



Vigor 3300 Series
Broadband VoIP/Security/Load Balance Router
User's Guide

Version: 2.1

Date: 2006/08/02

Copyright Information

Copyright

Copyright 2006 All rights reserved. This publication contains information that is protected by copyright. No part may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language without written permission from the copyright holders. The scope of delivery and other details are subject to change without prior notice.

Declarations

Trademarks

The following trademarks are used in this document:

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

Table of Contents

1

Preface	1
1.1 LED Indicators and Connection	2
1.1.1 LED Indicators and Connectors for Vigor3300V	2
1.1.2 LED Indicators and Connectors for Vigor3300	4
1.1.3 LED Indicators and Connectors for Vigor3300B+	6
1.2 Hardware Installation	8
1.2.1 Detailed Explanation for the Connector	9

2

Configuring Basic Settings	11
2.1 Changing Password	11
2.2 Quick Setup	13
2.2.1 Adjusting WAN Connection Mode	13
2.2.2 Static Mode	15
2.2.3 DHCP Mode	17
2.2.4 PPPoE	18
2.2.5 PPTP	20

3

Advanced Configuration	22
3.1 System setup	22
3.1.1 Status	22
3.1.2 Time	26
3.1.3 Syslog	27
3.1.4 Access Control	28
3.1.5 Configuration Setup	29
3.1.6 Firmware Upgrade Setup	30
3.1.7 Reboot	33
3.1.8 Diagnostic Tools	34
3.2 Network Setup	37
3.2.1 WAN and Internet Access Setup	37
3.2.2 LAN	44
3.2.3 Load Balance Policy	47
3.2.4 High Availability	48
3.2.5 Static DHCP	50
3.3 Advanced Setup	51
3.3.1 Static Route Setup	52
3.3.2 NAT Setup	54
3.3.3 RADIUS Setup	60
3.3.4 Port Block	62
3.3.5 DDNS Setup	62
3.3.6 Call Schedule Setup	65
3.3.7 WAN Port Mirroring Setup	67

3.3.8 LAN Port Mirroring Setup.....	68
3.3.9 LAN VLAN Setup.....	68
3.3.10 SNMP.....	71
3.4 Firewall Setup	76
3.4.1 IP Filter.....	76
3.4.2 DoS	81
3.4.3 URL Filter.....	83
3.5 Quality of Service Setup.....	88
3.5.1 Incoming/Outgoing Class Setup	90
3.5.2 Incoming/Outgoing Class Filter	90
3.6 VPN and Remote Access Setup	93
3.6.1 IPSec	94
3.6.2 PPTP.....	104
3.7 VoIP Setup	107
3.7.1 Protocol.....	107
3.7.2 Port Settings	110
3.7.3 Speed Dial	114
3.7.4 Advanced Speed Dial	115
3.7.5 Miscellaneous.....	116
3.7.6 Tone Settings.....	117
3.7.7 QoS.....	119
3.7.8 NAT Traversal.....	120
3.7.9 Incoming Call Barring	121
3.7.10 Call History	123
3.7.11 Status.....	124

4

Trouble Shooting 127

4.1 Checking If the Hardware Status Is OK or Not.....	127
4.2 Checking If the Network Connection Settings on Your Computer Is OK or Not	128
4.3 Pinging the Router from Your Computer	131
4.4 Checking If the ISP Settings Are OK or Not.....	132
4.5 Backing to Factory Default Setting If Necessary	135
4.6 Contacting Your Dealer	136

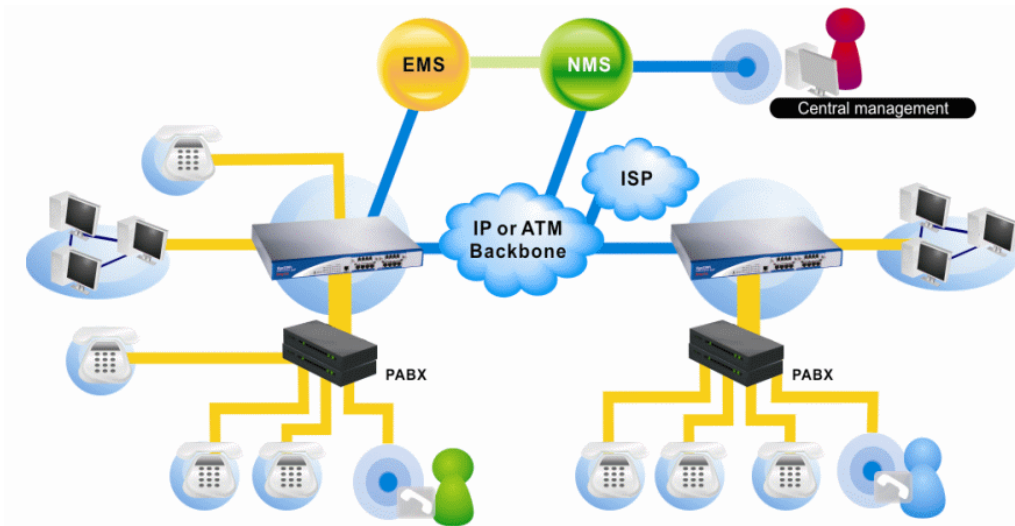
Appendix A Application for 802.1 VLAN 137

A.1 Block LAN-to-LAN Communication	137
A.2 How to Check/Edit VLAN ID on Your PC?.....	138
A.3 Applications.....	145
A.3.1 Four VLANs for Different Departments in A Company	145
A.3.2 Two VLANs for Different Departments in A Company	147
A.3.3 Example for the Companies in the Same Building.....	149
A.3.4 Example for A Company and Guest.....	151
A.3.5 Example for Trunk Usage.....	153

1

Preface

The Vigor3300 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 Figure 1-1, 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. Also, 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).

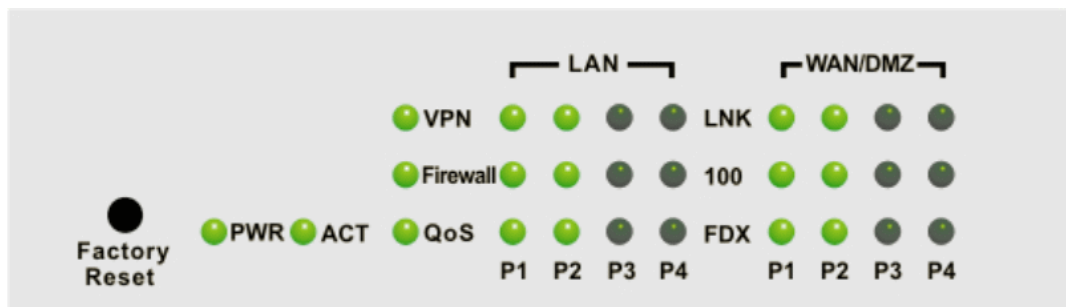
Internet Telephony, also known as Voice over Internet Protocol (VoIP), is a technology that allows you to make telephone calls using a broadband Internet connection instead of a regular (analog) phone line. Combining a PABX with a V3300V allows you to call anyone who has an Internet phone or a traditional 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 LED Indicators and Connection

The Vigor3300V has 4 WAN interfaces and Vigor3300/3300B+ has 3 WAN interfaces that support load balancing. This allows the system to reach peak performance and reduces the cost of maintaining a single high-speed trunk by sharing the load amongst the multiple WAN interfaces. Each interface can be connected to an individual Internet Service Provider. The Vigor3300 Series also supports a backup function for WAN interfaces— a user can select one WAN interface to be a backup interface. If the master interface fails, the backup interface will take the place of the master interface immediately. Lastly, the Vigor3300V has a DMZ function can be applied to any LAN or WAN interface.

1.1.1 LED Indicators and Connectors for Vigor3300V

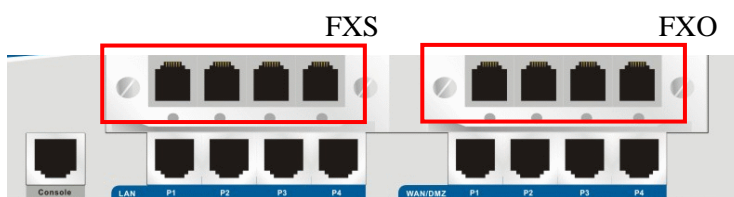


Factory Reset:

Used to restore the default settings. Turn on the router (**ACT** LED is blinking). Press the hole and hold 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.

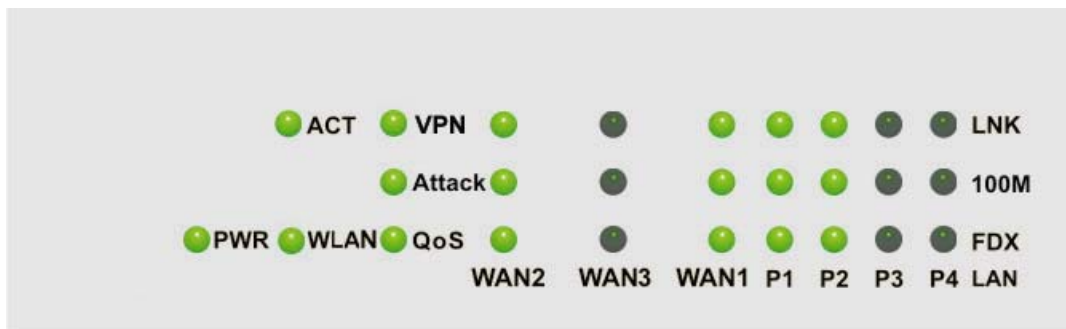
LED	Status	Explanation
PWR	On	The router is powered on.
	Off	The router is powered off.
ACT	On/Blinking	The system is active.
	Off	The system is hanged.
VPN	On	The VPN tunnel is launched.
	Off	The VPN tunnel is closed.
Firewall	On	The Firewall function is active.
	Off	The Firewall function is inactive.
QoS	On	The QoS function is active.
	Off	The QoS function is inactive.

LED	Status	Explanation	
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.



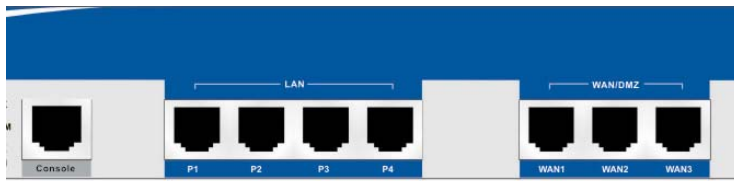
Interface	Description
Console	Provided for technician use.
LAN (P1 ~ P4)	Connector for local networked devices.
WAN/DMZ (P1 ~ P4)	Connector for remote networked devices.
FXS	Connector for telephone set.
FXO	Connector for FXS interface of PABX.

1.1.2 LED Indicators and Connectors for Vigor3300



LED	Status	Explanation	
PWR	On	The router is powered on.	
	Off	The router is powered off.	
ACT	On/Blinking	The system is active.	
	Off	The system is hanged.	
WLAN	No	Reserved for future use.	
VPN	On	The VPN tunnel is launched.	
	Off	The VPN tunnel is closed.	
Attack	On	The Attack function is active.	
	Off	The Attack function is inactive.	
QoS	On	The QoS function is active.	
	Off	The QoS function is inactive.	
WAN (2, 3, 1)	LNK	On	The Ethernet link is established on corresponding port.
		Off	No Ethernet link is established.
	100M	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.
LAN (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.

LED	Status	Explanation	
	100M	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.



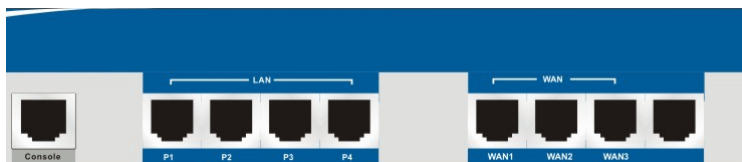
Interface	Description
Console	Provided for technician use.
LAN (P1 ~ P4)	Connector for local networked devices.
WAN/DMZ (WAN1 ~ WAN3)	Connector for remote networked devices.

1.1.3 LED Indicators and Connectors for Vigor3300B+



LED	Status	Explanation	
PWR	On	The router is powered on.	
	Off	The router is powered off.	
ACT	On/Blinking	The system is active.	
	Off	The system is hanged.	
Attack	On	The Attack function is active.	
	Off	The Attack function is inactive.	
QoS	On	The QoS function is active.	
	Off	The QoS function is inactive.	
WAN (2, 3, 1)	LNK	On	The Ethernet link is established on corresponding port.
		Off	No Ethernet link is established.
	100M	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.
LAN (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.
	100M	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.

LED	Status	Explanation
	FDX	On It means a full duplex connection on corresponding port.
		Off It means a half duplex connection on corresponding port.



Interface	Description
Console	Provided for technician use.
LAN (P1 ~ P4)	Connector for local networked devices.
WAN1 ~ WAN3	Connector for remote networked devices.

Connector Specification

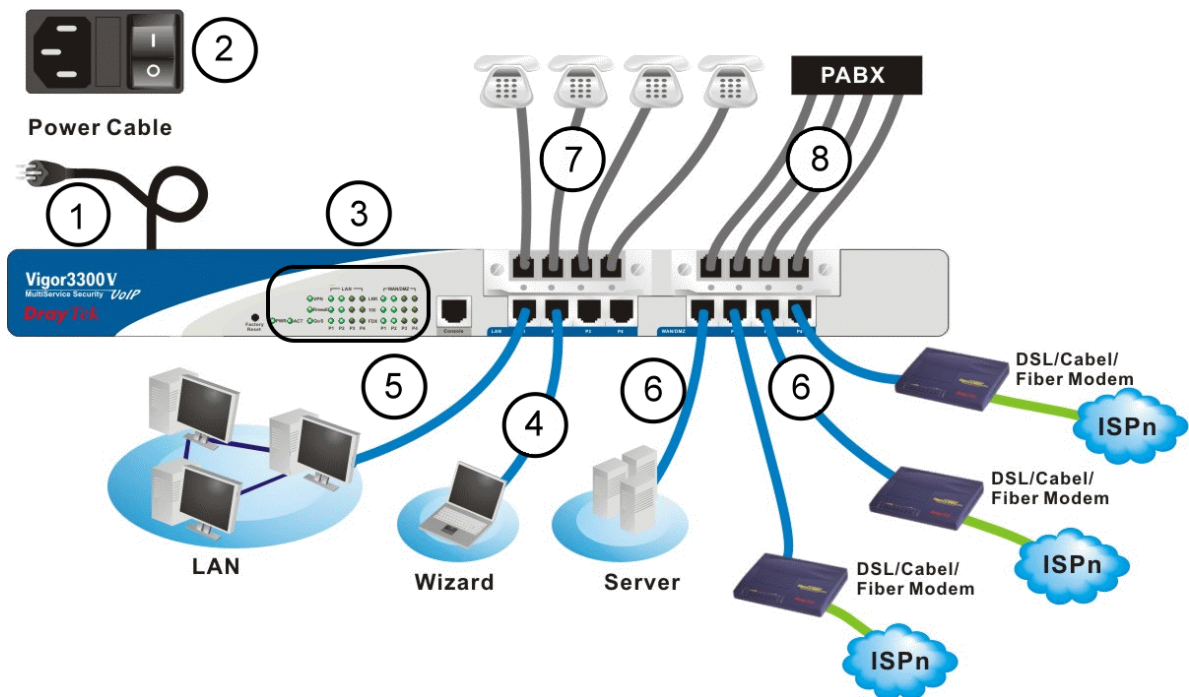
Auxiliary Cables	Type, Color	Connected to	Remarks
Power Cord	Black	AC Outlet	90-264VAC
Serial (Console)	RS232, Grey	PC RS232 port	--
Ethernet (LAN)	RJ-45, Blue	Ethernet switch or hub	--
Ethernet (DMZ)	RJ-45, Blue	Server	
Ethernet (WAN1)	RJ-45, Blue	DSL/Cable/Fiber Modem	--
Ethernet (WAN2)	RJ-45, Blue	DSL/Cable/Fiber Modem	
Ethernet (WAN3)	RJ-45, Blue	DSL/Cable/Fiber Modem	
Ethernet (WAN4)	RJ-45, Blue	DSL/Cable/Fiber Modem	

1.2 Hardware Installation

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

1. Connect the power cord to the power port of Vigor3300 router on the rear panel, and the other side into a wall outlet.
2. Power on the device by pressing 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 available WAN port of the device with Ethernet cable (RJ-45). The **WAN** LED will light up.
7. Connect telephone sets to the **FXS** ports of Vigor3300V with telephone lines (RJ-11 to RJ-11). For the users of Vigor3300 and Vigor3300B+, please skip this step.
8. Connect the **FXO** ports to PABX with telephone lines (RJ-11 to RJ-11). For the users of Vigor3300 and Vigor3300B+, please skip this step.

Below shows an outline of the hardware installation for your reference (take Vigor3300V as an example).



1.2.1 Detailed Explanation for the Connector

Here provides you detailed explanation for some specific connectors that you have to be familiar.

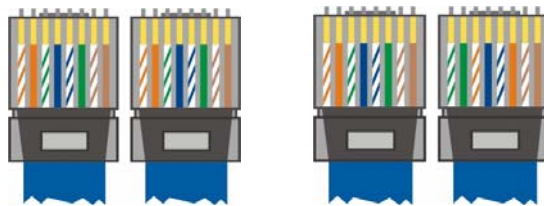
The RS232 Connector

The RJ45 connection jet is used for CLI commands for system configuration and control functions in the Vigor3300 Series. The jet is used for initialization of the Vigor3300 Series during preliminary installation. The “management cable”, as shown in Figure 1-5, converts the RJ45 to the RS232 interface. The RJ45 jet connects to a console interface in the Vigor3300 Series, while the RS232 DB9 connects to a console port on the computer. The default setting of the console port is “**baud rate 57600, no parity, and 8 bit with 1 stop bit.**”



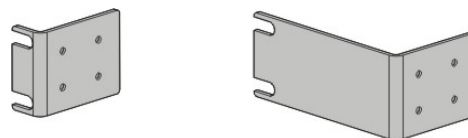
Standard 10/100 Base-T Ethernet Interface Connector

RJ45 jets provide 10/100 Base-T Ethernet interfaces. The interface supports MDI/MDIX auto-detection of either straight or crossover RJ45 cables. These cables are used on WAN, LAN, and DMZ interfaces.

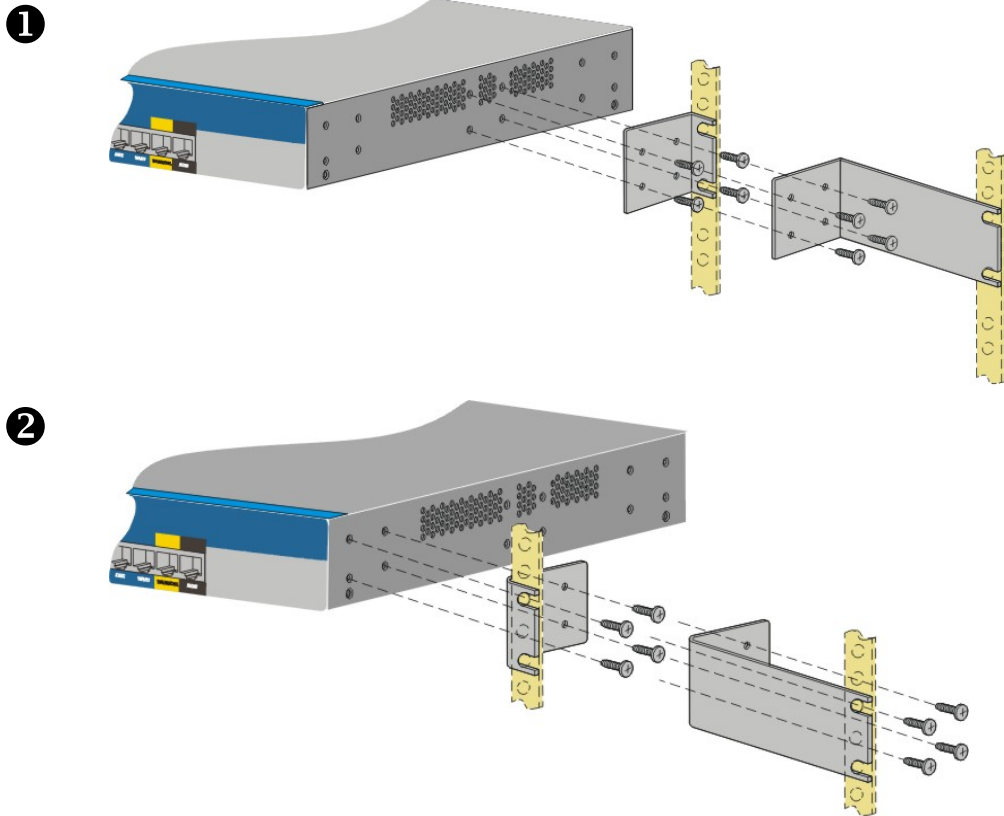


Chassis Connections

The Vigor3300 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 (as shown in the Figures 1-8 and 1-9). Repeat the above procedure for the second bracket, which attaches the other side of the chassis.



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 Vigor3300 Series. These rubber pads improve the air circulation and decrease unnecessary rubbing on the desktop.

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.

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.

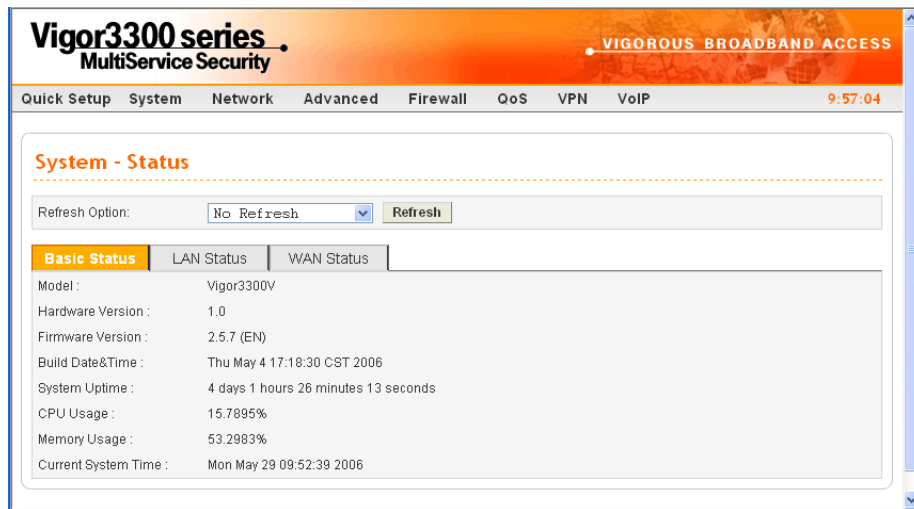


Notice: You may either simply set up your computer to get IP dynamically from the router or set up the IP address of the computer to be the same subnet as **the default IP address of Vigor router 192.168.1.1**. For the detailed information, please refer to the later section - Trouble Shooting of this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

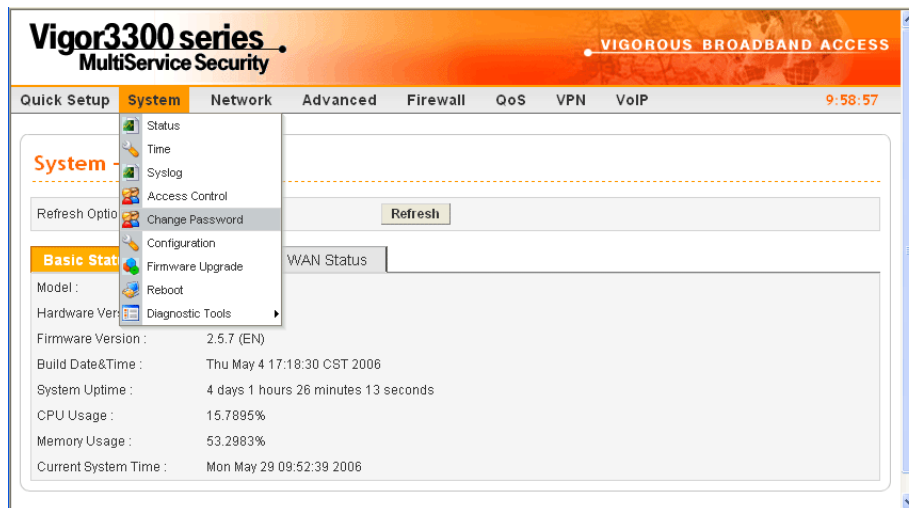
2. Open a web browser on your PC and type **http://192.168.1.1**. A pop-up window will open to ask for username and password. Please type default values on the window for the first time accessing. The default value for user name is **draytek** and the password is **1234**. Next, click **OK**.



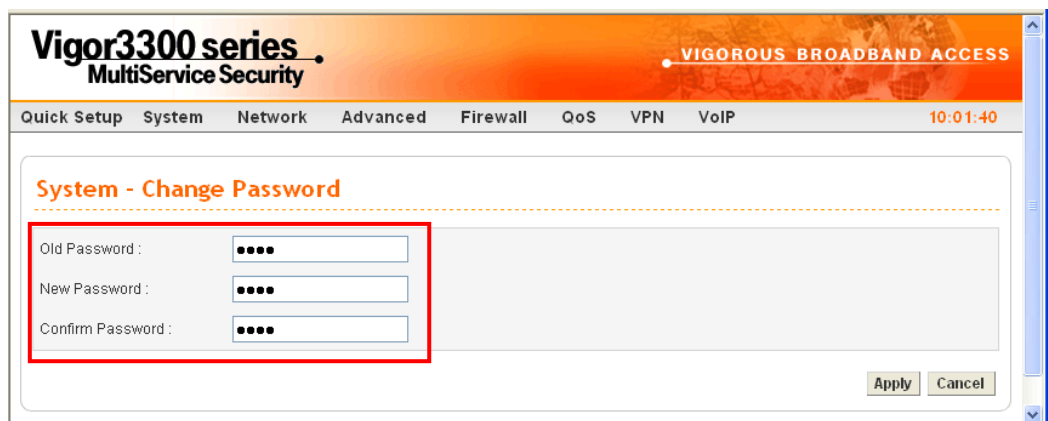
3. Now, the **Main Screen** will pop up.



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



5. The following screen will appear.



6. 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.

7. Now, the password has been changed. Next time, use the new password to access the Web Configurator for this router.
8. Next, you will see the login screen after clicking **Apply**. Please use new password to re-enter the system configuration.

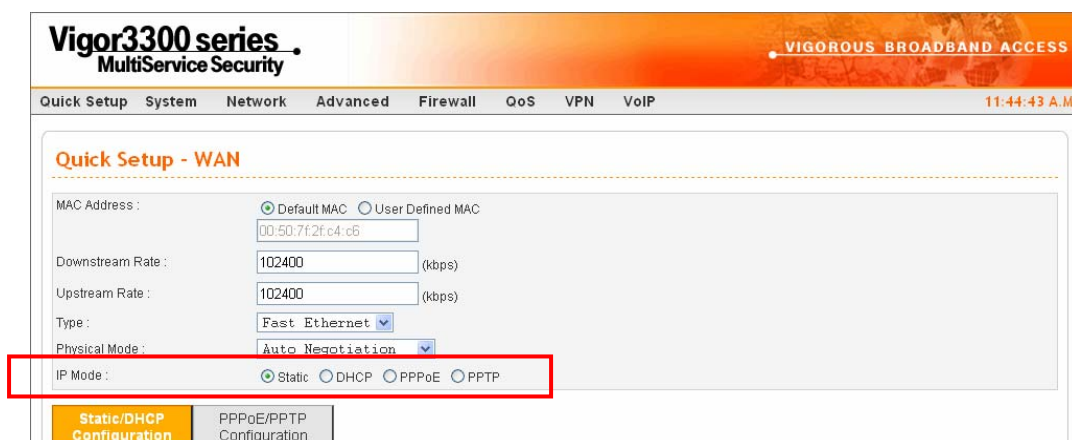


2.2 Quick Setup

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.

2.2.1 Adjusting WAN Connection Mode

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 settings in this section will be applied in the first WAN1 interface.



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

MAC Address	<p><i>Router Default-</i></p> <p>Use the default Mac address stored originally in router.</p> <p><i>User Definition-</i></p> <p>Use a MAC address defined by the user.</p>
Downstream Rate	<p>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.</p>
Upstream Rate	<p>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.</p>
Type	<p>Select a connection type for this WAN interface. Currently, there is only one setting offered for you to choose - Fast Ethernet.</p>
Physical Mode	<p>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.</p>
IP Mode	<p>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.</p>

2.2.2 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:

Static/DHCP Configuration		PPPoE/PPTP 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"/>		
IP Alias List			
1.	<input type="text" value="10.1.1.100"/>	2.	<input type="text" value="10.1.1.102"/>
3.	<input type="text" value="10.1.1.103"/>	4.	<input type="text"/>
5.	<input type="text"/>	6.	<input type="text"/>
7.	<input type="text"/>	8.	<input type="text"/>

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

- | | |
|------------------------|---|
| IP Address | Assign a private IP address to the WAN interface. |
| Subnet Mask | Assign a subnet mask value to the WAN interface. |
| Default Gateway | Assign a private IP address to the gateway. |
| Primary DNS | Assign a private IP address to the primary DNS. |
| Secondary DNS | Assign a private IP address to the secondary DNS. |
| IP Alias List | Assign 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, the user can 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) :

<<Previous Finish

IP Address

Assign an IP address for the LAN interface.

Subnet Mask

Assign 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

Assign the start IP address of the IP pool that DHCP server can use for clients in LAN.

End IP

Assign 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.

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

2.2.3 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.

Vigor3300 series
MultiService Security

VIGOROUS BROADBAND ACCESS

Quick Setup System Network Advanced Firewall QoS VPN VoIP 12:04:09 A.M.

Quick Setup - WAN

MAC Address : Default MAC User Defined MAC
00:50:7f:2f:c4:c6

Downstream Rate : (kbps)

Upstream Rate : (kbps)

Type :

Physical Mode :

IP Mode : Static DHCP PPPoE PPTP

Static/DHCP Configuration | PPPoE/PPTP Configuration

After setting up the **WAN** interface, the user can 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) :

<<Previous Finish

IP Address

Assign an IP address for the LAN interface.

Subnet Mask

Assign 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

Assign the start IP address of the IP pool that DHCP server can use for clients in LAN.

End IP Assign 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.

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

2.2.4 PPPoE

This mode is used for most of DSL modem users. All local users can share one PPPoE connection to access the Internet. Your service provider will give you the user name, password, and authentication mode for PPPoE settings.

Vigor3300 series
MultiService Security

VIGOROUS BROADBAND ACCESS

Quick Setup System Network Advanced Firewall QoS VPN VoIP 10:50:44 A.M.

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

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 : 88991234@hinet.net PPTP Local Address :

Password : Password masked with dots PPTP Subnet Mask :

Authentication : PAP PPTP Server Address :

Service Name (Optional): hinet

Next >>

User Name Assign a specific valid user name provided by the ISP.

Password Assign a valid password provided by the ISP.

Authentication Select **PAP** or **CHAP** protocol for PPP authentication. The default value is **PAP**.

Service Name Assign a service name required from ISP service.

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

Static/DHCP Configuration	PPPoE/PPTP Configuration		
User Name :	<input type="text" value="88991234@hinet.net"/>	PPTP Local Address :	<input type="text" value="10.66.99.88"/>
Password :	<input type="password" value="••••"/>	PPTP Subnet Mask :	<input type="text" value="255.255.255.0"/>
Authentication :	<input type="text" value="PAP"/> ▼	PPTP Server Address :	<input type="text" value="172.66.99.88"/>
Service Name (Optional):	<input type="text" value="hinet"/>		
<input type="button" value="Next >>"/>			

IP Address

Assign an IP address for the LAN interface.

Subnet Mask

Assign 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

Assign the start IP address of the IP pool that DHCP server can use for clients in LAN.

End IP

Assign 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.

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

2.2.5 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.

Vigor3300 series
MultiService Security

VIGOROUS BROADBAND ACCESS

Quick Setup System Network Advanced Firewall QoS VPN VoIP 10:50:44 A.M.

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

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 Remote Address** (e.g., 172.66.99.88) provided by your ISP on the web page.

Static/DHCP Configuration **PPPoE/PPTP Configuration**

User Name : 8877562685@hinet.net

Password :

Authentication : PAP

Service Name (Optional): hinet

PPTP Local Address : 10.66.99.88

PPTP Subnet Mask : 255.255.255.0

PPTP Remote Address : 172.66.99.88

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 Remote Address Assign a remote IP address of PPTP server.

After setting up the **WAN** interface, the user can 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

Assign an IP address for the LAN interface.

Subnet Mask

Assign 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

Assign the start IP address of the IP pool that DHCP server can use for clients in LAN.

End IP

Assign 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.

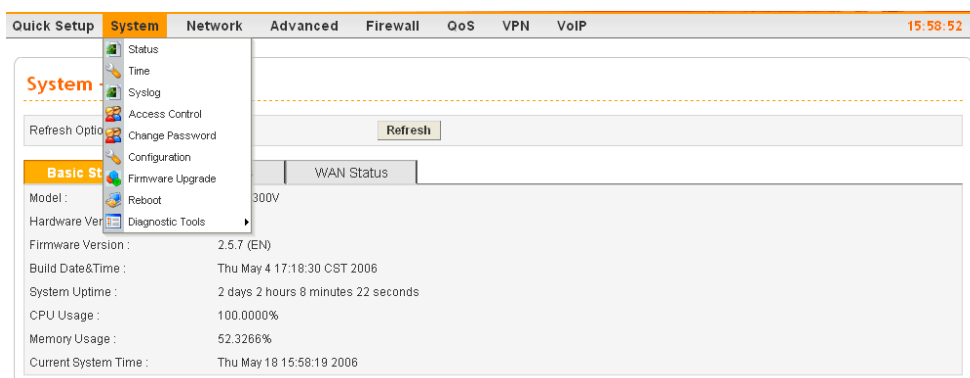
When you finished the above required settings, please click **Finish**. A system reboot page will appear.

3 Advanced Configuration

After finished basic configuration of the router, you can access Internet with ease. For the user who wants 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.

3.1 System setup

For the system setup, there are several items that you have to know the way of configuration: Status, Time Setup, Syslog Setup, Access Control Setup, Reboot and Firmware Upgrade Setup, Diagnostic Tools and Configuration Setup.



3.1.1 Status

The online **Status** function provides some useful system information on the current status of the Vigor3300 Series. A user can observe the system status on this Web page and determine which setting needed to be changed in corresponding web pages. In the **System** group, click the **Status** option. The online **Status** Web page contains three parts: **Basic Status**, **LAN Status**, and **WAN Status**.

Refresh Option You can choose to automatically refresh the Web page information. 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 on **Basic Status** page.

The screenshot shows the 'System - Status' page. At the top, there is a 'Refresh Option' dropdown menu set to 'No Refresh' and a 'Refresh' button. Below this are three tabs: 'Basic Status' (selected), 'LAN Status', and 'WAN Status'. The 'Basic Status' tab displays the following information:

Model :	Vigor3300V
Hardware Version :	1.0
Firmware Version :	2.5.7.1 (EN)
Build Date&Time :	Mon Jun 5 18:09:36 CST 2006
System Uptime :	0 days 4 hours 9 minutes 21 seconds
CPU Usage :	34.6667%
Memory Usage :	53.9401%
Current System Time :	Tue Aug 1 14:27:42 2006

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

LAN Status

The status of LAN connection is shown in this page. Simply click **LAN Status** tag to get the detailed.

The screenshot shows the 'LAN Status' page. At the top, there is a 'Refresh Option' dropdown menu set to 'Every 10 Seconds' and a 'Refresh' button. Below this are three tabs: 'Basic Status', 'LAN Status' (selected), and 'WAN Status'. The 'LAN Status' tab displays the following information:

IP Address :	192.168.1.99
MAC Address :	00:50:7F:64:3B:05
High Available Status :	Master
RX Packets :	1369086
TX Packets :	248268

- | | |
|--------------------|--|
| IP Address | Displays the IP address of the LAN interface. |
| MAC Address | Displays the MAC address of the LAN Interface. |

High Available Status

The High Available Status is shown when the function is enabled. When there are two Vigor3300 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 Vigor3300 plays the Master role in high availability feature.

Slave - It means that Vigor3300 plays the Slave role in high availability feature.

If there is only one Vigor3300 used in LAN, this line will be blank.

RX Packets

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

TX Packets

Displays 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.

The screenshot shows the 'System - Status' page of the Vigor3300 series MultiService Security device. The 'WAN Status' tab is selected, displaying configuration and statistics for four WAN interfaces: WAN1, WAN2, WAN3, and WAN4. Each interface shows its IP Address, MAC Address, Primary and Secondary DNS, Gateway, RX and TX Packets, Connection Status, and Up Time.

Basic Status	LAN Status	WAN Status
WAN1 :		
IP Address :	172.16.2.225	
MAC Address :	00:50:7f:2f:c4:c6	
Primary DNS :	168.95.1.1	
Secondary DNS :	168.95.192.1	
Gateway :	172.16.2.233	
RX Packets :	101580	
TX Packets :	12050	
Connection Status :	connected	
Up Time :	0 days 2 hours 0 minutes 0 seconds	
WAN2 :		
IP Address :		
MAC Address :		00:50:7f:2f:c4:c7
Primary DNS :		
Secondary DNS :		
Gateway :		
RX Packets :		
TX Packets :		
Connection Status :		
Up Time :		
WAN3 :		
IP Address :		
MAC Address :	00:50:7f:2f:c4:c8	
Primary DNS :		
Secondary DNS :		
Gateway :		
RX Packets :		
TX Packets :		
Connection Status :		
Up Time :		
WAN4 :		
IP Address :		
MAC Address :		00:50:7f:2f:c4:c9
Primary DNS :		
Secondary DNS :		
Gateway :		
RX Packets :		
TX Packets :		
Connection Status :		
Up Time :		

IP Address

Displays the IP address of the WAN interface.

MAC Address

Displays the MAC address of the WAN Interface.

Primary DNS

Displays the IP address of the primary DNS.

Secondary DNS

Displays the IP address of the secondary DNS.

Gateway

Displays the IP address of the default gateway.

RX Packets

Displays the total received packets for each WAN interface.

TX Packets

Displays the total transmitted packets for each WAN interface.

Connection Status

Displays the connection status of the WAN interface.

Up Time

Displays the total system uptime of the interface.

3.1.2 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

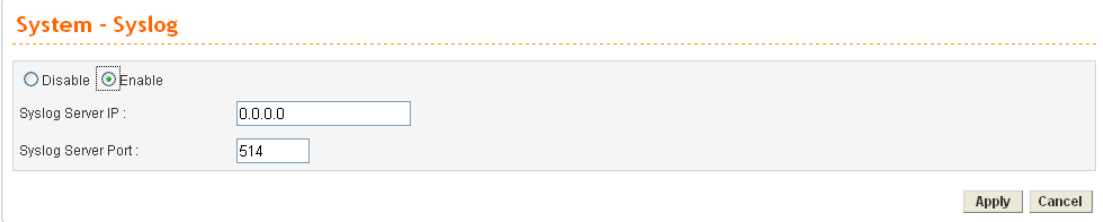
Update Interval : 30 seconds ▾

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** Assign a public IP address or domain name of the NTP server.
- Time Zone** Select the time zone where the Vigor3300 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.

3.1.3 Syslog

The Vigor3300 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 Vigor3300. In the **System** group, click the **Syslog** option. The Syslog web page is shown below:



System - Syslog

Disable Enable

Syslog Server IP :

Syslog Server Port :

- Status** 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, Vigor3300 will not send Syslog packets to the Syslog server.
- Syslog Server Port** Assign a port for the Syslog protocol.
- Apply** Click **Apply** to save these settings.

3.1.4 Access Control

This page allows you to determine which services (HTTP/Telnet/SSH) is used for the user to access Vigor3300 Series. In addition, you can also limit some hosts to access Vigor3300 Series with specified IP address.

In the **System** group, click the **Access Control** option. You will get the following page:

The screenshot shows the 'System - Access Control' configuration page. At the top, there is a navigation bar with 'Quick Setup', 'System', 'Network', 'Advanced', 'Firewall', 'QoS', 'VPN', and 'VoIP'. The 'System' tab is selected. The page title is 'System - Access Control'. Below the title, there are four main sections:

- Management Method:** 'Allow Management Method:' with checkboxes for HTTP (checked), Telnet (checked), and SSH (unchecked).
- Management Access Control:** 'Allow Management from the WAN' with radio buttons for 'Disable' (selected), 'Enable All', and 'Enable User Defined WAN IP'. Below this are three input fields for 'Allowed IP1:', 'Allowed IP2:', and 'Allowed IP3:'.
- Management Port:** Radio buttons for 'Default Ports (HTTP Port:80 Telnet Port:23)' (selected) and 'User Defined Ports'. Under 'User Defined Ports', there are input fields for 'HTTP Port:' (80), 'Telnet Port:' (23), and 'SSH Port:' (22).
- PING Restriction:** Checkboxes for 'Disable PING from the LAN' and 'Disable PING from the WAN', both of which are unchecked.

At the bottom right of the form, there are 'Apply' and 'Cancel' buttons.

Management Method

There are three management methods provided here for you to choose for your router. Check HTTP/Telnet/SSH for the router.

Allow Management from the WAN

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(to 3) - Type in IP address (up to three) for managing the system.

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.

3.1.5 Configuration Setup

Most of the settings can be saved locally as a configuration file, and can be applied to another router. The Vigor3300 Series supports the restore and upload functions of the **configuration files**. In the **System** group, click the **Configuration Setup** option. And you can see the following page.

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 Download the configuration file to a local host. The default file name is “v3300.cfg”.

Push Backup Button

3.1.6 Firmware Upgrade Setup

Vigor3300 Series allows users to upgrade firmware through a Web interface. In the **System** group, click the **Firmware Upgrade** option. You can see the following page then. 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 2.5.7.1 (EN)

Location : Local Remote

Firmware :

TFTP Server IP

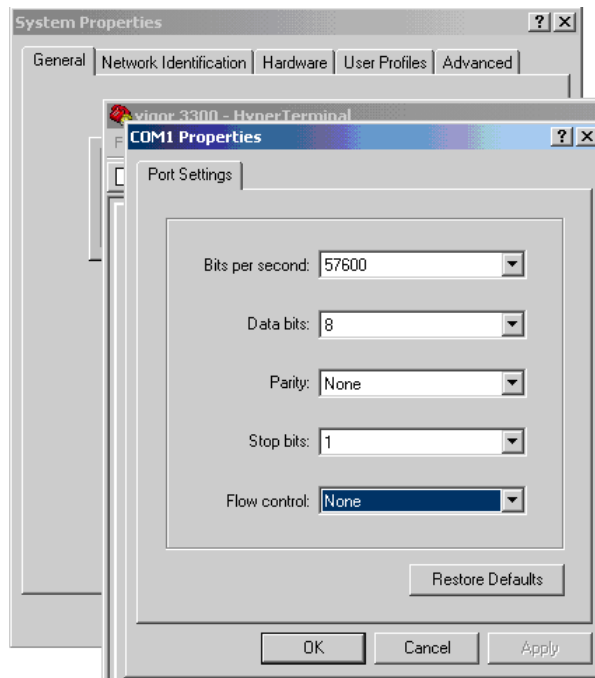
Remote File Name

- Caution** Displays a caution for your reference.
- Current Version** Displays current firmware version that you are using.
- Location** *Local* means upgrade firmware from browser.
Remote 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 Vigor3300, then press **ENTER** before the system reboots completely.
4. Open Hyper Terminal on the PC. Now, Vigor3300 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
Connected 0:05:41 Auto detect 57600 8-N-1 SCROLL CAPS NUM Capture Print echo

```

3.1.7 Reboot

The Vigor3300 Series 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.

In the **System** group, choose the **Reboot** option. In the web page of **Reboot**, a user must either keep the current configuration settings or use the default configuration after the Vigor3300 Series system has been rebooted.



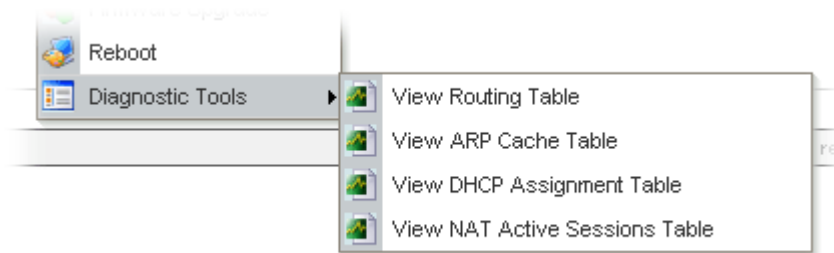
Click **Apply** to reboot the whole system. The rebooting procedure usually takes 70 or more seconds.



3.1.8 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 Vigor3300 Series supports four functions, **Routing Table**, **ARP Cache Table**, **DHCP Assignment Table**, and **NAT Active Sessions Table** 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:



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

Destination	Displays the destination IP address for various routings.
Gateway	Displays the default gateway.
Subnet Mask	Displays the subnet mask for various routings.
Flags	Displays 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:

Vigor3300 series
MultiService Security

VIGOROUS BROADBAND ACCESS

Quick Setup System Network Advanced Firewall QoS VPN VoIP 5:51:34 P.M.

System - Diagnostic Tools - View ARP Cache Table

IP Address	MAC Address	Interface
172.16.2.145	00:0E:A6:2A:D5:BE	eth0
172.16.2.249	00:40:F4:6B:57:61	eth0
172.16.2.222	00:11:2F:D5:D0:2B	eth0
172.16.2.88	00:50:7F:28:6E:1D	eth0
172.16.2.91	00:50:7F:23:48:14	eth0

Refresh

DrayTek Corp. © 1997 - 2005 All rights reserved. DrayTek provides enterprise network solution.

- IP Address** Displays the IP address for different ARP cache.
- MAC Address** Displays 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:

Vigor3300 series
MultiService Security

VIGOROUS BROADBAND ACCESS

Quick Setup System Network Advanced Firewall QoS VPN VoIP 5:53:44 P.M.

System - Diagnostic Tools - View DHCP Assignment Table

Assigned IP	MAC Address	Time Left
192.168.1.10	00:0E:0C:35:E3:EA	11 seconds

Refresh

DrayTek Corp. © 1997 - 2005 All rights reserved. DrayTek provides enterprise network solution.

- Assigned IP** Displays the IP address of the static DHCP server.
- MAC Address** Displays the MAC address of the static DHCP server.
- Time Left** Displays 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.

Vigor3300 series
MultiService Security

VIGOROUS BROADBAND ACCESS

Quick Setup System Network Advanced Firewall QoS VPN VoIP 5:38:13 P.M.

System - Diagnostic Tools - View NAT Active Sessions Table

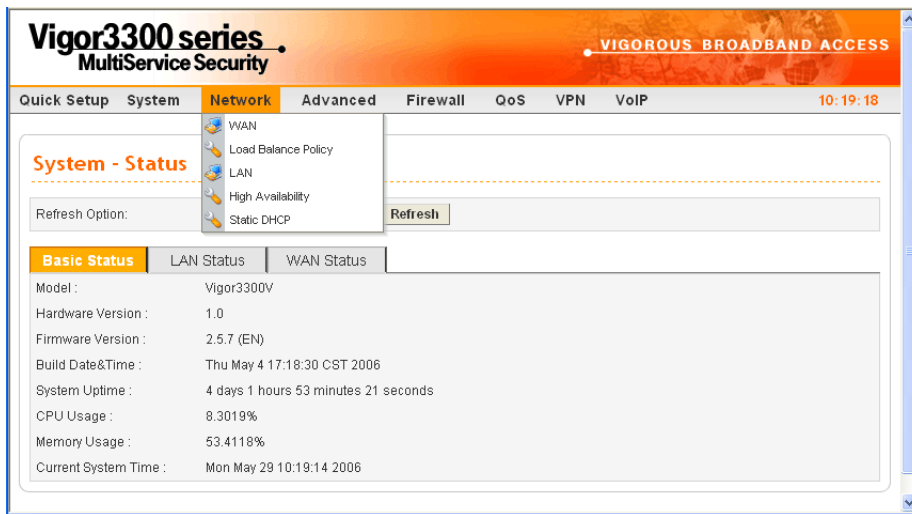
Type	Expire in	State	Source IP	Dest IP	sPort	dPort	Rep Source IP	Rep Dest IP	sPort	dPort
tcp	591	ESTABLISHED	192.168.1.222	207.46.6.24	3435	1863	207.46.6.24	172.16.2.225	1863	34682
tcp	598	ESTABLISHED	192.168.1.222	207.46.6.153	3476	1863	207.46.6.153	172.16.2.225	1863	34723

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

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

3.2 Network Setup

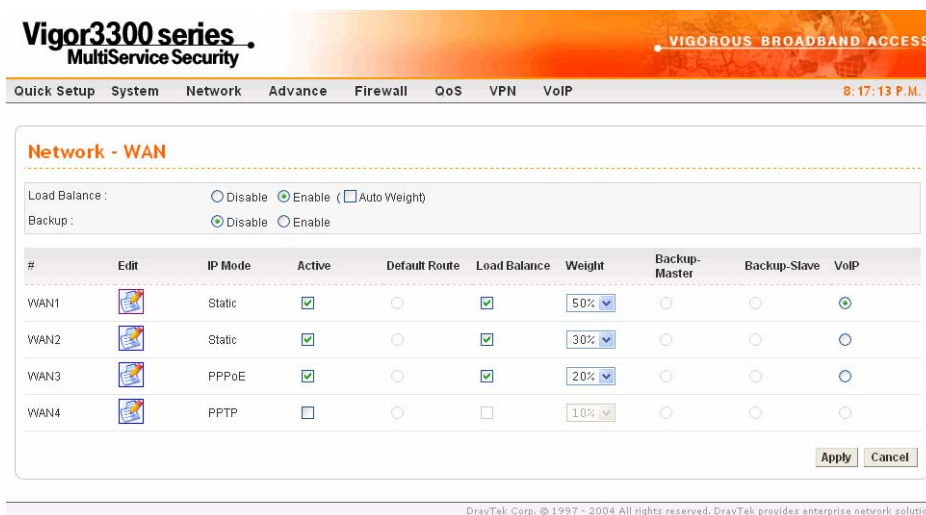
For Internet access, it is necessary for you to set **WAN** and **LAN** interfaces for the router.



3.2.1 WAN and Internet Access Setup

The Vigor3300 Series supports four WAN interfaces (Static, DHCP, PPPoE and PPTP), which share the same setting page. In the **Network** group, please click the **WAN** option. The following page will be shown.

Note: Vigor3300/3300V supports four WAN interfaces, yet Vigor3300B+ supports three WAN interfaces. That is, #WAN4 will be disabled for Vigor3300B+.



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	Displays current mode of this WAN interface. There are five options: Static, DHCP, PPPoE, PPTP and DHCP.
Active	Activates/closes this WAN interface.
Default Route	Sets this WAN interface as default route interface.
Load Balance	Adds this WAN interface to the load balance group.
Weight	Sets the weight load (10-90%) for this WAN interface for load balance. This selection is available only when Auto Weight is unchecked.
Backup-Master	Sets this WAN interface as a master interface. WAN1 must be assigned as Master interface if Backup function is enabled.
Backup-Slave	Sets this WAN interface as a slave interface.
VoIP	Sets this WAN interface as VoIP default interface.

Most users will use their routers primarily for Internet access. The Vigor3300 Series supports broadband Internet access and provides multiple WAN interfaces. The following sections will give a detailed illustration to broadband access methods.

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

Network - WAN - WAN1 - Fast Ethernet

MAC Address : Default MAC User Defined MAC

Downstream Rate : (kbps)
Upstream Rate : (kbps)
Type :
Physical Mode :
IP Mode : Static DHCP PPPoE PPTP DMZ

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	Sets downstream rate for this WAN interface. The default value is 102400 kbps (100 Megabit).
Upstream Rate	Sets transmission rate for this WAN interface. The default value is 102400 kbps (100 Megabit).
Type	Sets connection type for this WAN interface.
Physical Mode	Sets connection speed mode. There are five options including Auto negotiation, full duplex, half duplex, 10M and 100M.

IP Mode

Sets 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 Vigor3300 Series, you need to know what kind of Internet access your ISP provides. The following sections introduce four 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. Vigor3300 Series 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"/>	
Connection Detection		
Detect Type :	<input type="text" value="Send Http Request"/>	
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" value="172.16.3.88"/>	
IP Alias List		
1.	<input type="text" value="10.1.1.101"/>	2. <input type="text" value="10.1.1.102"/>
3.	<input type="text"/>	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

Sets the private IP address of WAN interface.

Subnet Mask

Sets the subnet mask value of WAN interface.

Default Gateway

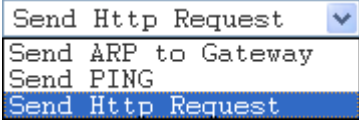
Sets the private IP address of gateway.

Primary DNS

Sets the private IP address of primary DNS.

Secondary DNS

Sets the private IP address of secondary DNS.

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	<p>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.</p> 
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	Sets 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.

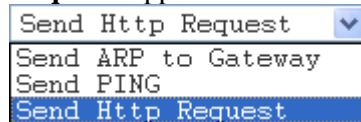
DHCP Client Setup

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. It is not necessary for users to manually configure the router.

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"/>	
Connection Detection		
Detect Type :	<input type="text" value="Send Http Request"/> ▼	
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" value="172.16.3.88"/>	
IP Alias List		
1.	<input type="text" value="10.1.1.101"/>	2. <input type="text" value="10.1.1.102"/>
3.	<input type="text"/>	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"/>		

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.

Static/DHCP Configuration	PPPoE/PPTP Configuration	DMZ Configuration
User Name :	<input type="text" value="889966666@hinet.net"/>	PPTP Local Address : <input type="text"/>
Password :	<input type="password" value="....."/>	PPTP Subnet Mask : <input type="text"/>
Authentication :	<input type="text" value="PAP"/> <input type="button" value="v"/>	PPTP Server Address : <input type="text"/>
Service Name :	<input type="text" value="hinet"/>	
PPPoE IP Alias :	<input type="checkbox"/> Enable	
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** or **CHAP** protocol 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 RAP.

Service Name Assign a service name required for some ISP services.

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.

PPTP with a DSL Modem Setup

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

The screenshot shows a configuration page with three tabs: 'Static/DHCP Configuration', 'PPPoE/PPTP Configuration' (selected), and 'DMZ Configuration'. The 'PPPoE/PPTP Configuration' section includes the following fields and options:

- User Name: draytek
- Password: [masked]
- Authentication: PAP (dropdown menu)
- Service Name: hinet
- PPPoE IP Alias: Enable
- PPTP Local Address: 10.0.0.2
- PPTP Subnet Mask: 255.255.255.0
- PPTP Server Address: 10.0.0.1

The 'IP Address Assignment Method (IPCP)' section has two radio buttons: 'No (Dynamic IP)' (selected) and 'Yes'. The 'Fixed IP Address' field is empty.

The 'Connection Detection' section has two input fields: 'Detect Interval' (10) and 'No-Reply Count' (2).

At the bottom right, there are three buttons: 'Apply', 'Reset', and '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** or **CHAP** protocol for widest compatibility. The default value is **PAP**. The password will be encrypted in CHAP but not in RAP.
- 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.

3.2.2 LAN

In the **Network** group, select **LAN** option. The following page for LAN IP/DHCP will be shown.

The screenshot shows the 'Network - LAN' configuration page. It has three tabs: 'LAN IP/DHCP' (selected), 'DHCP Relay Agent', and 'IP Routing'. Under 'LAN IP/DHCP', there are two sections: 'IP Configuration' and 'DHCP Server'. The 'IP Configuration' section has fields for 'IP Address' (192.168.1.1) and 'Subnet Mask' (255.255.255.0). The 'DHCP Server' section has a 'Status' field with radio buttons for 'Enable' (selected), 'Disable', and 'Relay Agent'. Below 'Status' are fields for 'Start IP' (192.168.1.10), 'End IP' (192.168.1.254), 'Primary DNS', 'Secondary DNS', 'Lease Time (Min)' (1440), and 'Gateway IP(Optional)'. At the bottom right are 'Apply' and 'Cancel' buttons.

For LAN IP/DHCP

In the Vigor3300 Series 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 | Sets the starting IP address of the IP address pool for DHCP server. |
| End IP | Sets the ending IP address of the IP address pool for DHCP server. |
| Primary DNS | Sets the private IP address of the primary DNS. |

- Secondary DNS** Sets the private IP address of the secondary DNS.
- Lease Time (Min)** Sets a lease time for the DHCP server. The time unit is minute.
- Gateway IP (Optional)** Sets 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. It has three tabs: 'LAN IP/DHCP', 'DHCP Relay Agent' (which is selected and highlighted in orange), and 'IP Routing'. Under the 'DHCP Relay Agent' tab, there is a section titled 'Relay Agent'. It contains two fields: 'WAN Interface' with a dropdown menu showing 'WAN1' selected, and 'DHCP Server IP Address' with a text input field containing '172.16.3.1'. At the bottom right of the form are 'Apply' and 'Cancel' buttons.

- 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.

Network - 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:

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

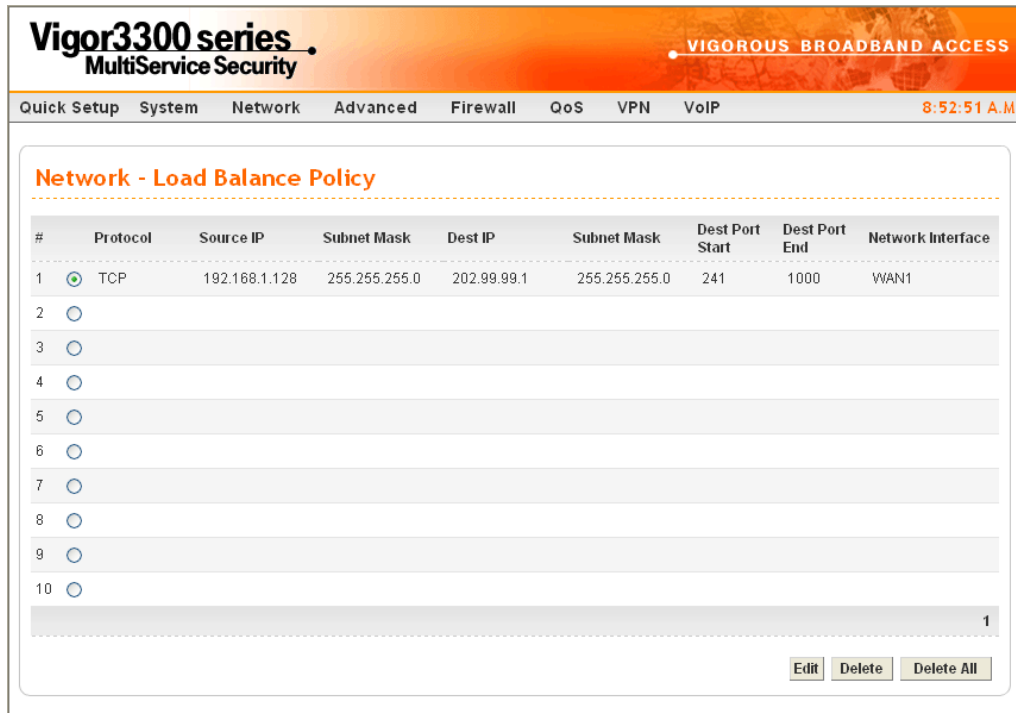
Select a proper LAN interface for WAN interface (WAN1/WAN2/WAN3/WAN4).

Note: Vigor3300V supports four WAN interfaces, yet Vigor3300/Vigor3300B+ support three WAN interfaces. That is, #WAN4 will be disabled for Vigor3300/Vigor3300B+.

3.2.3 Load Balance Policy

Vigor3300 Series 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.



- Protocol** Displays the protocol used for this entry.
- Source IP** Displays the source IP address specified for this entry.
- Subnet Mask** Displays the subnet mask address specified for the source IP of this entry.
- Dest IP** Displays the destination IP address specified for this entry.
- Subnet Mask** Displays the subnet mask address specified for the destination IP of this entry.
- Dest Port Start** Displays the start point specified in the **Dest Port Range** for this entry.
- Dest Port End** Displays the end point specified in the **Dest Port Range** for this entry.
- Network Interface** Displays the interface specified for this entry.
- 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 :

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.

Network Interface

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

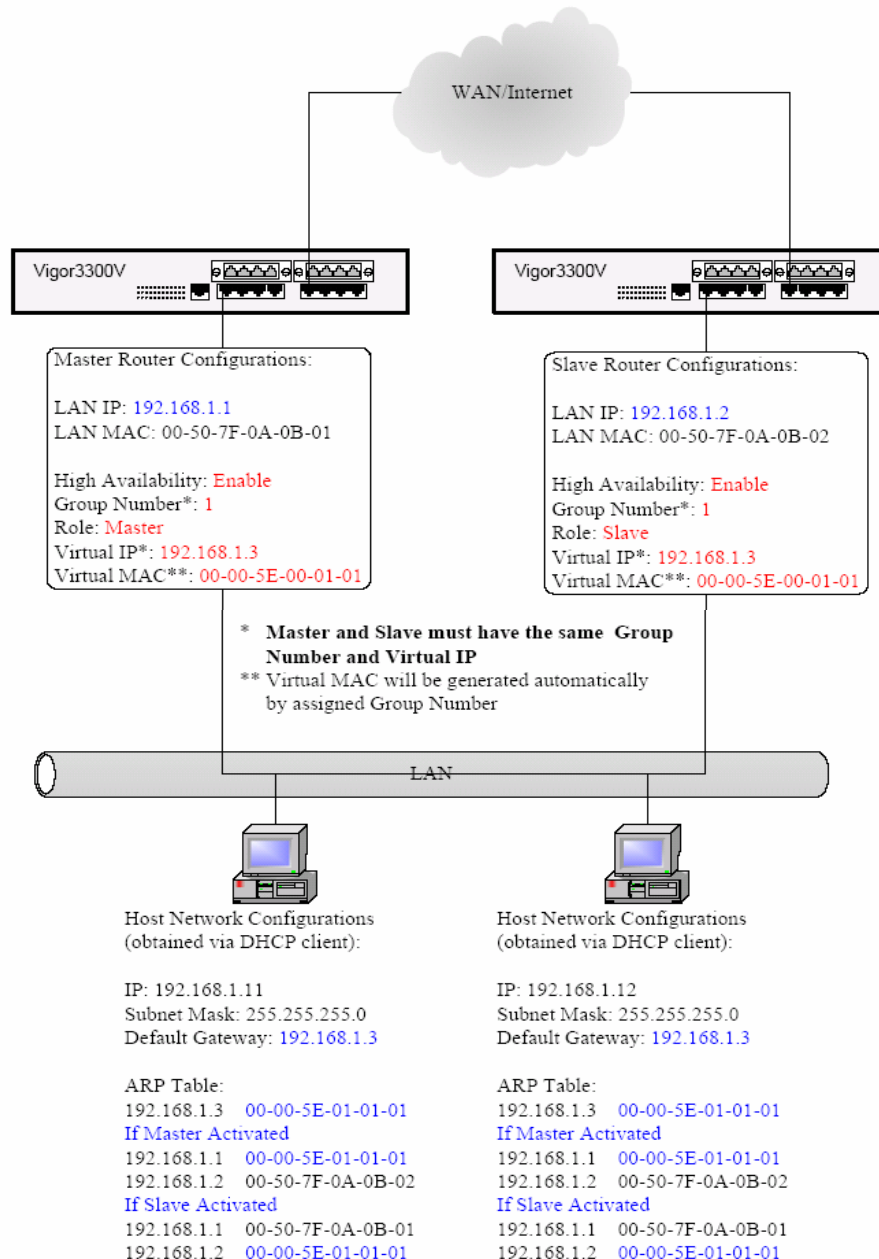
3.2.4 High Availability

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, that 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

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.

3.2.5 Static DHCP

This page can assign static IP address for specified clients in LAN.

MAC Address

Displays the MAC address of the static DHCP server.

Assign IP Address

Displays the IP address of the static DHCP server.

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 - Static DHCP - Edit

1

MAC Address: 21:56:89:45:42:36

Assign IP Address: 172.16.3.228

Apply Cancel

MAC Address Type the MAC Address for the host that you want to set as static DHCP server.

Assign IP Address Type the IP address for that host.

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

3.3 Advanced Setup

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

Vigor3300 series MultiService Security VIGOROUS BROADBAND ACCESS

Quick Setup System Network **Advanced** Firewall QoS VPN VoIP 10:00:54

System - Status

Refresh Option:

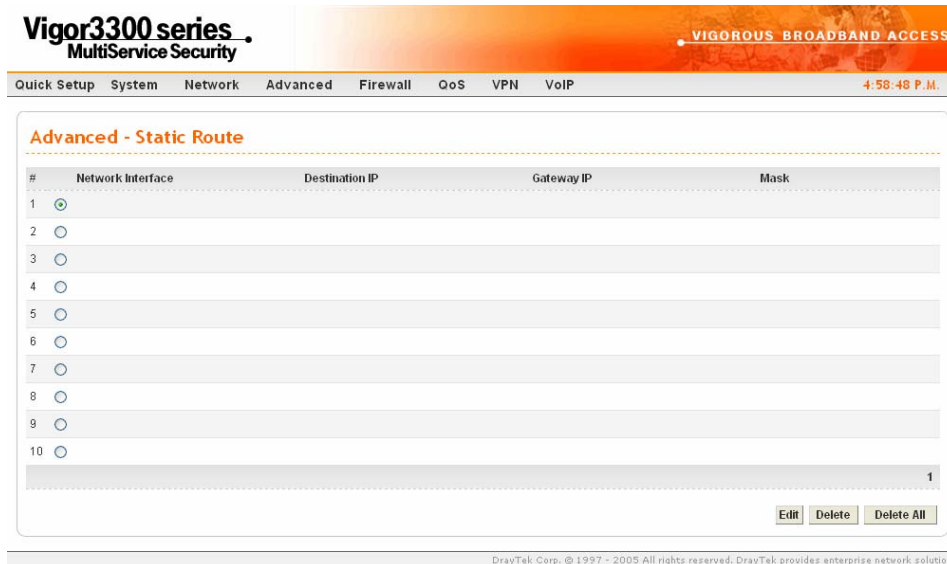
Basic Status	LAN Status
Model :	Vigor3300V
Hardware Version :	1.0
Firmware Version :	2.5.7 RC3 (t)
Build Date&Time :	Fri Apr 14 19:00:13 CST 2006
System Uptime :	7 days 21 hours 47 minutes 42 seconds
CPU Usage :	7.5138%
Memory Usage :	52.2377%
Current System Time :	Wed May 3 09:58:23 2006

DrayTek Corp. © 1997 - 2006 All rights reserved. DrayTek provides enterprise network solution.

3.3.1 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.

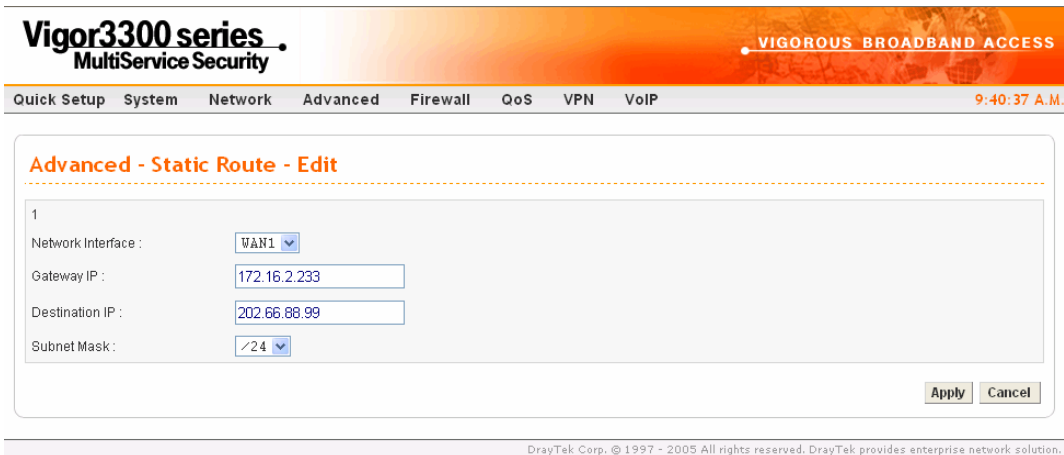


- Network Interface** Displays the network interface (LAN, WAN1, 2, 3 or 4).
- Destination IP** Displays the destination IP of the static route.
- Gateway IP** Displays the gateway address of the static route.
- Mask** Displays the subnet mask of this route.
- Edit** Allows users to edit the selected 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:



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.

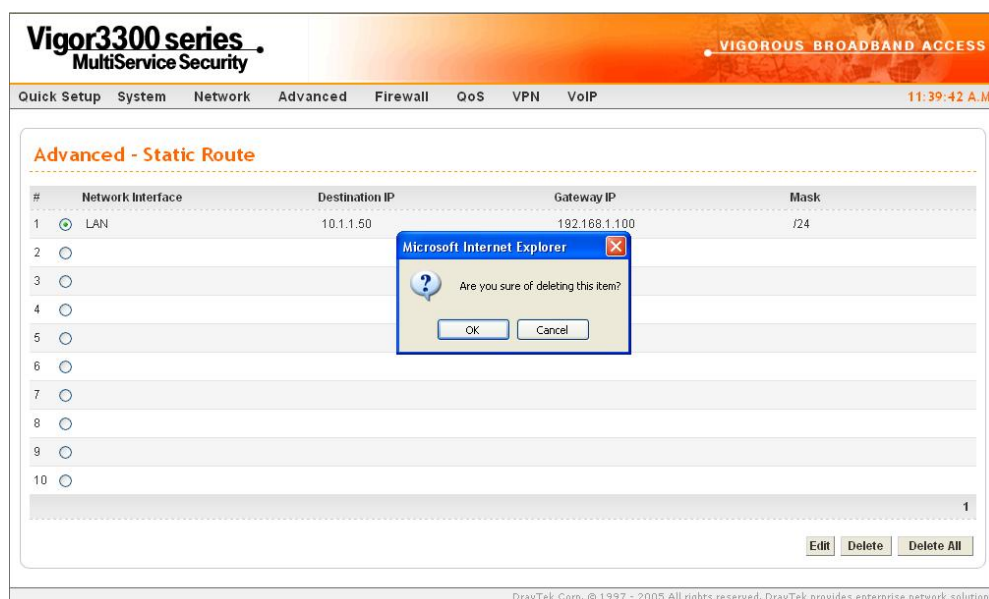
Subnet Mask

Assign a value of subnet mask for destination IP address.

Click **Apply** to reboot the system and apply the 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:



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

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

3.3.2 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.

In the **Advanced** group, click the **NAT** option.



There are four functions that NAT provides – **Port Redirection**, **Address Mapping**, **DMZ Host** and **Well-Known Parts 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. In the **Advanced** group, move to **NAT** option and choose **Port Redirection** to get the corresponding page.

Vigor3300 series
MultiService Security

VIGOROUS BROADBAND ACCESS

Quick Setup System Network Advanced Firewall QoS VPN VoIP 5:14:54 P.M.

Advanced - NAT - Port Redirection

#	Comment	Protocol	Public Port Start	Public Port End	Private IP	Private Port Start	Private Port End	Use IP Alias	WAN Interface	IP Alias
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

Edit Delete Delete All

- Comment** Displays the name of the entry.
- Protocol** Displays the protocol used for the entry.
- Public Port Start** Displays the start point in the range of public port.
- Public Port End** Displays the end point in the range of public port.
- Private IP** Displays the private IP used for this entry.
- Private Port Start** Displays the start point in the range of private port.
- Private Port End** Displays the end point in the range of private port.
- Edit** Allows 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.

Vigor3300 series
MultiService Security

VIGOROUS BROADBAND ACCESS

Quick Setup System Network Advanced Firewall QoS VPN VoIP 8:14:42 P.M.

Advanced - NAT - Port Redirection - Edit

1

Comment: a

Protocol: TCP

Public Port Range: 200 - 600

Private IP: 192.168.3.100

Private Port Range: 200 - 600

Use IP Alias: Disable Enable

WAN Interface: WAN1

IP Alias: 10.1.1.100

Apply Cancel

DrayTek Corp. © 1997 - 2005 All rights reserved. DrayTek provides enterprise network solution.

- 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.
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"/>			

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.

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. And 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.

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

#	WAN Interface	Private IP	Use IP Alias	IP Alias
1	WAN1	192.168.1.10	Disable	
2				
3				
4				
5				
6				
7				
8				
9				
10				

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.

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

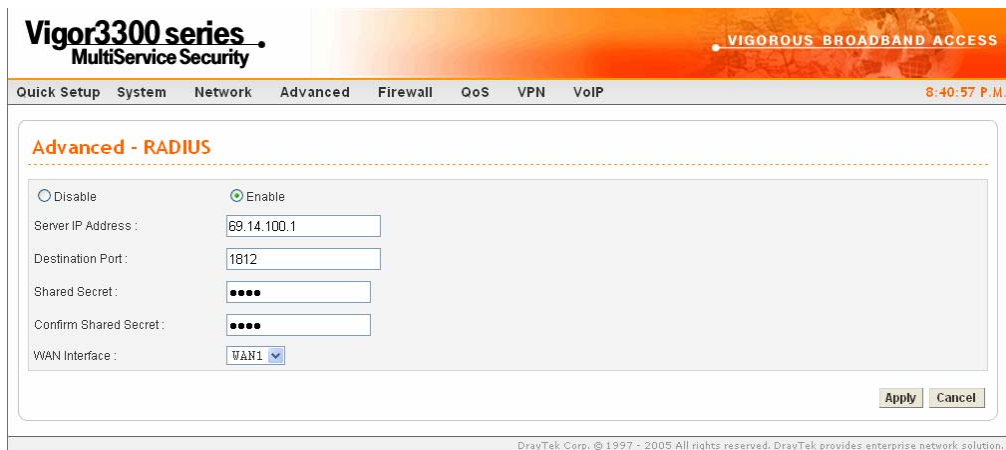
3.3.3 RADIUS Setup

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 3300 Series support 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.



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.

WAN Interface

Select one specific WAN interface to be used.

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

3.3.4 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.

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

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. The default port setting for V3300B and 3300B+ is 135.

3.3.5 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.

#	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.

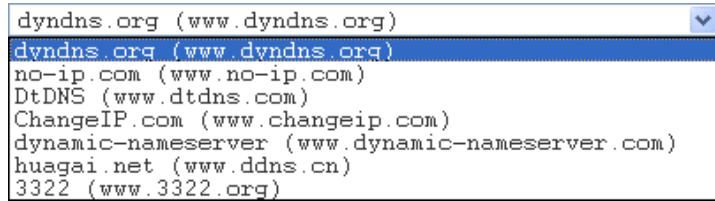
Status

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 V3300 series.

Server Provider Assign a provider name to support DDNS server. The Vigor3300 supports 7 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.
-

3.3.6 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. Vigor3300 Series support lots of profiles for call schedule usage. In the **Advanced** group, click the **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"/>					

1

- 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.

Advance - Call Schedule - Edit

Disable Enable
 Start Date : 2004 - 12 - 28 (Year - Month - Date)
 Start Time : 00 : 00 (Hour : Minute)
 Action : force down force on
 How often : Once Weekdays
 Monday Tuesday Wednesday Thursday Friday Saturday Sunday
 Network Interface : WAN1

Apply Cancel

DrayTek Corp. © 1997 - 2004 All rights reserved. DrayTek provides enterprise network solution.

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.

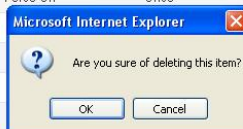
Click **Apply** to finish this setting.

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"/>					



Edit Delete Delete All

DrayTek Corp. © 1997 - 2005 All rights reserved. DrayTek provides enterprise network solution.

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

3.3.7 WAN Port Mirroring Setup

Vigor 3300 Series 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 user 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.

In the **Advanced** group, click the **WAN Port Mirroring** option. 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**.

3.3.8 LAN Port Mirroring Setup

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

In the **Advanced** group, click the **LAN Port Mirroring** option.



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**.

3.3.9 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

In the **Advanced** group, click the **LAN VLAN** option. There are two 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**

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

Management Port:

Port Setting

P1:
 P2:
 P3:
 P4:

Apply Reset Cancel

Active

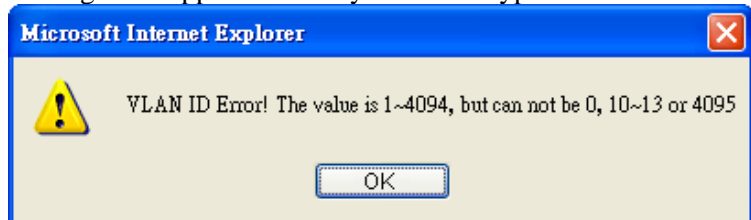
Check this box to activate the settings of this entry. If you check the **Management Port** box below, Index 4 will be unchangeable and locked. And, you have to set Port VLAN ID for P4 previously before you check **Management Port**.

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.

Management Port

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 Management Port.

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.

3.3.10 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.

In the **Advanced** group, click the **SNMP** option. There are two items for SNMP – **SNMP Community** and **SNMP Traps**.

SNMP Community

. Generally speaking, NMSs which are within the community exist within the same administrative domain.

#	Community	Host/mask	Max Access
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

[Edit](#) [Delete](#) [Delete All](#)

- 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.

The screenshot shows the web interface for the Vigor3300 series MultiService Security device. The page title is "EMS - SNMP Traps". The interface includes a navigation menu with the following items: Quick Setup, System, Network, Advanced, Firewall, QoS, VPN, and VoIP. The current time is 8:08:16 P.M. The main content area contains a table with the following columns: #, Trap Server, Trap Community, and Trap server port. The table has 10 rows, with the first row selected. At the bottom of the table, there are buttons for Edit, Delete, and Delete All.

#	Trap Server	Trap Community	Trap server port
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

Edit Delete Delete All

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.

EMS - SNMP Traps - Edit

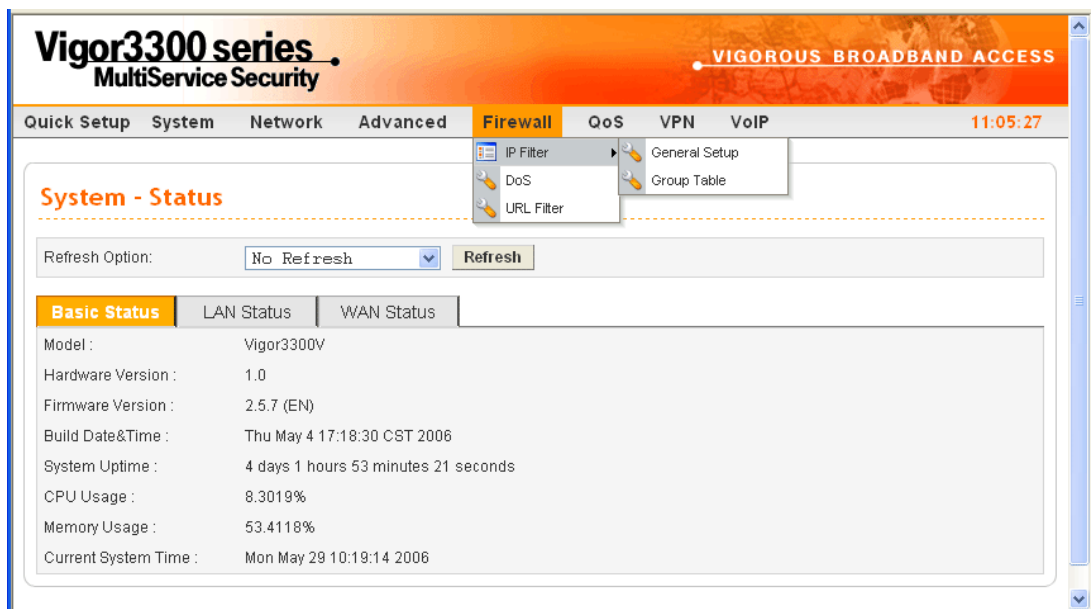
1	
Trap server :	<input type="text" value="192.168.1.100"/>
Trap community :	<input type="text" value="public"/>
Trap server port :	<input type="text" value="2048"/>

- 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.

3.4 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.



3.4.1 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.

Firewall - General Setup

Data Filter : Disable Enable

Start Filter Group : Pass
Pass
Block

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 Allows 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 Displays the group name.

Next Group Displays next group name.


Comment Displays the notice for current group.

Add Allows you to add a new IP filter table.

Edit Allows you to edit selected IP filter table.

Delete Allows 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**.



The screenshot shows a web interface titled "Firewall - IP Filter Table". Below the title is a dashed orange line. The main form area has a light gray background and contains three input fields: "Group Name" (a text box), "Next Group Name" (a dropdown menu with "none" selected), and "Comment" (a text box). At the bottom right of the form are two buttons: "Apply" and "Cancel".

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 select 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**.



The screenshot shows the same "Firewall - IP Filter Table" interface as above, but with the "Group Name" field containing the text "Pass", the "Next Group Name" dropdown menu set to "Block", and the "Comment" field containing "Group for pass rules". At the bottom right, there are three buttons: "Add Rule", "Apply", and "Cancel".

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

Source : IP :
Subnet Mask :
Port : -

Destination : IP :
Subnet Mask :
Port : -

Group Name :

Protocol :

Direction :

Fragment :

Action

Block or Pass :

Next Group Name :

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

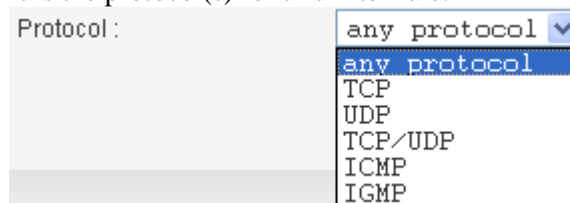
It means the port for the destination IP.

Group Name

It means the filter group for the current rule.

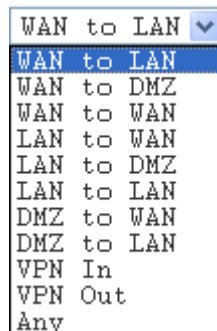
Protocol

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.



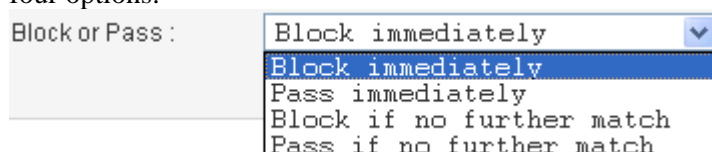
Do not care - Specifies no fragment options.

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 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 :

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	<input checked="" type="checkbox"/>

3.4.2 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.

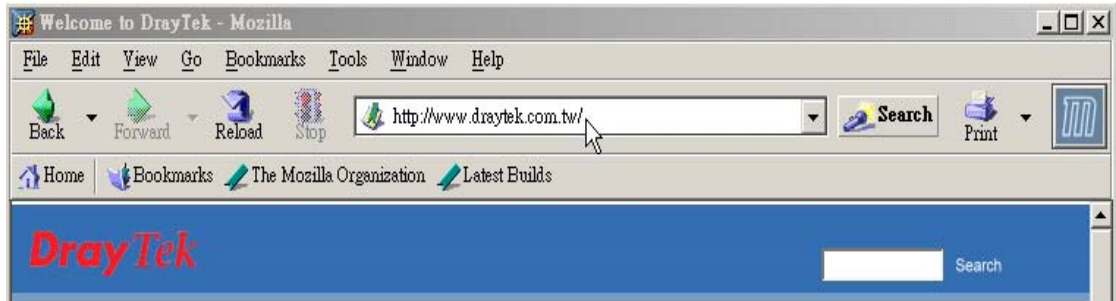
Click **Apply** to apply the settings when you finish the configuration.

3.4.3 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.

The URL content filter consists of the following functions: **URL Access Control**, **SurfControl**, **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.

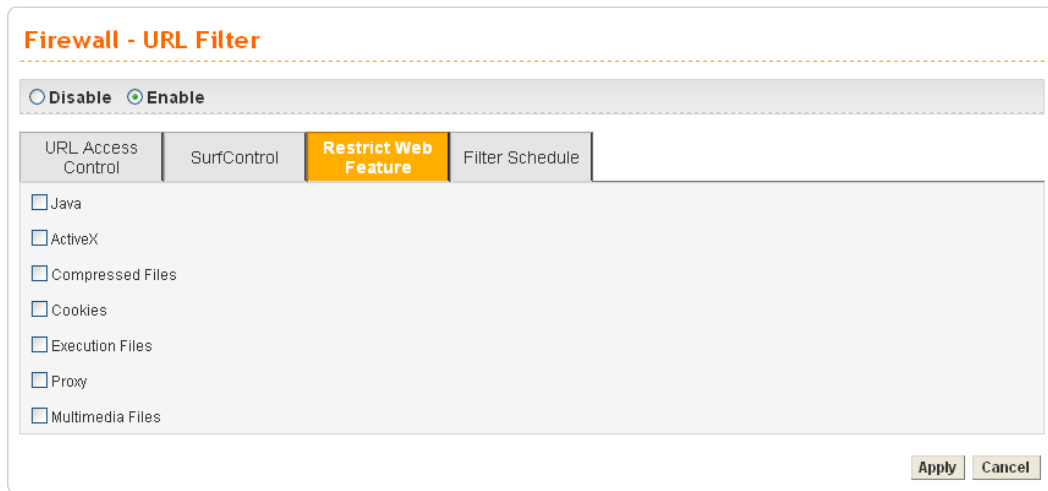
Exception List

The list of IP addresses where content filter rules are not applied.

SurfControl

SurfControl 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.

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 | SurfControl | 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.

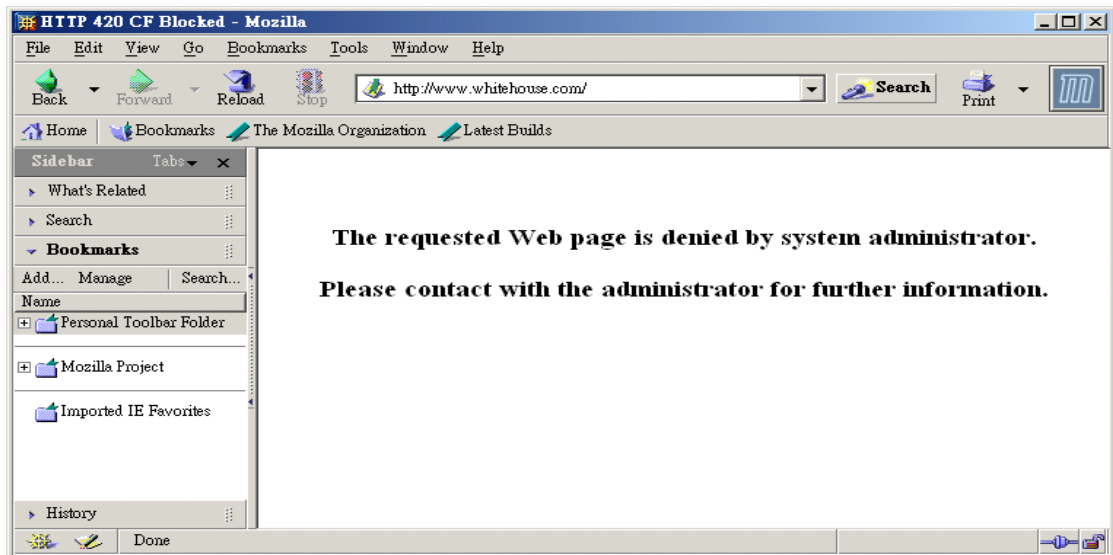
Block only at

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.

Days 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.



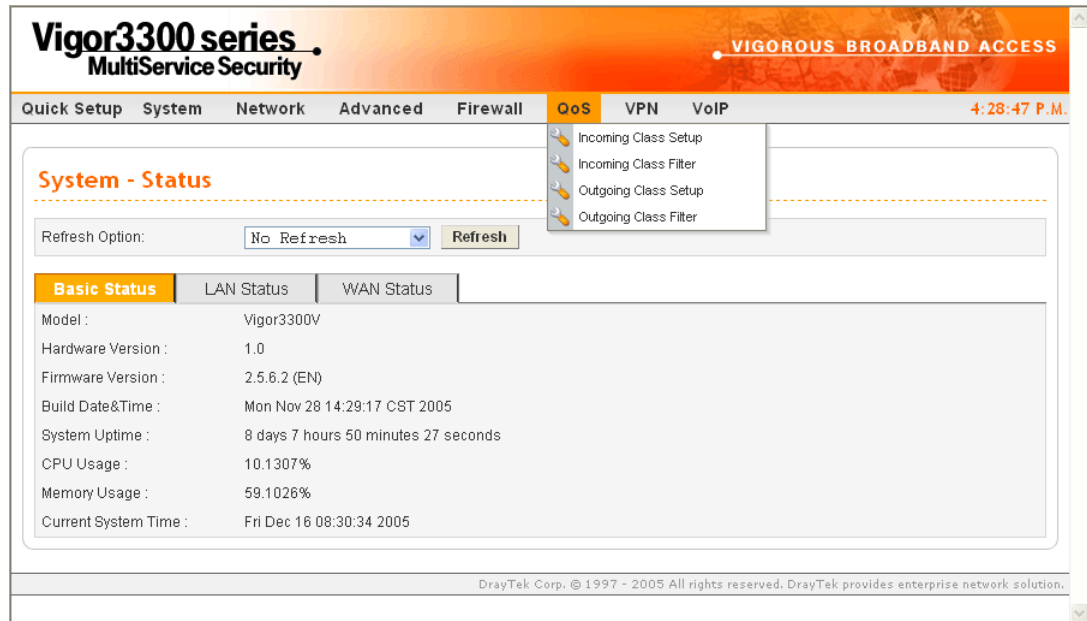
3.5 Quality of Service Setup

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 3300 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.

3.5.1 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.

3.5.2 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"/>				

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	Displays the source IP address for the filter.
Destination IP	Displays the destination IP address for the filter.
Service Type Status	Displays the service type that you choose for the filter.
DiffServ CodePoint Status	Displays the setting for DiffServ CodePoint.
Class	Displays 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: 10.1.1.1 /24

Destination IP: 10.1.2.1 /24

Service Type Status: Basic Advanced None

Service Type: FTP(TCP:20,21)

Protocol: TCP

Port:

DiffServ CodePoint Status: Basic Advanced None

DiffServ CodePoint Type: BE

DiffServ CodePoint: 0x (Hex)

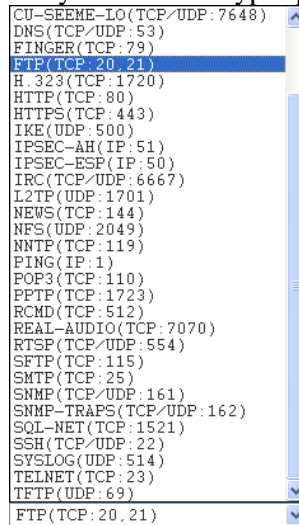
Class: undefined

Apply Cancel

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.



Protocol

There are three options: **TCP**, **UDP**, and **TCP/UDP**. Choose the one you need.

Port

Type the port number for this filter.

DiffServ CodePoint Status

There are three options:

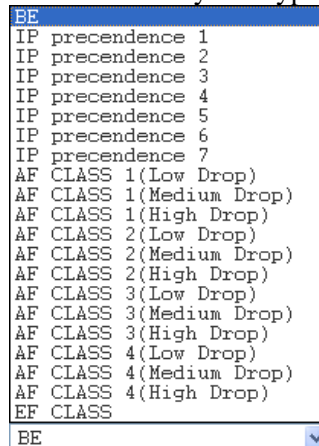
Basic – Only the **DiffServ CodePoint Type** field can be configured.

Advanced – Only the **DiffServ CodePoint** field can be configured.

None –No field is allowed to be configured.

DiffServ CodePoint Type

There are twenty-one types supported.



DiffServ CodePoint

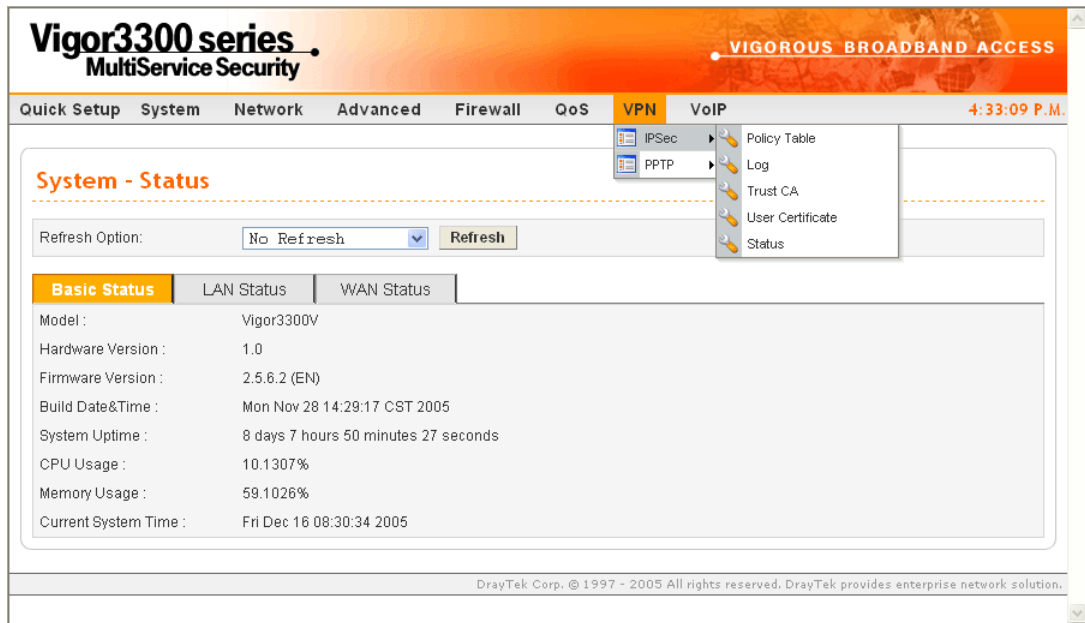
The number (by hex mode) to be applied.

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.

3.6 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 Vigor 3300, 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.

3.6.1 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.

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	Research	172.16.3.228/32	172.16.2.1	172.16.2.15/32	WAN1	enable	down	Initiate
2								
3								
4								
5								
6								
7								
8								
9								
10								

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 table, 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 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


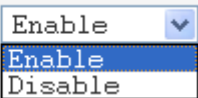
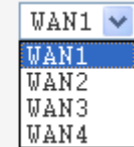
The name for VPN connection (ex. “VPN1”). The maximum length of name is 20 characters including spaces.

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	<p>AH - Specify the IPSec protocol for the Authentication Header protocol. The data will be authenticated but not be encrypted.</p> <p>ESP - Specify the IPSec protocol for the Encapsulating Security Payload protocol. The data will be encrypted and authenticated.</p> <p>Security Protocol : </p>
NAT Traversal	<p>Click Enable to let multi IPSec tunnels passing through this router.</p> <p>Click Disable to close this function.</p> <p>NAT Traversal : </p>
WAN Interface	<p>The WAN interface to be used.</p> <p>WAN Interface : </p>
Local Certificate	<p>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.</p>
Security Gateway	<p>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”.</p>
Network IP / Subnet Mask	<p>The subnet behind the local gateway.</p>
Next Hop	<p>The IP address of the next hop. The keyword default can be used to represent the gateway IP address of the selected WAN Interface.</p>
Remote ID	<p>The identification number for the remote gateway.</p>
DHCP-over-IPSEC	<p>Turns this function ON or OFF.</p>
Security Gateway	<p>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.</p>
Network IP / Subnet Mask	<p>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.</p>

- **For Advanced Configuration**

Click **Advanced** tab. The following page of default configuration will be shown:

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.

Accepted Proposal :

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	Research	172.16.3.228/32	172.16.2.1	172.16.2.15/32	WAN1	enable	down	Initiate
2								
3								
4								
5								
6								
7								
8								
9								
10								

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.

Log

At any time, you can click **VPN > 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

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		

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

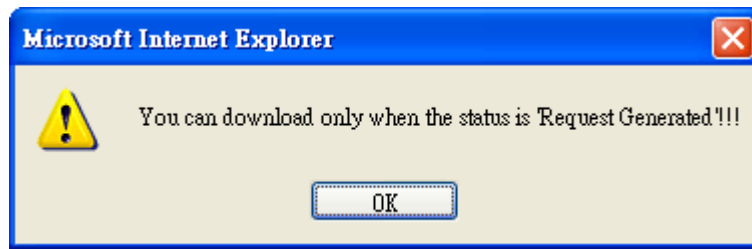
e-mail

Key Size Bits

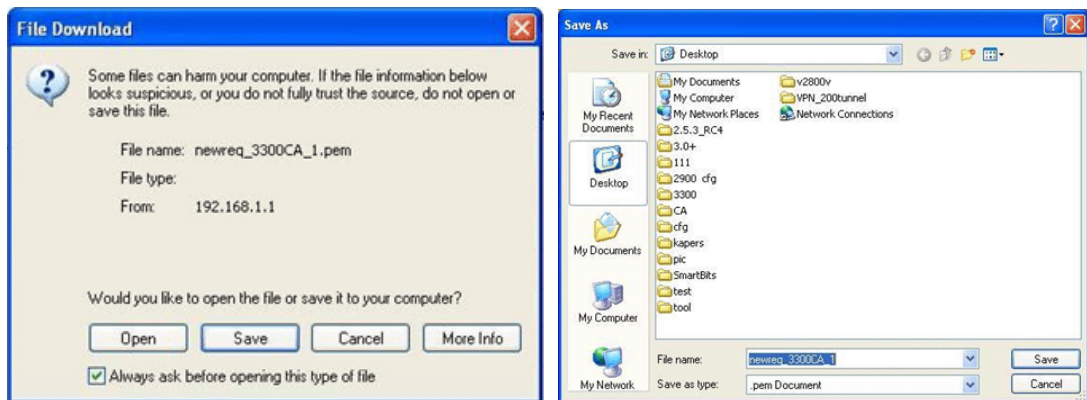
- Certification Name** The name of the certification entry.
- ID Type** The ID type for this entry. There are three types:
Domain Name: Certificated by domain name.
IP: Certificated by IP address.
Email: Certificated by email address.
- ID Value** The ID value for this entry.
- Organization Unit** The 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.

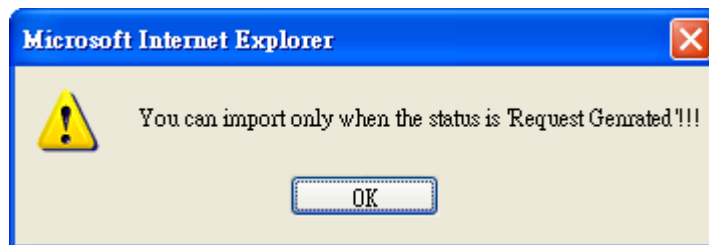
- **To download a user certificate**, please click index number one (with the status of Request Generated) and click the **Download** button. If not, you might see the following dialog to warn you.



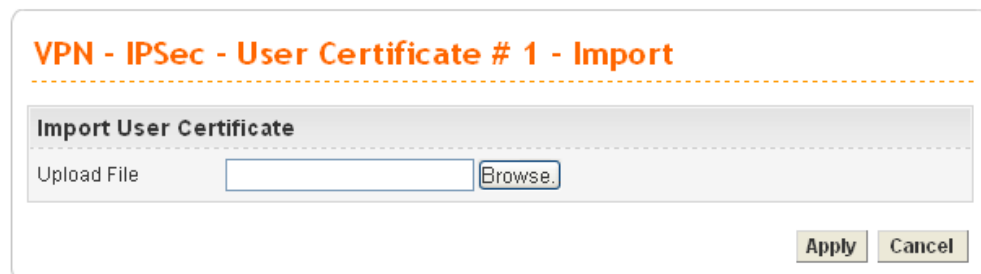
After you click the **Download** button, the system will guide you to save the downloaded file (newreq_RD-computer_1.pem) to a place that you assign.



- **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.



- **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

[Back](#)

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

[Refresh](#) [Disconnect](#)

Name	Displays the name of the IPsec tunnel.
Status	Displays the status of the tunnel (up or down).
Algorithm	Displays the algorithm used by this IPsec.
Remote IP	Displays remote IP address of the tunnel.
Remote Subnet	Displays remote subnet mask of the tunnel.
Packet In	Displays the packets count received by this tunnel.
Byte In	Displays the bytes count received by this tunnel.
Packet Out	Displays the packets count sent out by this tunnel.
Byte Out	Displays the bytes count sent out by this tunnel.
Uptime	Displays the time duration since the tunnel is established.
Refresh	Allows you to refresh current VPN status.
Disconnect	Allows you to disconnect the select VPN connection.

3.6.2 PPTP

General Setup

To configure the general setup, please click **VPN -> PPTP->General Setup**.

VPN - PPTP - General Setup

Status : Active Inactive

PPTP Authentication : PAP

PPTP Encryption : No Encryption

User Authentication : Local RADIUS Server

Mutual Authentication

Enable Disable

User Name : draytek

Password :

Apply Cancel

Status

Sets the function to **Active** or **Inactive**.

PPTP Authentication

Allows you to choose an authentication mode to be used. The default setting is **CHAP**.

PPTP Authentication : PAP

- PAP
- CHAP
- MS-CHAP
- MS-CHAP-V2

PPTP Encryption

Allows 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.

PPTP Authentication : MS-CHAP

PPTP Encryption : No Encryption

- No Encryption
- MPPE 40 bits
- MPPE 40 bits / 128 bits

User Authentication

Sets user authentication to **Local** server or **RADIUS** server.

Enable/Disable

Enables or disables the **Mutual Authentication** function.

User Name

Type in user name that the other side provides for carrying out mutual authentication whenever you want.

Password

Type in password that the other side provides for carrying out mutual authentication whenever you want.

When you finish the configuration, please click **Apply** to invoke it.

Group Table

To create a VPN PPTP group table, click the **Group Table** option under the **PPTP** menu.

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.

Authentication

This page allows you to set up to 30 sets of accounts for authentication.

VPN - PPTP - Authentication

#	User Name	Group
1	<input 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"/>	

User Name The user name for this entry.

User Password The password for this entry.

Group The group for this entry.

Edit Allows you to edit the selected group. Type in user name and password, then choose a proper group (A, B, C or D that configured in **PPTP>>Group Table**) for this entry. Next, click **Apply**.

VPN - PPTP - Authentication - Edit

1

User Name :

User Password :

Group : ▼

Type username, password and choose proper group for this entry. When you finish it, click **Apply**.

Delete

Allows you to remove the selected group.

Delete All

Allows you to remove all of the groups.

When you finish the configuration, please click **Apply** to invoke it.

Status

This page displays some relevant information about PPTP connection. It will refresh automatically every 10 seconds.

VPN - PPTP - 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

Displays the index number of the tunnel.

Remote IP

Displays remote IP address of the tunnel.

Assigned IP

Displays IP address assigned by Vigor3300.

User

Displays user account of this tunnel.

Byte In

Displays the bytes count received by this tunnel.

Byte Out

Displays the bytes count sent out by this tunnel.

Uptime

Displays the time duration since the tunnel is established.

Refresh

Allows you to refresh current VPN PPTP status.

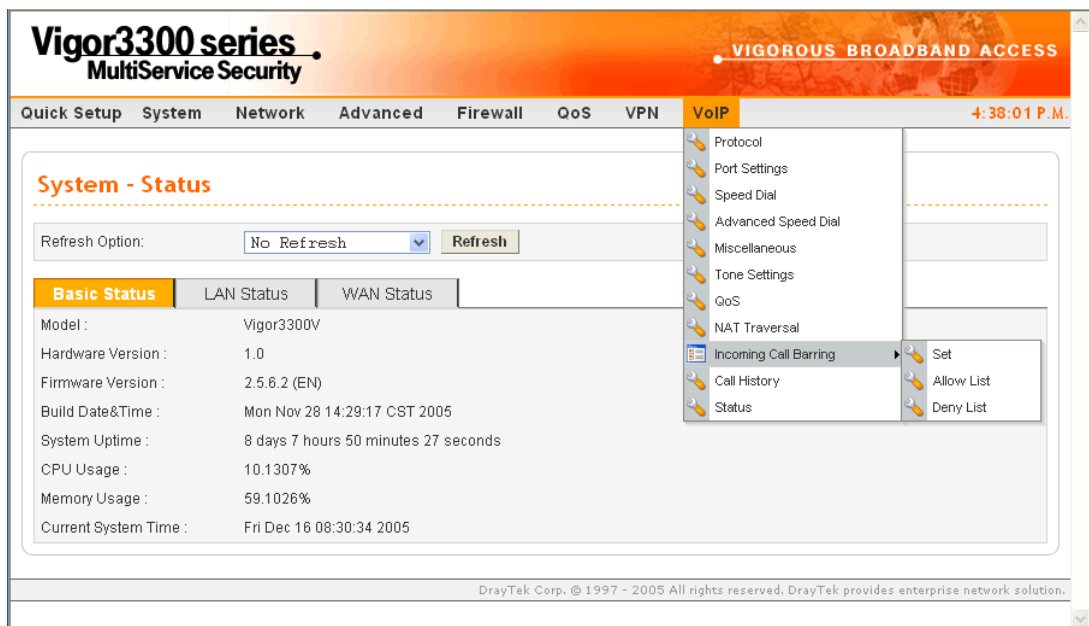
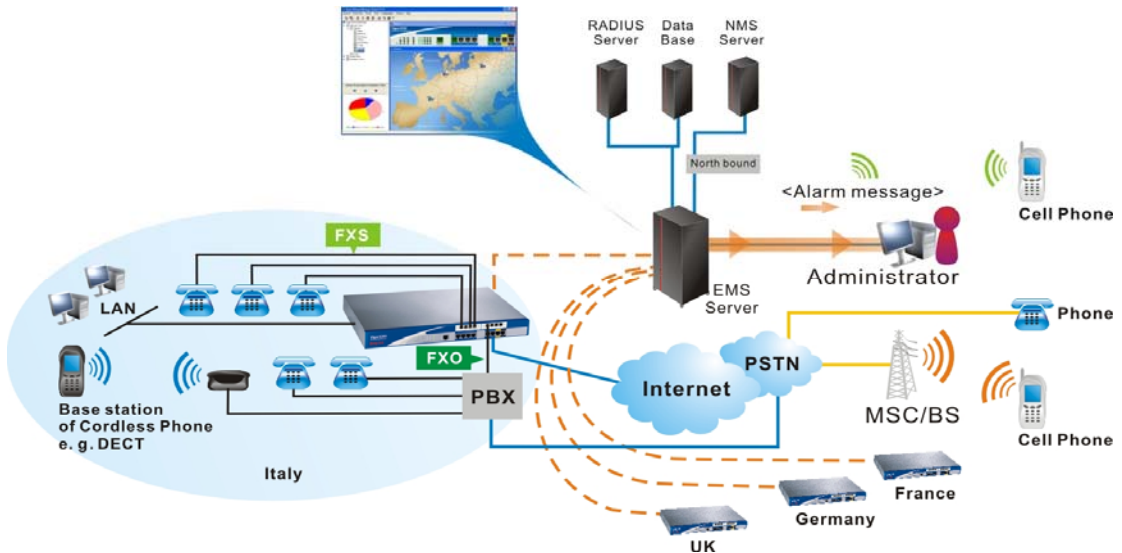
Disconnect

Allows you to disconnect the select VPN PPTP connection.

3.7 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.

The Vigor3300/Vigor3300V provides cost effective voice solution for SME customers which can be explained with the following diagram.



3.7.1 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.

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 checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="text"/>	<input type="text" value="0"/>	<input type="text" value="5060"/>	<input type="text" value="0"/>	<input type="text" value="5060"/>	<input type="text" value="300"/>	<input type="text" value="0"/>
2.	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="text"/>	<input type="text" value="0"/>	<input type="text" value="5060"/>	<input type="text" value="0"/>	<input type="text" value="5060"/>	<input type="text" value="300"/>	<input type="text" value="0"/>
3.	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="text"/>	<input type="text" value="0"/>	<input type="text" value="5060"/>	<input type="text" value="0"/>	<input type="text" value="5060"/>	<input type="text" value="300"/>	<input type="text" value="0"/>
Example			iptel	iptel.org		iptel.org			iptel.org

For SIP Configuration

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 timeout value for SIP protocols. The default value is 300.

Domain Type the IP address or domain name of the SIP Domain/Realm.

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/#@

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









- 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.

3.7.2 Port Settings

Port Settings page allows users to set phone number and phone groups for different call receivers.

For Phone Number

VoIP - Port Settings							
Phone Number		Group					
#	Edit	Type	Active	Group	Username	Proxy	Codec
1		FXS	V	1	1001		G.729A-8kbps
2		FXS	V	2	1002		G.729A-8kbps
3		FXS	V	3	1003		G.729A-8kbps
4		FXS	V	4	1004		G.729A-8kbps
5		FXS	V	5	1005		G.729A-8kbps
6		FXS	V	6	1006		G.729A-8kbps
7		FXS	V	7	1007		G.729A-8kbps
8		FXS	V	8	1008		G.729A-8kbps

Edit

Click this button to access into the Edit page for each phone number.

Type

Displays the type of the VoIP connection.

Active

Displays the status (active or not) for the VoIP connection.

Group

Displays the group number of the VoIP connection.,

Username

Displays the username that you typed for the VoIP connection.

Proxy

Displays the proxy information that you set on **VoIP >> Protocol** page for the VoIP connection.

Codec

Displays the codec settings for the VoIP connection.

When you click **Edit**, the following page will appear for you to configure.

VoIP - Port Settings - Port1 - Edit

Port 1 (FXS)

Disable Enable

Username:

Password:

Display Name:

Authentication ID:

Proxy Server:

VoIP IP Address:

Hotline

Hotline Number to Internet:

Hotline Number to PBX/ PSTN:

FXO

Manual Disconnection:

Codec

Preferred Codec:

Single Codec:

Codec Rate: (ms)

Codec VAD: Disable Enable

CAS

Microphone Gain: (Range: -32 ~ 31)

Speaker Gain: (Range: -32 ~ 31)

FAX

FAX Mode:

FAX Bypass Codec:

FAX Bypass Codec Rate: (ms)

DTMF

DTMF Mode: InBand OutBand(RFC2833) SIP INFO

DTMF Volume: (Range: 0 ~ 31)

Call Forwarding

Disable

Call forwarding all calls

Call forwarding busy

Call forwarding no answer after rings (Range:1~10)

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

Port 1 (FXS)

Click **Enable** to activate this port or **Disable** to close this port.

User Name – Type the user name (a number) for each phone line.

Password - Type the user password for each phone line.

Display Name - Type the user name to be displayed on another phone terminal.

Authentication ID - Type the characters for authenticate this port.

Proxy Server - Type the SIP proxy server to be applied on this port.

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.

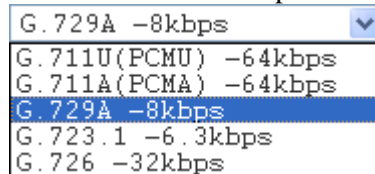
Hotline Number to PBX / PSTN- Pre-set a phone number to make the port dialing out to PBX/PSTN automatically.

FXO

Manual Disconnection - Click **Disconnect** to disconnect this phone line by manual.

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

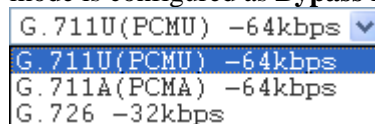
FAX Mode -The FAX function mode. There are three options:
Transparent: FAX will be transmitted via voice channel; no fax relay and no Codec change will be involved.

T.38 Relay: Using T.38 Fax Relay. This is the default value.

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.



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.

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 to receive forwarded calls.

Apply

When you finish all the configurations, please click this button to activate them.

For Group

It is very important to provide a Group function for voice service within a company. Customers can simultaneously call the same phone number. When the Vigor3300 gets a phone call, which is configured in the first port of a group from Internet, it will ring all available ports belonging to this group to provide voice service at the same time. It is easier for the customer to remember just one phone number corresponding to the company. By enabling this function, the 4- or 8-port VoIP will use the first enabled port phone setting on the table as their phone number.

Up to 8 groups can be configured and assigned a specific phone line. Each phone line must be unique and cannot be overlapped as shown below.

VoIP - Port Settings

Phone Number **Group**

Group : Disable Enable

Group	Port							
	1	2	3	4	5	6	7	8
1	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
2	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
3	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
4	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
5	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
6	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
7	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
8	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>

Incoming Call Rings

Rings all ports in the group Rings the first available port

Rings all ports in the group Click this radio button to make all ports in the same group ringing while receiving incoming calls.

Rings the first available port Click this radio button to make the first available port in the same group ringing while receiving incoming calls.

Default Group Click this button to return to the factory group settings.

3.7.3 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.

VoIP - Speed Dial

#	Speed Dial Phone Number	Speed Dial Destination	Memo
1	<input type="text" value="1001"/>	<input type="text" value="1001@iptel.org"/>	<input type="text" value="dial 1"/>
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 >

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.

3.7.4 Advanced Speed Dial

Speed dial allows users to call out with simple buttons instead of dialing long numbers. To set a speed dial with specified settings, please open the following page.

#	Prefix	Strip Length	Append	Destination	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"/>				

- Prefix** Displays the prefix number of the entry.
- Strip Length** Displays the strip length of the entry.
- Append** Displays the appended number of the entry.
- Destination** Displays the IP address of the destination of the entry.
- Memo** Displays the brief description stated in memo field of the entry.
- Edit** Click this button to access into the editing page of the speed dial.
- Delete/Delete All** Click this button to delete the selected setting or all settings.

To configure one entry, please click **Edit** to open the following page.

1

Prefix:

Strip Length:

Append:

Destination:

Memo:

- Prefix** Assign a prefix for checking the phone number that users dial out. If the prefix of the outgoing call matches to the number set in this field, that outgoing call can apply the speed dial. For example, suppose that there are two outgoing calls with phone

numbers of 03654321 and 04556890. In which, 03654321 is suitable for this speed dial rule.

Strip Length

Assign the length of digit to be removed from the original phone number. For example, suppose the original phone number is 03654321 and the strip length is 2. The first two numbers (03) will be removed and the final phone number becomes 654321.

Append

Assign a new number to be added before the phone number (after removing length of digit). For example, suppose the original phone number is 03654321. The strip length is 2 and the append number is 886. Then, the final phone number will be 886654321.

Destination

Assign an IP address for the destination which the SIP message would be sent to.

Memo

A description for this entry.

3.7.5 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: 13456

T.38 Starting Port: 49170

T.38 Redundancy number: 1 (Range: 0~4)

Dialing Completion Timeout: 4 sec (Range: 1~60)

VoIP ToS: 0x a0

Line Polarity Reversal as Callee Answer:

FXO auto disconnection if no packet is received in 3 minutes (Range: 1~60, 0: no auto disconnection)

FXS Ringing

Ringing Frequency: 25 (HZ)

Ringing Cadence - On: 2000 (msec)

Ringing Cadence - Off: 4000 (msec)

Apply Cancel

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

Users might dial with incomplete phone number and wait for

- Timeout** 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 as Callee Answer** Check this box to generate line polarity reversal while the remote user picks up the phone call.
- 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.
- Ringling Frequency** Please select a proper setting as the ringing frequency.
- Ringling Cadence - On** Determines the length of the ringing time for incoming calls.
- Ringling Cadence - Off** Determines the length for the incoming calls to stop ringing.

3.7.6 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: Finland Caller ID Type: DTMF

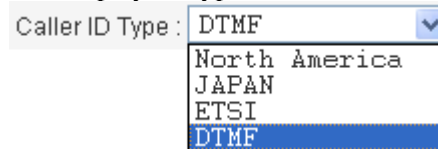
Tone Classification	Low Frequency(Hz)	High Frequency(Hz)	TOn1 (10msec)	TOff1 (10msec)	TOn2 (10msec)	TOff2 (10msec)
Dial tone	<input style="width: 50px;" type="text" value="425"/>	<input style="width: 50px;" type="text" value="0"/>	<input style="width: 50px;" type="text" value="500"/>	<input style="width: 50px;" type="text" value="0"/>	<input style="width: 50px;" type="text" value="0"/>	<input style="width: 50px;" type="text" value="0"/>
Ringing tone	<input style="width: 50px;" type="text" value="425"/>	<input style="width: 50px;" type="text" value="0"/>	<input style="width: 50px;" type="text" value="0"/>	<input style="width: 50px;" type="text" value="0"/>	<input style="width: 50px;" type="text" value="100"/>	<input style="width: 50px;" type="text" value="400"/>
Busy tone	<input style="width: 50px;" type="text" value="425"/>	<input style="width: 50px;" type="text" value="0"/>	<input style="width: 50px;" type="text" value="0"/>	<input style="width: 50px;" type="text" value="0"/>	<input style="width: 50px;" type="text" value="30"/>	<input style="width: 50px;" type="text" value="30"/>
Congestion tone	<input style="width: 50px;" type="text" value="425"/>	<input style="width: 50px;" type="text" value="0"/>	<input style="width: 50px;" type="text" value="0"/>	<input style="width: 50px;" type="text" value="0"/>	<input style="width: 50px;" type="text" value="20"/>	<input style="width: 50px;" type="text" value="20"/>

Region

Choose the country area that the Vigor3300 located for using VoIP feature. Or, select **User Defined** for proprietary settings.

**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.

**Dial tone**

A tone means the phone line is ready to make a call.

Ringling 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.

3.7.7 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).

3.7.8 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.

3.7.9 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.

Barring Class

There are five options for incoming calls from remote ends.

Choose either one of them to set the barring class.

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.

VoIP - Incoming Call Barring - Deny List

#	Name	IP/Domain
1	<input type="text" value="James"/>	<input type="text" value="172.16.3.221"/>
2	<input type="text" value="Steven"/>	<input type="text" value="arctel.com"/>
3	<input type="text"/>	<input type="text"/>
4	<input type="text"/>	<input type="text"/>
5	<input type="text"/>	<input type="text"/>
Example	John	192.168.1.1 or iptel.org

1 2 3 4 5 6

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.

3.7.10 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

#	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
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)

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.

3.7.11 Status

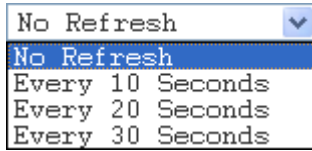
This page displays the connection status for VoIP phone calls.

VoIP - Status													
Refresh Option: <input type="button" value="No Refresh"/> <input type="button" value="Refresh"/>													
#	Register Status	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		Idle											
2		Idle											
3		Idle											
4		Idle											
5		Idle											
6		Idle											
7		Idle											
8		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)

Register Status	The status of registering in proxy server.
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.

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.



4

Trouble Shooting

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

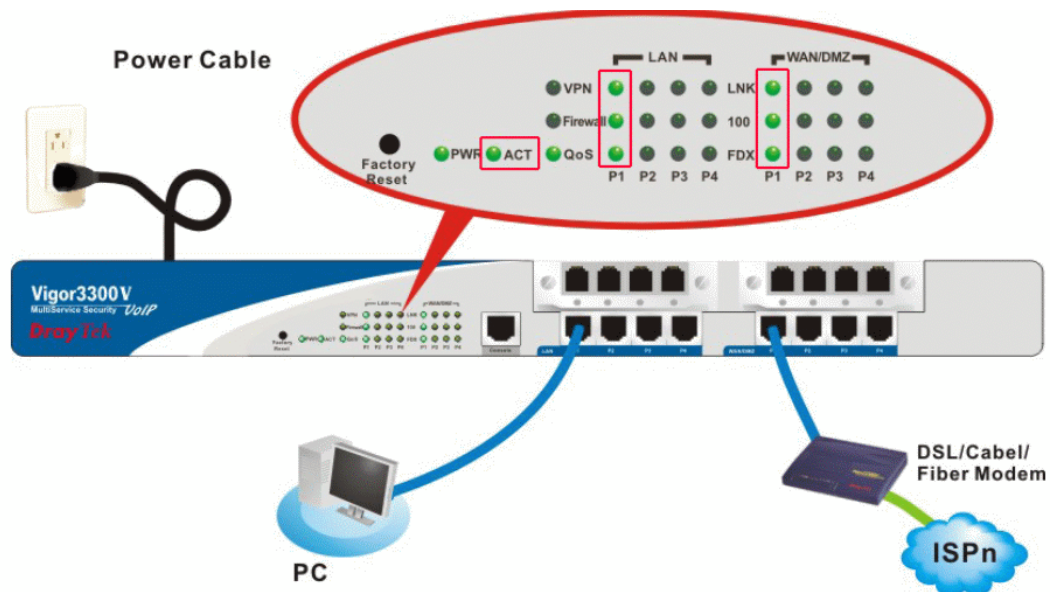
- Checking if the hardware status is OK or not.
- Checking if the Network Connection Settings on your computer is OK or not.
- Pinging the Router from your computer.
- Checking if the ISP Settings are OK or not.
- Backing to factory default setting if necessary.

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

4.1 Checking If the Hardware Status Is OK or Not

Follow the steps below to verify the hardware status.

1. Check if the power line and WLAN/LAN cable connections is OK.
If not, refer to “**2.1 Hardware Installation**” for reconnection.
2. Turn on the router. Make sure the **ACT LED** blinks once per second and the correspondent **WAN/LAN LED** is bright.



3. If not, there must be something wrong with the hardware connection. Simply back to “**2.1 Hardware Installation**” to execute the hardware installation. And then, try again.

4.2 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

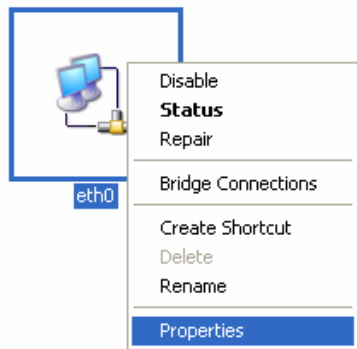


The example is based on Windows XP. As to the examples for other operation systems, please refer to the similar steps or find support notes in www.draytek.com.

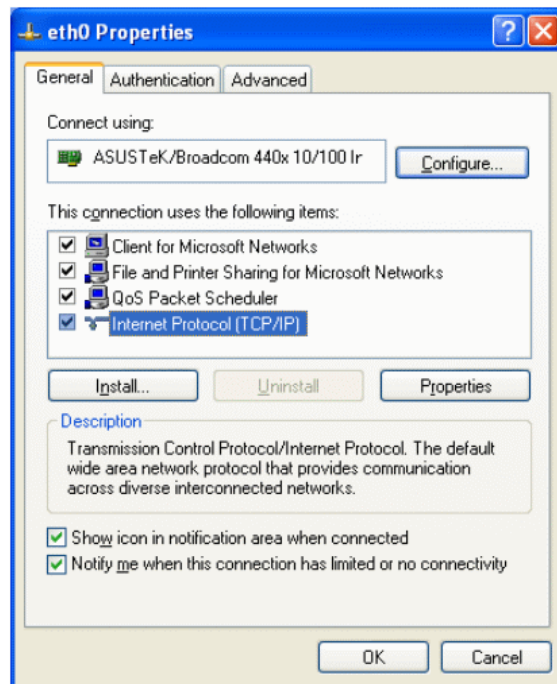
1. Go to Control Panel and then double-click on Network Connections.



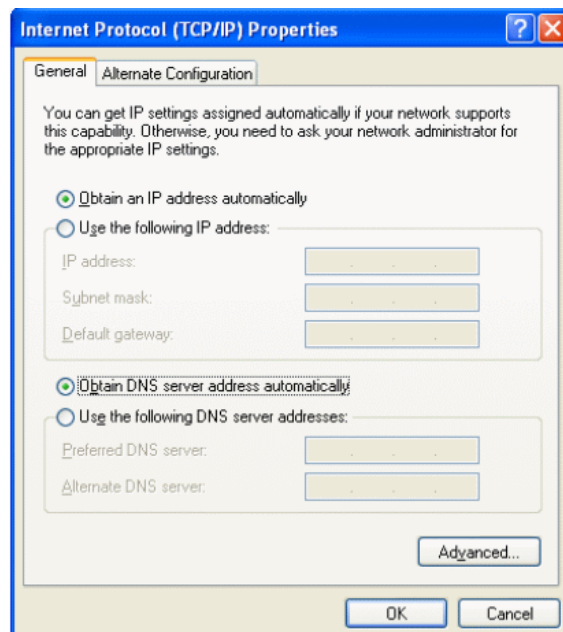
2. Right-click on Local Area Connection and click on Properties.



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

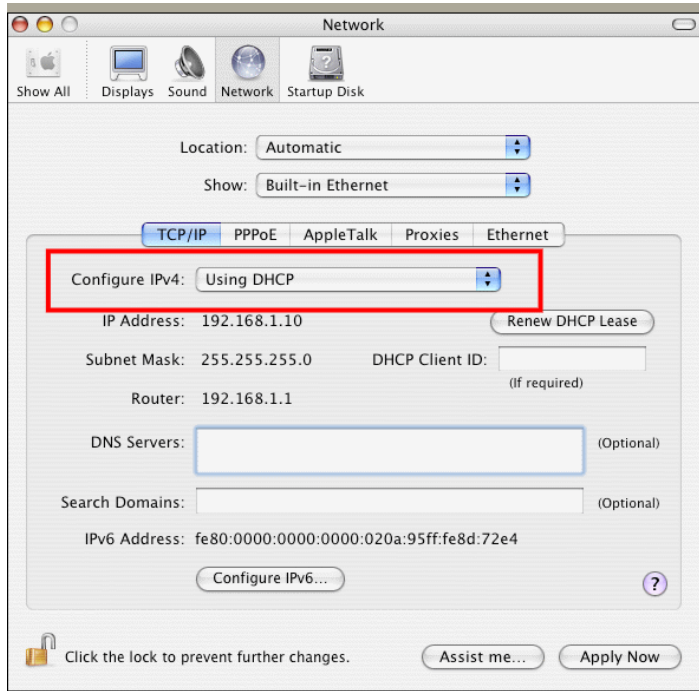


4. Select **Obtain an IP address automatically** and **Obtain DNS server address automatically**.



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.



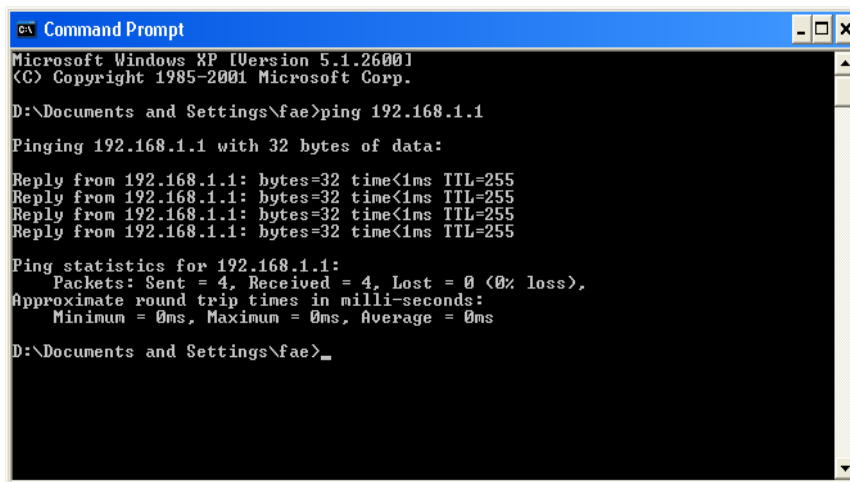
4.3 Pinging the Router from Your Computer

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 for this command is that the computer will receive a reply from 192.168.1.1 for correct link.** 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 3.2)

Please follow the steps below to ping the router correctly.

For Windows

1. Open the **Command Prompt** window (from **Start menu>> Run**).
2. Type **command** (for Windows 95/98/ME) or **cmd** (for Windows NT/ 2000/XP). The DOS command dialog will appear.



```
ca Command Prompt
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=25** 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.

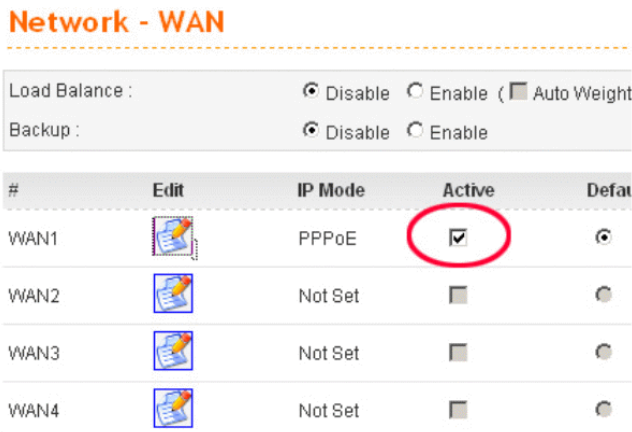
```

Terminal — bash — 80x24
Last login: Sat Jan  3 02:24:18 on ttty1
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$ █

```

4.4 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.



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="889966666@hinet.net"/> Password : <input type="password" value="•••••"/> Authentication : <input type="button" value="PAP"/> <input type="button" value="↓"/> Service Name : <input type="text" value="hinet"/>		PPTP Local Address : <input type="text"/> PPTP Subnet Mask : <input type="text"/> PPTP Server 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"/>		

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"/> Subnet Mask : <input type="text" value="255.255.255.0"/> Default Gateway : <input type="text" value="172.16.3.1"/> Primary DNS : <input type="text" value="168.95.1.1"/> Secondary DNS : <input type="text" value="168.95.192.1"/>		Host Name : <input type="text"/> Domain Name : <input type="text"/> (Host Name and Domain Name are required for some ISPs.)

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"/>	PPTP Local Address : <input type="text" value="10.0.0.150"/>
Password :	<input type="password" value="•••••"/>	PPTP Subnet Mask : <input type="text" value="255.255.255.0"/>
Authentication :	<input type="text" value="PAP"/>	PPTP Server Address : <input type="text" value="10.0.0.137"/>
Service Name :	<input type="text"/>	

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"/>	

4.5 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 70 seconds

Reset to factory default

Apply

Hardware Reset

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



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

4.6 Contacting Your Dealer

If the router settings are correct at all, and the router still does not connect to internet, please contact your ISP technical support representative to help you for configuration.

Also, if the router still cannot work correctly, please contact your dealer for help. For any further questions, please send e-mail to support@draytek.com.

Appendix A Application for 802.1 VLAN

A.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 :

4. 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"/>

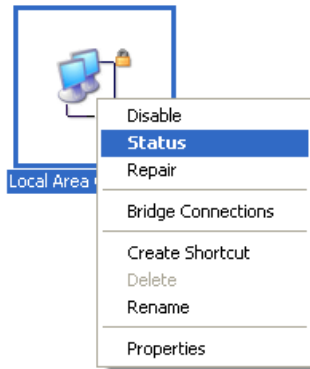
A.2 How to Check/Edit VLAN ID on Your PC?

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.

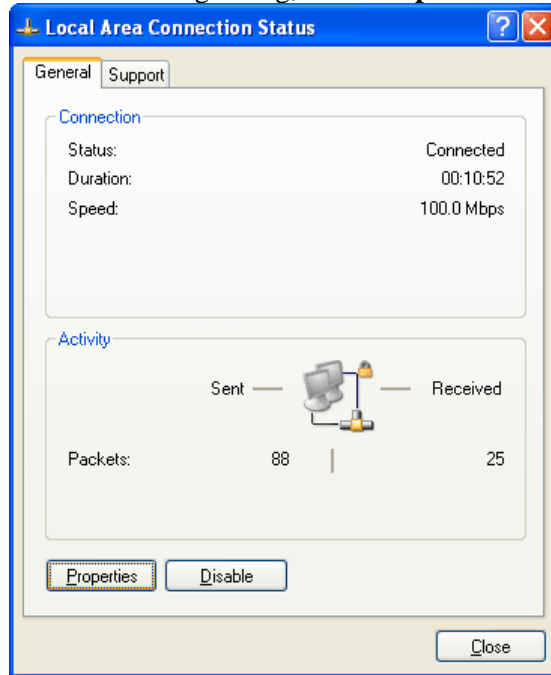
1. Go to **Control Panel** and then double-click on **Network Connections**.



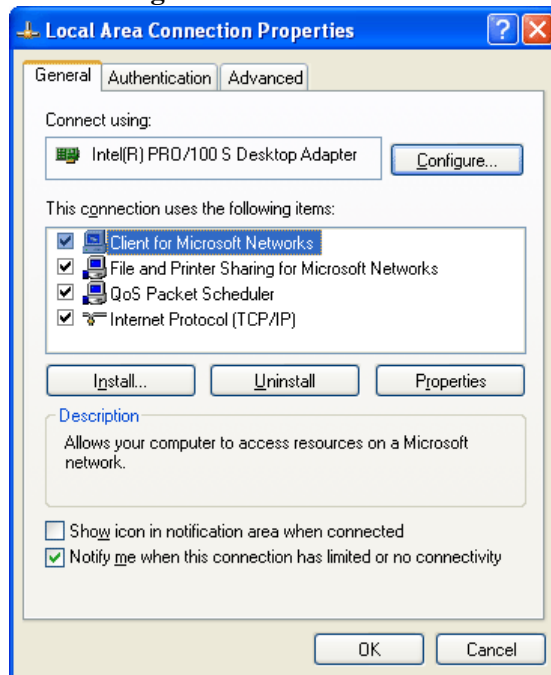
2. Right-click on **Local Area Connection** and click on **Status**.



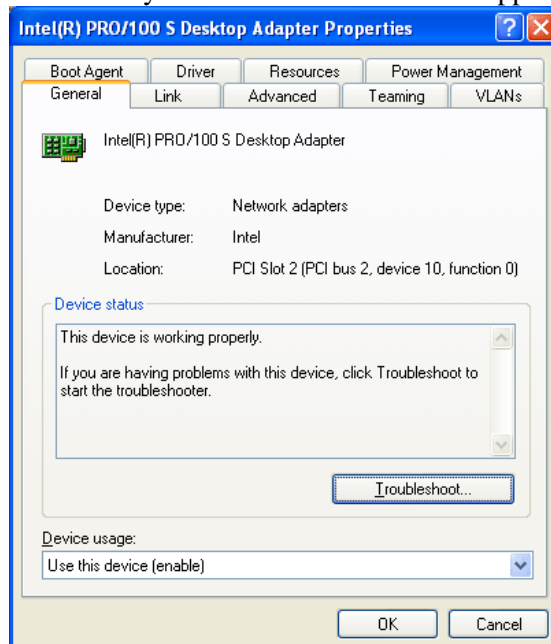
3. On the following dialog, click **Properties**.



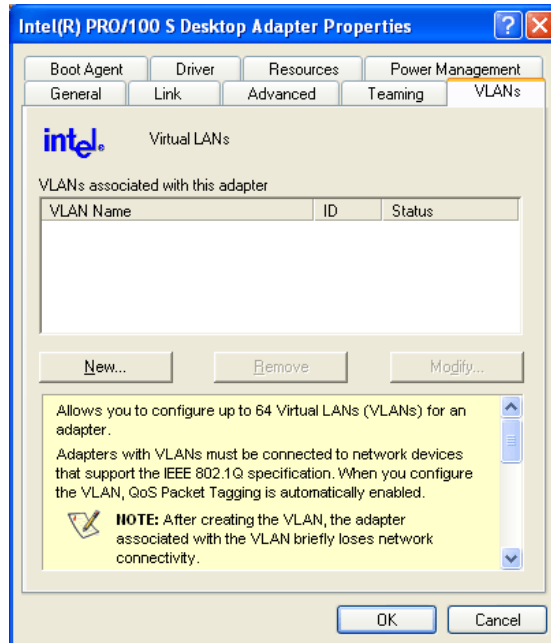
4. Click **Configure** to access into next screen.



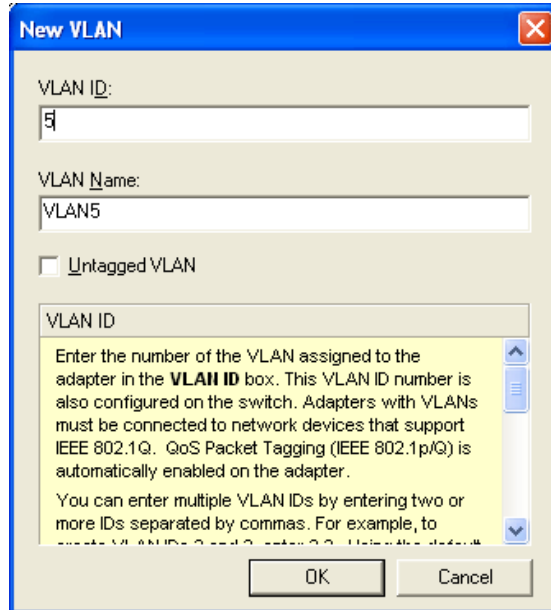
5. On this dialog box, locate **VLANs** tag and click on it. If you cannot find out VLANs tag, that means your network card does not support VLAN feature.



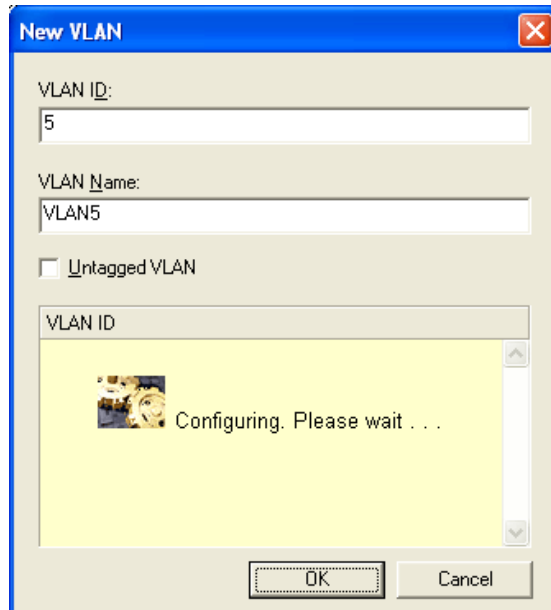
6. In this screen, there is no VALN existed. You can create a new one. Please click the **New...**button.



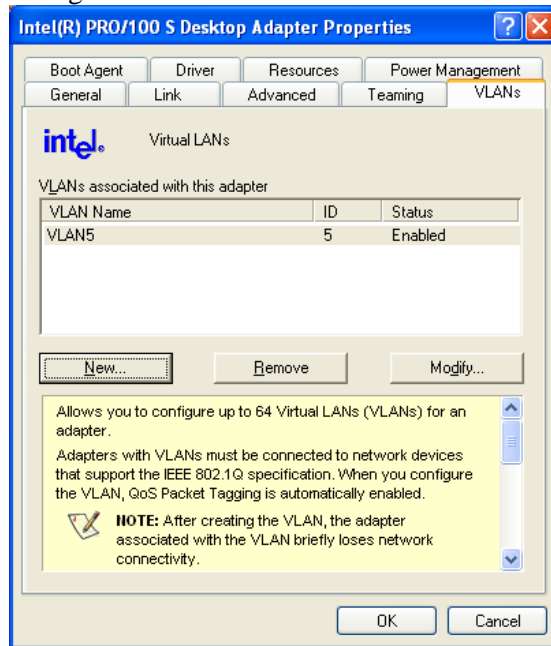
- In **New VLAN** dialog, please type a number in the box of VLAN ID. Here, “5” is entered. The corresponding VLAN Name will appear automatically. Next, click **OK** to create it.



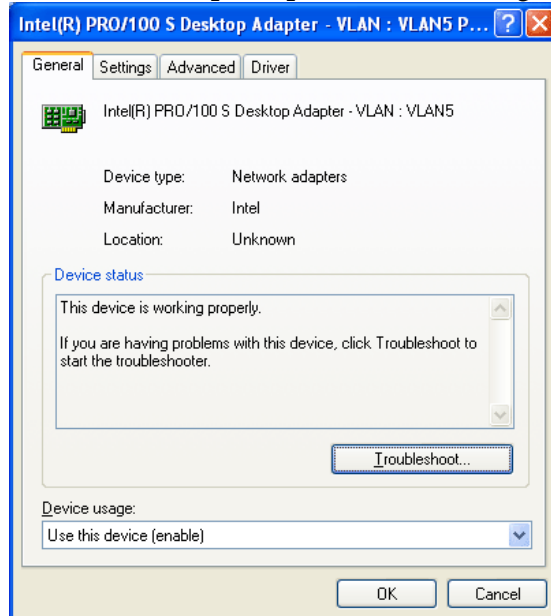
- After you click OK, the system will configure for the VLAN settings. Please wait for several seconds.



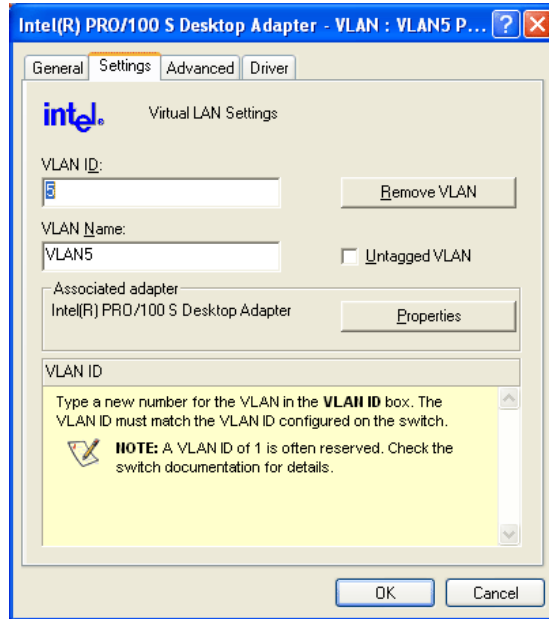
9. When the configuration is finished, the new VLAN settings with ID number and name will appear on previous dialog, **Desktop Adapter Properties**. Click **OK** to exit this dialog.



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



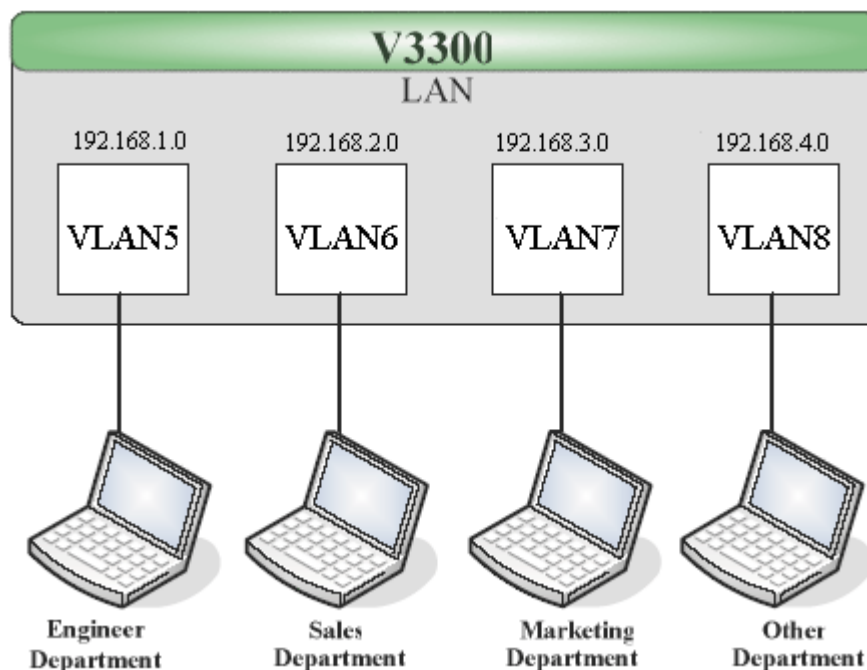
11. Next time, if you want to check VLAN setting again, please open **Settings** tag to modify it.



A.3 Applications

A.3.1 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

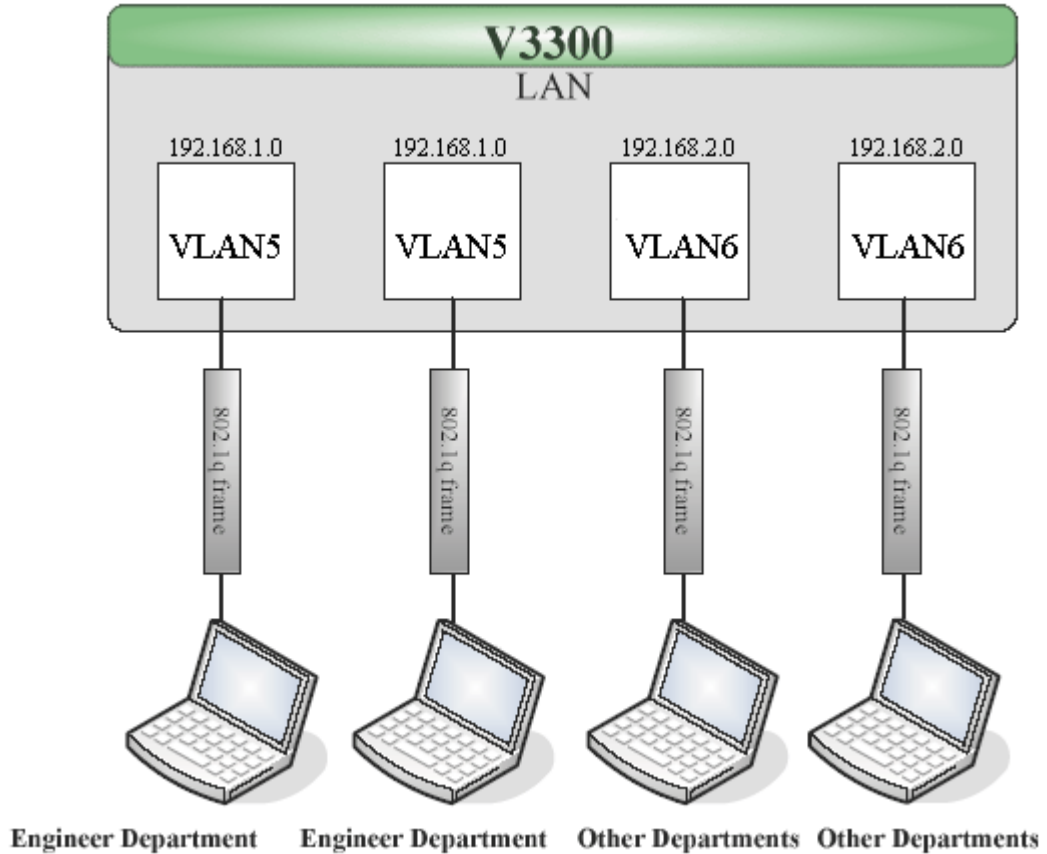
Port Setting

P1:
 P2:
 P3:
 P4:

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.

A.3.2 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

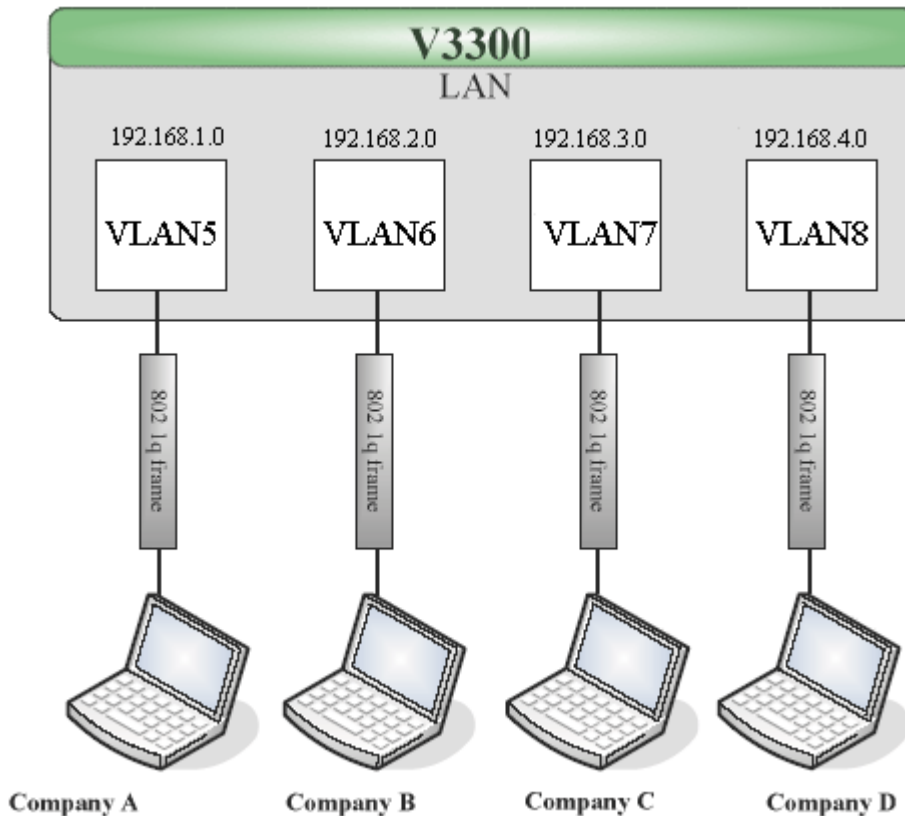
Port Setting

	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 click 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.

A.3.3 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

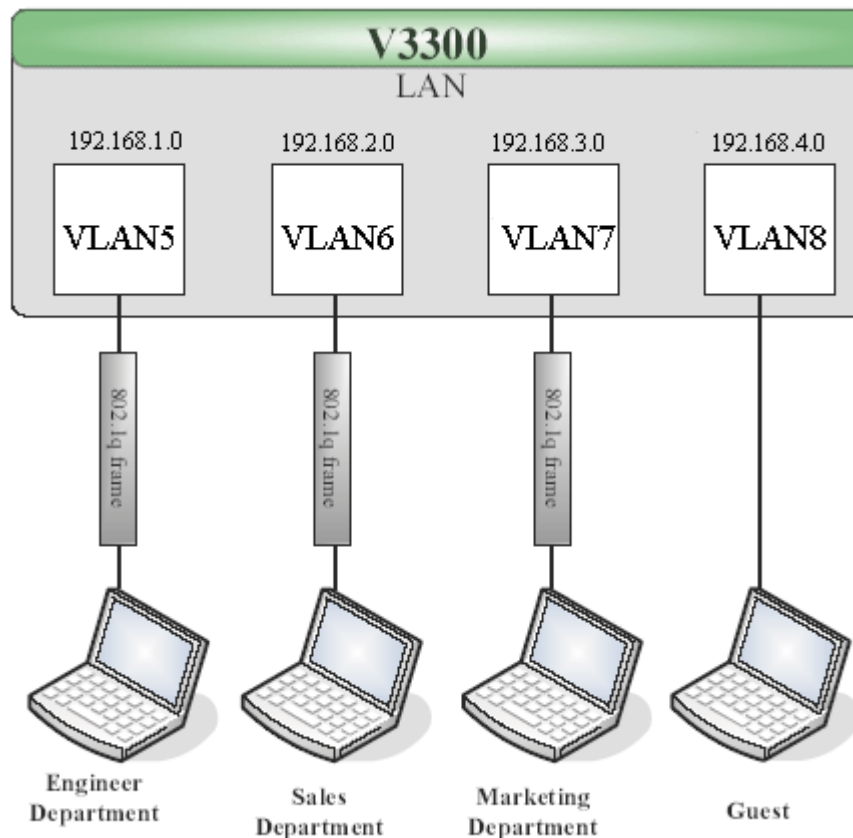
	P1	P2	P3	P4
Port VLAN ID	5	6	7	8

Apply Reset Cancel

- 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.

A.3.4 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

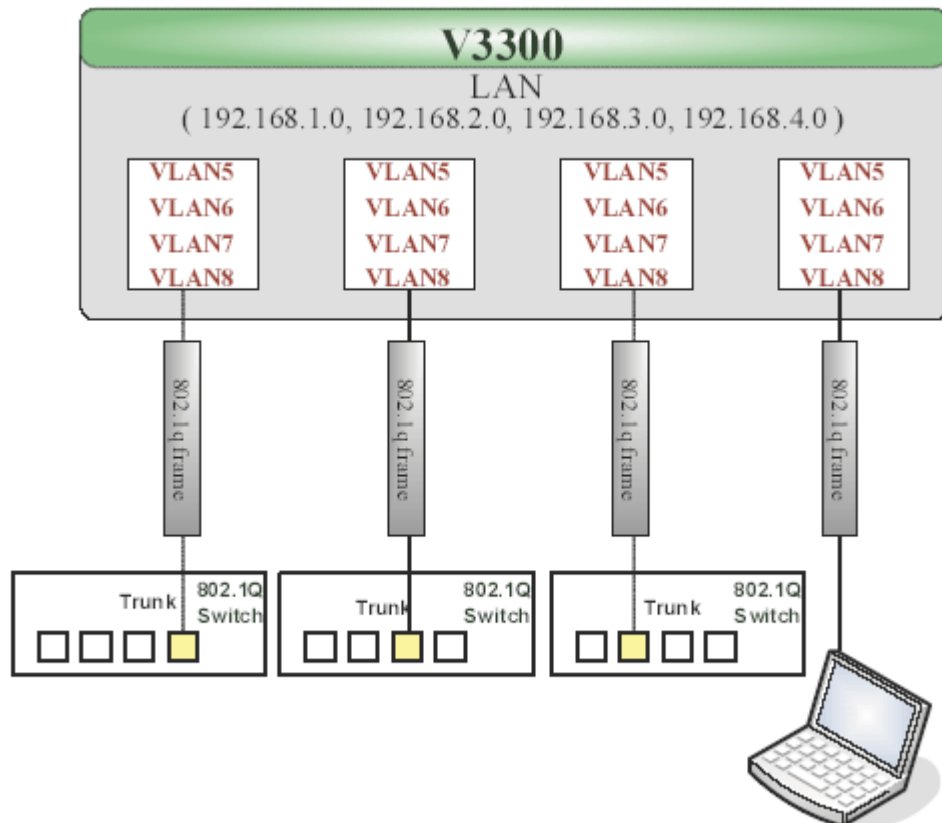
	P1	P2	P3	P4
Port VLAN ID	5	6	7	8

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.

A.3.5 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:

- 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.