redirection/DMZ Host**).

- MTU** Mean maximum transmission unit of one packet. The default value is 1442.
- Fixed IP/Fixed IP Address** Usually ISP dynamically assigns IP address to you each time you connect to it and request. In some case, your ISP provides service to always assign you the same IP address whenever you request. In this case, you can fill in this IP address in the Fixed IP field. Please contact your ISP before you want to use this function. Click **Yes** to use this function and type in a fixed IP address in the box of **Fixed IP Address**.
- Detect Interval** Assign an interval time for detecting if the WAN connection is on or off.
- No-Reply Count** Assign detecting times to ensure the connection of the WAN. After passing the times you set in this field and no reply received by the router, the connection of WAN interface will be regarded as breaking down.
- Always On** Click this button to make the connection of the WAN will be always on.
- Apply** Click **Apply** to go back to the WAN Interface Configuration page. To apply all settings, click **Apply** on the WAN Interface Configuration page and reboot your router.
- Reset** Click this button to clear all the configurations for this page.

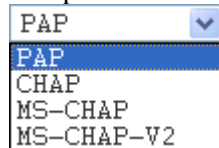
PPTP with a DSL Modem Setup

The service provider must provide the exact settings for this mode.

Static/DHCP Configuration	PPPoE/PPTP Configuration	DMZ Configuration
User Name :	<input type="text" value="dray"/>	PPTP Local Address : <input type="text" value="172.16.99.5"/>
Password :	<input type="password" value="••••"/>	PPTP Subnet Mask : <input type="text" value="255.255.0.0"/>
Authentication :	<input type="text" value="PAP"/> ▾	PPTP Server Address : <input type="text" value="172.16.99.55"/>
Service Name :	<input type="text"/>	Always On : <input checked="" type="checkbox"/> Enable
PPPoE IP Alias :	<input type="checkbox"/> Enable	
MTU :	<input type="text" value="1442"/>	
IP Address Assignment Method (IPCP)		
Fixed IP :	<input checked="" type="radio"/> No (Dynamic IP) <input type="radio"/> Yes	
Fixed IP Address :	<input type="text"/>	
Connection Detection		
Detect Interval :	<input type="text" value="10"/>	
No-Reply Count :	<input type="text" value="2"/>	
<input type="button" value="Apply"/> <input type="button" value="Reset"/> <input type="button" value="Cancel"/>		

- User Name** Assign a specific valid user name provided by local ISP.
- Password** Assign a valid password provided by local ISP.
- Authentication** Select **PAP**, **CHAP**, **MS-CHAP** or **MS-CHAP-V2** protocol for PPP authentication according to the feature that your ISP provided for widest compatibility. The default value is **PAP**.

The password will be encrypted in CHAP but not in PAP.



A dropdown menu with a blue border and a downward arrow on the right. The menu is open, showing four options: PAP (highlighted in blue), CHAP, MS-CHAP, and MS-CHAP-V2.

Service Name	Assign a service name required for some ISP services.
PPTP Local Address	Assign a local IP address.
PPTP Subnet Mask	Assign a subnet mask value of IP address.
PPTP Remote Address	Assign a remote IP address of PPTP server.
Detect Interval	Assign an interval time for detecting if the WAN connection is on or off.
No-Reply Count	Assign detecting times to ensure the connection of the WAN. After passing the times you set in this field and no reply received by the router, the connection of WAN interface will be regarded as breaking down.
Apply	Click Apply to go back to the WAN Interface Configuration page. To apply all settings, click Apply on the WAN Interface Configuration page and reboot your router.
Reset	Click this button to clear all the configurations for this page.

DMZ Configuration

In computer networks, a DMZ (De-Militarized Zone) is a computer host or small network inserted as a neutral zone between a company's private network and the outside public network. It prevents outside users from getting direct access to company network. A DMZ is an optional and more secure approach to a firewall and effectively acts as a proxy server as well. In a typical DMZ configuration for a small company, a separate computer (or host in network terms) receives requests from users within the private network for access to Web sites or other companies accessible on the public network. The DMZ host then initializes sessions for these requests on the public networks. However, the DMZ host is not able to initiate a session back into the private network. It can only forward packets that have already been requested. Users of the public network outside the company can access only the DMZ host. **The DMZ may typically also have the company's Web pages so these could be served to the outside world.** If an outside user penetrated the DMZ host's security, only the Web pages will be corrupted but other company information would not be exposed.

The service provider must provide the exact settings for this mode.

Static/DHCP Configuration	PPPoE/PPTP Configuration	DMZ Configuration
IP Address : <input type="text"/>		
Subnet Mask : <input type="text"/>		
DMZ Host Type : <input type="text" value="NAT Mode"/>		
Outgoing Interface : <input type="text" value="WAN2"/>		
DMZ Host IP List(Only Routing Mode)		
1.	<input type="text"/>	2. <input type="text"/>
3.	<input type="text"/>	4. <input type="text"/>
5.	<input type="text"/>	6. <input type="text"/>
7.	<input type="text"/>	8. <input type="text"/>
<input type="button" value="Apply"/> <input type="button" value="Reset"/> <input type="button" value="Cancel"/>		

- IP Address** Set the private IP address of WAN interface.
- Subnet Mask** Set the subnet mask value of WAN interface.
- DMZ Host Type** Choose **NAT Mode** or **Routing Mode** as the DMZ host type.
- Outgoing Interface** This setting is available when Routing Mode selected as DMZ host type.
- DMZ Host IP List** When DMZ Host type is set as **Routing Mode**, please type the IP address here to be chosen in IP Alias in **Advanced>>NAT>>DMZ Host**.
- Apply** Click **Apply** to go back to the WAN Interface Configuration page. To apply all settings, click **Apply** on the WAN Interface Configuration page and reboot your router.
- Reset** Click this button to clear all the configurations for this page.

4.2.2 Load Balance Policy

Vigor3300V+ supports a load balancing function. It can assign traffic with protocol type, IP address for specific host, a subnet of hosts, and port range to be allocated in WAN interface. User can assign traffic category and force it to go to dedicate network interface based on the following web page setup. VoIP and VPN traffic can also be assigned to specific WAN ports.

In the **Network** group, click the **Load Balance Policy** option. You will get the following page.

Network - Load Balance Policy

#	Protocol	Source IP	Subnet Mask	Dest IP	Subnet Mask	Dest Port Start	Dest Port End	Network Interface	Strict Bind
1	<input checked="" type="radio"/>								
2	<input type="radio"/>								
3	<input type="radio"/>								
4	<input type="radio"/>								
5	<input type="radio"/>								
6	<input type="radio"/>								
7	<input type="radio"/>								
8	<input type="radio"/>								
9	<input type="radio"/>								
10	<input type="radio"/>								

1

- Protocol** Display the protocol used for this entry.
- Source IP** Display the source IP address specified for this entry.
- Subnet Mask** Display the subnet mask address specified for the source IP of this entry.
- Dest IP** Display the destination IP address specified for this entry.
- Subnet Mask** Display the subnet mask address specified for the destination IP of this entry.
- Dest Port Start** Display the start point specified in the **Dest Port Range** for this entry.
- Dest Port End** Display the end point specified in the **Dest Port Range** for this entry.
- Network Interface** Display the interface specified for this entry.
- Strict Bind** Display the status of Strict Bind.
- Edit** Click this button to open the edit page for adjusting the settings.
- Delete/Delete All** Click this button to delete the selected setting or all settings. A confirmation dialog box will appear. Click **OK** to delete this entry from the Load Balance Policy table. In addition, click **Delete All** in the Load Balance Policy page to delete all of 10 entries on this page.

To edit an entry, select it by clicking the radio button (from 1 to 10). Then click the **Edit** button on the bottom to bring up the following Web page.

Network - Load Balance Policy - Edit

1

Protocol :

Source IP / Subnet Mask : /

Dest IP / Subnet Mask : /

Dest Port Range : -

Network Interface :

Strict Bind :

Protocol

Select the desired protocol for the selected entry.

- ALL
- TCP/UDP
- TCP
- UDP
- ICMP
- FTP
- TFTP
- HTTP
- SMTP
- POP3

Source IP/Subnet Mask

Assign a source IP address and subnet of certain host in LAN for applying load balance policy.

Dest IP/Subnet Mask

Assign a destination IP address and subnet of certain host in LAN for applying load balance policy.

Dest Port Range

Assign a destination port number range. The port range is from 1 to 65535. If you choose **All** as the protocol, you don't need to type any number here.

Network Interface

Select an interface (WAN1 to WAN4) to be forwarded to.

Strict Bind

Packets fitting the above settings can be routed through the selected interface only. Check this box to invoke this function.

Apply

Click **Apply** to save all configurations.

4.2.3 Auto Load Balance

Because the network between China Telecom and China CNC are disconnected, such function is designed to do auto load balance and separate the packets among China Telecom, China CNC and other regions via different WAN interfaces. For example, if you check WAN1 and WAN4 for China Telecom, packets belong to China Telecom will pass through the specified WAN interfaces only; and load balance will be done between WAN1 and WAN4.

Network - Auto Load Balance				
Auto Load Balance :				
	<input checked="" type="radio"/> Disable	<input type="radio"/> Enable		
	WAN1	WAN2	WAN3	WAN4
China Telecom :	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
China CNC :	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Other Traffic :	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Apply Cancel

Auto Load Balance

Choose **Enable** to invoke the auto load balance function for your devices.

China Telecom

A telecom company.

China CNC

A telecom company.

Other Traffic

Regions that are not belonged to China Telecom and China CNC.

Apply

Click **Apply** to save all configurations.

4.2.4 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.

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.

Network - LAN

LAN IP/DHCP | DHCP Relay Agent | IP Routing

IP Configuration

IP Address :

Subnet Mask :

DHCP Server

Status : Enable Disable Relay Agent

Start IP :

End IP :

Primary DNS :

Secondary DNS :

Lease Time (Min) :

Gateway IP(Optional) :

For LAN IP/DHCP

In the Vigor3300V+ router, there are some IP address settings for the LAN interface. The IP address/subnet mask is for private users or NAT users. The IP address of the default gateway on other local PCs should be set as the Vigor3300 Series' server IP address. When the DSL connection between the DSL and the ISP has been established, each local PC can directly route to the Internet. The IP address/subnet mask can also be used to connect to other private users (PCs). On this page you will see the private IP address defined in RFC-1918. Usually we use the 192.168.1.0/24 subnet for the route.

IP Address	Type the IP address for LAN/DHCP.
Subnet Mask	Type the subnet mask for the LAN IP/DHCP.
Status	Click Enable the DHCP server; click Disable to close DHCP server; click Relay Agent to close DHCP sever and do the job of DHCP server. Corresponding settings for Relay Agent can be configured in the page of DHCP Relay Agent .
Start IP	Set the starting IP address of the IP address pool for DHCP server.
End IP	Set the ending IP address of the IP address pool for DHCP server.
Primary DNS	Set the private IP address of the primary DNS.
Secondary DNS	Set the private IP address of the secondary DNS.
Lease Time (Min)	Set a lease time for the DHCP server. The time unit is minute.
Gateway IP (Optional)	Set a gateway IP address for the DHCP server.

Click **Apply** to reboot the system and apply the settings.

Note: If both the Primary and Secondary DNS 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.

For DHCP Relay Agent

This page allows users to specify which subnet that DHCP server is located the relay agent should redirect the DHCP request to.

The screenshot shows the 'Network - LAN' configuration page with the 'DHCP Relay Agent' tab selected. The 'Relay Agent' section contains a 'WAN Interface' dropdown menu set to 'WAN1' and a 'DHCP Server IP Address' text input field. 'Apply' and 'Cancel' buttons are located at the bottom right.

WAN Interface Choose the WAN interface for applying relay agent.

DHCP Server IP Address Type the IP address for the DHCP server.

For IP Routing

This page allows users to type in secondary IP address for connecting to a subnet. You can set IP routing for each WAN interface respectively.

The screenshot shows the 'Network - LAN' configuration page with the 'IP Routing' tab selected. It displays four WAN interface sections (WAN1, WAN2, WAN3, WAN4). Each section includes a 'Status' field with 'Enable' and 'Disable' radio buttons, and 'IP Address' and 'Subnet Mask' text input fields. WAN1 is currently enabled with IP 10.1.1.3 and mask 255.255.255.0. 'Apply' and 'Cancel' buttons are at the bottom right.

Status Click **Enable** or **Disable** to activate or close the IP routing of specific WAN interface.

IP Address Type an IP address for the WAN interface (WAN1/WAN2/WAN3/WAN4).

Subnet Mask Type the subnet mask for the WAN interface (WAN1/WAN2/WAN3/WAN4).

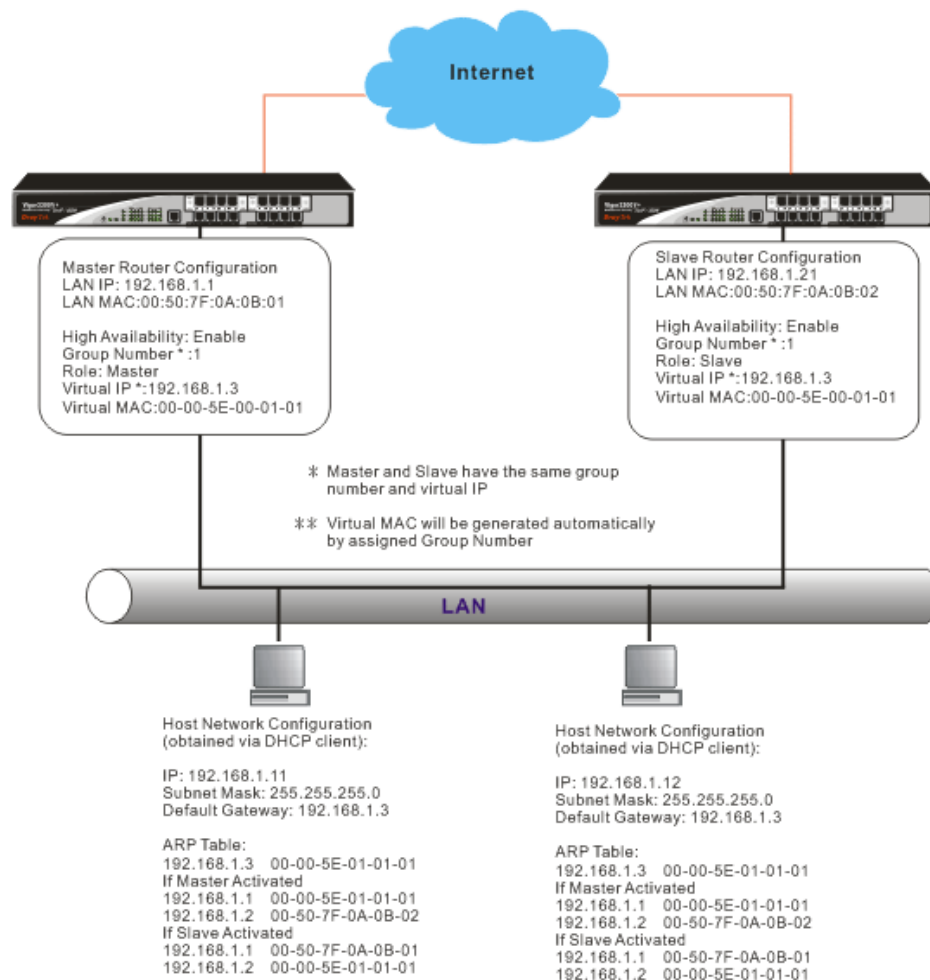
LAN Interface Select a proper LAN interface for WAN interface (WAN1/WAN2/WAN3/WAN4).

4.2.5 High Availability

The High Availability (HA) feature refers to the awareness of component failure and the availability of backup resources. The complexity of HA is determined by the availability needs and the tolerance of system interruptions. Systems, provides nearly full-time availability, typically have redundant hardware and software that makes the system available despite failures.

The high availability of the V3300 Series is designed to avoid single points-of-failure. When failures occur, the failover process moves processing performed by the failed component (the “Master”) to the backup component (the “Slave”). This process remains system-wide resources, recovers partial of failed transactions, and restores the system to normal within a matter of microseconds.

Take the following picture as an example. The left V3300 Series is regarded as Master device, the right V3300 Series is regarded as Slave device. When Master V3300 Series is broken down, the Slave device could replace the Master role to take over all jobs as soon as possible. However, once the original Master is working again, the Slave would be changed to original role to stand by.



In the Network group, click the **High availability** option.

High Availability

Network - LAN - High Availability

Basic Status | 802.1Q Status

High Availability: Disable Enable

Group Number: (Range: 1~255)

Role:

Virtual IP:

Slave Status: Not sync.

High Availability

Disables or enables this function. When the master device fails down, the slave device will take its work over.

Group Number

Assign a group number. The range is from 1 to 255. PCs on the same group (in LAN) can support for each other.

Role

Select a role for this device as Master or Slave.

Virtual IP

Assign an IP address as a virtual IP.

Slave Status

Display current status of slave device.

Click **Apply** to reboot the system and apply the settings.

802.1Q Status

This page allows you to set High Availability for LAN ports (1 ~ 4) respectively.

Network - LAN - High Availability

Basic Status | **802.1Q Status**

LAN1	LAN2
High Availability: <input checked="" type="radio"/> Disable <input type="radio"/> Enable	High Availability: <input checked="" type="radio"/> Disable <input type="radio"/> Enable
Group Number: <input type="text"/> (Range: 1~255)	Group Number: <input type="text"/> (Range: 1~255)
Role: <input type="text" value="Master"/>	Role: <input type="text" value="Master"/>
Virtual IP: <input type="text"/>	Virtual IP: <input type="text"/>
LAN3	LAN4
High Availability: <input checked="" type="radio"/> Disable <input type="radio"/> Enable	High Availability: <input checked="" type="radio"/> Disable <input type="radio"/> Enable
Group Number: <input type="text"/> (Range: 1~255)	Group Number: <input type="text"/> (Range: 1~255)
Role: <input type="text" value="Master"/>	Role: <input type="text" value="Master"/>
Virtual IP: <input type="text"/>	Virtual IP: <input type="text"/>

High Availability

Disables or enables this function. When the master device fails down, the slave device will take its work over.

Group Number

Assign a group number. The range is from 1 to 255. PCs on the same group (in LAN) can support for each other.

Role

Select a role for this device as Master or Slave.

Virtual IP

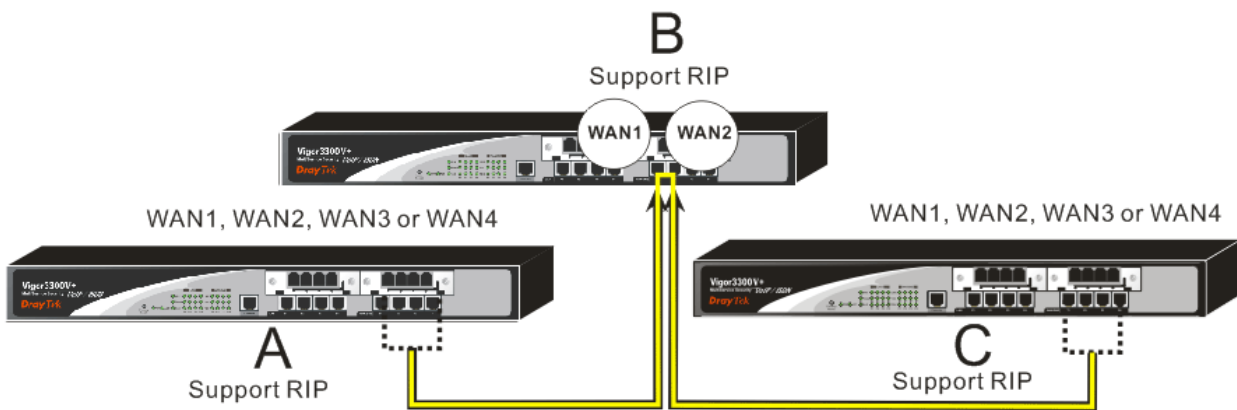
Assign an IP address as a virtual IP.

Click **Apply** to reboot the system and apply the settings.

4.2.6 RIP Configuration

The Routing Information Protocol (RIP) is a dynamic routing protocol used in local and wide area networks. The routing information packet will be sent out by web server or router periodically, and can be used to communicate with other routers. It will calculate the number of network nodes on the route to ensure there is no obstruction on the network routine. In addition, it will choose a correct route based on the method of Distance Vector Routing and use the Bellman-Ford algorithm to calculate the routing table.

RIP can update the routing table automatically and find a route to send packet. See the following figure as an example:



Suppose Vigor3300V+ A supports RIP on WAN1/WAN2/WAN3/WAN4, Vigor3300V+ B supports RIP on WAN1 and WAN2, and Vigor3300V+ C supports RIP on WAN1/WAN2/WAN3/WAN4.

Vigor3300V+ B will tell 3300V+ A "if you want to send packets to Vigor3300V+ C, please send it to me first", then Vigor3300V+ A will create a routing rule to forward packet that destination is Vigor3300V+ C to Vigor3300V+ B.

In another direction, Vigor3300V+ C will do the same thing.

Network - RIP Configuration

Disable
 Enable

Enabled Interface(s) :

- WAN 1
- WAN 2
- WAN 3
- WAN 4

Enable/Disable

Disables or enables this function.

Enabled Interface

Check the interface to apply the RIP configuration.

Apply

After finishing the configuration, please click this button to invoke these settings.

4.2.6 Bandwidth Management

This function is used to limit user bandwidth.



General Setup

This function allows users to configure general settings for bandwidth management. Click **Network >>Bandwidth Management** and then choose **General Setup**. You will get the following page.

A screenshot of the 'Network - Bandwidth Management - General Setup' configuration page. The page has a title bar with the text 'Network - Bandwidth Management - General Setup'. Below the title bar, there are three configuration items: 'Limit Bandwidth :', 'Default TX limit :', and 'Default RX limit :'. The 'Limit Bandwidth' item has two radio buttons: 'Disable' (which is selected) and 'Enable'. The 'Default TX limit' and 'Default RX limit' items each have a text input field containing the value '1024' and a label 'Kbps'. At the bottom right of the form, there are two buttons: 'Apply' and 'Cancel'.

Enable/Disable

Disables or enables this function.

Default TX Limit

Define the default speed of the upstream for each computer in LAN. The default value is 1024.

Default RX limit

Define the default speed of the downstream for each computer in LAN. The default value is 1024.

Apply

After finishing the configuration, please click this button to invoke these settings.

Limitation Table

This function allows users to set limitation for bandwidth. Click **Network >>Bandwidth Management** and then choose **Limitation Table**. You will get the following page.

Network - Bandwidth Management - Limitation Table

#	Start IP	End IP	TX Limit	RX Limit
1	<input checked="" type="radio"/>			
2	<input type="radio"/>			
3	<input type="radio"/>			
4	<input type="radio"/>			
5	<input type="radio"/>			
6	<input type="radio"/>			
7	<input type="radio"/>			
8	<input type="radio"/>			
9	<input type="radio"/>			
10	<input type="radio"/>			

1

- Start IP** Display the start IP address of bandwidth.
- End IP** Display the End IP address of bandwidth.
- TX Limit** Display the size limit for the transmitted packets.
- RX Limit** Display the size limit for the received packets.
- Edit** Click this button to open the edit page for adjusting the settings.
- Delete/Delete All** Click this button to delete the selected setting or all settings. A confirmation dialog box will appear. Click **OK** to delete this entry from the Load Balance Policy table. In addition, click **Delete All** in the Load Balance Policy page to delete all of 10 entries on this page.

To edit an entry, select it by clicking the radio button (from 1 to 10). Then click the **Edit** button on the bottom to bring up the following Web page.

Network - Bandwidth Management - Limitation Table - Edit

1

Start IP :

End IP :

TX Limit : Kbps

RX Limit : Kbps

- Start IP/End IP** Assign the IP range for the bandwidth management.
- 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.

Apply

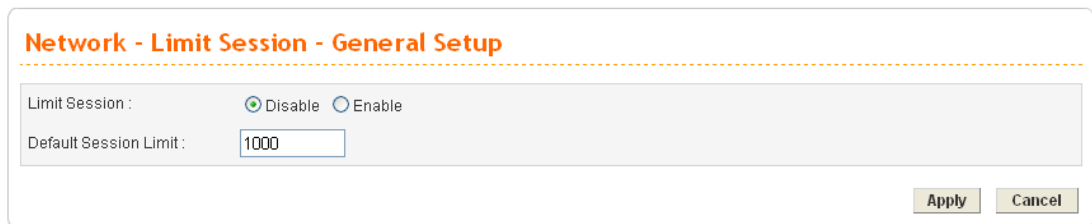
After finishing the configuration, please click this button to invoke these settings.

4.2.7 Limit Session

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

**General Setup**

This function allows users to configure general settings for limit session. Click **Network >>Limit Session** and then choose **General Setup**. You will get the following page.

**Enable/Disable**

Disables or enables this function.

Default Session Limit

Defines the default session number used for each computer in LAN.

Apply

After finishing the configuration, please click this button to invoke these settings.

Limitation Table

This function allows users to set limitation for limit session. Click **Network >>Limit Session** and then choose **Limitation Table**. You will get the following page.

Network - Limit Session - Limitation Table

#	Start IP	End IP	Session Number
1	<input checked="" type="radio"/>		
2	<input type="radio"/>		
3	<input type="radio"/>		
4	<input type="radio"/>		
5	<input type="radio"/>		
6	<input type="radio"/>		
7	<input type="radio"/>		
8	<input type="radio"/>		
9	<input type="radio"/>		
10	<input type="radio"/>		

1

Start IP

Display the start IP address.

End IP

Display the end IP address.

Session Number

Display the session number.

Edit

Click this button to open the edit page for adjusting the settings.

Delete/Delete All

Click this button to delete the selected setting or all settings. A confirmation dialog box will appear. Click **OK** to delete this entry from the Load Balance Policy table. In addition, click **Delete All** in the Load Balance Policy page to delete all of 10 entries on this page.

To edit an entry, select it by clicking the radio button (from 1 to 10). Then click the **Edit** button on the bottom to bring up the following Web page.

Network - Limit Session - Limitation Table - Edit

1

Start IP :

End IP :

Session Number :

Start IP

Assign the start IP address for limit session.

End IP

Assign the end IP address for limit session.

Session Number

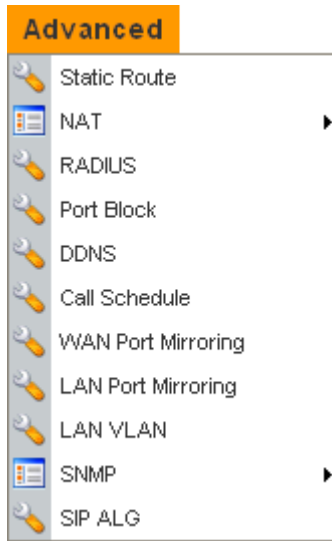
Assign the available session number for each host in the specific range of IP addresses. If you do not set the session number in this field, the system will use the default session limit for the specific limitation you set for each index.

Apply

After finishing the configuration, please click this button to invoke these settings.

4.3 Advanced Setup

In the **Advanced** menu, there are several items offered here for you to adjust for the router.



4.3.1 Static Route Setup

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 methods. You may simply set rules to forward data from one specified subnet to another specified subnet without the presence of RIP.

This function allows users to assign static routing information. In the **Advanced** group, choose **Static Route**. You will get the following page.

A screenshot of the 'Advanced - Static Route' configuration page. The page has a title bar 'Advanced - Static Route' in orange. Below the title bar is a table with the following columns: '#', 'Network Interface', 'Destination IP', 'Gateway IP', and 'Mask'. The table has 10 rows, numbered 1 to 10. Row 1 is selected, indicated by a radio button with a dot inside. Below the table, there are three buttons: 'Edit', 'Delete', and 'Delete All'. The number '1' is displayed in the bottom right corner of the table area.

Network Interface

Display the network interface (LAN, WAN1, 2, 3 or 4).

Destination IP

Display the destination IP of the static route.

Gateway IP

Display the gateway address of the static route.

Mask

Display the subnet mask of this route.

Edit

Allow users to edit the selected static route settings.

Delete/Delete All Removes one or all the selected static route settings.

The system allows users to set up to 10 static routes for the router.

Edit the Static Route

To edit static route for certain item, select the radio button of the item and click **Edit** on the bottom of the page. The following web page will be displayed:

Advanced - Static Route - Edit

1

Network Interface :

Gateway IP :

Destination IP :

Subnet Mask :

Network Interface Select a network interface as a destination to be sent. It includes **LAN**, and **WAN1~WAN4**.

Gateway IP Assign an IP address of the gateway for the interface selected above.

Destination IP Assign the IP address of the destination that data will be transferred to. Packets ready to destination will be sent out through the network interface chosen in this page.

Subnet Mask Assign a value of subnet mask for destination IP address.

Apply After finishing the configuration, please click this button to invoke these settings.

Delete the Static Route

Select the radio button of the item that you want to delete and click **Delete** on the bottom of the page. The following web page will be displayed:

Advanced - Static Route

#	Network Interface	Destination IP	Gateway IP	Mask
1	<input checked="" type="radio"/> LAN	10.1.1.50	192.168.1.100	/24
2	<input type="radio"/>			
3	<input type="radio"/>			
4	<input type="radio"/>			
5	<input type="radio"/>			
6	<input type="radio"/>			
7	<input type="radio"/>			
8	<input type="radio"/>			
9	<input type="radio"/>			
10	<input type="radio"/>			

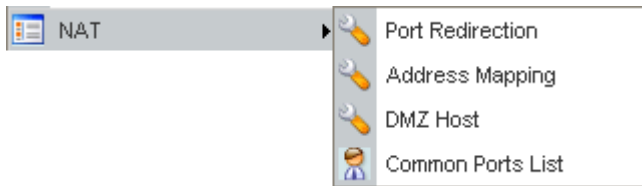
Click **OK** to delete the entry in static route table.

Users can click **Delete All** to remove all entries in static route table.

4.3.2 NAT Setup

NAT (Network Address Translation) is a method of mapping one or more IP addresses and/or service ports into different specified services. It allows the internal IP addresses of many computers on a LAN to be translated to one public address to save costs and resources of multiple public IP addresses. It also plays a security role by obscuring the true IP addresses of important machines from potential hackers on the Internet. The Vigor 3300 Series is NAT-enabled by default and gets one globally routable IP addresses from the ISP by Static, PPPoE, or DHCP mechanism. The Vigor3300 Series assigns private network IP addresses according to RFC-1918 protocol and translates the private network addresses to a globally routable IP address so that local hosts can communicate with the router and access the Internet.

Click **Advanced >>NAT**.



There are four functions that NAT provides – **Port Redirection, Address Mapping, DMZ Host and Common Ports List**.

Port Redirection

Port Redirection means port forwarding. It may be used to expose internal servers to the public domain or open a specific port to internal hosts. Internet hosts can use the WAN IP address to access internal network services, such as FTP, WWW and etc. The internal FTP server is running on the local host addressed as 192.168.1.2. When other users send this type of request to your network through the Internet, the router will direct these requests to an appropriate host inside. A user can also translate the port to another port by configuration. For example, port number with 1024 can be transferred into IP address of 192.168.1.100 of LAN. The packet is forwarded to a specific local host if the port number matches that defined in the table.

Advanced - NAT - Port Redirection

#	Profile Status	Comment	Protocol	Public Port Start	Public Port End	Private IP	Private Port Start	Private Port End	Public IP	WAN Interface	IP Alias
1	<input checked="" type="radio"/> Enable	Test	TCP	88	120	192.168.1.89	92	124	WAN Interface	WAN1	
2	<input type="radio"/>										
3	<input type="radio"/>										
4	<input type="radio"/>										
5	<input type="radio"/>										
6	<input type="radio"/>										
7	<input type="radio"/>										
8	<input type="radio"/>										
9	<input type="radio"/>										
10	<input type="radio"/>										

1

Profile Status Display the status (enabled or disabled) of this profile.

Comment Display the name of the entry.

Protocol	Display the protocol used for the entry.
Public Port Start	Display the start point in the range of public port.
Public Port End	Display the end point in the range of public port.
Private IP	Display the private IP used for this entry.
Private Port Start	Display the start point in the range of private port.
Private Port End	Display the end point in the range of private port.
Public IP	Display the channel used to perform port redirection.
WAN Interface	Display the WAN interface of this profile.
IP Alias	Display the selected WAN IP address.
Edit	Allow users to edit the selected port redirection settings.
Delete/Delete All	Removes one/all the selected port redirection settings.

To edit an item, click the radio button of the item that you want to modify. Then click **Edit** on the bottom of the page to add a new rule entry or modify an existed rule entry.

Advanced - NAT - Port Redirection - Edit

1

Profile Status : Disable Enable

Comment :

Protocol :

Public Port Range: -

Private IP :

Private Port Range: -

Public IP : WAN Interface IP Alias ALL

WAN Interface :

IP Alias :

Profile Status	Enable or disable this function.
Comment	Assign a name for this entry. The maximum is 20 characters.
Protocol	Assign the transport layer protocol with TCP or UDP .
Public Port Range	Assign a port range from starting to end public port number. The port range is from 1 to 65535.
Private IP	Assign a local IP address to be transferred into.
Private Port Range	Assign a port range from starting to end private port number.
Use IP Alias	“ Disable ” option uses IP address of WAN interface, “ Enable ” option uses IP alias addresses.
Public IP	Determine which channel will be used to perform port redirection (port forwarding) Wan interface: port redirection will be done via WAN IP. IP Alias: port redirection will be done via WAN IP alias. ALL: port redirection will be done via WAN IP or WAN IP alias.

- WAN Interface** It is a pull-down window; user can select one specific WAN interface.
- IP Alias** It is a pull-down window; user can select one specific IP address assigned in IP Alias group of WAN interfaces.

Click **Apply** to reboot the system and apply the settings.

Note: The port forwarding function could redirect the Internet traffic, which has the destination port within the public port range and has the same IP address as WAN Interface or IP Alias that you set. Please redirect only the ports that you have to forward rather than forward all ports. Otherwise, the intrinsic firewall type security of NAT facility will be affected.

By the way, user can click **Delete** to remove one current existed NAT entry in the **Advanced – NAT – Port Redirection** page and click **Delete All** to remove all entries.

Address Mapping

If you have a group of static IP addresses, then you can use the address-mapping feature to multiple open ports hosts in the Vigor3300 Series of broadband security routers. The following session will show you how to setup address-mapping feature.

In the **Advanced** group, move to **NAT** option and choose **Address Mapping** to get the corresponding page.

#	Protocol	Public IP	Private IP	Mask
1	<input checked="" type="radio"/>			
2	<input type="radio"/>			
3	<input type="radio"/>			
4	<input type="radio"/>			
5	<input type="radio"/>			
6	<input type="radio"/>			
7	<input type="radio"/>			
8	<input type="radio"/>			
9	<input type="radio"/>			
10	<input type="radio"/>			

1

- Protocol** Display the protocol used for this address mapping.
- Public IP** Display the public IP address selected for this entry.
- Private IP** Display the private IP set for this address mapping.
- Mask** Display the subnet mask selected fro this address mapping.
- Edit** Allow users to edit the selected address mapping settings.
- Delete/Delete All** Remove one/all the selected address mapping settings.

To edit an item, click the radio button of the item that you want to modify. Then click **Edit** on the bottom of the page to add a new rule entry or modify an existed rule entry.

Advanced - NAT - Address Mapping - Edit

1

Protocol :

Public IP :

Private IP :

Subnet Mask :

Protocol Select the transport layer protocol. It could be **TCP**, **UDP**, or **All** for selection.

Public IP Select an IP address (the selections provided here are set in **IP Alias List** of **Network >>WAN** interface). Local host can use this IP to connect to Internet.

If you want to choose any on of the Public IP settings, you must specify some IP addresses in the IP Alias List of the Static/DHCP Configuration page first. If you did not type in any IP address in the IP Alias List, the Public IP setting will be empty in this field. When you click **Apply**, a message will appear to inform you.

Private IP Assign an IP address or a subnet to be compared with the source IP address for incoming packets.

Subnet Mask Select a value of subnet mask for private IP address.

Click **Apply** to reboot the system and apply the settings.

By the way, user can click **Delete** to remove one current existed NAT entry in the **Advanced – NAT – Address Mapping** page and click **Delete All** to remove all entries.

DMZ Host

In computer networks, a DMZ (De-Militarized Zone) is a computer host or small network inserted as a neutral zone between a company's private network and the outside public network. It prevents outside users from getting direct access to company network. A DMZ is an optional and more secure approach to a firewall and effectively acts as a proxy server as well. In a typical DMZ configuration for a small company, a separate computer (or host in network terms) receives requests from users within the private network for access to Web sites or other companies accessible on the public network. The DMZ host then initializes sessions for these requests on the public networks. However, the DMZ host is not able to initiate a session back into the private network. It can only forward packets that have already been requested. Users of the public network outside the company can access only the DMZ host. **The DMZ may typically also have the company's Web pages so these could be served to the outside world.** If an outside user penetrated the DMZ host's security, only the Web pages will be corrupted but other company information would not be exposed.

Click **Advanced** >> **NAT** and choose **DMZ Host** to get the corresponding page.

Advanced - NAT - DMZ Host

#	WAN Interface	Private IP	Use IP Alias	IP Alias
1	<input checked="" type="radio"/> WAN1	192.168.1.10	Disable	
2	<input type="radio"/>			
3	<input type="radio"/>			
4	<input type="radio"/>			
5	<input type="radio"/>			
6	<input type="radio"/>			
7	<input type="radio"/>			
8	<input type="radio"/>			
9	<input type="radio"/>			
10	<input type="radio"/>			

1

WAN Interface

Display the WAN interface chosen for this entry.

Private IP

Display the private IP address of this entry.

Use IP Alias

Display the activation status (enable or disable) of this DMZ host.

IP Alias

Display the WAN IP address.

Edit

Allow users to edit the selected DMZ host settings.

Delete/Delete All

Remove one/all the selected DMZ host settings.

To edit an item, click the radio button of the item that you want to modify. Then click **Edit** on the bottom of the page to add a new rule entry or modify an existed rule entry.

Advanced - NAT - DMZ Host - Edit

1

WAN Interface :

Private IP :

Use IP Alias : Disable Enable

IP Alias :

WAN Interface

Select a WAN interface as the channel for DMZ host.

Private IP

Assign an IP address of DMZ server to be permitted for access from outside.

Use IP Alias

Disable option uses WAN interface, **Enable** option uses IP Alias addresses.

IP Alias

Select an IP address which are set within the list of IP Alias configured in **Network** >> **WAN** interface.

Apply

Click **Apply** to reboot the system and apply the settings.

Common Ports List

This page lists common ports used in Internet. The information includes service/application, protocol for that service and port number of that service.

Advanced - NAT - Common 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)	TCP	80
Post Office Protocol ver.3 (POP3)	TCP	110
Network News Transfer Protocol (NNTP)	TCP	119
Point-to-Point Tunneling Protocol (PPTP)	TCP	1723
pcANYWHEREdata	TCP	5631
pcANYWHEREstat	UDP	5632
WinVNC	TCP	5900

4.3.3 RADIUS Setup

A RADIUS (Remote Authentication Dial-In User Service) is a security authentication client/server protocol widely used by Internet service providers on other remote access service. A RADIUS is the most common means of authenticating and authorizing dial-up and tunneled network users. The built-in RADIUS client function allows you to extend the remote dial-in user accounts to the RADIUS server. **Your user accounts will not be limited by built-in accounts** (in VPN>>PPTP>>User Profile). It also lets you centralize remote access authentication for network management.

Radius is a server for remote user authentication and accounting. Its primary use is for Internet Service Providers, though it may as well be used on any network that needs a centralized authentication and/or accounting service. A Radius supports a wide variety of authentication schemes. A user supplies his authentication data to the server either directly by answering the terminal server's login/password prompts, or using **PAP** of **CHAP** protocols.

The Vigor 3300V+ supports Radius client function. A user can configure some authentication information to do an authentication with Radius server. **In Vigor3300 Series, it is only applied by VPN->PPTP function.**

In the **Advanced** group, click the **Radius** option. You will get the following page.

Advanced - RADIUS

Disable Enable

Server IP Address :

Destination Port :

Shared Secret :

Confirm Shared Secret :

Interface :
 LAN
 WAN1
 WAN2
 WAN3
 WAN4

- Enable/Disable** Click **Disable** to disable this function. Click **Enable** to activate this function.
- Server IP Address** Assign an IP address of a Radius server.
- Destination Port** Assign a destination port number used for Radius function.
- Shared Secret** Assign a code for authentication to server. The RADIUS server and client share a secret which is used to authenticate the messages sent between them. Both sides must be configured to use the same shared secret.
- Confirm Shared Secret** Confirm the code assigned in Shared Secret field.
- Interface** Select one specific WAN interface to be used.
- Click **Apply** to reboot the system and apply the settings.

4.3.4 Port Block

The **Port Block** function provides a user to set lots of proprietary port numbers. Packets will be dropped if destination ports (both TCP and UCP) of packets with these assigned port numbers are on WAN and LAN. The advantage of this feature is to filter some unnecessary packets or attacking packets on Internet environment or LAN network. Vigor3300 Series supports ten port numbers to be blocked.

Click **Advanced >> Port Block**. You will get the following page.

Advanced - Port Block

Index	Status	Port Number
1.	<input checked="" type="radio"/> Disable <input type="radio"/> Enable	<input type="text"/>
2.	<input checked="" type="radio"/> Disable <input type="radio"/> Enable	<input type="text"/>
3.	<input checked="" type="radio"/> Disable <input type="radio"/> Enable	<input type="text"/>
4.	<input checked="" type="radio"/> Disable <input type="radio"/> Enable	<input type="text"/>
5.	<input checked="" type="radio"/> Disable <input type="radio"/> Enable	<input type="text"/>
6.	<input checked="" type="radio"/> Disable <input type="radio"/> Enable	<input type="text"/>
7.	<input checked="" type="radio"/> Disable <input type="radio"/> Enable	<input type="text"/>
8.	<input checked="" type="radio"/> Disable <input type="radio"/> Enable	<input type="text"/>
9.	<input checked="" type="radio"/> Disable <input type="radio"/> Enable	<input type="text"/>
10.	<input checked="" type="radio"/> Disable <input type="radio"/> Enable	<input type="text"/>

- Index** The number of each entry.
- Status** User can **Disable** or **Enable** this port to be blocked.
- Port Number** Assign a port number to be blocked in system.
- Click **Apply** to finish this setting.

4.3.5 DDNS Setup

The Dynamic DNS function allows the router to update its online WAN IP address, which assigned by ISP or other DHCP server to 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. DDNS is more popular on dynamic IP users, who typically receive dynamic, frequently-changing IP addresses from their service provider.

Before you set up the Dynamic DNS function, you have to subscribe free domain names from the Dynamic DNS service providers. The router provides up to ten accounts for the function and supports the following providers: **www.dynsns.org**, **www.no-ip.com**, **www.dtdns.com**, **www.changeip.com**, **www.ddns.cn**. You should visit their websites for registering your own domain name on the router.

In the **Advanced** group, click **DDNS** option. You will get the following page.

Advanced - DDNS

#	Domain Name	Server Provider	Server Type	Active	Status
1		dyndns.org	dynamic	Disable	Not Connected
2		dyndns.org	dynamic	Disable	Not Connected
3		dyndns.org	dynamic	Disable	Not Connected
4		dyndns.org	dynamic	Disable	Not Connected
5		dyndns.org	dynamic	Disable	Not Connected
6		dyndns.org	dynamic	Disable	Not Connected
7		dyndns.org	dynamic	Disable	Not Connected
8		dyndns.org	dynamic	Disable	Not Connected
9		dyndns.org	dynamic	Disable	Not Connected
10		dyndns.org	dynamic	Disable	Not Connected

- Domain Name** Display the domain name set for the entry.
- Service Provider** Display the service provider that supports DDNS.
- Service Type** Display the service type for the entry.
- Active** Display the activation status (disable or enable) for this entry.
- Status** Display the connection status of this entry.

Click **Refresh** to re-display the whole page information.

To modify DDNS setting, click an entry number to get into edit mode.

Advanced - DDNS Setting

Status : Disable Enable

Interface :

Server Provider :

Server Type :

Domain Name :

Login Name :

Login Password :

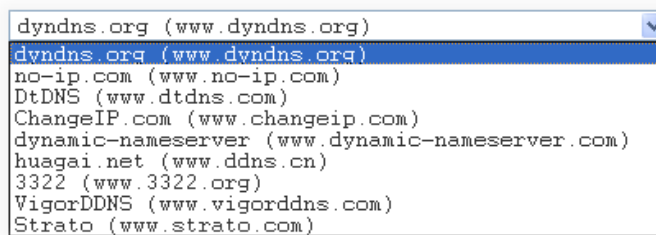
Wild Card : Disable Enable

Backup MX : Disable Enable

Mail Extender :

- Status** Click **Disable** to disable this function. Click **Enable** to activate this function.
- Interface** Select a specific interface for registering on DDNS server. The Interface should be any WAN port on router.
- Server Provider** Assign a provider name to support DDNS server. The Vigor3300V+ supports several domain server providers as

default.



- | | |
|-----------------------|---|
| Server Type | Select Static , Dynamic or Custom type for this entry of DDNS settings. |
| Domain Name | Assign a private domain name to be accessed. |
| Login Name | Assign a name to login into DDNS server. |
| Login Password | Assign a password to login into DDNS server. |
| Wild Card | If you want anything-here.yourhost.dyndns.org to work (EX. To make things like www.yourhost.dyndns.org work), click “Enable” to active this function. |
| Backup MX | MX stands for Mail Exchanger. Mail Exchangers are used for directing mail to specific servers other than the one a hostname points at. |
| Mail Extender | Assign an email address. |
- Click **Apply** to finish these settings and return to previous page.

Note:

1. The Wildcard and Backup MX features are not supported for all Dynamic DNS providers. You could get more detailed information from their websites.
2. Backup MX provides a secondary mail server to hold your e-mail if your main email server go offline for any reason. Once you go back online, your email will be delivered to you.

4.3.6 Call Schedule Setup

These call schedule profiles will control the up or down time of the router's dialer or connection manager. In order to do the proper call schedule function, a user must have to setup time function and arrange schedules for specified Internet access profile or LAN-to-LAN profile. Vigor3300V+ supports lots of profiles for call schedule usage. Click **Advanced >> Call Schedule** option. You will get the following page.

Advanced - Call Schedule

#	Status	Date & Time	Action	How often	Week Option	WAN
1	<input checked="" type="radio"/> Enable	2006-4-18, 00:00	Force On	Once		WAN1
2	<input type="radio"/>					
3	<input type="radio"/>					
4	<input type="radio"/>					
5	<input type="radio"/>					
6	<input type="radio"/>					
7	<input type="radio"/>					
8	<input type="radio"/>					
9	<input type="radio"/>					
10	<input type="radio"/>					

- Status** Display the activation status (enable or disable) for this entry.
- Date & Time** Display the start date and time for this schedule.
- Action** Display the action that this schedule adopts.
- How often** Display the using frequency (once or specific day in a week) of this schedule.
- Week Option** Display the specific day in a week if you choose **Weekdays** as the **How often** setting.
- WAN** Display the WAN interface used for this entry.
- Edit** Allow users to edit the selected call schedule settings.
- Delete/Delete All** Remove one/all the selected call schedule settings.

Edit Call Schedule

To edit an item, click the radio button of the item that you want to modify. Then click **Edit** on the bottom of the page to add a new rule entry or modify an existed rule entry.

Advanced - Call Schedule - Edit

Disable Enable

Start Date : - - (Year - Month - Date)

Start Time : : (Hour : Minute)

Action : Force Down Force On

How often : Once Weekdays

Monday Tuesday Wednesday Thursday Friday Saturday Sunday

Network Interface :

Enable/Disable

Click **Disable** to disable this function. Click **Enable** to activate this function.

Start Date

Assign a date for starting this profile.

Start Time

Assign a time for starting this profile.

Action

Force down means to inactivate the Network Interface. **Force up** means to activate the Network Interface.

How often

Once means only for one time. **Weekdays** means that user can select some weekdays to apply.

Network Interface

Select one specific WAN interface to be applied.

Click **Apply** to finish this setting.

Delete Call Schedule

To delete an item, click the radio button of the item that you want to delete. Then click **Delete** on the bottom of the page to remove the entry.

Advanced - Call Schedule

#	Status	Date & Time	Action	How often	Week Option	WAN
1	<input checked="" type="radio"/> Enable	2000-1-26, 00:00	Force On	Once		WAN1
2	<input type="radio"/>					
3	<input type="radio"/>					
4	<input type="radio"/>					
5	<input type="radio"/>					
6	<input type="radio"/>					
7	<input type="radio"/>					
8	<input type="radio"/>					
9	<input type="radio"/>					
10	<input type="radio"/>					

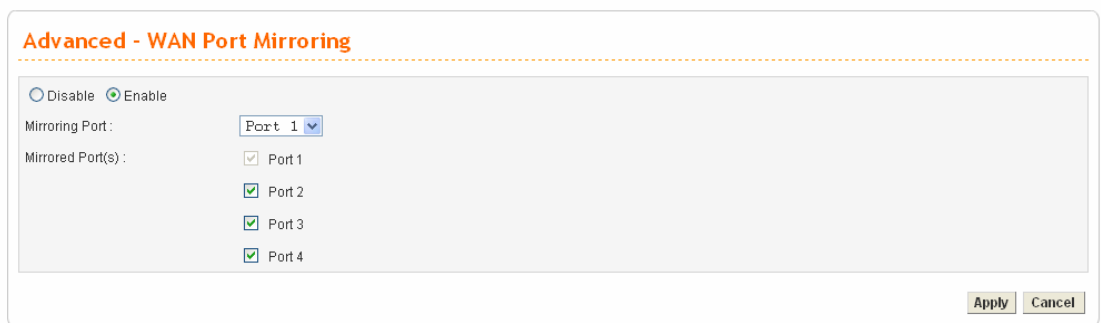
Also, users can click **Delete All** to remove all entries in the table.

4.3.7 WAN Port Mirroring Setup

Vigor3300V+ supports port mirroring function in WAN interfaces. Generally speaking, this function copies traffic from one or more specific ports to a target port. This mechanism helps manager track the network errors or abnormal packets transmission without interrupting the flow of data access the network. By the way, user can apply this function to monitor all traffics which user needs to check.

There are some advantages supported in this feature. Firstly, it is more economical without other detecting equipments to be set up. Secondly, it may be able to view traffic on one or more ports within a VLAN at the same time. Thirdly, it can transfer all data traffics to be mirrored to one analyzer connect to the mirroring port. Last, it is more convenient and easy to configure in user's interface.

Click **Advanced**>>**WAN Port Mirroring**. You will see the following page.



Enable/Disable

Click **Disable** to disable this function. Click **Enable** to activate this function.

Mirroring Port

Select a port to view traffic sent from mirrored ports.

Mirrored Port(s)

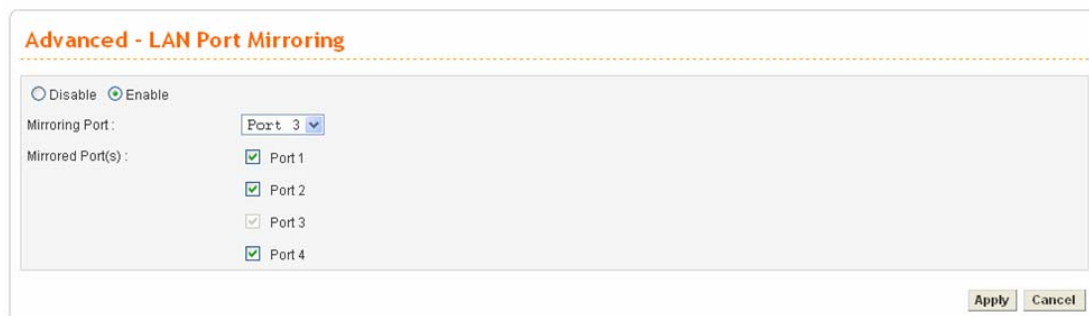
Click which ports are necessary to be mirrored.

After finishing the settings, please click **Apply**.

4.3.8 LAN Port Mirroring Setup

Port mirror can be applied for the users in LAN. It has the same mechanism like WAN port mirroring.

Click **Advanced >> LAN Port Mirroring**.



Enable/Disable Click **Disable** to disable this function. Click **Enable** to activate this function.

Mirroring Port Select a port to view traffic sent from mirrored ports.

Mirrored Port(s) Click which ports are necessary to be mirrored.

After finishing the settings, please click **Apply**.

4.3.9 LAN VLAN Setup

Virtual LANs (VLANs) are logical, independent workgroups within a network. These workgroups communicate as if they had a physical connection to the network. However, VLANs are not limited by the hardware constraints that physically connect traditional LAN segments to a network. As a result, VLANs allow the network manager to segment the network with a logical, hierarchical structure. VLANs can define a network by application or department. For instance, in the enterprise, a company might create one VLAN for multimedia users and another for e-mail users; or a company might have one VLAN for its Engineering Department, another for its Marketing Department, and another for its guest who can only use Internet not Intranet. VLANs can also be set up according to the organization structure within a company. For example, the company president might have his own VLAN, his executive staff might have a different VLAN, and the remaining employees might have yet a different VLAN. VLANs can also set up according to different company in the same building to save the money and reduce the device establishment.

This router supports Virtual LAN only in LAN site. User can select some ports to add into a VLAN group. In one VLAN group, the port number can be single one or more.

The purpose of VLAN is to isolate traffic between different users and it can provide better security application.

For Port Base VLAN

There are three VLAN settings offered here for you to configure. If you click **Disable**, no configuration can be completed. Please choose **Port Base VLAN** to open the following page.

Advanced - LAN VLAN Setting

Disable
 Port Base VLAN
 802.1Q VLAN

Port Base VLAN	802.1Q VLAN	P1	P2	P3	P4
VLAN0		<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
VLAN1		<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
VLAN2		<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
VLAN3		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>

P1 – P4

Check the box to make the computer connecting to the port being grouped in the specified VLAN. Be aware that each port can be grouped in different VLAN at the same time only if you check the box. For example, if you check the boxes of VLAN0-P1 and VLAN1-P1, you can make P1 to be grouped under VLAN0 and VLAN1 simultaneously.

VLAN 0- 3

This router allows you to set 4 groups of virtual LAN.

Apply

After finishing the settings, please click **Apply**.

Reset

In addition, you can click **Reset** to reset the VLAN setting as default. A dialog will be prompted for you to ask confirmation. Click **OK**.

For 802.1Q VLAN

Another way to set VLAN is based on 802.1Q. Please choose **802.1Q VLAN** to open the following page. This page is available only for the PCs with certain network cards which support 802.1Q VLAN feature. It is useless for general network cards.

Advanced - LAN VLAN Setting

Disable Port Base VLAN 802.1Q VLAN

Port Base VLAN 802.1Q VLAN

Group

Index	Active	Name	VLAN ID	Member				Frame Tag Operation			
				P1	P2	P3	P4	P1	P2	P3	P4
1	<input type="checkbox"/>	VLAN5	<input type="text" value="5"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Untagged	Tagged	Tagged	Tagged
2	<input type="checkbox"/>	VLAN6	<input type="text" value="6"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Tagged	Untagged	Tagged	Tagged
3	<input type="checkbox"/>	VLAN7	<input type="text" value="7"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Tagged	Tagged	Untagged	Tagged
4	<input checked="" type="checkbox"/>	VLAN8	<input type="text" value="8"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Tagged	Tagged	Tagged	Untagged

Enable management port for P4
 Enable packet forwarding between VLANs

Port Setting

	P1	P2	P3	P4
Port VLAN ID	<input type="text" value="5"/>	<input type="text" value="6"/>	<input type="text" value="7"/>	<input type="text" value="8"/>

Active

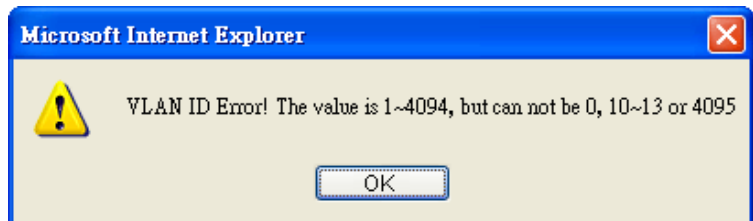
Check this box to activate the settings of this entry. If you check the **Management Port** box below, Index 4 will be unchangeable and locked. And, you have to set Port VLAN ID for P4 previously before you check **Management Port**.

Name

Specify the name for the four groups of VLAN.

VLAN ID

Type a number used for identification on VLAN for your computer. Later, you have to type the same ID number for each PC which wants to be grouped within the same VLAN group. In addition, if you type wrong ID number, the following message will appear to warn you. Please type correct number.



By the way, if you don't know how to configure a VLAN setting on your computer, please refer to **How to Check/Edit VLAN ID on Your PC** below for more detailed information.

Member

To make the hosts (with the same VLAN ID) of different ports communicating with each other, please check the port box (P1 to P4) according to your necessity.

Frame Tag Operation

Basically, the default settings for tagged or untagged VLAN will be shown automatically when you type VLAN ID/Name and check the Active box. By the way, you can modify the tag

operation for each VLAN in this page for obtaining proper control. Use the drop down list to choose a tag operation for each port.

Tagged – All the computers behind that port must support VLAN and are tagged with certain VLAN groups with specified ID numbers.

Untagged - All the computers behind that port do not support VLAN feature.

Note: It is recommended to group computers that do not support VLAN feature or support VLAN feature but their Untagged VLAN settings are checked in one port with untagged. This device will tag proper port VLAN ID for untagged PC respectively for making them communicating with the router.

Enable Management Port for P4

It can help users to communicate with router still even though configuring the wrong setting in the 802.1Q VLAN tag. The management port will lock index 4. We recommend that users enable the management port to fix the fourth VLAN settings unless users want to use the fourth VLAN and ensure the settings are correct. You have to set Port VLAN ID for P4 previously before you check this box.

Enable packet forwarding between VLANs

Packets can be transmitted and forwarded among VLAN groups if this box is checked. In default, it is unchecked.

Port VALN ID

Type the ID for each port used for identification on VLAN. When the tag operation for each port (representing for different computers connected to this router) is marked by untagged, to avoid conflict occurred, the system will apply the ID listed in these boxes automatically for each port (P1 to P4) to ensure proper and correct network operation.

4.3.10 SNMP

The Simple Network Management Protocol (SNMP) is an application layer protocol that facilitates the exchange of management information between network devices. There is a set of protocols for managing complex networks. SNMP works by sending messages, called protocol data units (PDUs), to different parts of a network. SNMP enables network administrators to manage network performance, find and solve network problems, and plan for network growth.

A SNMP-managed network consists of three key components, **managed devices, agents, and network-management systems (NMSs).**

A managed device is a network node that contains an SNMP agent and that resides in a managed network. Managed devices collect and store management information and make this information available to NMSs by using SNMP. Managed devices, sometimes called network elements, can be routers and access servers, switches and bridges, computers hosts, or printers.

This function is to define a community string name. An agent is a network-management software module that resides in a managed device. An agent has local knowledge of management information and translates that information into a form compatible with SNMP.

An NMS executes applications that monitor and control managed devices. NMSs provide the bulk of the processing and memory resources required for network management. One or more NMSs must exist on any managed network.

There are two items for SNMP – **SNMP Community** and **SNMP Traps**.

SNMP Community

In general, NMSs in the community exist within the same administrative domain.

Advanced - SNMP - SNMP Community

#	Community	Host/mask	Max Access
1	<input checked="" type="radio"/> public		Read only
2	<input type="radio"/>		
3	<input type="radio"/>		
4	<input type="radio"/>		
5	<input type="radio"/>		
6	<input type="radio"/>		
7	<input type="radio"/>		
8	<input type="radio"/>		
9	<input type="radio"/>		
10	<input type="radio"/>		

1

Community	Display the community string used for the specified entry.
Host/mask	Display the mask address for the host.
Max Access	Display the authority (read only or read/write)for this entry.
Edit	Allow users to edit the selected SNMP community settings.
Delete/Delete All	Remove one/all the selected SNMP community settings. A dialog will be prompted for you to ask confirmation. Click OK .

To edit an item, click the radio button of the item that you want to modify. Then click **Edit** on the bottom of the page to add a new rule entry or modify an existed rule entry.

Advanced - SNMP - SNMP Community - Edit

1

Community :

Host/mask :

Max Access : Read only Read/Write

Community	Type the community string (e.g., public) for SNMP.
Host/mask	Assign a value of subnet mask for host IP address.
Max Access	Select the authority as Read only or Read/Write . Read only means user only can monitor managed devices. Read/Write means user can control managed devices including change the values of variable stored within managed devices.
Apply	Click Apply to save this setting and return the previous page.

To delete an item, click the radio button of the item that you want to delete. Then click **Delete** on the bottom of the page to remove the entry. A dialog will be prompted for you to ask confirmation. Click **OK**.

SNMP Traps

In managed network by SNMP protocol, agent will send a specific packet as an attention for administrator, called **Trap**. Trap is the only **PDU(Protocol data unit)** sent by an agent on its own initiative. It is used to notify the management station of an unusual event that may demand further attention (like a link down).

Choose **SNMP Traps** option to see the following page.

#	Trap Server	Trap Community	Trap server port
1	<input checked="" type="radio"/>		1
2	<input type="radio"/>		
3	<input type="radio"/>		
4	<input type="radio"/>		
5	<input type="radio"/>		
6	<input type="radio"/>		
7	<input type="radio"/>		
8	<input type="radio"/>		
9	<input type="radio"/>		
10	<input type="radio"/>		

- Trap Server** Display the IP address of the trap server.
- Trap Community** Display the community string of the trap server.
- Trap server port** Display the port number used for the trap server.
- Edit** Allow users to edit the selected SNMP traps settings.
- Delete/Delete All** Remove one/all the selected SNMP traps settings. A dialog will be prompted for you to ask confirmation. Click **OK**.

To edit an item, click the radio button of the item that you want to modify. Then click **Edit** on the bottom of the page to add a new rule entry or modify an existed rule entry.

1

Trap server :

Trap community :

Trap server port :

- Trap server** Assign an IP address of trap server.
- Trap community** Assign a community string for Trap packet using.
- Trap server port** Assign a port number for Trap server using.
- Apply** Click **Apply** to save this setting and return the previous page.

4.3.11 SIP ALG

This page allows you to configure settings to make SIP message and RTP packets of voice being transmitting and receiving correctly via NAT by Vigor3300V+ while using VoIP function with SIP protocol.

Advanced - SIP Application-level gateway

Disable Enable

SIP listen port:

RTP port start:

Allow registrations: Anyone Register from: /
 /
 /

Timeout for an RTP stream: Seconds

Default expires: Seconds

VoIP Port Setting

VoIP SIP local port:

Disable / Enable

Click **Enable** to enable the SIP ALG function.

SIP listen port

Set the listen incoming SIP message port (range: 1~65535).

RTP port start

Set the starting value of RTP port range used by SIP ALG (range: 1~65535).

For example, if you set 7070 as RTP port start value, the SIP ALG will use 7070 (including 7070) and port value after for RTP transmission.

Allow registrations

Limit the registration condition for the clients in LAN.

Anyone – All the SIP devices under NAT can finish the registration through SIP ALG.

Register from - Specify a network segment for registration. Only the IP addresses within the same segment are allowed to do registration.

Timeout for an RTP stream If there is no data transmitted within the time, such RTP stream will be discarded.

Default expires

Set the expire time for SIP ALG to send out SIP message.

VoIP SIP local port

Type the port number for SIP protocol for VoIP. The default value is 5060.

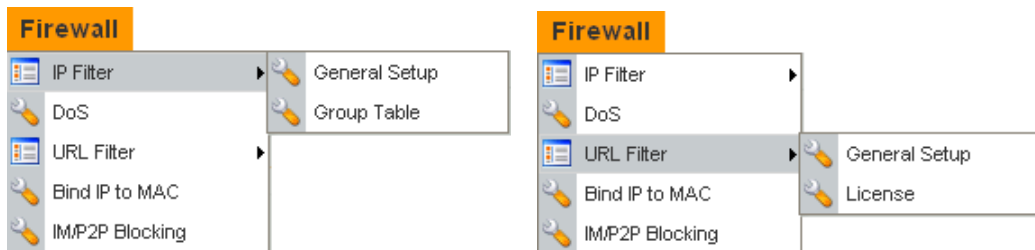
Apply

Click **Apply** to save the setting and go to **System – Reboot** to reboot the device for activating the setting.

4.4 Firewall Setup

The firewall controls the allowance and denial of packets through the router. The **Firewall Setup** in the Vigor 3300 Series mainly consists of packet filtering, Denial of Service (DoS) and URL (Universal Resource Locator) content filtering facilities. These firewall filters help to protect your local network against attack from outsiders. A firewall also provides a way of restricting users on the local network from accessing inappropriate Internet content and can filter out specific packets, which may trigger unexpected outgoing connection such as a Trojan.

The following sections will explain how to configure the **Firewall**. Users can select **General Setup**, **IP Filter**, **DoS** and **URL Filter** options from Firewall menu. The **DoS** facility can detect and mitigate the DoS attacks. The **URL Filter** can block inappropriate websites for SME.

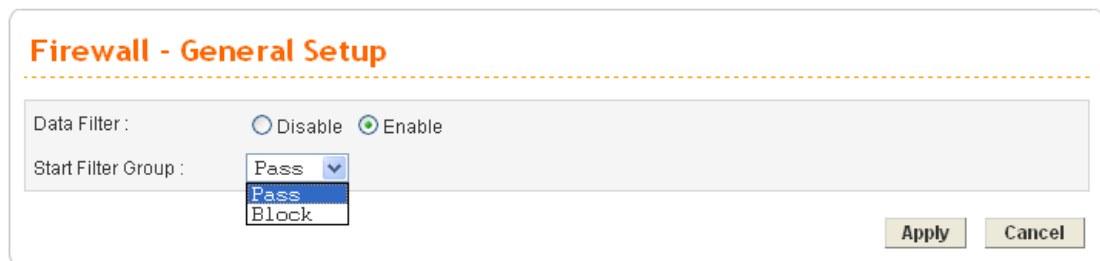


4.4.1 IP Filter

First, you should create at least one Group in the **IP Filter >> Group Table**. Then you can enable the **Data Filter** and select a **Start Filter Group** in **General Setup**. The following sections explain **IP Filter** functions with details.

General Setup

The page allows you to set general settings such as enabling the data filter function and choosing proper filter group.



Data Filter

Disable or **Enable** the firewall function. This firewall can only be enabled if at least one filter group exists. The default is **Disable**.

Start Filter Group

Default group names provided here are Pass and Block. Select the first filter group to begin filtering mechanism. The group in this list must exist and had been pre-configured. The system provides three types of filter for you to choose in default. The available settings provided here can be added or edited in **Firewall>>IP Filter>>Group Table**.

Group Table

Group Table allows you to set definitions for different groups of the filters that will be applied for the function of IP filter.

Firewall - IP Filter - Group Table

IP Filter Group Table				
	Index	Group Name	Next Group	Comment
<input checked="" type="radio"/>	1	Pass	Block	Group for pass rules
<input type="radio"/>	2	Block	none	Group for block rules

Index Allow you to change current IP filter table or add new rule for current group. Click the number link to get into the IP filter table page for editing.

Group Name Display the group name.

Next Group Display next group name.

Comment Display the notice for current group.

Add Allow you to add a new IP filter table.

Edit Allow you to edit selected IP filter table.

Delete Allow you to delete selected IP filter table configuration. If this entry is assigned as the started filter group already, it cannot be deleted.

To add a new group, please click **Add** on the **Group Table** page to access into the following page. In this page, you can type in new group name and decide the next group name. Also, you can type in your comment for such group. After you click **Apply**, the new group will be added and you will see it from the drop down menu of **Start Filter Group**.

Firewall - IP Filter Table

Group Name :

Next Group Name :

Comment :

Group Name Type in the name of the group.

Next Group Name Select next group to filter packets.

Comment Type in your comment or description for the group.

To edit a selected group, please click the number link to open the following page. You can change the next group name and modify the comment for your necessity. When you finish the modification, simply click **Apply**.

Firewall - IP Filter Table

Group Name :

Next Group Name :

Comment :

Besides, you can add new filter rule for the group. On the edit page of **IP Filter Table**, click the **Add Rule** button. The following page will be shown.

Firewall - IP Filter - Add Filter Rule

Filter Condition

Active

Comment :

Source : IP :
Subnet Mask :
Port : -

Destination : IP :
Subnet Mask :
Port : -

Group Name :

Protocol :

Direction :

Fragment :

Action

Block or Pass :

Next Group Name :

Comment

Type the name for the rule.

Source IP

It means the source IP address. Placing the symbol “!” before a particular IP address will prevent this rule from being applied to that IP address. It is equal to the logical **NOT** operator.

Subnet Mask

It means the subnet mask for the source IP.

Source Port

It means the port for the source IP. Type the values in the boxes of **start port** and **end port**. As for the operators

Port :

- =
- !=
- >
- <
- between

If the **Start Port** column 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** column is empty, the filter rule will set

the port number to be the value of the **Start Port** column. Otherwise, the port number ranges from the **Start Port** to the **End Port** including the **Start Port** and the **End Port**.

(!) - If the **End Port** column is empty, the port number is not equal to the value of the **Start Port** column. Otherwise, this port number is not between the **Start Port** and the **End Port** including the **Start Port** and **End Port**.

(>) - Specifies the port number is larger than or equal to the **Start Port**.

(<=) - Specifies the port number is less than or equal to the **Start Port**.

Between - Specifies the port number is between the **Start Port** and **End Port**.

Destination IP

It means the destination IP address for this filter rule. Placing the symbol “!” before a particular IP address will prevent this rule from being applied to that IP address. It is equal to the logical NOT operator.

Destination Mask

It means the subnet mask for the destination IP.

Destination Port

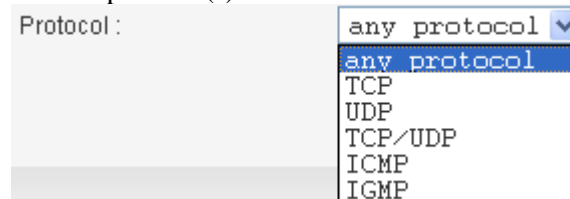
It means the port for the destination IP.

Group Name

It means the filter group for the current rule.

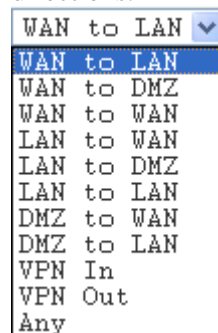
Protocol

It is the protocol(s) for this filter rule.



Direction

The direction of packet flow **VPN In** is for incoming packets. **VPN Out** is for outgoing packets, and **Any** is for both directions.



Fragments

It is the response to fragmented packets. There are three options as below.



Do not care - Specifies no fragment options.

Unfragment - Applies the rule to unfragment packets.

Fragmented - Applies the rule to fragmented packets.

Block or Pass

The action to be taken when packets match the rule. There are four options:

Block or Pass : Block immediately ▾

Block immediately

Pass immediately

Block if no further match

Pass if no further match

Block immediately - Block the packet immediately.

Pass immediately - Pass the packet immediately.

Block if no further match - means to locks the packet if no further rules are matched.

Pass if no further match - means to passes the packet if no further rules are matched.

Note: It is recommended placing pass rules in “pass” group and block ones be in “block” group.

Next Group Name

It indicates the next filter group. If the option **Block if no further match** or **Pass if no further match** of **Block or Pass** parameter is selected, the unmatched packets will be compared with rules in **Next Group**. The option **None** must be chosen while **Block or Pass** is selected as **Block or Pass**.

Apply

Click this button to return to IP Filter Table setting page. The new added rule information will be displayed on this page too. Refer to the following graphic.

Firewall - IP Filter Table

Group Name :

Next Group Name : none ▾

Comment :

IP Filter Table

Index	Source IP	Subnet Mask	Port	Destination IP	Subnet Mask	Port	Protocol	Direction	Block	Active
1	192.168.3.1	255.255.255.0	130	192.168.3.58	255.255.255.0	130	TCP	LAN to LAN	Block immediately	☑

4.4.2 DoS

The DoS function helps to detect and mitigates DoS attacks. These include flooding-type attacks and vulnerability attacks. Flooding-type attacks attempt to use up all your system's resources while vulnerability attacks try to paralyze the system by offending the vulnerabilities of the protocol or operation system.

In the **Firewall** group, click the **DOS** option. You will see the following page. The DoS Defense Engine inspects each incoming packet against the attack signature database. Any packet that may paralyze the host in the security zone is blocked. The DoS Defense Engine also monitors traffic behavior. Any anomalous situation violating the DoS configuration is reported and the attack is mitigated.

Firewall - DoS

DoS Defense : Disable Enable

<input type="checkbox"/> Enable SYN flood defense :	Threshold: <input type="text" value="300"/> Packets/sec	Timeout: <input type="text" value="10"/> sec
<input type="checkbox"/> Enable UDP flood defense :	Threshold: <input type="text" value="300"/> Packets/sec	Timeout: <input type="text" value="10"/> sec
<input type="checkbox"/> Enable ICMP flood defense:	Threshold: <input type="text" value="300"/> Packets/sec	Timeout: <input type="text" value="10"/> sec
<input type="checkbox"/> Enable Port Scan detection :	Threshold: <input type="text" value="300"/> Packets/sec	
<input type="checkbox"/> Block IP options	<input type="checkbox"/> Block TCP flag scan	
<input type="checkbox"/> Block Land	<input type="checkbox"/> Block Tear Drop	
<input type="checkbox"/> Block Smurf	<input type="checkbox"/> Block Ping of Death	
<input type="checkbox"/> Block trace route	<input type="checkbox"/> Block ICMP fragment	
<input type="checkbox"/> Block SYN fragment	<input type="checkbox"/> Block Unknown Protocol	
<input type="checkbox"/> Block Fraggle Attack		

- DoS Defense** Enables or disables the DoS Defense function. The default value is **Disable**.
- Enable SYN Flood Defense** Activates the SYN flood defense function. If the amount of TCP SYN packets from the Internet exceeds the user-defined threshold value, the router will be forced to randomly discard the subsequent TCP SYN packets within the user-defined timeout period. The default setting for threshold and timeout are **300** packets per second and **10** seconds, respectively.
- Enable UDP Flood Defense** Activates the UDP flood defense function. If the amount of UDP packets from the Internet exceeds the user-defined threshold value, the router will be forced to randomly discard the subsequent UDP packets within the user-defined timeout period. The default setting for threshold and timeout are **300** packets per second and **10** seconds, respectively.
- Enable ICMP Flood Defense** Activates the ICMP flood defense function. If the amount of ICMP echo requests from the Internet exceeds the user-defined threshold value, the router will discard the subsequent echo requests within the user-defined timeout period. The default setting for threshold and timeout are **300** packets per second and **10** seconds, respectively.
- Enable Port Scan Detection** Activates the Port Scan detection function. Port scan sends packets with different port numbers to find available services, which respond. The router will identify it and report a warning message if the port scanning rate in packets per second exceeds the user-defined threshold value. The default threshold is **300** pps (packets per second).
- Enable Block IP Options** Activates the Block IP options function. The router will ignore any IP packets with IP option field appearing in the datagram header.
- Enable Block Land** Activates the Block Land function. A Land attack occurs when an attacker sends spoofed SYN packets with identical source address, destination addresses and port number as those of the victim.

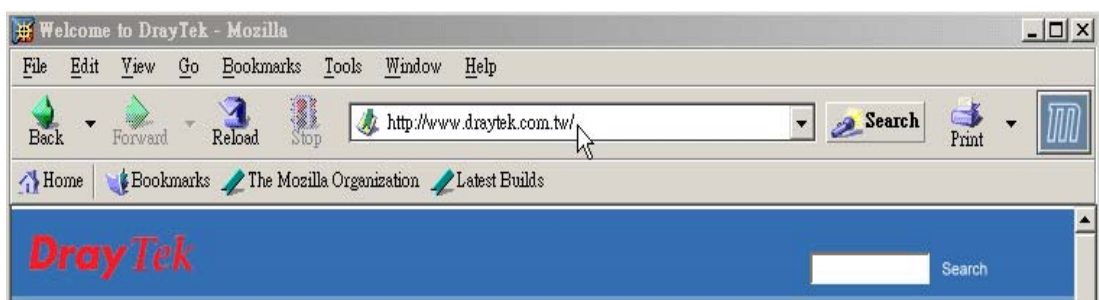
Enable Block Smurf	Activates the Block Smurf function. The router will reject any ICMP echo request destined for the broadcast address.
Enable Block Trace Route	Activates the Block trace route function. The router will not forward any trace route packets.
Enable Block SYN Fragment	Activates the Block SYN fragment function. Any packets having the SYN flag and fragmented bit sets will be dropped.
Enable Block Fraggle Attack	Activates the Block fraggle Attack function. Any broadcast UDP packets received from the Internet are blocked.
Enable TCP Flag Scan	Activates the Block TCP flag scan function. Any TCP packet with an anomalous flag setting is dropped. These scanning activities include no flag scan, FIN without ACK scan, SYN FIN scan, Xmas scan and full Xmas scan .
Enable Tear Drop	Activates the Block Tear Drop function. This attack involves the perpetrator sending overlapping packets to the target hosts so that target host will hang once they re-construct the packets. The routers will block any packets resembling this attacking activity.
Enable Ping of Death	Activates the Block Ping of Death function. Many machines may crash when receiving an ICMP datagram that exceeds the maximum length. The router will block any fragmented ICMP packets with a length greater than 1024 octets.
Enable Block ICMP Fragment	Activates the Block ICMP fragment function. Any ICMP packets with fragmented bit sets are dropped.
Enable Block Unknown Protocol	Activates the Block Unknown Protocol function. The router will block any packets with unknown protocol types.

Click **Apply** to apply the settings when you finish the configuration.

4.4.3 URL Filter

The Internet contains a wide range of offenses or illegal materials. Unlike traditional media, the Internet does not have any obvious tools to segregate materials based on URL strings or content. URL content filtering systems are seen as tools that would provide the cyberspace equivalent of the physical separations that are used to limit access to particular materials. By rating a site as objectionable, and refusing to display it on user's browser, URL content filter can prevent employee on SME from accessing inappropriate Internet resources.

Instead of traditional firewall inspects packets based on the fields of TCP/IP headers, the URL content filter checks the URL strings or the payload of TCP/IP packets.



The URL content filter in the series of broadband security routers inspects every URL string in the HTTP request. If the entire or part of the URL string (for instance, <http://www.draytek.com>, as shown above) matches any activated rule, the first and the

following associate HTTP request will be blocked. The system will discard any request, which tries to retrieve the malicious code.

Notice that you must clear your browser cache first so that the URL content filter operates properly on a Web page that you visited before.

First, you should create at least one Group in the **IP Filter >> URL Filter**. Then you can enable the **Data Filter** and select a **Start Filter Group** in **General Setup**. The following sections explain **IP Filter** functions with details.

URL Filter – General Setup

The URL content filter consists of the following functions: **URL Access Control**, **Content Filter**, **Restrict Web Feature** and **Filter Schedule**.

● URL Access Control

The **URL Access Control** controls Web site access by inspecting the URL string against user-defined keywords. In the **Firewall** group, click the **URL Filter** option. You will see the following page.

Enable/Disable

Disable or **Enable** URL Filter function.

Keyword

The keyword(s) used to filter URLs. Keywords can be partial words or complete URLs. The router will reject any Website which whole or partial URL matches any keywords.

Keyword List

The list of keywords.

Block Direct IP Web Access

Deny any Web surfing activity that directly uses an IP address.

Enable Exception List	Click it to allow specified IP addresses or subnets to be passed through.
IP Address	The allowed IP address.
Subnet Mask	The allowed subnet mask of IP address.
Exception List	The list of IP addresses where content filter rules are not applied.

● Content Filter

Content Filter can help to avoid your employees accessing into improper websites and affecting the work efficiency; protect your children from viewing inappropriate websites and accessing chat rooms; and monitor and control web access from all computers connected to your router.

Server	Enable or Disable Content Filter.
Permitted Categories List	The permitted categories are obtained from the selected a server.
Forbidden Categories List	The forbidden categories are obtained from the selected a server.
URL	The URL domain name.
Option	Allow or Deny the selected URL.
Exception URL List	The list of filtered URLs.

● Restrict Web Feature

This feature blocks malicious codes hidden in Web pages, such as Java Applet, Active X, Cookies, Proxy, compressed files, and executable files. It is also able to block all downloads of multimedia files from Web pages in order to control the bandwidth usage.

Malicious code may be embedded in some executable objects, such as ActiveX, Java Applet, compressed files, executable files, Proxy, and Multimedia. For example, an ActiveX object with malicious code may gain unlimited access to the system.

- | | |
|-------------------------|---|
| Java | Activates the Block Java object function. The router will discard Java objects from the Internet. |
| ActiveX | Activates the Block ActiveX object function. The router will discard ActiveX object from the Internet. |
| Compressed Files | Activates the Block Compressed file function to prevent from downloading of any compressed file. These following types of compressed files are blocked by the router.
.zip / .rar / .arj / .ace / .cab / .sit |
| Execution Files | Activates the Block Executable file function to prevent from downloading of any executable file. The following types of executable files are blocked by the router.
.exe / .com / .scr / .pif / .bas / .bat / .inf / .reg |
| Cookie | Activates the Block Cookie function. Cookies are used by many websites to create “stateful” sessions for tracking Internet users, which would violate the users’ privacy. The router will filter out all cookies-related transmissions. |
| Proxy | Activates the Block Proxy function. The router will filter out all proxy-related transmissions. |
| Multimedia Files | Activates the Block Multimedia function. The router will filter out multimedia from any website. |

● Filter Schedule

Filter Schedule function controls what times the URL content filter should be active. It can specify what times the URL content filtering facility should be active.

Firewall - URL Filter

Disable Enable

URL Access Control | Content Filter | Restrict Web Feature | **Filter Schedule**

Always Block
 Block only at

8 : 00 To 18 : 00

Day of Week:
 All Days Sun Mon Tue Wed Thu Fri Sat

Apply Cancel

Always Block

The URL content filtering facility is always active.

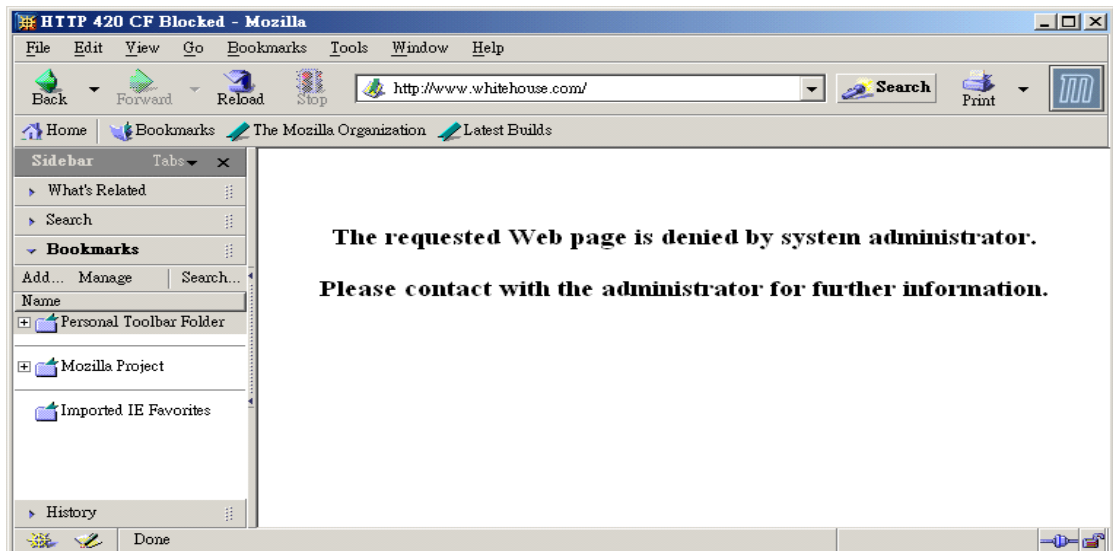
Block only at

The URL content filtering facility is active during the specified times from H1:M1 to H2:M2 in one day, where H1 and H2 indicate the hours and M1 and M2 represent the minutes.

Day of Week - The URL content filtering facility is active during the specified days of the week. The default value is 8:00 to 18:00 from Monday to Friday.

● Warning Page

After the configuration of URL Filter is configured properly, an alert page will appear in the browser when an HTTP request is denied. Refer to the following graphic.



URL Filter – License

Display the corresponding information for the WCF license. Click auth.draytek.com to authenticate the license and activate the WCF service.

Firewall - URL Filter License

INFO :

Serial Number :

Start Date :

Expire Date :

Activate URL : auth.draytek.com

4.4.4 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.

Firewall - Bind IP to MAC

Enable Disable Strict Bind

Note: If choose Strict Bind, all IPs not bind to MAC cannot gain access to internet.

ARP Table [Select All](#) | [Sort](#) | [Refresh](#)

IP Address	Mac Address
192.168.1.10	00:0E:A6:2A:D5:A1

IP Bind List [Select All](#) | [Sort](#)

Index	IP Address	Mac Address
-------	------------	-------------

Add and Edit

IP Address:

Mac Address: : : :

Enable

Click this radio button to invoke this function. However, IP/MAC which is not listed in IP Bind List also can connect to Internet.

Disable

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

Strict Bind

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

ARP Table

This table is the LAN ARP table of this router. The information for IP and MAC will be displayed in this field. Each pair of IP and MAC address listed in ARP table can be selected and added to IP Bind List by clicking **Add** below.

Add and Edit

IP Address – Type the IP address that will be used for the specified MAC address.

Mac Address – Type the MAC address that is used to bind with the assigned IP address.

Refresh	It is used to refresh the ARP table. When there is one new PC added to the LAN, you can click this link to obtain the newly ARP table information.
IP Bind List	It displays a list for the IP bind to MAC information.
Add	It allows you to add the one you choose from the ARP table or the IP/MAC address typed in Add and Edit to the table of IP Bind List .
Edit	It allows you to edit and modify the selected IP address and MAC address that you create before.
Remove	You can remove any item listed in IP Bind List . Simply click and select the one, and click Remove . The selected item will be removed from the IP Bind List .

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

4.4.5 IM/P2P Blocking

IM Blocking means instant messenger blocking. P2P is the short name of peer to peer. You will see a list of common P2P applications. You can define blocking rules (such as specified an IP address for passing through or blocking) for IM (Instant Messenger)/P2P (Peer to Peer) application.

Firewall - IM/P2P Blocking

#	Source IP	Subnet Mask	Action	Option
1	<input checked="" type="radio"/>			
2	<input type="radio"/>			
3	<input type="radio"/>			
4	<input type="radio"/>			
5	<input type="radio"/>			
6	<input type="radio"/>			
7	<input type="radio"/>			
8	<input type="radio"/>			
9	<input type="radio"/>			
10	<input type="radio"/>			

Edit Delete Delete All

To edit IM/P2P blocking rule, please choose one of the radio buttons under “#” and click **Edit**. The following page will be shown automatically.

Firewall - IM/P2P Blocking - Edit

1

Source IP :

Subnet Mask :

Action : Allow Disallow

IM

MSN Yahoo Messenger ICQ

AIM QQ iChat

Google Talk Web IM (<http://www.e-messenger.net/>) Web MSN (<http://webmessenger.msn.com/>)

VoIP

Skype

P2P

Protocol	Applications
<input type="checkbox"/> SoulSeek	SoulSeek
<input type="checkbox"/> eDonkey	eDonkey, eMule, Shareaza
<input type="checkbox"/> FastTrack	KazaA, iMesh
<input type="checkbox"/> Gnutella	BearShare, Limewire, Shareaza, Foxy
<input type="checkbox"/> BitTorrent	BitTorrent, BitSpirit, BitComet

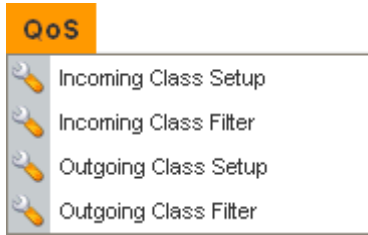
- Source IP** Specify an IP address for Vigor router to perform IM/P2P blocking.
- Subnet Mask** Type the subnet mask for the IP address specified.
- Action** Choose **Allow** to make the packet passing through. Choose **Disallow** to block the packet in or out.
- IM/VoIP/P2P** Check the boxes for different applications filtering by this rule.

4.5 Quality of Service Setup

The QoS (Quality of Service) guaranteed technology in the Vigor 3300 Series allows the network administrator to monitor, analyze, and allocate bandwidth for various types of network traffic in real-time and/or for business-critical traffic. Thus, timing-sensitive applications will not be impacted by web surfing traffic or other non-critical applications, such as file transfer. Without QoS-guaranteed control, there would be virtually no way to prioritize users/services or guarantee allocation of finite bandwidth resources to network or servers for supporting timing-sensitive and mission-critical network applications, such as VoIP (Voice over IP) and online gaming applications.

Differentiated quality of service is therefore one of the most important issues over the Internet infrastructure. In the Vigor 3300V+ Series, DSCP (Differentiated Service Code Point) support is also taken into consideration in the design of the QoS-guaranteed control module.

The QoS function handles incoming and outgoing classes independently. Users can configure incoming or outgoing separately without any impact on the other.



For the web pages for incoming class setup and outgoing class setup (incoming class filter and outgoing class filter) are similar, they will be explained in the same sections.

4.5.1 Incoming/Outgoing Class Setup

Incoming/Outgoing Class Setup allows you to configure bandwidth percentage for data and voice signals transmission. Click the **QoS** option and choose **Incoming Class Setup/Outgoing Class Setup**. There are eight queues that can be configured. The total sum of bandwidth has to be 100 percent for all configured queues. Any leftover bandwidth is assigned to eight queues to meet 100 percent totally.

QoS - Incoming Class Setup

Disable Enable

Index	Class Name	Bandwidth
1.	<input type="text"/>	<input type="text"/> %
2.	<input type="text"/>	<input type="text"/> %
3.	<input type="text"/>	<input type="text"/> %
4.	<input type="text"/>	<input type="text"/> %
5.	<input type="text"/>	<input type="text"/> %
6.	<input type="text"/>	<input type="text"/> %
7.	<input type="text"/>	<input type="text"/> %
8.	others	<input type="text"/> %

Disable/Enable

Click **Disable** to close this setting. Click **Enable** to activate this setting.

Index

It represents the number for each queue.

Class Name

Please type the name for each queue.

Bandwidth

Please type the usage percentage for each queue.

Apply

Click this button to apply all the settings set in this page.

4.5.2 Incoming/Outgoing Class Filter

Click the **QoS** option and choose **Incoming Class Filter/Outgoing Class Filter**.

QoS - Incoming Class Filter

Priority	Source IP	Destination IP	Service Type Status	DiffServ CodePoint Status	Class
1	<input checked="" type="radio"/>				
2	<input type="radio"/>				
3	<input type="radio"/>				
4	<input type="radio"/>				
5	<input type="radio"/>				
6	<input type="radio"/>				
7	<input type="radio"/>				
8	<input type="radio"/>				
9	<input type="radio"/>				
10	<input type="radio"/>				

1

Priority

You are allowed to set ten filters. The priority for the filter of number 1 is the highest; and the priority for number 10 is the lowest.

Source IP

Display the source IP address for the filter.

Destination IP

Display the destination IP address for the filter.

Service Type Status

Display the service type that you choose for the filter.

DiffServ CodePoint Status

Display the setting for DiffServ CodePoint.

Class

Display the class name that you specified for the incoming/outgoing class filter.

Edit

Click this button to open the edit page for adjusting the settings.

Delete/Delete All

Click this button to delete the selected setting or all settings.

To edit an incoming class filter, please choose one of the radio buttons under **Priority** and click **Edit**. The following page will be shown automatically.

QoS - Incoming Class Filter - Edit

Source IP: /24

Destination IP: /24

Service Type Status: Basic Advanced None

Service Type:

Protocol:

Source Port: -

Destination Port: -

DiffServ CodePoint Status: Basic Advanced None

DiffServ CodePoint Type:

DiffServ CodePoint: 0x (Hex)

Class:

Source IP

Type the source IP address with subnet mask value to be applied for this filter.

Destination IP

Type the destination IP address with subnet mask value to be applied for this filter.

Service Type Status

There are three options for you to choose:
Basic – Only the **Service Type** field is allowed to be configured.
Advanced – The **Protocol** and **Port** fields are allowed to be configured.
None – No field is allowed to be configured.

Service Type

Select the service type that you want to use. There are **thirty-five** service types provided.

- CU-SEEME-IO(TCP/UDP:7648)
- DNS(TCP/UDP:53)
- FINGER(TCP:79)
- FTP(TCP:20,21)**
- H.323(TCP:1720)
- HTTP(TCP:80)
- HTTPS(TCP:443)
- IKE(UDP:500)
- IPSEC-AH(IP:51)
- IPSEC-ESP(IP:50)
- IRC(TCP/UDP:6667)
- L2TP(UDP:1701)
- NEWS(TCP:144)
- NFS(UDP:2049)
- NNTP(TCP:119)
- PING(IP:1)
- POP3(TCP:110)
- PPTP(TCP:1723)
- RCMD(TCP:512)
- REAL-AUDIO(TCP:7070)
- RTSP(TCP/UDP:554)
- SFTP(TCP:115)
- SMTP(TCP:25)
- SNMP(TCP/UDP:161)
- SNMP-TRAPS(TCP/UDP:162)
- SQL-NET(TCP:1521)
- SSH(TCP/UDP:22)
- SYSLOG(UDP:514)
- TELNET(TCP:23)
- TFTP(UDP:69)
- FTP(TCP:20,21)

Protocol

There are three options: **TCP**, **UDP**, and **TCP/UDP**. Choose the one you need.

Source/Destination Port

Type the port range number for source/destination port of this filter.

DiffServ CodePoint Status

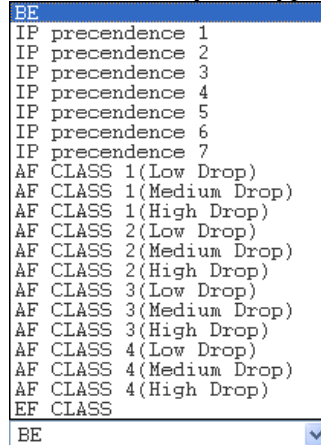
There are three options:
Basic – Only the **DiffServ CodePoint Type** field can be

configured.

Advanced – Only the **DiffServ CodePoint** field can be configured.

None –No field allowed to be configured.

DiffServ CodePoint Type There are twenty-one types supported.

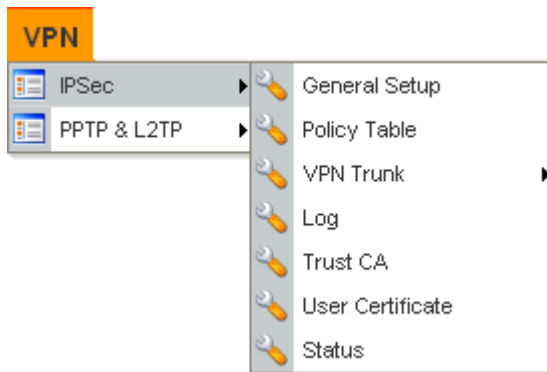


DiffServ CodePoint The number (by hex mode) to be applied.

Class Choose a filtering condition to be applied. All the class names set in **Incoming/Outgoing Class Setup** page will be displayed in this field.

4.6 VPN and Remote Access Setup

This page allows you to setup the configuration of VPN and Remote Access to create a virtual private network for security in the Internet.



A Virtual Private Network (VPN) is an extension of a private network that encompasses links across shared or public networks like the Intranet. A VPN enables you to send data between two hosts across a shared or public network in a manner that emulates the properties of a point-to-point private link.

There are two types of VPN connections: remote dial-in access and LAN-to-LAN connection. The “Remote dial-In Access” facility allows a remote access node, a NAT router or a single computer to dial into a VPN router through the Internet to access the network resources of the remote network. The “LAN-to-LAN Access” facility connects two independent LANs for mutual sharing of network resources. For example, the head office network can access the branch office network, and vice versa.

The VPN technology implemented in the Vigor3300 Series of broadband security routers supports Internet-industry standards to provide customers with interoperable VPN solutions, such as X.509 and DHCP over Internet Protocol Security (IPSec). This VPN feature is only

supported for Vigor3300V routers. IPSec is the security architecture for IP networks. IPSec provides security services at the IP layer by enabling a system to select required security protocols. It determines the algorithms to use for the services, and puts in place any cryptographic keys required to provide the requested services. IPSec can be used to protect one or more "paths" between a pair of hosts, between a pair of security gateways, or between a security gateway and a host.

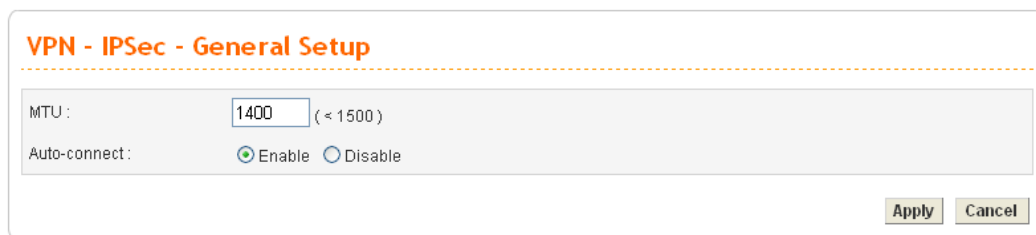
The Vigor3300 Series supports ESP Tunnel mode with IKE for key management. Internet Key Exchange (IKE) Protocol, a key protocol in the IPSec architecture, is a hybrid protocol using part of Oakley and part of SKEME in conjunction with ISAKMP to obtain authenticated keying material for use with ISAKMP, and for other security associations such as AH and ESP for the IPsec DOI.

4.6.1 IPSec

The IPSec services can provide access control, connectionless integrity, data origin authentication, rejection of replayed packets that is a form of partial sequence integrity, and confidentiality by encryption. These objectives are met through the use of two traffic security protocols, the Authentication Header (AH) and the Encapsulating Security Payload (ESP), and through the use of cryptographic key management procedures and protocols.

General Setup

General Setup allows you to set MTU value for VPN. The default number is 1400.



The screenshot shows a configuration window titled "VPN - IPSec - General Setup". It contains two main settings: "MTU:" with a text input field containing "1400" and a note "(< 1500)", and "Auto-connect:" with two radio buttons, "Enable" (which is selected) and "Disable". At the bottom right of the window are "Apply" and "Cancel" buttons.

MTU

The default value is 1400.

Auto-connect

If you click **Enable** for **Auto-connect**, once the packets match the source/destination subnet settings of some VPN rule, that rule will perform auto-connection and make the packets passing through. However, if you click **Disable**, you have to make the VPN connection manually. If the VPN connection is failed, the packets will not be transmitted, either.

Policy Table

To create a VPN IPsec policy, click the **Policy Table** option under the **IPsec** menu.

VPN - IPsec - Policy Table

#	Connection Name	Local Subnet	Remote Gateway	Remote Subnet	Interface	Profile Status	Operational Status	Action
1	<input checked="" type="radio"/> Research	172.16.3.228/32	172.16.2.1	172.16.2.15/32	WAN1	enable	down	Initiate
2	<input type="radio"/>							
3	<input type="radio"/>							
4	<input type="radio"/>							
5	<input type="radio"/>							
6	<input type="radio"/>							
7	<input type="radio"/>							
8	<input type="radio"/>							
9	<input type="radio"/>							
10	<input type="radio"/>							

1

[Refresh](#) [Edit](#) [Delete](#) [Delete All](#)

Refresh

Refresh the page information.

Edit

Configure an entry. Clicking this button can guide you accessing into editing page for that IPsec tunnel. For detailed information, refer to the following section of **For Default Configuration**.

Delete

Delete a designated entry.

Delete All

Delete all entries in the table.

To edit or add a policy table, please click one of the radio buttons and click **Edit**.

- **For Default Configuration**

Click **Default** tab. The following page of default configuration will be shown:

Profile Status

Set the initialization of IPSec Tunnel with this profile settings.

Enable – Choose this one to invoke this profile manually. In addition to select Enable, you have to click Initiate under the page of VPN-IPSec Tunnel-Policy Table.

Always-On – Choose this one to invoke this profile automatically by the system for every 30 seconds.

Disable – Choose this one to inactivate this profile.

Name

The name for VPN connection (ex. “VPN1”). The maximum length of name is 20 characters including spaces.

Authentication

The authentication to be used by PreShared Key or RSA Signature.

PreShared Key

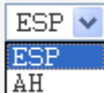
The shared key for peer identification. The maximum length is 40 characters, including spaces.

Security Protocol

AH - Specify the IPSec protocol for the Authentication Header protocol. The data will be authenticated but not be encrypted.

ESP - Specify the IPSec protocol for the Encapsulating Security Payload protocol. The data will be encrypted and

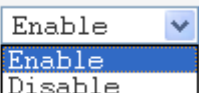
authenticated.

Security Protocol : 

NAT Traversal

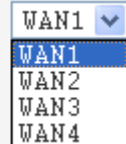
Click **Enable** to let multi IPSec tunnels passing through this router.

Click **Disable** to close this function.

NAT Traversal : 

WAN Interface

The WAN interface to be used.

WAN Interface : 

Netbios Naming Packet

Pass – Click it to have an inquiry for data transmission between the hosts located on both sides of VPN Tunnel while connecting.

Block – When there is conflict occurred between the hosts on both sides of VPN Tunnel in connecting, such function can block data transmission of Netbios Naming Packet inside the tunnel.

Local Certificate

The local certificate is active for authentication if the **RSA Signature** option is selected in the **Authentication** field.

These options come from the user certificate file.

Security Gateway

The IP address of the local gateway's public-network interface. The keyword “default” can be used to represent the IP Address of the selected “WAN Interface”.

Network IP / Subnet Mask

The subnet behind the local gateway.

Next Hop

The IP address of the next hop. The keyword **default** can be used to represent the gateway IP address of the selected **WAN Interface**.

Remote ID

The identification number for the remote gateway.

DHCP-over-IPSEC

Turns this function **ON** or **OFF**.

Security Gateway

The IP address of the remote client/gateway. This field is mandatory. The setting for 0.0.0.0 is used for the road-warrior with a dynamic IP address.

Network IP / Subnet Mask

The subnet behind the remote gateway. If the remote gateway IP address is 0.0.0.0, this field can be omitted, but you can specify it as 0.0.0.0/32 for clarity.

● **For Advanced Configuration**

Click **Advanced** tab. The following page of default configuration will be shown:

VPN - IPSec Tunnel - Edit

Default **Advanced**

IKE Phase1

Mode : Main mode Aggressive mode

Peer ID :

Key Lifetime : minutes

Proposal :

IKE Phase2(quick mode)

Key Lifetime : minutes

Proposal :

PFS (Perfect Forward Secrecy)

Accepted Proposal :

Dead Peer Detection

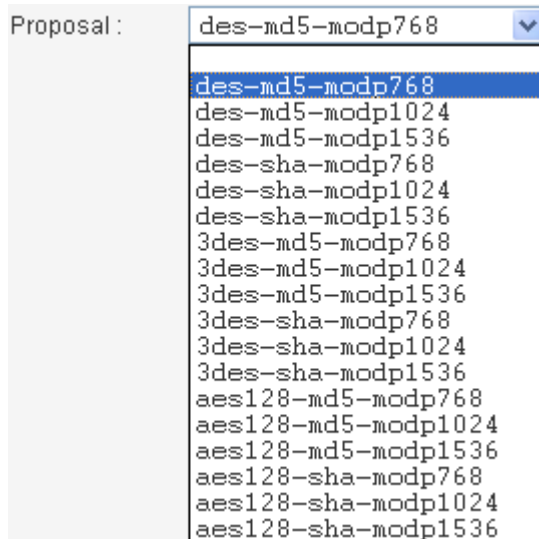
Status : Disable Enable

Delay : seconds

Timeout : seconds

Apply Cancel

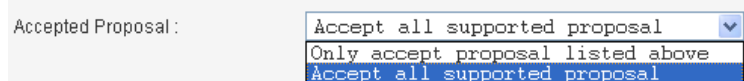
- Mode** Select from **Main** mode and **Aggressive** mode. The ultimate outcome is to exchange security proposals to create a protected secure channel. **Main** mode is more secure than **Aggressive** mode since more exchanges are done in a secure channel to set up the IPSec session. However, the **Aggressive** mode is faster. The default value in Vigor router is Main mode.
- Peer ID** In **Aggressive** mode, Peer ID is on behalf of the IP address while identity authenticating with remote VPN server. The length of the ID is limited to 47 characters.
- Key Lifetime (main)** The rekey-renegotiated period of the IKE Phase1 keying channel of a connection. The acceptable range is from 5 to 480 minutes (8 hours).
- Proposal (main)** The proposed encryption and/or authentication algorithms for IKE Phase1 negotiation. There are several proposals offered in this page with combination of three types of algorithms:
Encryption algorithms - DES/3DES/AES
Authentication algorithms - MD5/SHA1
DH (Diffie-Hellman) Group - MODP768/MODP1024/MODP1536.



Key Lifetime (quick) The rekey-renegotiated period of the IKE Phase2 keying channel. The acceptable range is from 5 to 1440 minutes (24 hours).

Proposal (quick) The proposed encryption and/or authentication algorithms for IKE Phase2 negotiations. There are 2 options.
Encryption algorithms –NULL/DES/3DES/AES.
Authentication algorithms - MD5/SHA1

Accepted Proposal If you choose **Only accept proposal listed above**, only the selected proposal will be accepted and applied by this device. If you choose **Accept all supported proposal**, all the proposals supported by this device will be accepted and applied.



PFS Enables the PFS (Perfect Forward Secrecy) function. A new Diffie-Hellman Key Exchange is included every time an encryption and/or authentication key are computed on PFS.

Status **Enables** or **Disables** the dead peer detection function.

Delay The keep-alive timer. A Hello message will be emitted periodically when a tunnel is idle. Use the value 0 to disable this function. The recommended value is 30 seconds if enabled.

Timeout The timeout timer. The peer will be declared dead once no acknowledge message is received after timeout value. Use the value 0 to disable this function. The recommended value is 120 seconds if enabled.

After finish the configuration, click **Apply** to apply the IPSec policy setting into the policy table.

VPN - IPSec - Policy Table

#	Connection Name	Local Subnet	Remote Gateway	Remote Subnet	Interface	Admin Status	Operational Status	Action
1	<input checked="" type="radio"/> Research	172.16.3.228/32	172.16.2.1	172.16.2.15/32	WAN1	enable	down	Initiate
2	<input type="radio"/>							
3	<input type="radio"/>							
4	<input type="radio"/>							
5	<input type="radio"/>							
6	<input type="radio"/>							
7	<input type="radio"/>							
8	<input type="radio"/>							
9	<input type="radio"/>							
10	<input type="radio"/>							

1

Significant fields will be summarized in the IPSec Table. **Operational Status** reflects the current status of the tunnel. **UP** means the IPSec tunnel has been established. **DOWN** means no tunnel existing, or termination status of the tunnel.

If user expects the local gateway to act as the IKE initiator, i.e., emit the first IKE main mode message, user can click the hyperlink **Initiate** to start the IKE negotiation or set admin status to be always on to automatically restart IKE negotiation. During the negotiation, you can press **Refresh** to show the latest status of all policies.

VPN Trunk - Policy Table

VPN trunk includes two features - VPN backup and VPN load balance.

Features of VPN TRUNK – VPN Backup Mechanism

VPN TRUNK Management is a backup mechanism which can set multiple VPN tunnels as backup tunnel. It can assure the network connection not to be cut off due to network environment blocked by any reason.

- VPN TRUNK-VPN Backup mechanism can judge abnormal situation for the environment of VPN server and correct it to complete the backup of VPN Tunnel in real-time.
- VPN TRUNK-VPN Backup mechanism is compliant with all WAN modes (single/multi)
- The web page is simple to understand and easy to configure
- Fully compliant with VPN Server LAN Sit Single/Multi Network
- Syslog support, please refer to **System >> SysLog** for detailed configuration

Features of VPN TRUNK – VPN Load Balance Mechanism

VPN Load Balance Mechanism can set multiple VPN tunnels for using as traffic load balance tunnel. It can assist users to do effective load sharing for multiple VPN tunnels according to real line bandwidth.

The TCP Session transmitted by using VPN TRUNK-VPN Load Balance mechanism will not be lost due to one of VPN Tunnels disconnected. Users do not need to reconnect with

setting TCP/UDP Service Port again. The VPN Load Balance function can keep the transmission for internal data on tunnel stably.

To create a VPN IPsec policy for VPN Trunk, click the **Policy Table** option under the **IPSec >>VPN Trunk** menu.

VPN - IPsec - VPN Trunk - Policy Table

#	Connection Name	Local GRE IP	Remote Gateway	Remote GRE IP	Interface	Profile Status	Operational Status
1							<input checked="" type="radio"/>
2							<input type="radio"/>
3							<input type="radio"/>
4							<input type="radio"/>
5							<input type="radio"/>
6							<input type="radio"/>
7							<input type="radio"/>
8							<input type="radio"/>
9							<input type="radio"/>
10							<input type="radio"/>

1

Refresh

Refresh the page information.

Edit

Configure an entry. Clicking this button can guide you accessing into editing page for that IPsec tunnel. For detailed information, refer to the following section of **For Default Configuration**.

Delete

Delete a designated entry.

Delete All

Delete all entries in the table.

- **For Default Configuration**

To edit or add a policy, please click one of the radio buttons and click **Edit**. The following page of default configuration will be shown:

Profile Status

Set the initialization of IPSec Tunnel with this profile.

Enable – Choose this one to activate this profile.

Disable – Choose this one to inactivate this profile.

Profile Status :

Name

The name for VPN connection (ex. “VPN1”). The maximum length of name is 20 characters including spaces.

Authentication

The authentication to be used by PreShared Key or RSA Signature.

Authentication :

PreShared Key

The shared key for peer identification. The maximum length is 40 characters, including spaces.

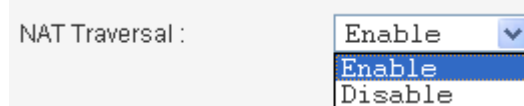
Security Protocol

AH - Specify the IPSec protocol for the Authentication Header protocol. The data will be authenticated but not be encrypted.

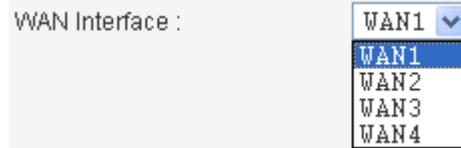
ESP - Specify the IPSec protocol for the Encapsulating Security Payload protocol. The data will be encrypted and authenticated.

Security Protocol :

NAT Traversal Click **Enable** to let this IPSec tunnel pass through next router. Click **Disable** to close this function.

A screenshot of a web interface showing a dropdown menu for 'NAT Traversal :'. The menu is open, showing three options: 'Enable', 'Enable', and 'Disable'. The first 'Enable' option is highlighted in blue.

WAN Interface The WAN interface to be used.

A screenshot of a web interface showing a dropdown menu for 'WAN Interface :'. The menu is open, showing four options: 'WAN1', 'WAN2', 'WAN3', and 'WAN4'. The 'WAN1' option is highlighted in blue.

Local Certificate The local certificate is active for authentication if the **RSA Signature** option is selected in the **Authentication** field. These options come from the user certificate file.

Security Gateway The IP address of the local gateway's public-network interface. The keyword "default" can be used to represent the IP Address of the selected "WAN Interface".

Local GRE IP The virtual IP address of the router, specified for this tunnel.

Next Hop The IP address of the next hop. The keyword **default** can be used to represent the gateway IP address of the selected **WAN Interface**.

Remote ID The identification number for the remote gateway.

Security Gateway The IP address of the remote client/gateway. This field is mandatory. The setting for 0.0.0.0 is used for the road-warrior with a dynamic IP address.

Remote GRE IP The virtual IP address of the remote client, specified for this tunnel.

- **For Advanced Configuration**

Click **Advanced** tab. This page allows you to set advanced configuration for the specified policy. The following page of default configuration will be shown:

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.

Peer ID

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

Key Lifetime (main)

The renegotiated period of the IKE Phase1 keying channel of a connection. The acceptable range is from 5 to 480 minutes (8 hours).

Proposal (main)

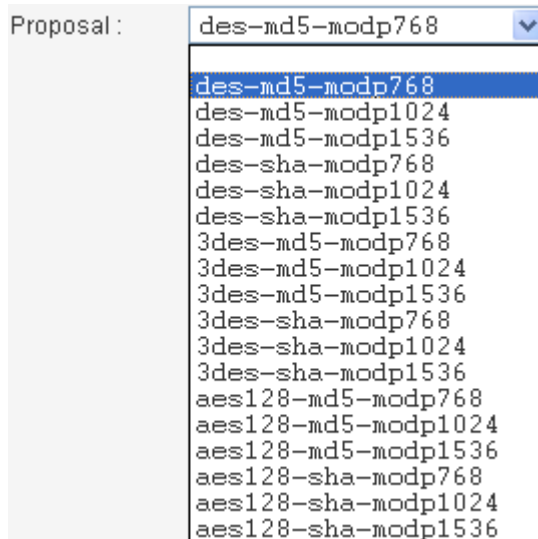
The proposed encryption and/or authentication algorithms for IKE Phase1 negotiation. There are several proposals offered in this page with combination of three types of algorithms:

Encryption algorithms - DES/3DES/AES

Authentication algorithms - MD5/SHA1

DH (Diffie-Hellman) Group -

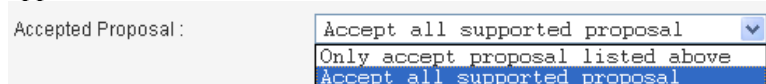
MODP768/MODP1024/MODP1536.



Key Lifetime (quick) The renegotiated period of the IKE Phase2 keying channel. The acceptable range is from 5 to 1440 minutes (24 hours).

Proposal (quick) The proposed encryption and/or authentication algorithms for IKE Phase2 negotiations. There are 2 options.
Encryption algorithms –NULL/DES/3DES/AES.
Authentication algorithms - MD5/SHA1

Accepted Proposal If you choose **Only accept proposal listed above**, only the selected proposal will be accepted and applied by this device. If you choose **Accept all supported proposal**, all the proposals supported by this device will be accepted and applied.



Delay The keep-alive timer. A Hello message will be emitted periodically when a tunnel is idle. Use the value 0 to disable this function. The recommended value is 2 seconds if enabled.

Timeout The timeout timer. The peer will be declared dead once no acknowledge message is received after timeout value. Use the value 0 to disable this function. The recommended value is 4 seconds if enabled.

Auto GRE Key Check this box to automatically generate GRE key. Or, type the GRE key on the fields below manually

GRE Key In This value is used for the router to authenticate the source of the packet. The length is 4 bytes.

GRE Key Out This value is used for the remote client to authenticate the source of the packet. The length is 4 bytes.

After finish the configuration, click **Apply** to apply the IPSec policy setting into the policy table.

Significant fields will be summarized in the IPSec Table. **Operational Status** reflects the current status of the tunnel. **UP** means the IPSec tunnel has been established. **DOWN** means no tunnel existing, or termination status of the tunnel.

If user expects the local gateway to act as the IKE initiator, i.e., emit the first IKE main mode message, user can click the hyperlink **Initiate** to start the IKE negotiation or set admin status to be always on to automatically restart IKE negotiation. During the negotiation, you can press **Refresh** to show the latest status of all policies.

VPN Trunk - Group Table

Vigor3300 series allows users to configure policies. In addition, it also allows users to combine several policies into one group for VPN usage. Each group can combine four policies for fitting different requirement of VPN application.

Simply click **VPN>>VPN Trunk>>Group Table** to access into the following page. There are ten groups offered for users to configure.

VPN - VPN Trunk - Group Table				
#	Profile Status	Name	Local Subnet	Remote Subnet
1	<input checked="" type="radio"/>			
2	<input type="radio"/>			
3	<input type="radio"/>			
4	<input type="radio"/>			
5	<input type="radio"/>			
6	<input type="radio"/>			
7	<input type="radio"/>			
8	<input type="radio"/>			
9	<input type="radio"/>			
10	<input type="radio"/>			
				1
<input type="button" value="Edit"/> <input type="button" value="Delete"/> <input type="button" value="Delete All"/>				

Edit Configure an entry. Clicking this button can guide you accessing into editing page for that group. For detailed information, refer to the following section of **For Default Configuration**.

Delete Delete a designated entry.

Delete All Delete all entries in the table.

To edit or add a group table, please click one of the radio buttons and click **Edit**. The default configuration will be shown as below:

VPN - VPN Trunk - Group Table - Edit

1

Profile Status : Disable Enable

Name :

Local Subnet : /

Remote Subnet : /

Tunnel 1 : Weight :

Tunnel 2 : Weight :

Tunnel 3 : Weight :

Tunnel 4 : Weight :

Backup

Active	Master	Slave
<input type="checkbox"/>	<input type="button" value="v"/>	<input type="button" value="v"/>
<input type="checkbox"/>	<input type="button" value="v"/>	<input type="button" value="v"/>

Profile Status

Set the initialization of IPSec Tunnel with this profile.

Enable – Choose this one to activate this profile.

Disable – Choose this one to inactivate this profile.

Name

Type a name for this group.

Local Subnet

LAN subnet of this device.

Remote Subnet

LAN subnet of the remote client.

Tunnel 1~ Tunnel 4

Specify which tunnel will be included in this trunk. You can choose up to four tunnels at one time.

Weight

Determine how many flow rates can pass through on this tunnel. For example, type 1 for tunnel 1 and type 4 for tunnel 2. If such device has 5 packets needing to send to the remote subnet, it will send 4 packets through tunnel 2 and 1 packet through tunnel 1.

Active

Check this box to enable VPN tunnel backup.

Master/Slave

Choose the master and slave roles for this backup configuration.

After finish the configuration, click **Apply** to apply the group table setting.

Log

At any time, you can click **VPN >>IPSec>> Log** to monitor the VPN tunnel status. The log is helpful for solving some setting problems. The system will keep the 100 most recent messages. Click **Clear** to clear the log.

VPN - IPSec - Log

#	Date/Time	Description
1	04:37:06 12/08	connection {1_Research} is deleted
2	04:36:47 12/08	connection {1_Research} is added

Date/Time	It displays the date and time for the operation of IPSec.
Description	It displays the results of the IPSec operation.
Refresh	It allows you to refresh the whole table.
Clear	It allows you to clear all the table information.

Trust CA

This page allows you to set up the CA configuration. Click the **VPN>>IPSec >>Trust CA** option. It can make users loading double key certificate issued by trusted CA server.

VPN - IPSec - Trust CA

#	Name	Issuer
1	<input checked="" type="radio"/>	
2	<input type="radio"/>	
3	<input type="radio"/>	
4	<input type="radio"/>	
5	<input type="radio"/>	
6	<input type="radio"/>	
7	<input type="radio"/>	
8	<input type="radio"/>	
9	<input type="radio"/>	
10	<input type="radio"/>	

To upload a new Trust CA, please select any one of the entry and click the **Upload** button. The following page will appear.

VPN - IPSec - Trust CA # 1 - Upload

Upload CA Certificate

Upload File

Use the **Browse..** button to locate the file you want to upload, and click **Apply**.

User Certificate

This page allows you to set up the CA configuration to generate user's certificate. Click the **VPN>>IPSec >>User Certificate** option.

VPN - IPsec - User Certificate

#	Status	Name	Issuer
1	<input checked="" type="radio"/> Import OK	3300CA_0804	/C=TW/ST=Hsin-Chu/L=Houko/O=Draytek/OU=RD3/CN=presto/emailAddress=pcho@draytek.com.tw
2	<input type="radio"/> Import OK	3300CA_RD3	/C=TW/ST=Hsin-Chu/L=Houko/O=Draytek/OU=RD3/CN=presto/emailAddress=pcho@draytek.com.tw
3	<input type="radio"/> Import OK	3300CA_attel	/C=TW/ST=Hsin-Chu/L=Houko/O=Draytek/OU=RD3/CN=presto/emailAddress=pcho@draytek.com.tw
4	<input type="radio"/> Empty		
5	<input type="radio"/> Empty		
6	<input type="radio"/> Empty		
7	<input type="radio"/> Empty		
8	<input type="radio"/> Empty		
9	<input type="radio"/> Empty		
10	<input type="radio"/> Empty		

1

- Generate** Generate a new entry for user certification.
- Download** Download a certification file generated from router to be stored in local host.
- Import** Import a certificated file from the local host.
- Delete** Delete an assigned entry.
- View** Show configuration of the assigned entry.

- **To generate a user certificate**, please click one radio button to select the entry and click the **Generate** button.

VPN - IPsec - User Certificate # 2 - Generate

Generate Certificate Signing Request

Certification Name:

ID Type:

ID Value:

User Certificate Information

Organization Unit:

Organization:

Locality(City):

State/Province:

Common Name:

Country:

e-mail:

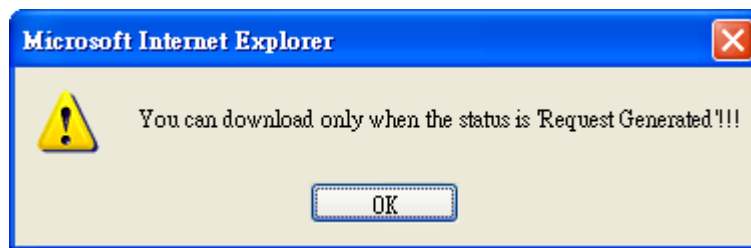
Key Size: Bits

- Certification Name** The name of the certification entry.
- ID Type** The ID type for this entry. There are three types:
Domain Name: Certificated by domain name.
IP: Certificated by IP address.
Email: Certificated by email address.
- ID Value** The ID value for this entry.
- Organization Unit** The unit value of this organization.

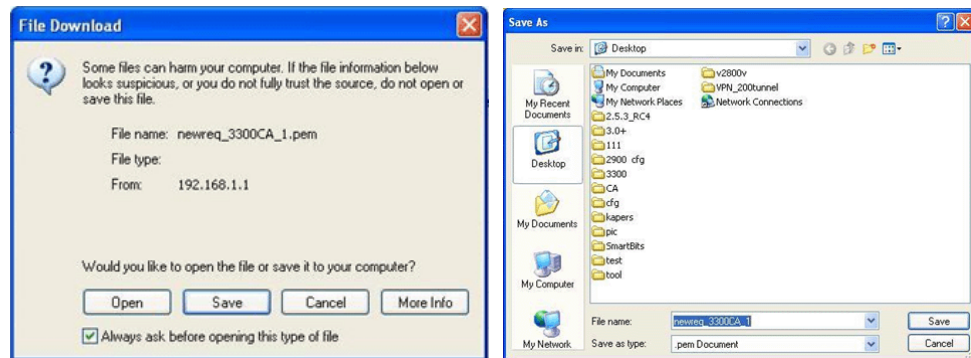
Organization	The value of this organization.
Locality (City)	The local city name of this entry.
State/Province	The state name of this entry.
Common Name	The common name for this entry.
Country	The country name of this entry.
E-mail	The email address of this entry.
Key Size	The key size for this entry. There are 3 options: 1024 Bits, 1536 Bits and 2048 Bits.

When you finish the configuration, please click **Apply** to invoke it.

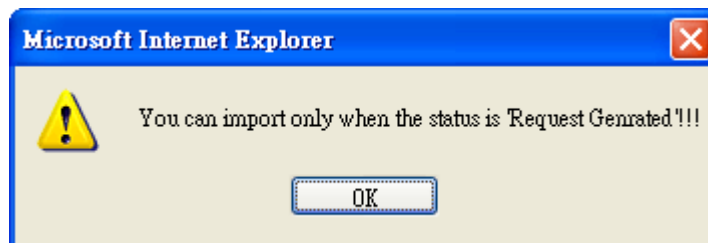
- **To download a user certificate**, please click index number one (with the status of Request Generated) and click the **Download** button. If not, you might see the following dialog to warn you.



After you click the **Download** button, the system will guide you to save the downloaded file (newreq_RD-computer_1.pem) to a place that you assign.



- **To import a user certificate** that you saved previously, please click index number one (with the status of Request Generated) and click the **Import** button. If not, you might see the following dialog to warn you.



After you click the **Import** button, the system will guide you to import a saved file to a place that you want.

VPN - IPSec - User Certificate # 1 - Import

Import User Certificate

Upload File

- **To delete a user certificate**, please click the index number that you want to delete and click the **delete** button. A dialog box will appear to ask your confirmation. Click **OK** to delete it or click **Cancel** to leave the dialog without deletion.



- **To view a user certificate**, please click the index number that you want to view the detailed information of the certificate and click the **View** button. The following page will be shown for your reference.

VPN - IPSec - User Certificate # 1 View

Certificate Detail Information

Certificate Name : 3300CA_0804
 Issuer : /C=TW/ST=Hsin-Chu/L=HouKo/O=Draytek/OU=RD3/CN=presto/emailAddress=pcho@draytek.com.tw
 Subject : /C=TW/ST=HouKo/L=Hsin-Chu/O=RD3/OU=Draytek/CN=3300CA_0804/emailAddress=pcho@draytek.com
 Valid From : Aug 4 11:57:40 2005 GMT
 Valid To : Aug 4 11:57:40 2007 GMT

Status

This page will show the VPN connection status.

VPN - IPSec - Status

#	Name	Status	Algorithm	Remote IP	Remote Subnet	Packet In	Byte In	Packet Out	Byte Out	Uptime
1	2900V	up	DES_0-HMAC_SHA1-NO_PFS	61.230.211.232	192.168.29.0/24	13	716	12	624	29

Name	Display the name of the IPSec tunnel.
Status	Display the status of the tunnel (up or down).
Algorithm	Display the algorithm used by this IPSec.
Remote IP	Display remote IP address of the tunnel.
Remote Subnet	Display remote subnet mask of the tunnel.
Packet In	Display the packets count received by this tunnel.

Byte In	Display the bytes count received by this tunnel.
Packet Out	Display the packets count sent out by this tunnel.
Byte Out	Display the bytes count sent out by this tunnel.
Uptime	Display the time duration since the tunnel is established.
Refresh	Allow you to refresh current VPN status.
Disconnect	Allow you to disconnect the select VPN connection.

4.6.2 PPTP & L2TP

PPTP General Setup

To configure the general setup for PPTP, please click **VPN>> PPTP & L2TP>>General Setup>>PPTP General Setup**.

Status

Set the function to **Active** or **Inactive**.

PPTP Authentication

Allow you to choose an authentication mode to be used. The default setting is **CHAP**.

PPTP Encryption

Allow you to choose an encryption mode to be used. If PPTP authentication mode is set to **CHAP** or **PAP**, PPTP Encryption mode does not need to be set.

User Authentication

Set user authentication to **Local** server or **RADIUS** server.

Enable/Disable

Enables or disables the **Mutual Authentication** function.

User Name Type the user name that the other side provides for carrying out mutual authentication whenever you want.

Password Type the password that the other side provides for carrying out mutual authentication whenever you want.

Get DNS Server from LAN Setting Use DNS setting of LAN configuration.

Get DNS Server by Manual Setting If you click this radio button, please type the primary DNS and secondary DNS IP address manually in the following fields.

Primary DNS Type the IP address for primary DNS.

Secondary DNS Type the IP address for secondary DNS.

When you finish the configuration, please click **Apply** to invoke it.

L2TP General Setup

To configure the general setup for L2TP, please click **VPN>> PPTP & L2TP>>General Setup>>L2TP General Setup**.

VPN - L2TP - General Setup

Status : Active Inactive

L2TP Authentication : CHAP

User Authentication : Local RADIUS Server

Mutual Authentication

Enable Disable

User Name :

Password :

DNS Server

Get DNS Server from LAN Setting Get DNS Server by Manual Setting

primary DNS :

Secondary DNS :

Apply Cancel

Status Set the function to **Active** or **Inactive**.

L2TP Authentication Allow you to choose an authentication mode to be used. The default setting is **CHAP**.

PAP

CHAP

MS-CHAP

MS-CHAP-V2

User Authentication Set user authentication to **Local** server or **RADIUS** server.

Enable/Disable Enable or disable the **Mutual Authentication** function.

User Name Type the user name that the other side provides for carrying out mutual authentication whenever you want.

Password Type the password that the other side provides for carrying out mutual authentication whenever you want.

Get DNS Server from LAN Setting Use DNS setting of LAN configuration.

Get DNS Server by Manual Setting If you click this radio button, please type the primary DNS and secondary DNS IP address manually in the following fields.

Primary DNS Type the IP address for primary DNS.

Secondary DNS Type the IP address for secondary DNS.

Group Table

To create a VPN PPTP/L2TP group table, click **VPN>>PPTP & L2TP>> Group Table**.

VPN - PPTP - Group Table

Group	Start IP	Subnet Mask	Accessed IP	Subnet Mask
A	<input type="text" value="192.168.1.224"/>	<input type="text" value="/28"/>	<input type="text"/>	<input type="text" value="/24"/>
B	<input type="text"/>	<input type="text" value="/24"/>	<input type="text"/>	<input type="text" value="/24"/>
C	<input type="text"/>	<input type="text" value="/24"/>	<input type="text"/>	<input type="text" value="/24"/>
D	<input type="text"/>	<input type="text" value="/24"/>	<input type="text"/>	<input type="text" value="/24"/>

Start IP Type the starting IP address. The default group value is 192.168.1.224/28.

Subnet Mask Select the value of subnet mask for the Start IP.

Accessed IP Type the accessed IP address.

Subnet Mask Select the value of subnet mask for the Accessed IP.

User Profile

This page allows you to set up to 30 sets of accounts.

VPN - User Profile

#	Profile Status	User Name	Group
1	<input checked="" type="radio"/>		
2	<input type="radio"/>		
3	<input type="radio"/>		
4	<input type="radio"/>		
5	<input type="radio"/>		
6	<input type="radio"/>		
7	<input type="radio"/>		
8	<input type="radio"/>		
9	<input type="radio"/>		
10	<input type="radio"/>		

Profile Status Display status (disable or enable) for this entry.

- User Name** The user name for this entry.
- Group** The group for this entry.
- Edit** Allow you to edit the selected group.
- Delete** Allow you to remove the selected group.
- Delete All** Allow you to remove all of the groups.

To add or edit a user profile, click **Edit** for the selected entry.

VPN - User Profile - Edit

1

Profile Status : Disable Enable

User Name :

User Password :

Enable Mobile One-Time Passwords(mOTP)

PIN Code :

Secret :

Group : ▼

- Profile Status** Click **Enable** to invoke such entry.
- User Name** Type the user name for this entry.
- User Password** Type the password for this entry.
- Enable Mobile One-Time Password (mOTP)** Check this box to make the authentication with mOTP function.

mOTP (**Mobile-OTP**) is a free authentication solution for mobile devices like phones, PDAs and so on. It is based on time synchronous of one time password. Such function can authenticate users at routers, firewalls, web servers, access points, and etc.

PIN Code – Type the code for authentication (e.g, 1234).

Secret – Use the 32 digit-secret number generated by mOTP in the mobile phone (e.g., e759bb6f0e94c7ab4fe6).
- Group** Choose a proper group (A, B, C or D that configured in **VPN>>PPTP & L2TP>>Group Table**) for this entry.

When you finish the configuration, please click **Apply** to save and invoke such profile.

Status

This page displays some relevant information about PPTP / L2TP connection. It will refresh automatically every 10 seconds.

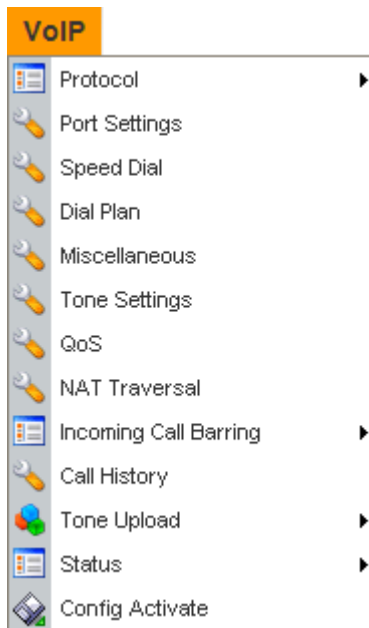
VPN - Status

#	Index	Remote IP	Assigned IP	User	Byte In	Byte Out	Up Time
●	1	61.31.162.252	192.168.1.224	3300	1280	74	11

Index	Display the index number of the tunnel.
Remote IP	Display remote IP address of the tunnel.
Assigned IP	Display IP address assigned by Vigor3300.
User	Display user account of this tunnel.
Byte In	Display the bytes count received by this tunnel.
Byte Out	Display the bytes count sent out by this tunnel.
Uptime	Display the time duration since the tunnel is established.
Refresh	Allow you to refresh current VPN status.
Disconnect	Allow you to disconnect the select VPN connection.

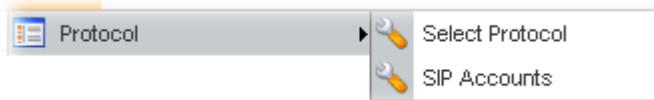
4.7 VoIP Setup

Voice over Internet Protocol (VoIP) is a technology that allows you to make telephone calls using a broadband Internet connection instead of a regular (or analog) phone line.



4.7.1 Protocol

You have to choose suitable protocol and specify SIP accounts for using VoIP.



Select Protocol

There are two protocols can be used for VoIP - SIP and MGCP. You should click either one of buttons to set corresponding settings for VoIP phones. Be aware that both sides (local end and remote end) should use same protocol for VoIP phones.

For SIP Configuration

VoIP - Protocol

Select Protocol : SIP MGCP

SIP Configuration

MGCP Configuration

SIP Local Port :

#	Active	Outbound Proxy	Proxy Name	Proxy Address	Proxy Port	Registrar Addr	Registrar Port	Expires (sec)	Domain
1.	<input type="checkbox"/>	<input type="checkbox"/>	<input style="width: 80px;" type="text"/>	<input style="width: 100px;" type="text" value="0"/>	<input style="width: 50px;" type="text" value="5060"/>	<input style="width: 100px;" type="text" value="0"/>	<input style="width: 50px;" type="text" value="5060"/>	<input style="width: 50px;" type="text" value="300"/>	<input style="width: 50px;" type="text" value="0"/>
2.	<input type="checkbox"/>	<input type="checkbox"/>	<input style="width: 80px;" type="text"/>	<input style="width: 100px;" type="text" value="0"/>	<input style="width: 50px;" type="text" value="5060"/>	<input style="width: 100px;" type="text" value="0"/>	<input style="width: 50px;" type="text" value="5060"/>	<input style="width: 50px;" type="text" value="300"/>	<input style="width: 50px;" type="text" value="0"/>
3.	<input type="checkbox"/>	<input type="checkbox"/>	<input style="width: 80px;" type="text"/>	<input style="width: 100px;" type="text" value="0"/>	<input style="width: 50px;" type="text" value="5060"/>	<input style="width: 100px;" type="text" value="0"/>	<input style="width: 50px;" type="text" value="5060"/>	<input style="width: 50px;" type="text" value="300"/>	<input style="width: 50px;" type="text" value="0"/>
Example			iptel	iptel.org		iptel.org			iptel.org

Proxy User-Agent Name

1.	<input style="width: 150px;" type="text" value="DrayTek V3300V-1.0.0"/>
2.	<input style="width: 150px;" type="text" value="DrayTek V3300V-1.0.0"/>
3.	<input style="width: 150px;" type="text" value="DrayTek V3300V-1.0.0"/>

SIP Local Port

Type the port number for SIP protocol. The default value is 5060.

Active

Click this box to activate this SIP proxy server setting.

Outbound Proxy

Check this box to enable this function for sending SIP protocol packets to an SIP proxy server.

Proxy Name

Type the name of the SIP proxy server.

Proxy Address

Type the IP address of the SIP proxy server.

Proxy Port

Type the port number of the SIP proxy server.

Registrar Address

Type the IP address or domain name of the SIP registrar server.

Registrar Port

Type the port number of the SIP registrar server.

Expires

Type the register expire time for SIP protocols. The default value is 3600.

Domain

Type the IP address or domain name of the SIP Domain/Realm.

User Agent Name

Type the name which will be displayed in SIP message User-Agent parameter. You can set up to 3 sets of SIP configurations in this page.

For MGCP Configuration

VoIP - Protocol

Select Protocol : SIP MGCP

SIP Configuration | **MGCP Configuration**

MGCP Local Port :

MGCP Call Agent Address :

MGCP Call Agent Port :

EndPoint Name Style : aaln/#@[ip_addr] mac_addr/#@[ip_addr] aaln/#@mac_addr

aaln/#@

Logic ID Starting Number :

Wild-carded RSIP : Each endpoint sends its own RSIP Send only one wild RSIP

- MGCP Local Port** The UDP port number in MGCP local terminal.
- MGCP Call Agent Address** The IP address of the Call Agent server in MGCP.
- MGCP Call Agent Port** The UDP port number for the Call Agent server.
- EndPoint Name Style** Choose a proper name style for the VoIP settings. There are three options for you to choose.
- aaln/#@[ip_addr]** - ex: aaln/1@[1.1.1.1]
 - mac_addr/#@[ip_addr]**- ex: 000504030201/1@[1.1.1.1]
 - aaln/#@mac_addr**- ex: aaln/1@000504030201
 - aaln/#@** - ex: aaln/1@v3300.draytek.com
- Logic ID Starting Number** Determine the starting number for the endpoint name. There are eight ports in Vigor3300 series. The default name for endpoint will be “aaln”. If you type “1” in this field, the endpoint name will be “aaln/1, aaln/2...,aaln/8”. If you type “11” in this field, the endpoint name will be “aaln/11, aaln/12...aaln/18”, etc. Simply keep the default value (1).
- Wild-carded RSIP** For VoIP phone call with MGCP configuration, each port will send RSIP to call agent for notifying that port is initiated or restarted.
- Each endpoint sends its own RSIP** – Each port must send one RSIP message (e.g., aaln/1@[172.16.3.5]) to call agent respectively.
 - Send only one wild RSIP** – Only one RSIP message (e.g., aaln/*@[172.16.3.5]) will be sent to call agent to indicate all ports are initiated/restarted.

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 AccountName@Domain/Realm. After that, your call will be bypassed by SIP Proxy to the destination using AccountName@Domain/Realm as identity.

VoIP - SIP Accounts

#	User Name	Display Name	Proxy Server	Ring Port	Ring Type	Call Forwarding
1	<input checked="" type="radio"/> 1001	1001		1	All Ports	
2	<input type="radio"/> 1002	1002		2	All Ports	
3	<input type="radio"/> 1003	1003		3	All Ports	
4	<input type="radio"/> 1004	1004		4	All Ports	
5	<input type="radio"/> 1005	1005		5	All Ports	
6	<input type="radio"/> 1006	1006		6	All Ports	
7	<input type="radio"/> 1007	1007		7	All Ports	
8	<input type="radio"/> 1008	1008		8	All Ports	

1 2 3 4

You can set up to 32 SIP accounts. To edit an existing SIP Accounts, simply choose the radio button for the one you want to modify and click **Edit**.

VoIP - SIP Accounts - Edit

1

Disable Enable

Username:

Password:

Display Name:

Authentication ID:

Proxy Server:

Call without Registration: Disable Enable

VoIP IP Address:

Call Forwarding

Disable

Callforwarding all calls

Callforwarding busy

Callforwarding no answer after rings (Range:1~10)

SIP URL (Example:8001@iptel.org)

Subscribe for MWI

Disable Enable

Expires time:

MWI Inform

Play Special Dial Tone

CLIP

IncomingCall CLIP display:

OutgoingCall CLIP hidden:

Call Park

Call Park Dial Number:

IncomingCall Rings

Rings all ports in the group

Rings the first available port

Rings by round robin Force start form the port: , and ring each port for seconds

Ring Port Setting

P1 P2 P3 P4 P5 P6 P7 P8

Apply **Cancel**

Disable/Enable

Click the radio button to enable or disable the SIP account.

Username

Define the account name or number.

Password

Define the password for this account. You can change it if required.

Display Name

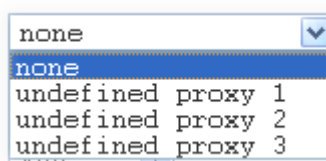
Define the name recognized by the remote end.

Authentication ID

Type the name or number used for SIP Authorization with SIP Registrar.

Proxy Server

Choose the proxy server (pre-configured in **VoIP>>Protocol>>SIP Configuration**) for such account.



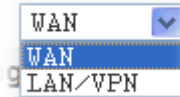
Call without Registration

If you want to make VoIP call without register personal information, please choose **Enable** and check the box to

achieve the goal. Some SIP server allows user to use VoIP function without registering.

VoIP IP Address

The interface is used to apply VoIP traffics. There are two options: **WAN** and **LAN/VPN**. If LAN/VPN is selected, VoIP can be applied through a VPN tunnel to create a high security voice phone.



Call Forwarding

Disable - Disable forwarding function.

Call forwarding all calls - Forward all incoming calls to the specified SIP URL site.

Call forwarding busy - Forward incoming calls to the specified SIP URL site when this line is busy.

Call forwarding no answer after (Range: 1~10) rings- Forward incoming calls to the specified SIP URL site after ringing the times that you set here.

SIP URL - Assign a SIP URL site (e.g., aaa@draytel.org or abc@iptel.org) to receive forwarded calls.

Subscribe for MWI

This function is used to set SIP account for sending a message to the proxy server for subscribing MWI (Message Waiting Indicator). Part proxy server may need such subscription, yet not all of the proxy servers need.

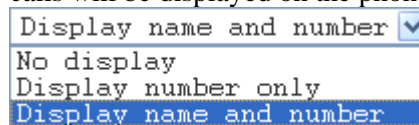
MWI Inform

Play Special Dial Tone – Play congest tone for five seconds while off-hook to inform you MWI message.

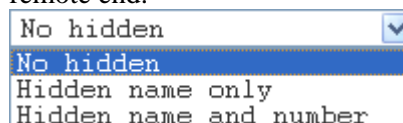
CLIP

Hide the caller ID on the display panel of the phone set.

IncomingCall CLIP display – If you choose **No display**, no name and number of the incoming calls will be displayed. If you choose **Display number only**, just the number of the incoming calls will be displayed. If you choose **Display name and number**, then the name and number of all the incoming calls will be displayed on the phone set.



OutgoingCall CLIP display – If you choose **No hidden**, then the name and number of the outgoing calls will be displayed on remote end. If you choose **Hidden name only**, just the number of the outgoing call will be displayed. If you choose **Hidden name and number**, the name and number of all the outgoing calls will not be displayed on the phone set of remote end.



Call Park

It allows a person to put a call on hold at one telephone set and continue the conversation from any other telephone set.

Such number you type here is determined by your ISP. The default Call Park Dial Number is “700”.

IncomingCall Rings

Rings all ports in the group – Click this radio button to make all ports in the same SIP account ringing while receiving incoming calls.

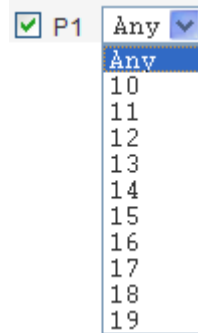
Rings the first available port –Click this radio button to make the first available port in the same SIP account ringing while receiving incoming calls.

Rings by round robin - Click this radio button to make the phone port ringing in sequence within the same SIP account.

Force start from the port – with round robin configuration, you can check this box to force the incoming call ringing from specified port and determine the time for phone ringing.

Ring Port Setting

When someone calls this SIP account, the port (P1- P8) selected here will ring. If someone calls this SIP account via ISDN phone and **Any** is chosen as the ring port setting, all the ISDN phones connected to this port will ring. Yet, if you choose only one MSN number (10, 11, 12, 13, 14, 15, 16, 17, 18,19) for that port, only the phone with the number you selected will ring.



P1 Any ▼









- Any
- 10
- 11
- 12
- 13
- 14
- 15
- 16
- 17
- 18
- 19

4.7.2 Port Settings

Port Settings page allows users to set phone number for different call receivers.

Note: Users might have ISDN module or VoIP Module inserted into Vigor router. Different modules will have different web page configurations. Therefore this page will change slightly based on the modules installed on your router. If there is no ISDN or VoIP module installed, it is not necessary for you to access into this page for configuration.

VoIP - Port Settings

#	Edit	Type	Active	SIP Account	Supplemental Service	Hotline	Mic/Spk Gain	FAX	Codec	DTMF
1		ISDN-NT	V	1 - 1001			0 / 0	Transparent	G.729A	RFC2833
2		ISDN-TE	V	2 - 1002			0 / 0	Transparent	G.729A	RFC2833
3		ISDN-NT	V	3 - 1003			0 / 0	Transparent	G.729A	RFC2833
4		ISDN-TE	V	4 - 1004			0 / 0	Transparent	G.729A	RFC2833
5		FXO	V	5 - 1005			0 / 0	Transparent	G.729A	RFC2833
6		FXO	V	6 - 1006			0 / 0	Transparent	G.729A	RFC2833
7		FXO	V	7 - 1007			0 / 0	Transparent	G.729A	RFC2833
8		FXO	V	8 - 1008			0 / 0	Transparent	G.729A	RFC2833

- Edit** Click this button to access into the Edit page for each phone number.
- Type** Display the type of the VoIP connection, e.g. ISDN-NT, ISDN-TE, FXO and FXS. It depends on the modules you have installed to the router.
- Active** Display the status (active or not) for the VoIP connection.
- SIP Account** Display the SIP account index number and username.
- Supplemental Service** Display the supplemental service mode for the VoIP connection.
- Hotline** Display the hotline is established or not.
- Mic/Spk Gain** Display the microphone gain value and speaker gain value.
- FAX** Display the FAX mode setting (e.g., Transparent) for the VoIP connection.
- Codec** Display the codec settings for the VoIP connection.
- DTMG** Display the DTMF mode setting for the VoIP connection.

- When you click **Edit**, the following page will appear for you to configure. (Such page is available for ISDN module)

VoIP - Port Settings - Port1 - Edit

Port 1 (ISDN-NT)

Disable Enable

Default SIP Accounts: 1-1001

VoIP IP Address: WAN

Hotline

Hotline Number to Internet:

Hotline Number to PBX: (*p':delay 1.8sec)

FXO

Manual Disconnection:

Codec

Preferred Codec: G.729A -8kbps

Single Codec:

Codec Rate: 20 (ms)

Codec VAD: Disable Enable

CAS

Microphone Gain: 0 (Range: -14 ~ 6)

Speaker Gain: 0 (Range: -14 ~ 6)

FAX

FAX Mode: Transparent

FAX Bypass Codec: G.711U (PCMU) -64kbps

FAX Bypass Codec Rate: 20 (ms)

DTMF

DTMF Mode: InBand OutBand(RFC2833) SIP INFO Cisco

DTMF Volume: 27 (Range: 0 ~ 31)

Supplemental Service

Supplemental Service Mode: Disable Normal CHT

Supplemental Service Items: Call Waiting Call Transfer

ISDN Mode

NT TE

ISDN Type

P-MP P-P

MSN numbers

#	MSN Number	Default Account
1.	50	5-1005
2.	51	5-1005
3.	52	5-1005
4.	53	5-1005
5.	54	5-1005
6.	55	5-1005
7.	56	5-1005
8.	57	5-1005
9.	58	5-1005
10.	59	5-1005

Default Call Route

Default call route to: VoIP, Dial ## for route to ISDN-TE port

ISDN-TE port, Dial ## for route to VoIP

Route to Account: 0-none

Port 1

Click **Enable** to activate this port or **Disable** to close this port.
Default SIP Accounts – Use the drop down list to choose one item as the default SIP account.

VoIP IP Address - The interface is used to apply VoIP traffics. There are two options: **WAN** and **LAN/VPN**. If **LAN/VPN** is selected, VoIP can be applied through a VPN tunnel to create a high security voice phone.

Hotline

Hotline Number to Internet - Pre-set a phone number to make the port dialing out to Internet automatically.

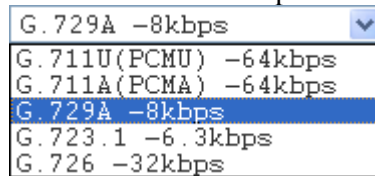
Hotline Number to PBX - Pre-set a phone number to make the port dialing out to PBX automatically.

FXO

Manual Disconnection - Click **Disconnect** to disconnect this phone line manually.

Codec

Preferred Codec - It can be applied on this port. Vigor3300 supports five Codecs. The default setting is G.729A. You can choose another one as preferred Codec for outgoing calls.



Single Codec - If you checked this box, only preferred codec will be used for outgoing and incoming calls. And if the remote end does not support such Codec, the VoIP communication will be failed.

Codec Rate - Type the rate value to be applied on this port.

Codec VAD- Enable or Disable VAD (Voice Activity Detection). It can detect whether the voice activity is progressing or not. If not, RTP packets transmission will be stopped for saving more bandwidth.

CAS

Microphone Gain- The gain value while transmitting voice. The default value is 0. The range is from -32 to 31.

Speaker Gain- The gain value while receiving voice. The default value is 0. The range is from -32 to 31.

FAX

FAX Mode -The FAX function mode. There are several options:

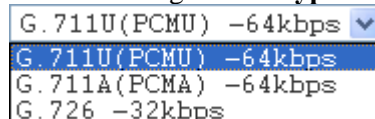
Transparent: FAX will be transmitted via voice channel; no fax relay and no Codec change will be involved. This is the default value.

T.38 Relay: Using T.38 Fax Relay.

Bypass: Once FAX is detected, the Codec will automatically switch to a high bit rate type (G.711a/u or G.726) to make sure FAX can transmit successfully.

If this option is selected, the Vigor3300V+ will apply these two following settings (FAX Bypass Codec and FAX Bypass Codec Rate).

FAX Bypass Codec - Select one option to be applied if FAX mode is configured as **Bypass** mode.



FAX Bypass Codec Rate - Select one option (20 or 40) to be applied if FAX mode is configured as **Bypass** mode. The stability for the faxing result of documents with codec rate 20ms is higher than 40ms. Yet, the bandwidth request for 40ms is less than 20ms.

DTMF

DTMF Mode -

InBand: Choose this one then the Vigor will send the DTMF tone as audio directly when you press the keypad on the phone.

OutBand (RFC2833): 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 Volume – Determine the volume of DTMF voice signal. The more the number is set, the greater the sound is.

Supplemental Service

If you want to use call waiting or call transfer function, you have to enable supplemental service mode by clicking **Normal** or **CHT**.

Click **Disable** to close this service.

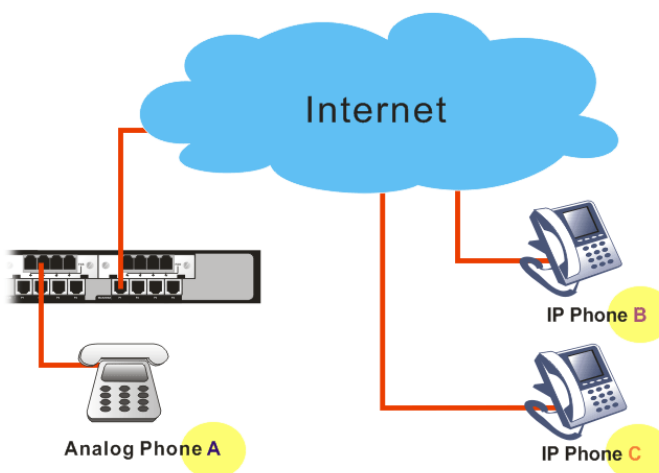
Supplemental Service	
Supplemental Service Mode:	<input checked="" type="radio"/> Disable <input type="radio"/> Normal <input type="radio"/> CHT
Supplemental Service Items:	<input type="checkbox"/> Call Waiting
	<input type="checkbox"/> Call Transfer

Under **Normal** mode, call waiting and call transfer function will be:

Call Waiting -You can hear waiting tone while a new phone call is incoming, then you can do:

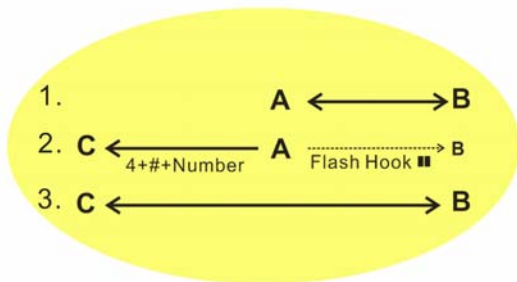
- (1) Flash hook and dial 0: This procedure keeps the current connection and reject the new phone call.
- (2) Flash hook and dial 1: This procedure disconnects the current connection and connect with the new phone call.
- (3) Flash hook and dial 2: This procedure always holds the current connection and connect with the second connection.

Call transfer – Check this box to execute call transfer function.



There are three types of operating procedure used in Call Transfer. Take a look at the diagram above.

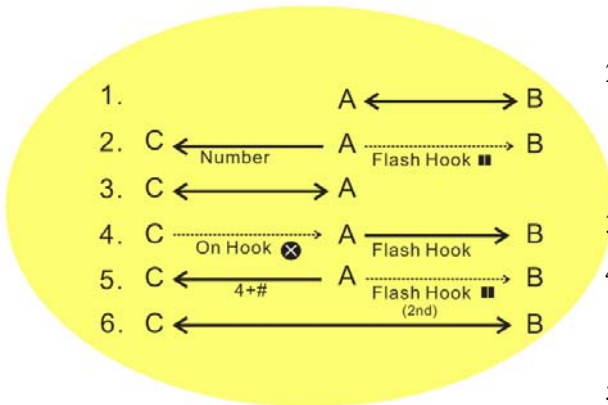
◆ **Unattended mode –**



1. At the first, phone A and phone B talk on the phone.
2. Phone A presses flash hook.
(phone A will play dialtone, yet phone B will hold and wait)
Next, phone A dials "4" and presses "#" immediately
(phone A still plays dial tone)
Phone A dials the phone number of phone C for phone A wants to transfer phone B to Phone C.
3. When phone C picks up the phone, then phone C can talk with phone B.

The call transfer is done now. Phone A plays busy tone.

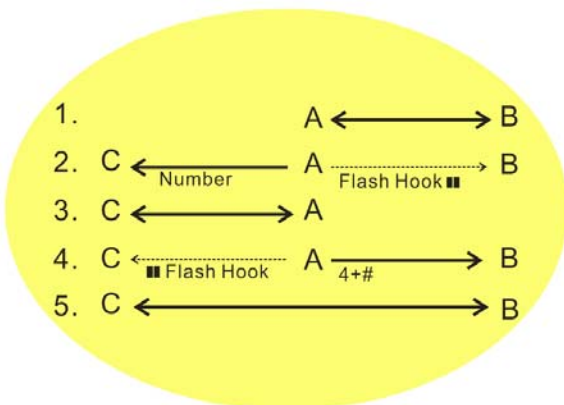
◆ **Attended mode –**



1. At the first, phone A and phone B talk on the phone.
2. Phone A presses flash hook.
(phone A will play dialtone, yet Phone B will hold and wait)
Next, phone A dials the phone number of phone C.
3. Phone C picks up the phone to connect with phone A.
4. Phone C is on-hook to disconnect with phone A.
Phone A presses flash hook to resume the call with Phone B.
5. Phone A presses flash hook again
(phone A will play dialtone, yet phone B will hold)
Phone A dials "4" and press "#" immediately, and then phone A will transfer phone B to C.
6. When phone C picks up the phone, then phone C can talk with phone B.

The call transfer is done now.

◆ **Attended mode –**



1. At the first, phone A and phone B talk on the phone.
2. Phone A presses flash hook
(phone A will play dialtone, yet phone B will hold and wait). Then, phone A dials the phone number of phone C.
3. Phone C picks up the phone to talk with phone A.
4. Phone A presses flash hook
(phone A will play dialtone, yet Phone C will hold).
Phone A dials "4" and press "#" immediately, and then phone A will transfer phone B to C.
5. Phone C will hear waiting tone, and Phone C presses flash hook to talk with phone B.

The call transfer is done now. Phone A plays busy tone.

Under **CHT** mode, call waiting and call transfer function will be:

Call Waiting - You can hear waiting tone while a new phone call is incoming, then you can do:

(1) **Flash hook**: This procedure always holds the current connection and connect with the second connection.

(2) **On hook**: This procedure disconnects the current connection and connects with the new phone call.

Call transfer - Flash hook to initiate another phone call. When the new phone call connected, hang up the phone, and then the other two sides can communicate.

Do Not Disturb	Reject all of the incoming calls to this port. Click Enable to activate this function.
ISDN Mode	Port 1 and Port 3 are fixed in NT mode. Therefore you cannot change it. Port 2 and Port 4 are switchable between NT and TE mode. Port 1 ~ Port 4 are fixed in NT mode if you have installed ISDN All TE module in the router.
ISDN Type	Set the type for Vigor router the same as the one that your ISDN service provider uses. P-MP – Choose this item to specify Point-to-multipoint telecommunications as ISDN type. P-P – Choose this item to specify Point-to-point telecommunications as ISDN type.
MSN numbers	MSN Numbers mean that the router is able to accept only number-matched incoming calls. In addition, local ISDN network provider should support MSN services. The router provides ten fields for MSN numbers. Note that MSN service must be acquired from your local telecom operators. 1-10 fields – Fill in the portion that is different with the own number. If the MSN number of ISDN phone matches with the configured MSN number, the ISDN phone will use default account which matches with MSN number pre-configured. Example: Suppose ISDN phone is connected to Port 5 with MSN number set 51. The router uses the default ten MSN number from 51 – 59. When a user calls out via ISDN phone, the router finds that the MSN number of the ISDN phone matches with the first configured MSN number. Then the router will use the SIP account set for MSN number 51 for calling out.
Default Call Route to	It determines the default direction for the call route of the router. VoIP –The router is set by using VoIP call. To change VoIP call into ISDN call via ISDN TE port, please dial the character in this field for transferring. The character that you can type can be *, #, and 0~9. ISDN – The router is set by using ISDN call via ISDN TE port. To change ISDN call into VoIP call, please dial the character in this field for transferring. The character that you

can type can be *, #, and 0~9.

Route to Account – Choose the number from the drop down list to specify ISDN TE port number.

Apply

When you finish all the configurations, please click this button to activate them.

- When you click **Edit**, the following page will appear for you to configure. (Such page is available for FXO module)

VoIP - Port Settings - Port5 - Edit

Port 5 (FXO)
 Disable Enable
Default SIP Accounts: 5-1005
VoIP IP Address: WAN

Hotline
Hotline Number to Internet:
Hotline Number to PBX: (*p*:delay 1.8sec)

FXO
Manual Disconnection:

Codec
Preferred Codec: G.729A -8kbps
Single Codec:
Codec Rate: 20 (ms)
Codec VAD: Disable Enable

CAS
Microphone Gain: 0 (Range: -14 ~ 6)
Speaker Gain: 0 (Range: -14 ~ 6)

FAX
FAX Mode: Transparent
FAX Bypass Codec: G.711U (PCMU) -64kbps
FAX Bypass Codec Rate: 20 (ms)

DTMF
DTMF Mode: InBand OutBand(RFC2833) SIP INFO Cisco
DTMF Volume: 27 (Range: 0 ~ 31)

PIN Code
 On-Net PIN Service 0000
 Off-Net PIN Service 0000

Do Not Disturb
Do Not Disturb: Disable Enable

Port

Click **Enable** to activate this port or **Disable** to close this port.
Default SIP Accounts – Use the drop down list to choose one item as the default SIP account.

VoIP IP Address - The interface is used to apply VoIP traffics. There are two options: **WAN** and **LAN/VPN**. If **LAN/VPN** is selected, VoIP can be applied through a VPN tunnel to create a high security voice phone.

Hotline

Hotline Number to Internet - Pre-set a phone number to make the port dialing out to Internet automatically.

Hotline Number to PBX - Pre-set a phone number to make the port dialing out to PBX automatically.

FXO

Manual Disconnection - Click **Disconnect** to disconnect this phone line manually.

Codec

Preferred Codec - It can be applied on this port. Vigor3300 supports five Codecs. The default setting is G.729A. You can choose another one as preferred Codec for outgoing calls.

G.729A -8kbps	▼
G.711U(PCMU) -64kbps	
G.711A(PCMA) -64kbps	
G.729A -8kbps	
G.723.1 -6.3kbps	
G.726 -32kbps	

Single Codec - If you checked this box, only preferred codec will be used for outgoing and incoming calls. And if the remote end does not support such Codec, the VoIP communication will be failed.

Codec Rate - Type the rate value to be applied on this port.

Codec VAD- Enable or Disable VAD (Voice Activity Detection). It can detect whether the voice activity is progressing or not. If not, RTP packets transmission will be stopped for saving more bandwidth.

CAS

Microphone Gain- The gain value while transmitting voice. The default value is 0. The range is from -32 to 31.

Speaker Gain- The gain value while receiving voice. The default value is 0. The range is from -32 to 31.

FAX

FAX Mode -The FAX function mode. There are several options:

Transparent: FAX will be transmitted via voice channel; no fax relay and no Codec change will be involved. This is the default value.

T.38 Relay: Using T.38 Fax Relay.

Bypass: Once FAX is detected, the Codec will automatically switch to a high bit rate type (G.711a/u or G.726) to make sure FAX can transmit successfully.

If this option is selected, the Vigor3300 will apply these two following settings (FAX Bypass Codec and FAX Bypass Codec Rate).

FAX Bypass Codec - Select one option to be applied if FAX mode is configured as **Bypass** mode.

G.711U(PCMU) -64kbps	▼
G.711U(PCMU) -64kbps	
G.711A(PCMA) -64kbps	
G.726 -32kbps	

FAX Bypass Codec Rate - Select one option (20 or 40) to be applied if FAX mode is configured as **Bypass** mode. The stability for the faxing result of documents with codec rate 20ms is higher than 40ms. Yet, the bandwidth request for 40ms is less than 20ms.

DTMF

DTMF Mode -

InBand: Choose this one then the Vigor will send the DTMF tone as audio directly when you press the keypad on the phone.

OutBand (RFC2833): 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 Volume – Determine the volume of DTMF voice signal. The more the number is set, the greater the sound is.

PIN Code

On-Net PIN Service - If the phone call is from PSTN to Internet via FXO port, the caller should input 4-digit PIN (Personal identification number) to authenticate the permission.

Off-Net PIN Service - If the call is from Internet to PSTN via FXO port, the caller should input 4-digit PIN (Personal identification number) to authenticate the permission.

Do Not Disturb

Reject all of the incoming calls to this port. Click **Enable** to activate this function.

Apply

When you finish all the configurations, please click this button to activate them.

4.7.3 Speed Dial

This page allows you to set a simple way to dial a specific number. Up to 150 numbers can be stored in Vigor3300V+.

#	Speed Dial Phone Number	Speed Dial Destination	Memo
1	1001	1001@iptel.org	dial 1
2			
3			
4			
5			

Example 101 101@iptel.org

1 2 3 4 5 6 7 8 9 10 >

Apply Cancel Clear This Page

Speed Dial Phone Number Type the phone number to be used as quick dial.

Speed Dial Destination Type the destination address of the dial.

Memo Type a description for the specified number.

Apply Click this button to activate the page settings.

Clear This Page Click this button to remove all the settings in this page.

4.7.4 Dial Plan

Dial Plan defines how V3300V+ handles the outgoing number that the user dials. Usually, it would be tedious to dial a long digits number. Therefore we could establish a dial plan pattern to simplify the dial process. Up to 60 dial plan entries can be stored in Vigor3300V+.

VoIP - Dial Plan

#	Match String	Min Length	Max Length	Prefix Strip	Prefix Add	SIP IP Address	Time Out	Memo
1	<input checked="" type="radio"/>							
2	<input type="radio"/>							
3	<input type="radio"/>							
4	<input type="radio"/>							
5	<input type="radio"/>							
6	<input type="radio"/>							
7	<input type="radio"/>							
8	<input type="radio"/>							
9	<input type="radio"/>							
10	<input type="radio"/>							

- Match String** Display the pattern of a dial plan entry.
- Min Length** Display the minimum length of digits.
- Max Length** Display the maximum length of digits.
- Prefix Strip** Display the number of prefix digits to strip of the entry.
- Prefix Add** Display the prefix string to be added of the entry.
- SIP IP Address** Display the IP address of the destination of the entry
- Time Out** Display the inter-digits timeout value of the entry.
- Memo** Description for this entry.

Click **Edit** to modify the dial plan. Below shows an example.

VoIP - Dial Plan - Edit

1

Match String :

Min Length:

Max Length :

Prefix Strip :

Prefix Add :

SIP IP Address :

Inter Digit TimeOut :

Memo :

- Match String** Set the pattern of a dialplan entry. It is composed by digits (0-9, *, #) and special symbols, which includes dot, brackets, hyphen, letter "X", and letter "T". The letter "X" means any digit. The dot symbol means repeat of the previous symbol.

The brackets and hyphen are used for a range of digits. The letter "T" means waiting for timeout value while matches this pattern.

Matched string, ex: 9011x.T, maximum 63 characters.

Min Length	Set the minimum length of digits, range: 0~63, default:0.
Max Length	Set the Maximum length of digits, range: 0~63, default:32.
Prefix Strip	Set the number of prefix digits to strip, range: 0~63. For example, if you set "1" here, Vigor3300V+ will delete the first digit of the phone number. If you set a number in Prefix Add, Vigor3300V+ will use that one instead.
Prefix Add	Set the Prefix string to be added, -1: none, maximum 63 char. For example, if you set "886" here, Vigor3300V+ will delete the digit of the phone number (based on the setting on Prefix Strip) and use "886" instead.
SIP IP Address	Set the Remote SIP IP address or domain name. Type "0" for non specific address.
Inter Digit TimeOut	Override the inter-digits timeout, range: 1~60(sec), default: 4 (sec). Even if you are in a daze while dialing a phone call, Vigor3300V+ will send it out automatically according to the Inter Digit TimeOut setting.
Memo	Type a description for this entry.

When the caller dials “02111199999”, Vigor3300V+ find the first digit is "0". This number is matched the setting in Match String: 0x.T. Next, Vigor3300V+ will delete the first digit number “0” and add “886” instead. At last, the new number “8862111199999@draytek.com” will be dialed out. From the above figure, we know the Max Length is set with “10”. Therefore, if the caller dials “035972727” (only 9 digits), he must dial “#” immediately or wait for 4 seconds to send the call out. Vigor3300V+ will change the number with “88635972727”, yet the caller still dials “035972727”. In addition, when the caller dials “035” and is in a daze more than 4 seconds, the phone number will be called out and be changed with “88635@draytek.com” directly by Vigor3300V+.

Example:

VoIP - Dial Plan

#	Match String	Min Length	Max Length	Prefix Strip	Prefix Add	SIP IP Address	Time Out	Memo
1	0T	1	32	0	-1	172.16.1.13	8	entry#1
2	00T	1	32	0	-1	172.16.1.13	8	entry#2
3	[1-7]xxx	1	32	0	-1	172.16.1.13	8	entry#3
4	8xxxxxxx	1	32	0	-1	172.16.1.13	8	entry#4
5	#xxxxxxx	1	32	0	-1	172.16.1.13	10	entry#5
6	*xx	1	32	0	-1	172.16.1.13	8	entry#6
7	9011x.T	4	15	0	-1	172.16.1.13	8	entry#7
8								
9								
10								

1

4.7.5 Miscellaneous

This page includes **RTP** and **T.38 Starting Port**, **T.38 Redundancy Number**, **VoIP ToS**, and **FAX Ringing** settings.

VoIP - Miscellaneous

RTP Starting Port:

T.38 Starting Port:

T.38 Redundancy number: (Range: 0~4)

Dialing Completion Timeout: sec (Range: 1~60)

VoIP ToS:

Line Polarity Reversal: as Callee on-hook as Callee Answer

FXO auto disconnection if no packet is received in seconds.(Range:5~3600, 0:no auto disconnection)

FXS On-hook Tip/Ring Voltage:

Dummy Account:

FXS Ringing

Ringing Frequency: (HZ)

Ringing Cadence - On: (msec)

Ringing Cadence - Off: (msec)

RTP Starting Port

The starting port number for RTP protocol packet. The default setting is 13456.

T.38 Starting Port	The starting port number for T.38 protocol packet. The default setting is 49170.
T.38 Redundancy Number	The redundancy number (how many payloads attaching to the tail of the packet) for T.38 protocol. The default value is 1.
Dialing Completion Timeout	Users might dial with incomplete phone number and wait for several seconds but not finish the complete dialing. The system will force to dial the incomplete number after the time you set in this field to finish that call. For example, the phone number is 03654321 and the dialing completion timeout is set to 4 (secs). The user dials with 036 and stops to dial. After passing through 4 seconds, the router will send out that phone call automatically.
VoIP ToS	The ToS value in VoIP protocol packet. The default setting is 0xa0.
Line Polarity Reversal	<p>as Callee Answer - Check this box to generate line polarity reversal while the remote user picks up the phone call.</p> <p>as Callee on-hook - Check this box to generate line polarity reversal while the remote user hangs up the phone call.</p>
FXO auto disconnection if no packet is received in X minutes	Determine the time length for the FXO disconnecting automatically when there is no packet received.
FXS On-hook Tip/Ring Voltage	Determine the voltage of FXS port (on hook). Choose Low to save the power.
Dummy Account	If a user wants to dial out a VoIP call with the SIP account not registered on the router, the system will remember such account information and deem it as a dummy account. Later, it will be dialed out via PSTN line and FXO port.
Ringling Frequency	Please select a proper setting as the ringling frequency.
Ringling Cadence - On	Determine the length of the ringling time for incoming calls.
Ringling Cadence - Off	Determine the length for the incoming calls to stop ringling.

4.7.6 Tone Settings

This 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 - Tone Settings

Region: Caller ID Type:

Tone Classification	Low Frequency(Hz)	High Frequency(Hz)	TON1 (10msec)	Toff1 (10msec)	TON2 (10msec)	Toff2 (10msec)
Dial tone	<input type="text" value="350"/>	<input type="text" value="440"/>	<input type="text" value="500"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>
Ringing tone	<input type="text" value="440"/>	<input type="text" value="480"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="200"/>	<input type="text" value="400"/>
Busy tone	<input type="text" value="480"/>	<input type="text" value="620"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="50"/>	<input type="text" value="50"/>
Congestion tone	<input type="text" value="480"/>	<input type="text" value="620"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="25"/>	<input type="text" value="25"/>

Tone Timer

Dial Tone : Busy Tone : Howler Tone : Ringing Tone :

Special Dial Tone : Call Waiting Tone : Congestion Tone : Reorder Tone :

Region

Choose the country area that the Vigor3300 located for using VoIP feature. Or, select **User Defined** for proprietary settings.

- User Defined
- Australia
- Canada, US
- China
- Denmark
- Finland
- France
- Germany
- Hong Kong
- Japan
- Netherlands
- Norway
- Poland
- Singapore
- Taiwan
- UK**

Caller ID Type

If **User Defined** is selected in the **Region** field, users can select one of the supported values. If a country is selected, this field will display ID type value automatically.

- North America
- JAPAN
- ETSI(during ring)
- ETSI DT-AS(prior to ring)
- ETSI LR+DT-AS(U.K. BT)**
- DTMF

Dial tone

A tone means the phone line is ready to make a call.

Ringing tone

A tone means the call is ringing.

Busy tone

A tone means the phone line is busy.

Congestion tone

A tone means the network is busy.

Low Frequency (Hz)

Type the low frequency number in Hertz.

High Frequency (Hz)

Type the high frequency number in Hertz.

TON1 (10msec)

Type the duration of the first ring.

Toff1 (10msec)

Type the silence duration after the first ring.

TOn2 (10msec)	Type the duration of the next continuous ring.
TOff2 (10msec)	Type the silence duration after the next continuous ring.
Tone Timer	Determine the timeout for the tone invoked.

4.7.7 QoS

This Quality of Service (QoS) function is only for the VoIP feature. When this function is enabled, the Vigor 3300 Series will set rate limitation for incoming and outgoing transmissions to ensure the best quality of service in VoIP.

VoIP - QoS

Disable (non-guaranteed voice quality, higher data throughput)

Enable (guaranteed voice quality, normal data throughput)

Advanced QoS

Link Fragmentation and Interleaving: (For uplink bandwidth < 768 kbps)

Apply Cancel

Disable Click this button to disable QoS function. The voice quality cannot be guaranteed and the data throughput will be higher.

Enable Click this button to invoke QoS function. The voice quality can be good and the data throughput will be lower.

Link Fragmentation and Interleaving Each packet size is determined by the bandwidth of WAN interface. The smaller the bandwidth is, the smaller the packet will be. Such activity can reduce the time delay of packet transmitting. Meanwhile, the VoIP packets will be inserted in the front of queue of signal for transmitting quickly and obtaining best audio quality. Please check this box to invoke this function (shrinking the packet for fast sending).

4.7.8 NAT Traversal

NAT traversal is a challenge that all Service Providers looking to deliver public IP-based voice and multimedia services must solve. The goal of this function is to provide secure connection to subscribers behind NAT (Network Address Translation) devices and Firewalls. Overcoming this traversal problem will lead to widespread deployment of profitable voice and multimedia over IP services to any subscriber with broadband connection.

VoIP - NAT Traversal

NAT Traversal

Disable

Manually Input NAT IP Address

Auto Discover NAT IP Address

NAT IP Address :

Semi-auto, need to config NAT

Full-auto, no need to config NAT (only for SIP)

STUN Local Port :

STUN Server Address :

STUN Server Port :

Symmetric Media

Disable symmetric RTP and T.38

Enable symmetric RTP and T.38

NAT Status

NAT Type: N/A, Local IP Address: 172.16.3.229, WAN IP Address: 172.16.3.229

Apply Cancel

Disable

Disables this function. The feature is used if Vigor3300 has a public WAN IP address and not behind a NAT router.

Manually Input NAT IP Address

NAT IP Address - Type the IP address to be used as the NAT IP address. The feature is used when Vigor 3300V is behind a NAT router, and the NAT router uses a static WAN IP address. This value is the same as the WAN IP of the front NAT router.

Auto Discovery NAT IP Address

It is used when Vigor3300 is behind a NAT router, and the NAT router uses a dynamic WAN IP address such as a DHCP or PPPoE client. The Vigor3300 requires a STUN server for this option.

The “STUN” (Simple Traversal of UDP through NATs) server is an implementation of the STUN protocol that enables STUN functionality in SIP-based systems. It is an application-layer protocol that can determine the public IP and nature of a NAT device sitting between the STUN client and STUN server.

Semi-auto, need to config NAT – If you click this function; the user needs to configure NAT information.

Full-auto, no need to config NAT (only for SIP)- If you click this function; the user does not configure NAT information.

STUN Local Port - Type the port number of the STUN server.

STUN Server Address - Type the IP address of the STUN server.

STUN Server Port - Type the port number of the STUN server.

Symmetric Media

Disable symmetric RTP and T.38 – Click this button to make RTP and T.38 being not symmetrical.

Enable symmetric RTP and T.38 - Click this button to make RTP and T.38 being symmetrical. When Vigor3300 detects the IP address of the receiving packets differing with the address informed by remote end, Vigor3300 will change the IP address automatically according to the real IP address of the packets to ensure the remote receiver can get the packets.

4.7.9 Incoming Call Barring

This feature is used to bar incoming VoIP calls from the Internet. Barring classes can be specified to allow or deny incoming calls. There are five barring classes on the device. The default setting is **Allow all incoming calls**.

Set

This page allows you to choose a barring class, match method and set a range for speed dial entries for the incoming call barring.

VoIP - Incoming Call Barring - Set

Barring Class
Deny only calls from deny list

Match Method

Name: Disable Enable Remind:

IP/Domain: Disable Enable Remind:

Speed Dial Entries
From: 1 To: 150

Apply Cancel

Barring Class

There are five options for incoming calls from remote ends. Choose either one of them to set the barring class.

Deny only calls from deny list

Allow all incoming calls

Allow only calls from allow list

Allow only calls from speed dial entries

Deny only calls from deny list

Deny all incoming calls

Allow all incoming calls – All incoming calls from remote ends are accepted by this router.

Allow only calls from allow list – Only the calls listed in the Allow List page will be accepted by this router.

Allow only calls from speed dial entries – Only the calls listed in the speed dial entries will be accepted by this router.

Deny only calls from deny list – The calls listed on Deny List page will not be accepted by this router. And others calls are accepted.

Deny all incoming calls – All incoming calls from remote ends are not accepted by this router.

Match Method

Name - Enable or Disable this function to take value of Speed Dial Phone Number to be checked.

IP/Domain - Enable or Disable this function to take the value of **Speed Dial Destination** to be checked.

Speed Dial Entries

Type the range to be checked. The default value is from 1 to 150.

Allow List

The Vigor3300 Series supports up to **30** entries in the Allow List table. When you choose **Allow only calls from allow list** as the Barring Class, only the people listed in this list can call this router.

#	Name	IP/Domain
1	Tom	192.168.1.6
2	John	iptel.org
3		
4		
5		
Example	John	192.168.1.1 or iptel.org

Name

The name or number in the allow list.

IP/Domain

The IP address or domain name to be allowed. If the peer is registered in SIP proxy server, use the domain name of the SIP proxy server. Otherwise, use the static IP address or DDNS domain name.

Deny List

The Vigor3300 Series supports up to **30** entries in the Deny List table. When you choose **Deny only calls from deny list** as the Barring Class, people listed in this list **cannot** call this router.

#	Name	IP/Domain
1	James	172.16.3.221
2	Steven	arctel.com
3		
4		
5		
Example	John	192.168.1.1 or iptel.org

Name

The name or number in the deny list.

IP/Domain

The IP address or domain name to be denied. If the peer is registered in SIP proxy server, use the domain name of the SIP proxy server. Otherwise, use the static IP address or DDNS domain name.

4.7.10 Call History

This page lists the call history through Vigor3300. You can click **Refresh** to get the latest history information for these VoIP phones. Besides, this page refreshes automatically every 10 seconds.

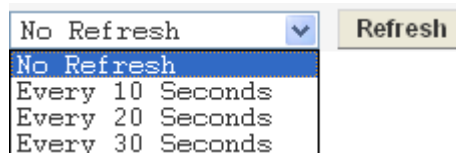
VoIP - Call History

Refresh Option: Every 10 Seconds Refresh

#	Port Number	Call Type	Caller Number	Callee Number	Start Time	End Time	Duration	Release Reason	Remote RTP Address	Remote RTP Port	RTP Statistic	Codec Type	Packet Period	VAD	DTMF Relay
* PS: Packets Sent, OS: Octets Sent, PR: Packets Received, OR: Octets Received, PL: Packets Lost, JI: Interarrival Jitter Estimate (ms), LA: Avg TX Delay(ms)															
1	5	Incoming	888846	888845	Fri Sep 23 17:01:51 2005	Fri Sep 23 17:02:00 2005	0 days, 00h:00m:09s	Normal Drop	61.230.213.114	13466	PS=275, OS=5500, PR=143, OR=2860, PL=0, JI=0, LA=0	G.729A 8kbps	20ms	Off	RFC2833
2	6	Outgoing	888846	888845	Fri Sep 23 17:01:47 2005	Fri Sep 23 17:02:00 2005	0 days, 00h:00m:13s	Normal Drop	61.230.213.114	13464	PS=143, OS=2860, PR=144, OR=2880, PL=0, JI=0, LA=0	G.729A 8kbps	20ms	Off	RFC2833
* PS: Packets Sent, OS: Octets Sent, PR: Packets Received, OR: Octets Received, PL: Packets Lost, JI: Interarrival Jitter Estimate(ms), LA: Avg TX Delay(ms)															

Refresh Option

You can click **Refresh** to get the latest status information for these VoIP phones. In addition, you can set the time interval of refreshing. Use the drop down list of **Refresh Option** to choose an automatic refreshing setting. If you choose **No Refresh**, the system will not refresh this page until you click **Refresh** button.



Port Number

The port number of VoIP.

Call Type

The dialing direction for this call (Incoming/Outgoing).

Caller Number

The phone number of the caller.

Callee Number

The phone number of the receiver.

Start Time

The starting time of the call.

End Time

The ending time of the call.

Duration

The duration of the call.

Release Reason

The reason for the call termination.

Remote RTP Address

The IP address of remote voice site.

Remote RTP Port

The used port number of remote voice site.

RTP Statistic

The statistic of RTP with abbreviation will be shown in this field (e.g., PS: Packets Sent; OS: Octets Sent; PR: Packets

Received; OR: Octets Received; PL: Packets Lost; JI: Interarrival Jitter Estimate (ms); LA: Average TX Delay(ms)).

Codec Type	The Codec mode used for this phone calling.
Packet Period	The period of time for sampling on voice signal.
VAD	The status of VAD.
DTMF Relay	The status of DTMF.

4.7.11 Tone Upload

This page allows you to upload tone settings such as G.711a Pin Prompt, G.711a Pin Error, G.729 Pin Prompt and G.729 Pin Error to Vigor3300 series. Click **Browse..** to choose the file and click **Apply** to upload it.

The figure displays four sequential screenshots of a web-based configuration interface for uploading VoIP tones. Each screenshot is contained within a rounded rectangular frame and features a dashed orange line at the top. The first screenshot is titled 'VoIP - G.711 Tone Upload' and shows the 'G.711a Pin Prompt' configuration. The second screenshot is titled 'VoIP - G.711 Tone Upload' and shows the 'G.711a Pin Error' configuration. The third screenshot is titled 'VoIP - G.729 Tone Upload' and shows the 'G.729 Pin Prompt' configuration. The fourth screenshot is titled 'VoIP - G.729 Tone Upload' and shows the 'G.729 Pin Erro' configuration. In each screenshot, there is a text input field followed by a 'Browse...' button, and 'Apply' and 'Cancel' buttons are located in the bottom right corner.

When a user wants to dial out via FXO port, a sound would be played to ask the user typing PIN code first. If the PIN code is correct, the user can dial out. If not, prompt sound of PIN Error would be played.

4.7.12 Status

Port Status

This page displays the connection status for VoIP phone calls.

VoIP - Status

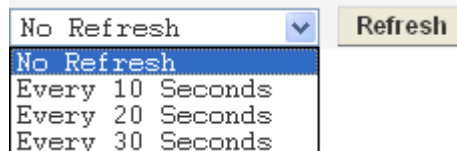
Refresh Option:

#	Call Status	Call Type	Caller Number	Callee Number	Start Time	Remote RTP Address	Remote RTP Port	RTP Statistic	Codec Type	Packet Period	VAD	DTMF Relay
1-1	Idle											
2-1	Idle											
3-1	Idle											
4-1	Idle											
5-1	Idle											
5-2	Idle											
6-1	Idle											
6-2	Idle											
7-1	Idle											
7-2	Idle											
8-1	Idle											
8-2	Idle											

* PS: Packets Sent, OS: Octets Sent, PR: Packets Received, OR: Octets Received, PL: Packets Lost, JI: Interarrival Jitter Estimate(ms), LA: Avg TX Delay(ms)

Refresh Option

You can click **Refresh** to get the latest status information for these VoIP phones. In addition, you can set the time interval of refreshing. Use the drop down list of **Refresh Option** to choose an automatic refreshing setting. If you choose **No Refresh**, the system will not refresh this page until you click **Refresh** button.



Call Status

The calling status.

Call Type

The dialing direction for this call (Incoming/Outgoing).

Caller Number

The phone number of the caller.

Callee Number

The phone number of the receiver.

Start Time

The starting time of the call.

Remote RTP Address

The IP address of the remote voice site.

Remote RTP Port

The used port number of the remote voice site.

Codec Type

The Codec mode used for this phone call.

Packet Period

The period of time for sampling on voice signal.

VAD

The status of VAD.

DTMF Relay

The status of DTMF.

SIP Status

This page displays the registration status for SIP accounts.

VoIP -SIP Status

Refresh Option:

#	Register Status	#	Register Status	#	Register Status	#	Register Status
1		9		17		25	
2		10		18		26	
3		11		19		27	
4		12		20		28	
5		13		21		29	
6		14		22		30	
7		15		23		31	
8		16		24		32	

Refresh Option

You can click **Refresh** to get the latest status information for these VoIP phones. In addition, you can set the time interval of refreshing. Use the drop down list of **Refresh Option** to choose an automatic refreshing setting. If you choose **No Refresh**, the system will not refresh this page until you click **Refresh** button.

No Refresh
Every 10 Seconds
Every 20 Seconds
Every 30 Seconds

Register Status

The status of registering in proxy server.

4.7.13 Config Activate

After configuring VoIP settings, please open **VoIP>>Config Activate** to access into the following page. Then, click **Apply** to activate VoIP configuration.

VoIP - Configure Activate

Warning !
The action may cause all of the VoIP calls disconnected !
Please confirm you really want to execute Configure Activate right now !

Chapter 5: Trouble Shooting

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

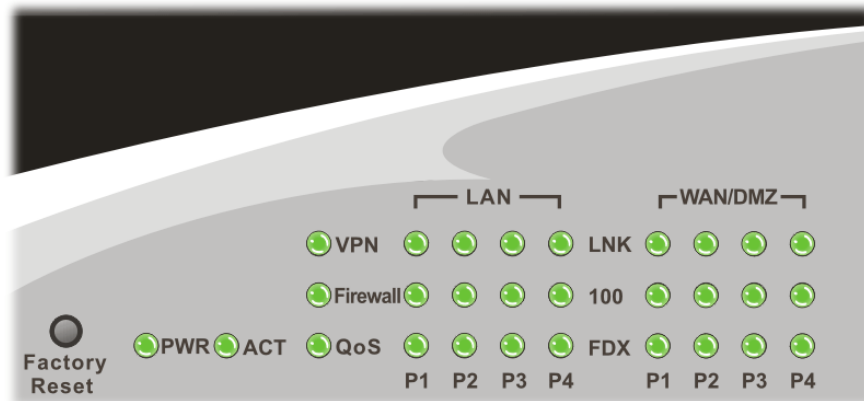
- Checking if the hardware status is OK or not.
- Checking if the network connection settings on your computer are OK or not.
- Pinging the router from your computer.
- Checking if the ISP settings are OK or not.
- Backing to factory default setting if necessary.

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

5.1 Checking If the Hardware Status Is OK or Not

Follow the steps below to verify the hardware status.

1. Check the power line and WLAN/LAN cable connections.
Refer to “**1.3 Hardware Installation**” for details.
2. Turn on the router. Make sure the **ACT LED** blink once per second and the correspondent **LAN LED** is bright.



3. If not, it means that there is something wrong with the hardware status. Simply back to “**1.3 Hardware Installation**” to execute the hardware installation again. And then, try again.

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

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

For Windows

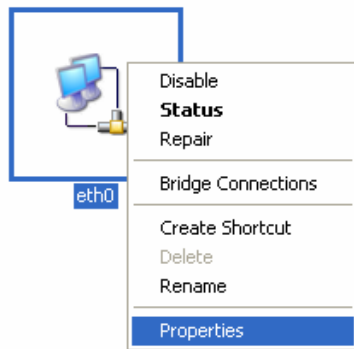


The example is based on Windows XP. As to the examples for other operation systems, please refer to the similar steps or find support notes in www.draytek.com.

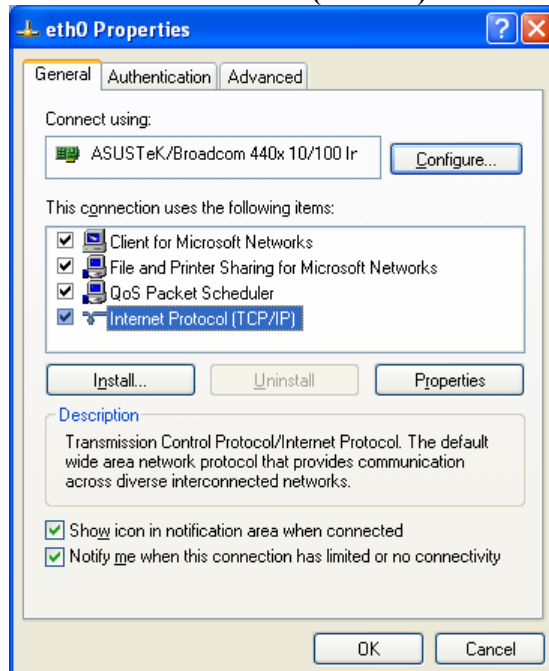
1. Go to **Control Panel** and then double-click on **Network Connections**.



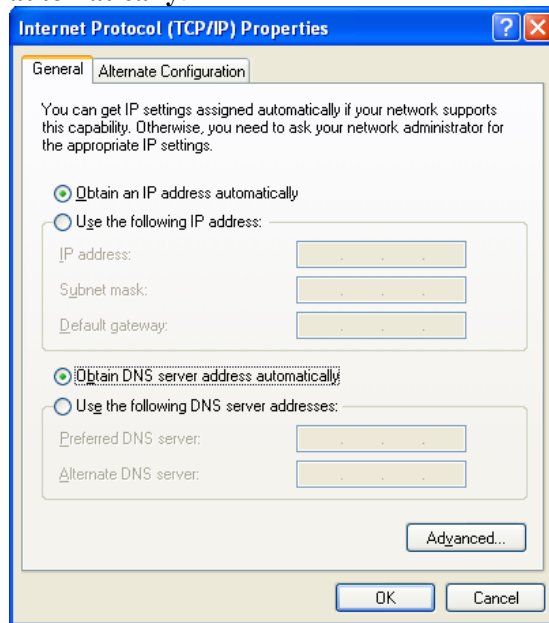
2. Right-click on **Local Area Connection** and click on **Properties**.



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

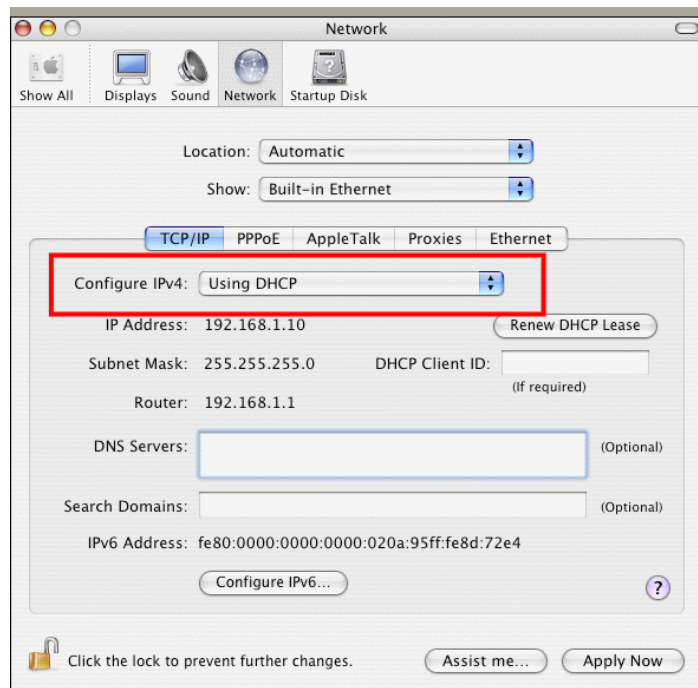


4. Select **Obtain an IP address automatically** and **Obtain DNS server address automatically**.



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.



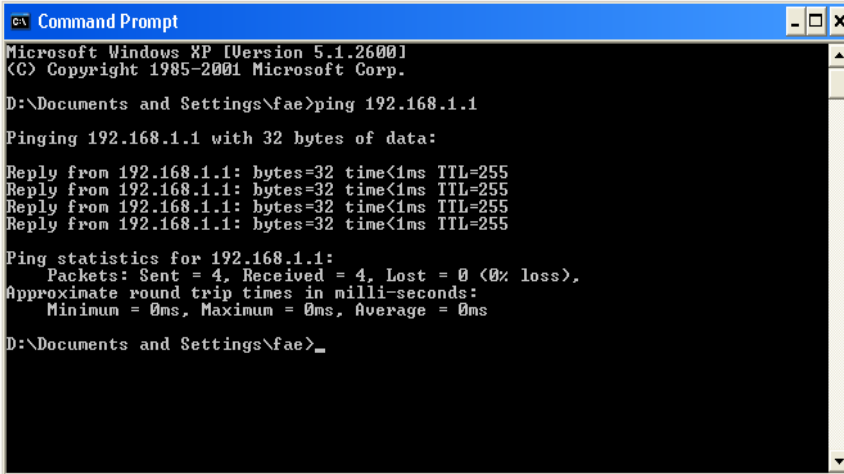
5.3 Pinging the Router from Your Computer

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

Please follow the steps below to ping the router correctly.

For Windows

1. Open the **Command Prompt** window (from **Start menu> Run**).
2. Type **command** (for Windows 95/98/ME) or **cmd** (for Windows NT/ 2000/XP/Vista). The DOS command dialog will appear.



```
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

D:\Documents and Settings\fae>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:

Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

D:\Documents and Settings\fae>_
```

3. Type **ping 192.168.1.1** and press [Enter]. If the link is OK, the line of **“Reply from 192.168.1.1:bytes=32 time<1ms TTL=255”** will appear.
4. If the line does not appear, please check the IP address setting of your computer.

For MacOs (Terminal)

1. Double click on the current used MacOs on the desktop.
2. Open the **Application** folder and get into **Utilities**.
3. Double click **Terminal**. The Terminal window will appear.
4. Type **ping 192.168.1.1** and press [Enter]. If the link is OK, the line of **“64 bytes from 192.168.1.1: icmp_seq=0 ttl=255 time=xxxx ms”** will appear.

```

Terminal — bash — 80x24
Last login: Sat Jan  3 02:24:18 on ttys1
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
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

1. Go to the web configuration GUI (<http://192.168.1.1>), click **Network >> WAN** to check your ISP settings for IP modes.
2. Make sure the **Active** check box has been selected.

Network - WAN

Load Balance : Disable Enable (Auto Weight)

Backup : Disable Enable

#	Edit	IP Mode	Active	Defau
WAN1		PPPoE	<input checked="" type="checkbox"/>	<input checked="" type="radio"/>
WAN2		Not Set	<input type="checkbox"/>	<input type="radio"/>
WAN3		Not Set	<input type="checkbox"/>	<input type="radio"/>
WAN4		Not Set	<input type="checkbox"/>	<input type="radio"/>

3. Click the **Edit** icon to open the WAN setting page. There are four IP modes, Static, DHCP, PPPoE and PPTP provided by the router. Each mode will guide different web page.

For PPPoE Mode

1. Check if **Username** and **Password** are entered with correct values that you **got from** your **ISP**.
2. Check if the setting of **Authentication** is correct or not. You may need to try both **PAP** and **CHAP**.

3. Check if **Service Name** (optional) is correct or not. It is required by some ISPs.

Static/DHCP Configuration	PPPoE/PPTP Configuration	DMZ Configuration	
User Name : <input type="text" value="1234@hinet.net"/>			
Password : <input type="password" value="••••"/>			
Authentication : <input type="text" value="PAP"/>			
Service Name : <input type="text"/>			
PPPoE IP Alias : <input checked="" type="checkbox"/> Enable			
MTU : <input type="text" value="1442"/>			
IP Address Assignment Method (IPCP)			
Fixed IP : <input checked="" type="radio"/> No (Dynamic IP) <input type="radio"/> Yes			
Fixed IP Address : <input type="text"/>			
Connection Detection			
Detect Interval : <input type="text" value="10"/>			
No-Reply Count : <input type="text" value="2"/>			
IP Alias List			
1.	<input type="text" value="10.1.1.100"/>	2.	<input type="text" value="10.1.1.101"/>
3.	<input type="text" value="10.1.1.102"/>	4.	<input type="text"/>
5.	<input type="text"/>	6.	<input type="text"/>
7.	<input type="text"/>	8.	<input type="text"/>
9-32			
			<input type="button" value="Apply"/> <input type="button" value="Reset"/> <input type="button" value="Cancel"/>

After finishing the settings, go to **System - Status** page and click **WAN Status**. You will get a correct web page of WAN settings.

Basic Status	LAN Status	WAN Status
WAN1 :		
IP Address :		218.168.228.27
MAC Address :		00:50:7f:28:80:e6
Primary DNS :		168.95.1.1
Secondary DNS :		
Gateway :		61.230.192.254
RX Packets :		95
TX Packets :		40
Connection Status :		connected
Up Time :		0 days 0 hours 4 minutes 45 seconds
<input type="button" value="Disconnect"/>		

For Static Mode

1. Check if the values of **IP Address**, **Subnet Mask**, **Gateway IP Address** and **Primary DNS** that you got from ISP are set properly or not. If you forget, please contact with ISP for getting new ones.

Static/DHCP Configuration	PPPoE/PPTP Configuration	DMZ Configuration
IP Address :	<input type="text" value="172.16.3.229"/>	Host Name : <input type="text"/>
Subnet Mask :	<input type="text" value="255.255.255.0"/>	Domain Name : <input type="text"/>
Default Gateway :	<input type="text" value="172.16.3.1"/>	(Host Name and Domain Name are required for some ISPs.)
Primary DNS :	<input type="text" value="168.95.1.1"/>	
Secondary DNS :	<input type="text" value="168.95.192.1"/>	

2. If anything wrong, please retype correct values and try the network connection again.
3. After finishing the settings, go to **System - Status** page and click **WAN Status**. You will get a correct web page of WAN settings.

Basic Status	LAN Status	WAN Status
WAN1 :		
IP Address :	220.130.52.221	
MAC Address :	00:50:7f:28:80:e4	
Primary DNS :	168.95.1.1	
Secondary DNS :		
Gateway :	220.130.52.209	
RX Packets :	708	
TX Packets :	384	
Connection Status :	connected	
Up Time :	0 days 0 hours 5 minutes 7 seconds	

For DHCP Mode

1. Check if **Host Name** (optional) and **Domain Name** (optional) are correct or not. Both them are required for some ISPs.

Static/DHCP Configuration	PPPoE/PPTP Configuration	DMZ Configuration
IP Address :	<input type="text" value="172.16.3.229"/>	Host Name : <input type="text"/>
Subnet Mask :	<input type="text" value="255.255.255.0"/>	Domain Name : <input type="text"/>
Default Gateway :	<input type="text" value="172.16.3.1"/>	(Host Name and Domain Name are required for some ISPs.)
Primary DNS :	<input type="text"/>	
Secondary DNS :	<input type="text"/>	

2. If anything wrong, please check and retype correct values. Then try the network connection again.
3. After finishing the settings, go to **System >> Status** page and click **WAN Status**. You will get a correct web page of WAN settings.

Basic Status	LAN Status	WAN Status
WAN1 :		
IP Address :	172.16.100.10	
MAC Address :	00:50:7f:28:80:e5	
Primary DNS :	172.16.100.1	
Secondary DNS :		
Gateway :	172.16.100.1	
RX Packets :	96	
TX Packets :	100	
Connection Status :	connected	
Up Time :	0 days 0 hours 4 minutes 51 seconds	

For PPTP Mode

1. Check if the settings of **Username** and **Password** are correct or not.
2. Check if the setting of **Authentication** is correct or not. You may need to try both **PAP** and **CHAP**.
3. Check if the value of **PPTP Local Address**, **PPTP Subnet Mask**, and **PPTP Remote Address** are correct or not.

Static/DHCP Configuration	PPPoE/PPTP Configuration	DMZ Configuration
User Name :	<input type="text" value="draytek"/>	
Password :	<input type="password" value="•••••"/>	
Authentication :	<input type="button" value="PAP"/> ▾	
Service Name :	<input type="text"/>	
		<input type="text" value="PPTP Local Address : 10.0.0.150"/> <input type="text" value="PPTP Subnet Mask : 255.255.255.0"/> <input type="text" value="PPTP Server Address : 10.0.0.137"/>

4. After finishing the settings, go to **System - Status** page and click **WAN Status**. You will get a correct web page of WAN settings.

Basic Status	LAN Status	WAN Status
WAN1 :		
IP Address :	61.230.208.202	
MAC Address :	00:50:7f:28:80:e7	
Primary DNS :	194.109.6.66	
Secondary DNS :	194.98.0.1	
Gateway :	61.230.208.245	
RX Packets :	341	
TX Packets :	86	
Connection Status :	connected	
Up Time :	0 days 0 hours 4 minutes 39 seconds	
	<input type="button" value="Disconnect"/>	

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 lose all settings you did before. Make sure you have recorded all useful settings before you pressing. The password of the factory default is null.

Software Reset

You can reset router to factory default via Web page.

Go to **System >> Reboot** on the web page. The following screen will appear. Choose **Reset to factory default** and click **Apply**. After few seconds, the router will return all the settings to the factory settings.

System - Reboot

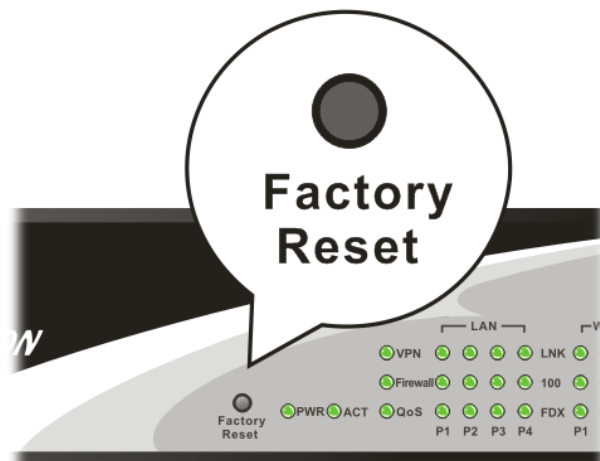
System rebooting will take 20 seconds

Reset to factory default

Apply

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.

This page is left blank.

Appendix: Hardware Specifications

Temperature	Operating : 0°C ~ 45°C
	Storage : -25°C ~ 65°C
Humidity	10% ~ 90% (non-condensing)
Max. Power Consumption	60 Watt
Dimension	L440 * W280 * H44 (mm)
Power	100 ~ 240 V AC