Vigor3300B+, 3300, 3300V
Installation Guide

DrayTek

Table of Contents

About This User's Manual

This manual is designed to assist in using one of the Vigor 3300 series of multiservice Internet routers. The information contained in this document is subject to change without notice. If you have any inquiries, please feel free to contact our support team via E-mail, Fax or phone. For the latest product information and features, please visit our website at **www.draytek.com**

Copyright

Trademark

DrayTek is a registered trademark of DrayTek Corp. Vigor product series are trademarks of DrayTek Corp. Other trademarks and registered trademarks of products mentioned in this manual may be the properties of their respective owners and are only used for identification purposes.

Target Readers

This guide is intended for those responsible for hardware installation, and configuration for Vigor 3300 series.

DrayTek Limited Warranty

We warrant to the original end user (purchaser) that the routers will be free from any defects in workmanship or materials for a period of two (2) years from the date of purchase from the dealer. Please keep your purchase receipt in a safe place because it serves as the proof of purchase date.

During the warranty period, and upon proof of purchase, should the product have indications of failure due to faulty workmanship and/or materials, we will, at our discretion, repair or replace the defective products or components, without charge for either parts or labor, to whatever extent we deem necessary to restore the product to proper operating condition. Any replacement will consist of a new or remanufactured functionally equivalent product of equal value, and will be offered solely at our discretion. This warranty will not apply if the product is modified, misused, tampered with, damaged by an act of God, or subject to abnormal working conditions.

The warranty does not cover the bundled or licensed software of other vendors. Defects that do not significantly affect the usability of the product will not be covered by the warranty.

We reserve the right to revise the manual and online documentation and to make changes from time to time in the contents hereof without obligation to notify any person of such revision or changes.

Be a Registered Owner

Online web registration at **www.draytek.com** is preferred. Alternatively, fill in the registration card and mail it to the address found on the reverse side of the card. Registered owners will receive future product and update information.

Caution

There is the risk of explosion if an incorrect type of battery is replaced.

Dispose of used batteries according to local environmental instructions.

Safety Instructions

■ Operation Environment

- Make sure that the AC power source is in the range of AC 90-240V. The router should be used in a sheltered area, within a temperature range from 0 to +50 °C and relative humidity in the range of 10% and 90%.
- Do not expose the router to direct sunlight or other heat sources. The housing and electronic components may be damaged by direct sunlight or heat sources.

■ Installation

- Read the quick start guide and installation manual before turning on the power switch of device.
- Locate the emergency power-off switch near the device prior to power connection.
- Fixing the device on chassis to maintain air circulation and stable condition is recommended.
- Do not work alone if the operation environment is dangerous.
- Check and avoid the potential hazard for moist environment, and grounding issue for power cable.
- Please turn off the power switch when replace fuse, install or remove chassis.
- Do not place the device in a damp or humid place, e.g. a bathroom-like environment.
- Avoid operating cable connection during lightning period.
- When you want to dispose of the router, please follow local regulations on conservation of the environment.

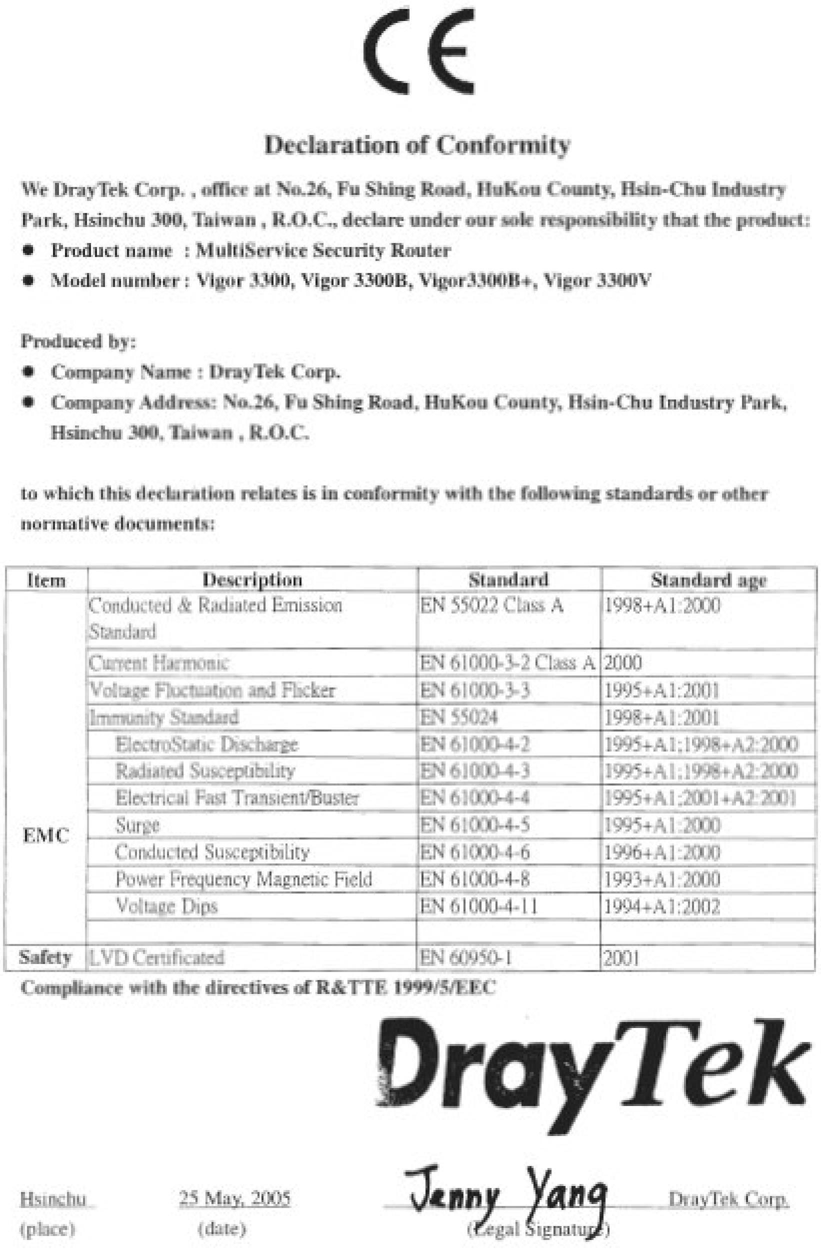
■ Maintenance

- User can replace fuses by removing the module and replace it when necessary. Others components should be repaired by authorized and qualified personnel. Do not try to open or repair the device by yourself.
- The fuse should be identical to the following standard: 250VAC, 1A

European Community Declarations

DrayTek Corporation declares that the Vigor 3300 series of routers is in compliance with the essential requirements and other relevant provisions of R&TTE Directive 99/5/EC.

CE Declarations of Conformity



CE

Declaration of Conformity

We DrayTek Corp. , office at No.26, Fu Shing Road, HuKou County, Hsin-Chu Industry Park, Hsinchu 300, Taiwan , R.O.C., declare under our sole responsibility that the product:

- Product name : MultiService Security Router
- Model number : Vigor 3300, Vigor 3300B, Vigor3300B+, Vigor 3300V

Produced by:

- Company Name : DrayTek Corp.
- Company Address: No.26, Fu Shing Road, HuKou County, Hsin-Chu Industry Park, Hsinchu 300, Taiwan , R.O.C.

to which this declaration relates is in conformity with the following standards or other normative documents:

Item	Description	Standard	Standard age
EMC	Conducted & Radiated Emission Standard	EN 55022 Class A	1998+A1:2000
	Current Harmonic	EN 61000-3-2 Class A	2000
	Voltage Fluctuation and Flicker	EN 61000-3-3	1995+A1:2001
	Immunity Standard	EN 55024	1998+A1:2001
	ElectroStatic Discharge	EN 61000-4-2	1995+A1;1998+A2:2000
	Radiated Susceptibility	EN 61000-4-3	1995+A1;1998+A2:2000
	Electrical Fast Transient/Buster	EN 61000-4-4	1995+A1:2001+A2:2001
	Surge	EN 61000-4-5	1995+A1:2000
	Conducted Susceptibility	EN 61000-4-6	1996+A1:2000
	Power Frequency Magnetic Field	EN 61000-4-8	1993+A1:2000
	Voltage Dips	EN 61000-4-11	1994+A1:2002
Safety	LVD Certificated	EN 60950-1	2001

Compliance with the directives of R&TTE 1999/5/EEC

DrayTek

Hsinchu 25 May, 2005 Jenny Yang DrayTek Corp.

(place) (date) (Legal Signature)

Customer Support

Please prepare the following information before you contact your customer support.

- Product model and serial number,
- Warranty information,
- Date that you received Vigor 3300,
- Product configuration,
- Software release version number,
- Brief description of your problem,
- Steps that you may take to solve it and their associated SysLog messages.

The information of customer support and sales representatives are support@draytek.com and sales@draytek.com, respectively.

Organization

This document is separated into the following chapters:

CHAPTER 1

Preface and Installation

1.1 Preface

The Vigor3300 product 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 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.

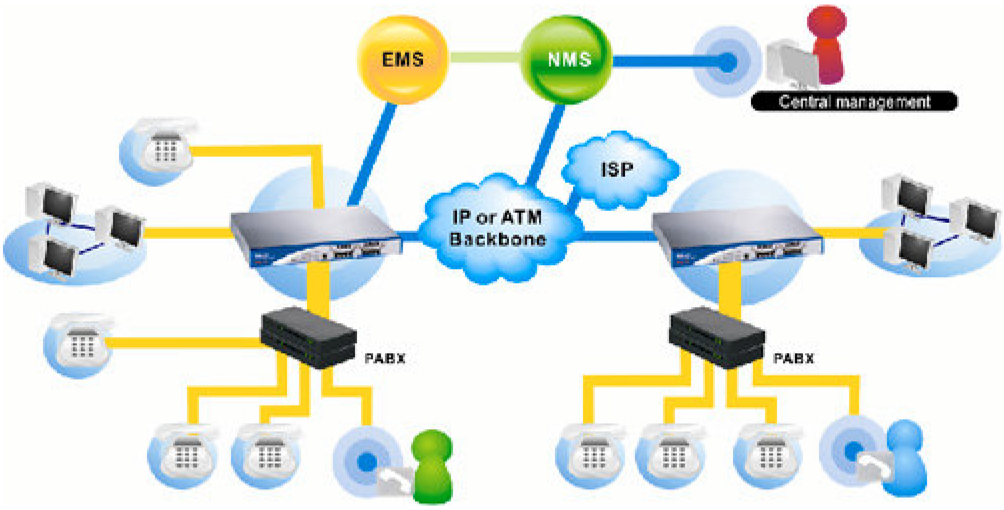


Figure 1-1. An application scenario of the Vigor3300 series

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.

The rest of this chapter is organized as following:

- Section 1.2: Connections and LED Indicators
- Section 1.3: Hardware Installation

1.2 Connections and LED Indicators

The Vigor3300 series has 4 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 over as the master interface immediately. Lastly, the Vigor3300 series has a DMZ function can be applied to any LAN or WAN interface. Figure 1-2 illustrates the application of each interface in Vigor3300V.

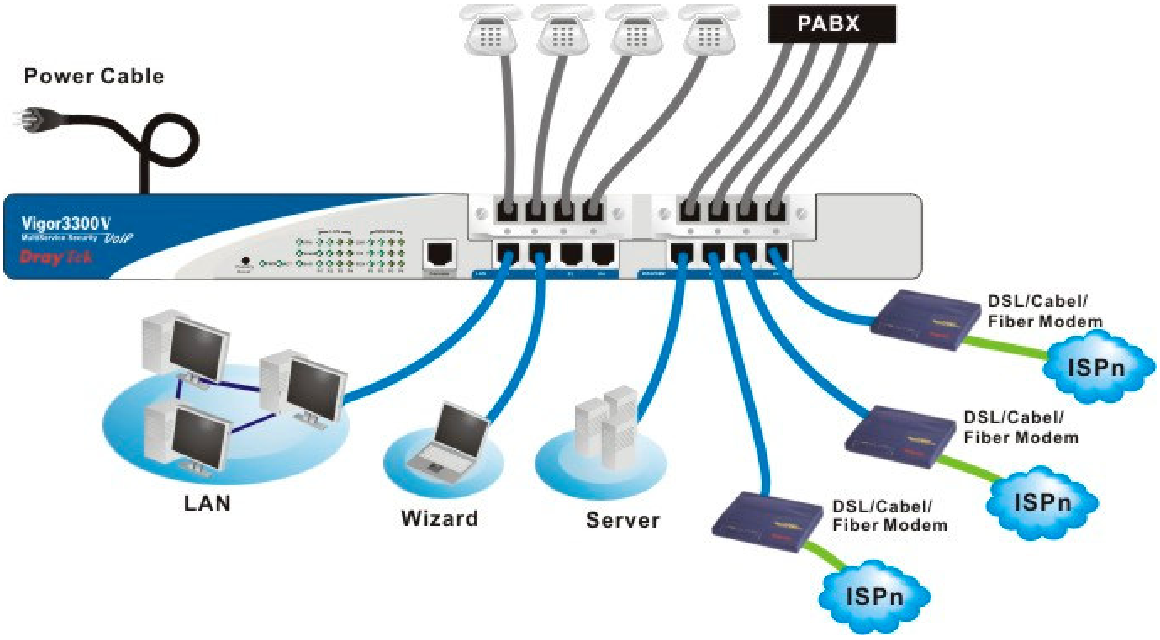


Figure 1-2. Vigor3300 series network connection

The included auxiliary cables are listed in Table 1-1.

Table 1-1. The Vigor3300 connector specification

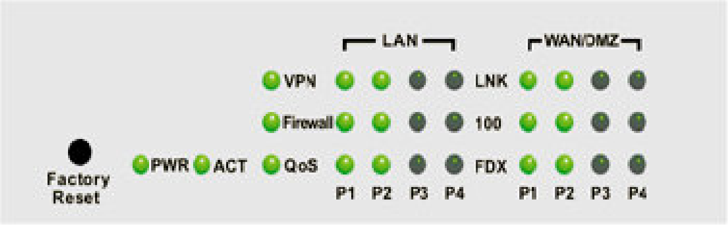
Auxiliary Cables	Type, Color	Connected to	Remarks
Power Cord	Black	AC Outlet	90-264VAC
Serial (Console)	RS232, Grey	PC RS232 port	--
Ethernet (LAN)	RJ-45, Blue	Ethernet switch or hub	--
Ethernet (DMZ)	RJ-45, Blue	Server	
Ethernet (WAN1)	RJ-45, Blue	DSL/Cable/Fiber Modem	--
Ethernet (WAN2)	RJ-45, Blue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

To connect the router to your system:

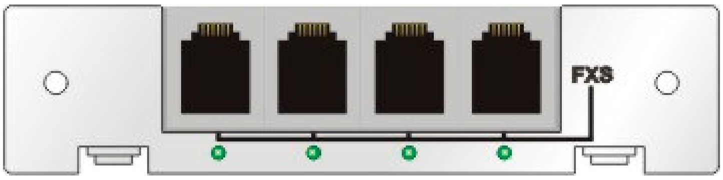
- 1. Connect the power cord in the rear panel of the Vigor3300 to an AC outlet. The PWR LED should light up.
- 2. After system testing is completed, the ACT LED will begin to blink.
- 3. Connect your local network to any of the 4 LAN ports on the Vigor3300 with a blue RJ-45 cable, and the LAN LED will blink.

The Vigor3300 provides LEDs for VPN, Firewall, QoS, VoIP, and the 4 WAN ports. All of these LEDs are depicted in Figure 1-3 and the function of each LED is described in Table 1-2.

(Vigor 3300 Front Panel LED)



(VoIP Module-FXS)



(VoIP Module-FXO)

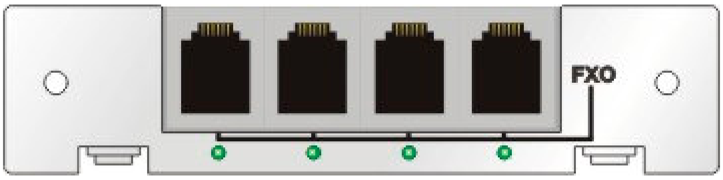


Figure 1-3. LED indicators of the Vigor3300

Table 1-2. The Vigor3300V front panel LED and its description

LED Indication		**Color**	**Description**	**Remarks**
PWR		Green	Power ON	
		OFF	Power OFF	
ACT		Green/Blinking	Blinks when system is active	
		OFF	When System is hanging	
WAN, Px	LNK	Green/Blinking	Green when Ethernet link is established, Blinks during data transit	Px: Port x, where x is 1, 2, 3, or 4
		OFF	No Ethernet link established	
	100M	Green	The speed for Ethernet is 100Mbps	
		OFF	The speed for Ethernet is 10Mbps	
	FDX	Green	The Ethernet is in full duplex mode	
		OFF	The Ethernet is in half duplex mode	
LAN, Px	LNK	Green	Ethernet link is established on port Px	Px: Port x, where x is 1, 2, 3, or 4
		OFF	No Ethernet established on port Px	
	100M	Green	The speed for Ethernet is 100Mbps on port Px	
		OFF	The speed for Ethernet is 10Mbps on port Px	
	FDX	Green	The Ethernet is in full duplex mode on port Px	
		OFF	The Ethernet is in half duplex mode on port Px	
DMZ		As WAN	As WAN ports	As WAN ports
VPN		Green	VPN is active	Not in V3300B and V3300B+
		OFF	VPN is not active	
Firewall		Green	Firewall is active	
		OFF	Firewall is not active	
QoS		Green	QoS is active	
		OFF	QoS is not active	
FXO, Px		Green	VoIP call is in use for corresponding port	Px Port for FXO module, x is 1-4
FXS , Px		Green	VoIP call is in use for corresponding port	Px Port for FXS module, x is 1-4

1.3 Hardware Installation

Figure 1-4 shows the interface of the Vigor3300 series. The Vigor3300V supports console, 4 LAN switch ports, 4 WAN interfaces, and two 4-port extensible VoIP channels. The Vigor3300 series also provides different color-type cables for each individual interface. The interface and color types are listed on Table 1-3. Figure 1-4 illustrates the front panel connectors of the Vigor3300 series.

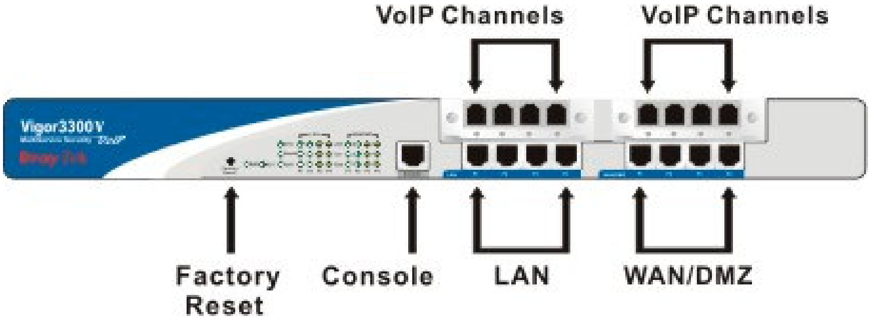


Figure 1-4. Hardware interface on front panel

Table 1-3. Connector types and color types

Connector Type	**Color**	**Description**	**Remarks**
Console	Gray	RJ45 and DB9 cable to PC	For craft command control
LAN	Blue	RJ45 to RJ45 cable to WAN	For LAN network connection
WAN	Blue	RJ45 to RJ45 cable to LAN	For WAN network connection
Phone		RJ11 to PABX cable or RJ11 to Phone cable	Requires an RJ11 phone cable (not included)

1.3.1 Descriptions of Connectors and Interfaces

1.3.1.1 The RS232 Connector

The RJ45 connection jet is used for CLI commands for system configuration and control functions in the Vigor3300. The jet is used for initialization of the Vigor3300 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 theVigor3300, 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**."

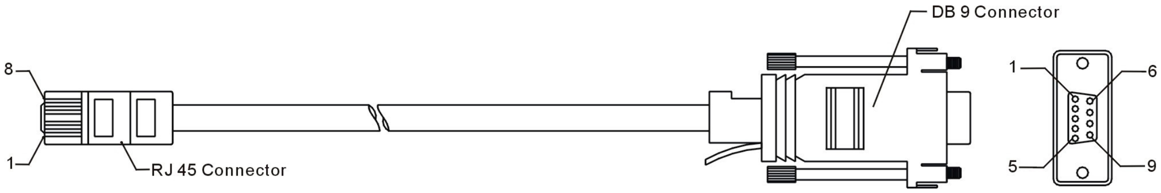


Figure 1-5. Console management cable

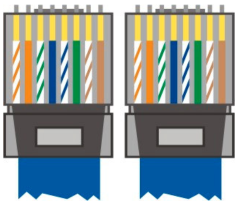
The pin-out for this connector is shown in Table 1-4 as follows:

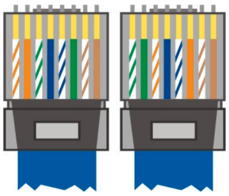
Table 1-4. The RS232 connector pinout

RJ45	DB9	Signal
X	1	CD
3	2	TD
6	3	RD
7	4	DTR
5	5	GND
2	6	DSR
8	7	RTS
1	8	CTS
X	9	RI

1.3.1.2 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.





RJ-45 **Straight-through** Cable Pin-outs

Signal	Pin	Pin	Signal
Tx+	1	1	Tx+
Tx-	2	2	Tx-
Rx+	3	3	Rx+
--	4	4	--
--	5	5	--
Rx-	6	6	Rx-
-	7	7	-
-	8	8	-

RJ-45 **Crossover** Cable Pin-outs

Signal	Pin	Pin	Signal
Tx+	1	1	Tx+
Tx-	2	2	Tx-
Rx+	3	3	Rx+
--	4	4	--
--	5	5	--
Rx-	6	6	Rx-
-	7	7	-
-	8	8	-

1.3.2 Chassis Connections

1.3.2.1 Rack-Mounting the Chassis

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 in Figure 1-7.

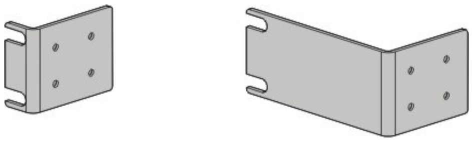


Figure 1-7. Bracket for 19-, 23-inch rack

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.

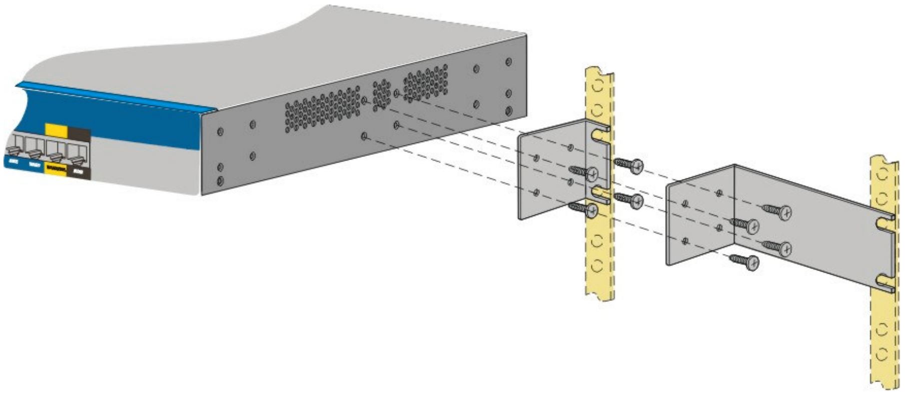


Figure 1-8. Bracket installation for front mounting on a 19- and a 23-inch rack

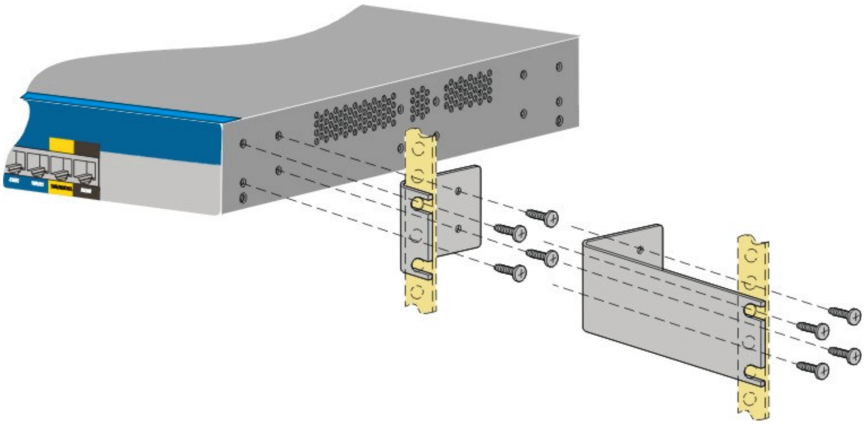


Figure 1-9. Bracket installation for front mounting on a 19- or a 23-inch rack

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

1.3.2.2 Desktop Type Installation

Rubber pads are included with the Vigor3300. These rubber pads improve the air circulation and decrease unnecessary rubbing on the desktop.

1.3.2.3 Power, Ground Connections on the Rear Panel

The AC input and ground connections are on the rear panel and shown on Figure 1-10. You can connect the rack to the ground with screws.

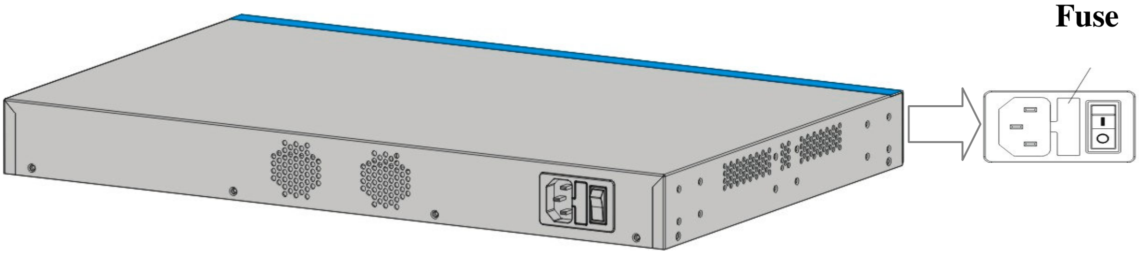


Figure 1-10. The rear panel and AC power input

CHAPTER 2

Administrator Password Setup

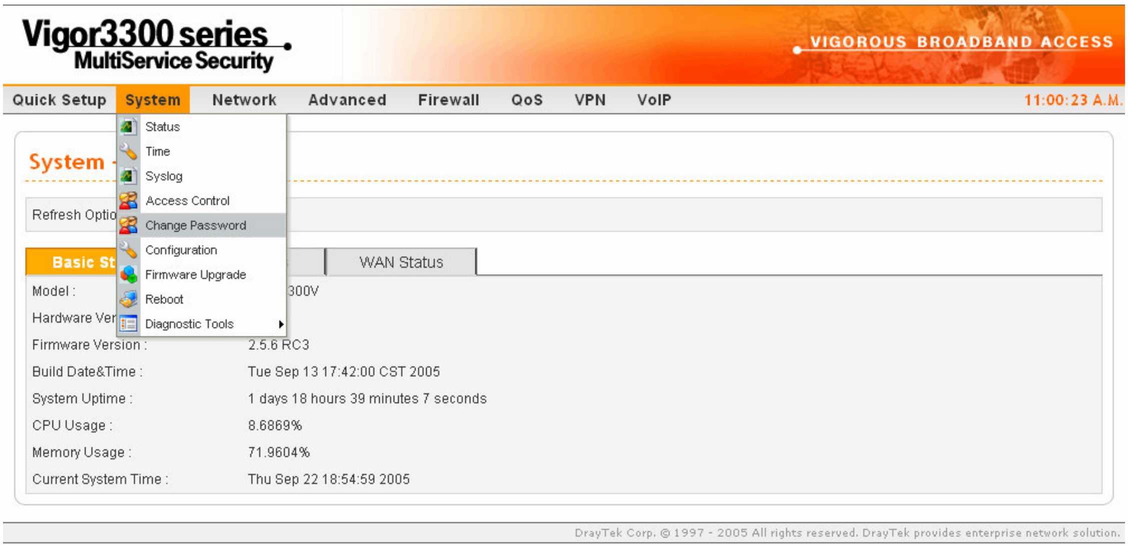
This chapter explains how to setup a password for an administrator. This allows only the administrator to change the router configuration.

This chapter is divided into the following sections.

- Section 2.1: Introduction
- Section 2.2: Changing the Administrator Password

2.1 Introduction

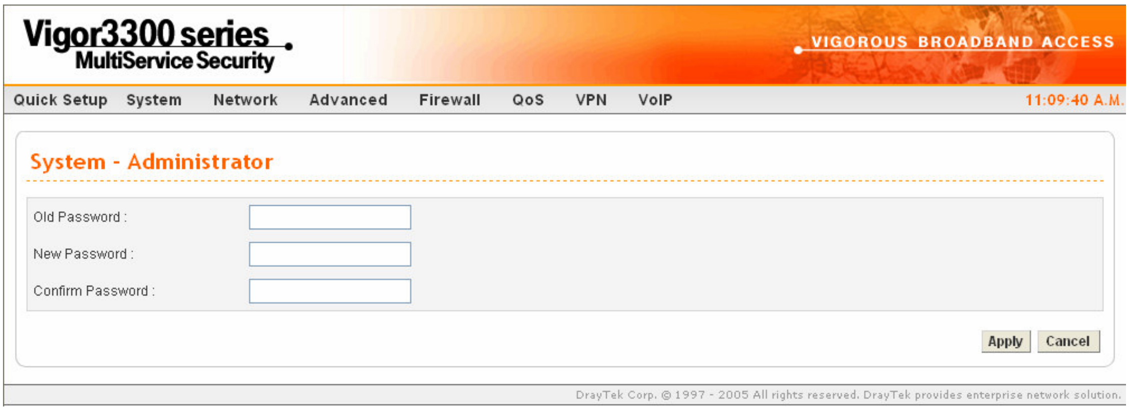
In the **System** group, click the **Change Password** option. The user can then setup a password for the administrator. Figure 2-1 illustrates the location of the Change Password option.



Model : 300V
Hardware Ver
Firmware Version : 2.5.6 RC3
Build Date&Time : Tue Sep 13 17:42:00 CST 2005
System Uptime : 1 days 18 hours 39 minutes 7 seconds
CPU Usage : 8.6869%
Memory Usage : 71.9604%
Current System Time : Thu Sep 22 18:54:59 2005

Figure 2-1.Option of change password

Click the **Change Password** option to bring up the following page. Figure 2-2 illustrates the Web page as an example.



Vigor3300 series
MultiService Security
VIGOROUS BROADBAND ACCESS
Quick Setup
System
Network
Advanced
Firewall
QoS
VPN
VoIP
11:09:40 A.M.
Apply
Cancel
DrayTek Corp. © 1997 - 2005 All rights reserved. DrayTek provides enterprise network solution.

System - Administrator

Old Password :

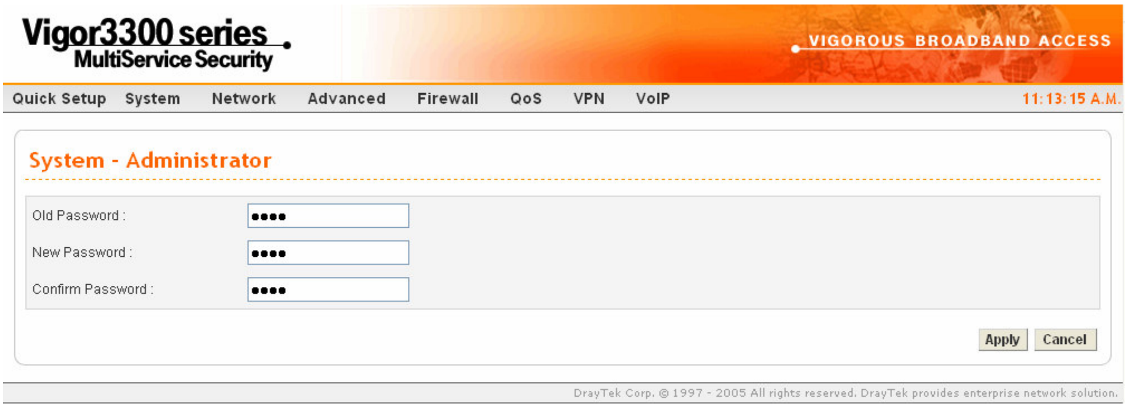
New Password :

Confirm Password :

Figure 2-2. Administrator of system group

2.2 Changing the Administrator Password

It is recommended that you set a password for the router for security. The default user name for the Vigor3300 series is "**draytek**" and password is "**1234**". Figure 2-3 illustrates the Web page after changing the settings.



Vigor3300 series
MultiService Security
VIGOROUS BROADBAND ACCESS
Quick Setup
System
Network
Advanced
Firewall
QoS
VPN
VoIP
11:13:15 A.M.
Apply
Cancel
DrayTek Corp. © 1997 - 2005 All rights reserved. DrayTek provides enterprise network solution.

System - Administrator

Old Password : ••••

New Password : ••••

Confirm Password : ••••

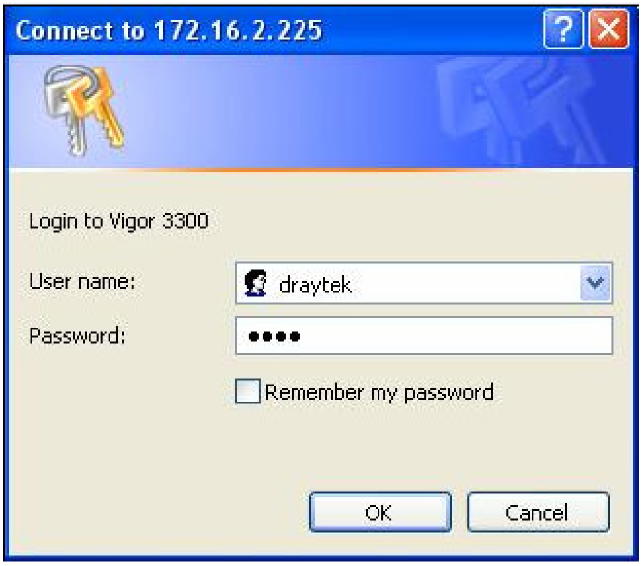
Figure 2-3. Administrator password settings

Administrator Password Setup

Old Password	Assign the current administrator password. If this is your first time setting a password, please type the default password "**1234**".
New Password	Assign a new administrator's password.
Confirm Password	Retype the new password for confirmation.

Please click **Apply** to apply these settings into the Vigor3300 device.

You will see the login screen after clicking **Apply**. You should use the new password to re-enter the system configuration. Figure 2-4 illustrates the login screen after clicking **Apply**.



Connect to 172.16.2.225

Login to Vigor 3300

User name: draytek

Password: ●●●●

□ Remember my password

Figure 2-4. Login screen

CHAPTER 3

Quick Setup

This chapter explains more details about the Quick Setup. The Quick Setup provides an easy way to configure the Vigor3300.

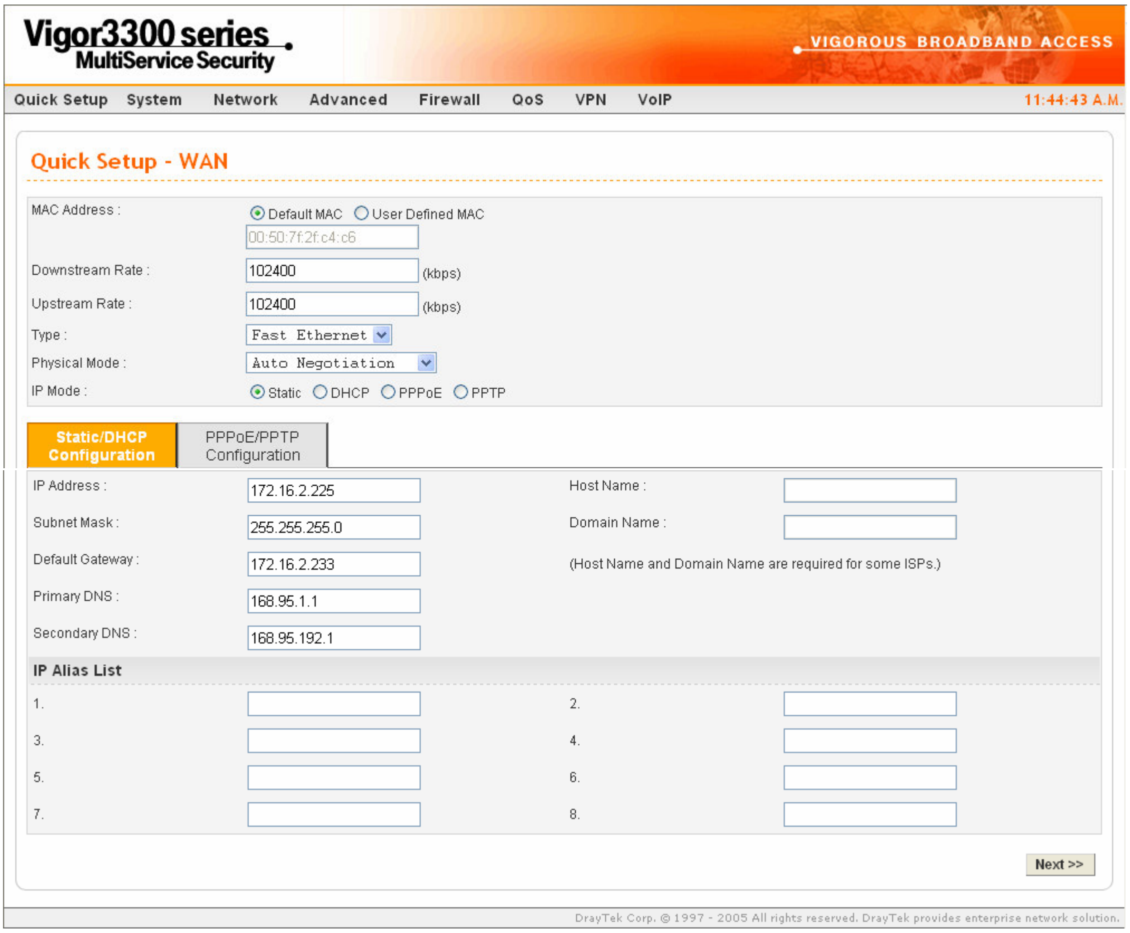
This chapter is divided into the following sections.

- Section 3.1: WAN Setting
- Section 3.2: LAN Interface Configuration

If your Vigor3300 is used under a high speed NAT environment, these settings can help you to install and deploy quickly.

3.1 WAN Setting

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. Figure 3-1 illustrates the web page as an example.


Vigor3300 series
MultiService Security
VIGOROUS BROADBAND ACCESS
Quick Setup System Network Advanced Firewall QoS VPN VoIP
11:44:43 A.M.

Quick Setup - WAN

MAC Address :	● Default MAC ○ User Defined MAC 00:50:7f:2f:c4:c6
Downstream Rate :	102400 (kbps)
Upstream Rate :	102400 (kbps)
Type :	Fast Ethernet
Physical Mode :	Auto Negotiation
IP Mode :	● Static ○ DHCP ○ PPPoE ○ PPTP

Static/DHCP Configuration | PPPoE/PPTP Configuration

IP Address :	172.16.2.225	Host Name :	
Subnet Mask :	255.255.255.0	Domain Name :	
Default Gateway :	172.16.2.233	(Host Name and Domain Name are required for some ISPs.)	
Primary DNS :	168.95.1.1		
Secondary DNS :	168.95.192.1		

IP Alias List

1.		2.	
3.		4.	
5.		6.	
7.		8.	

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

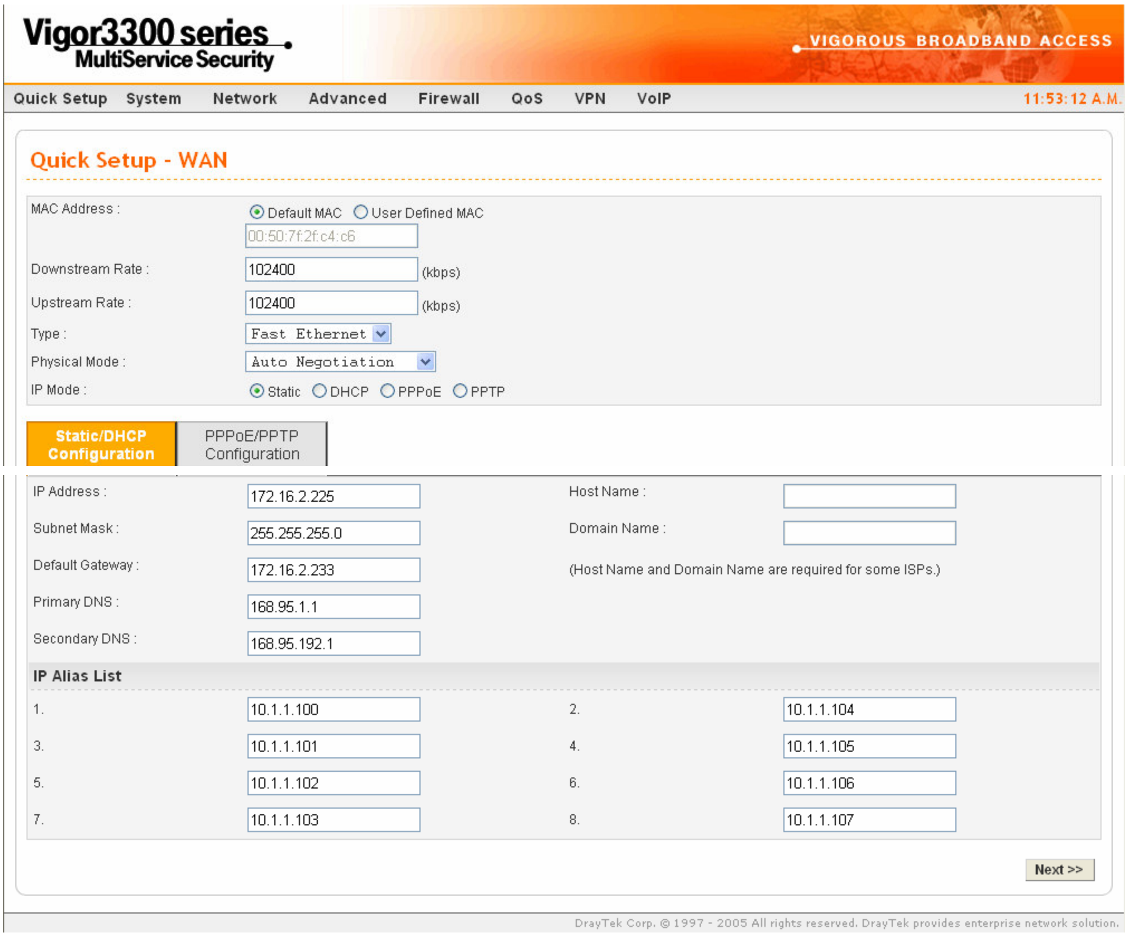
Figure 3-1. The quick setup

MAC Address	
Router Default	Use the default Mac address stored originally in router.
User Definition	Use a MAC address defined by the user.

Downstream Rate	Assign the downstream rate for this WAN interface. The default value is 102400 kbps (100 Megabit). The setting is very important for Vigor3300 incoming buffer adjustment. If you use a DSL subscriber service with a 2Mbps downstream, set the downstream rate setting is 2Mbps.
Upstream Rate	Assign the transmission rate for this WAN interface. The default value is 102400 kbps (100 Megabit). The setting is very important for Vigor3300 incoming buffer adjustment. If you use a DSL subscriber service with a 256Kbps downstream, set the downstream rate setting is 256Kbps.
Type	Select a connection type for this WAN interface.
Physical Mode	Select connection speed mode for this WAN interface. There are **auto negotiation**, **full duplex**, and **half duplex** of either 10M or 100M speed options for the WAN Interface.
IP Mode	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.

3.1.1 Static Setup

You can manually assign a static IP address to the WAN interface and complete the configuration by applying the settings and rebooting your router. Then you will see the following web page. Figure 3-2 illustrates the web page as an example.



Quick Setup - WAN

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

Downstream Rate : 102400 (kbps)

Upstream Rate : 102400 (kbps)

Type : Fast Ethernet

Physical Mode : Auto Negotiation

IP Mode : ● Static ○ DHCP ○ PPPoE ○ PPTP

IP Address :	172.16.2.225	Host Name :	
Subnet Mask :	255.255.255.0	Domain Name :	
Default Gateway :	172.16.2.233	(Host Name and Domain Name are required for some ISPs.)	
Primary DNS :	168.95.1.1		
Secondary DNS :	168.95.192.1		

IP Alias List

1.	10.1.1.100	2.	10.1.1.104
3.	10.1.1.101	4.	10.1.1.105
5.	10.1.1.102	6.	10.1.1.106
7.	10.1.1.103	8.	10.1.1.107

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

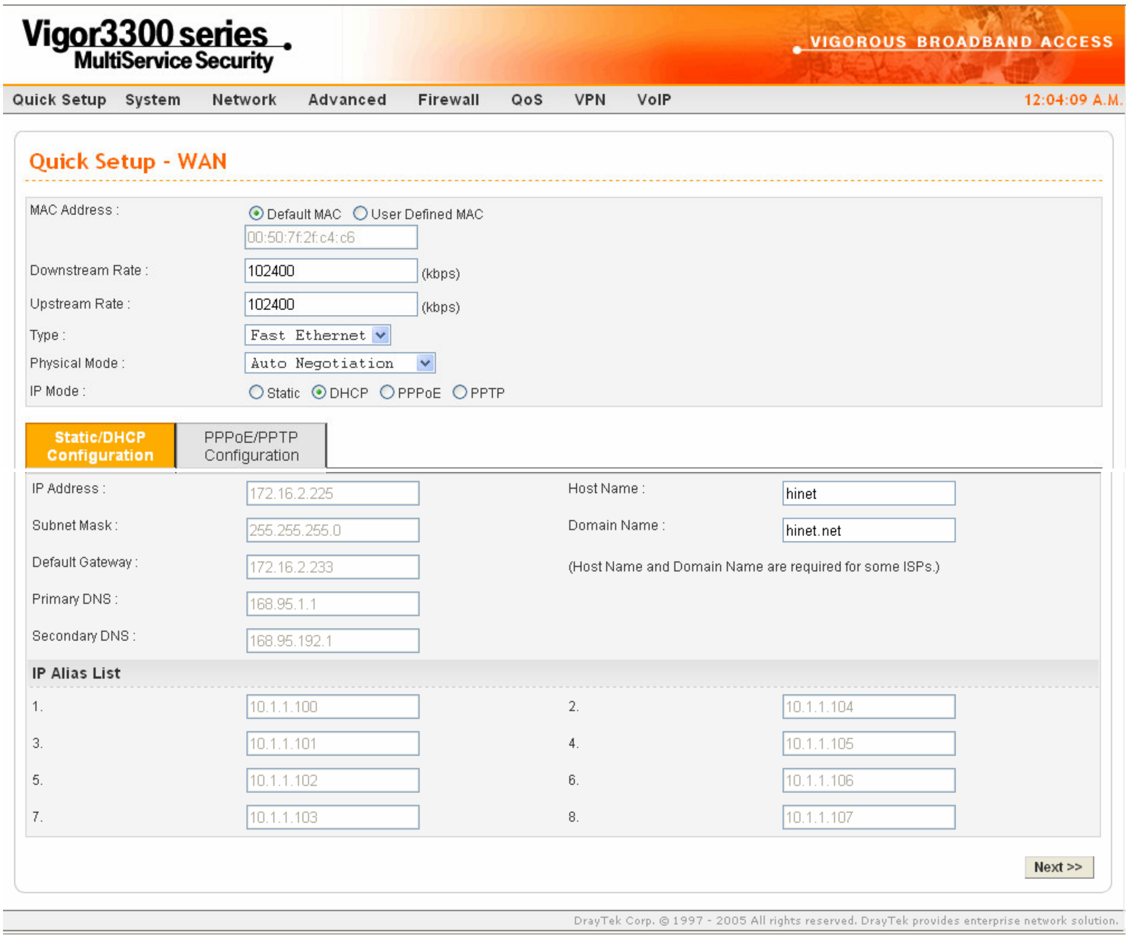
Figure 3-2. Static configuration

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.

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

3.1.2 DHCP Client Setup

DHCP allows a user to obtain an IP address automatically from a DHCP server on the Internet. If the **WAN** interface is set as a DHCP client, it will ask for a specific IP address and network settings from a DHCP server or DSL modem. If a user selects this mode, it is not necessary for the user to setup any configuration. (Host Name and Domain Name are required for some ISPs). Figure 3-3 illustrates the web page as an example.



Quick Setup - WAN

MAC Address :	● Default MAC ○ User Defined MAC 00:50:7f:2f:c4:c6
Downstream Rate :	102400 (kbps)
Upstream Rate :	102400 (kbps)
Type :	Fast Ethernet
Physical Mode :	Auto Negotiation
IP Mode :	○ Static ● DHCP ○ PPPoE ○ PPTP

IP Address :	172.16.2.225	Host Name :	hinet
Subnet Mask :	255.255.255.0	Domain Name :	hinet.net
Default Gateway :	172.16.2.233	(Host Name and Domain Name are required for some ISPs.)	
Primary DNS :	168.95.1.1		
Secondary DNS :	168.95.192.1		

IP Alias List

1.	10.1.1.100	2.	10.1.1.104
3.	10.1.1.101	4.	10.1.1.105
5.	10.1.1.102	6.	10.1.1.106
7.	10.1.1.103	8.	10.1.1.107

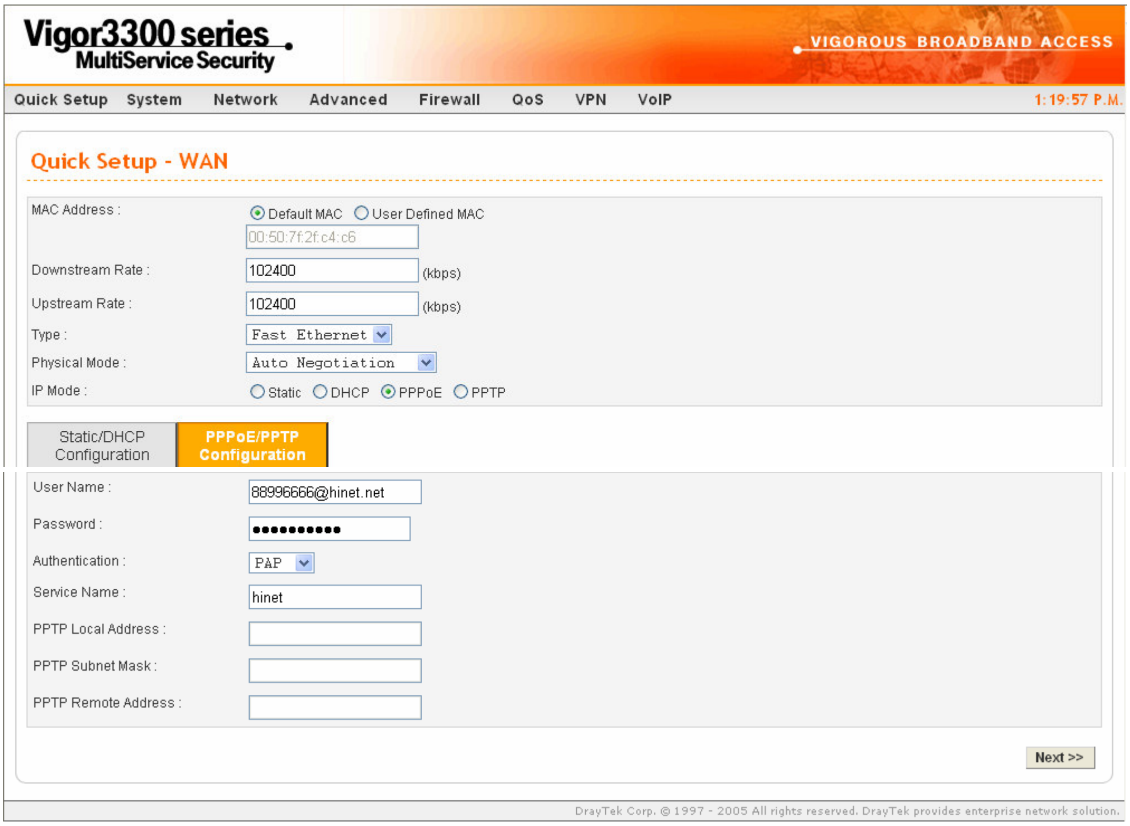
DrayTek Corp. © 1997 - 2005 All rights reserved. DrayTek provides enterprise network solution.

Figure 3-3. The DHCP configuration

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

3.1.3 PPPoE with a DSL Modem

This mode is used for most of DSL modem users. All local users can share one PPPoE connection to access the Internet. The following setup web page is just as an example. Your service provider should provide the user name, password, and authentication mode for PPPoE settings. Figure 3-4 illustrates the web page after clicking the **PPPoE** option.


Vigor3300 series
MultiService Security
VIGOROUS BROADBAND ACCESS
Quick Setup System Network Advanced Firewall QoS VPN VoIP
1:19:57 P.M.
Static/DHCP Configuration
PPPoE/PPTP Configuration
Next >>

Quick Setup - WAN

MAC Address :	● Default MAC ○ User Defined MAC 00:50:7f:2f:c4:c6
Downstream Rate :	102400 (kbps)
Upstream Rate :	102400 (kbps)
Type :	Fast Ethernet
Physical Mode :	Auto Negotiation
IP Mode :	○ Static ○ DHCP ● PPPoE ○ PPTP

User Name :	88996666@hinet.net
Password :	●●●●●●●●●●●
Authentication :	PAP
Service Name :	hinet
PPTP Local Address :	
PPTP Subnet Mask :	
PPTP Remote Address :	

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

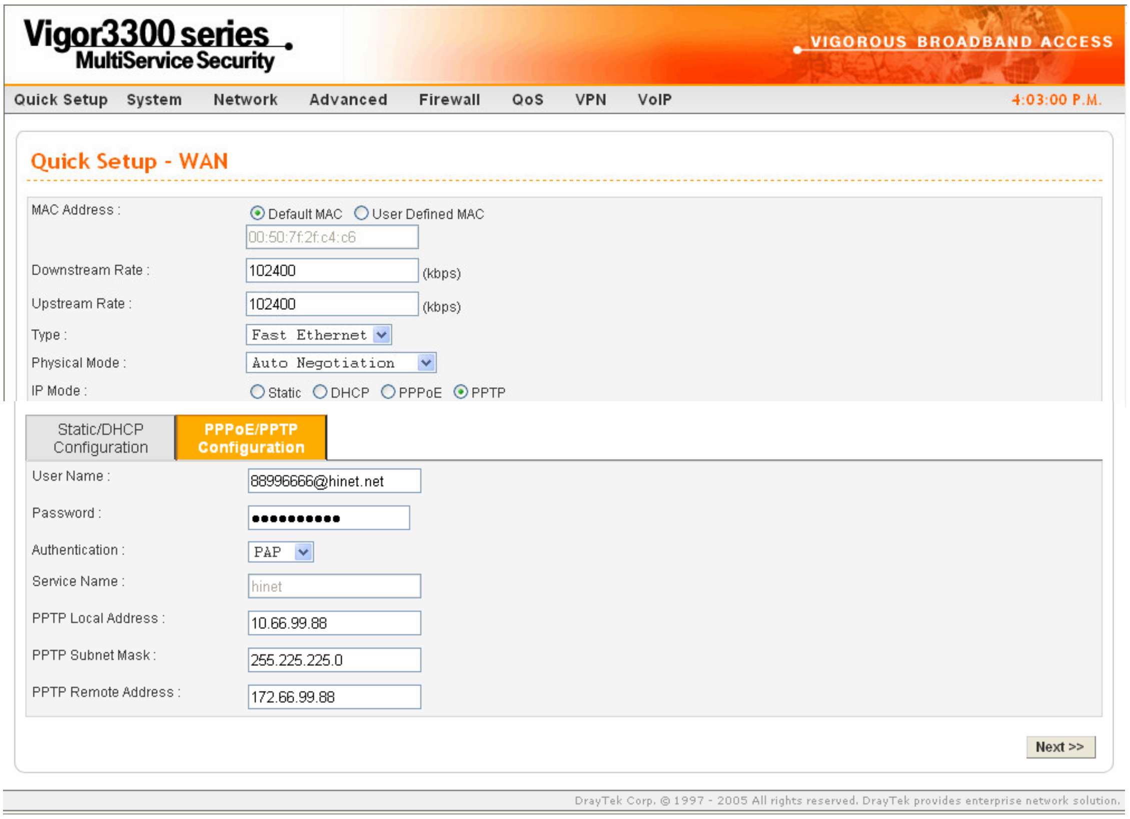
Figure 3-4. The PPPoE configuration

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.

3.1.4 PPTP with a DSL Modem setup

This mode is to let user get the IP group information by a DSL modem with PPTP service from an ISP. The following setup web page is used as an example. Your service provider should provide the user name, password, and authentication mode for a PPTP setting. Figure 3-5 illustrates the example web page as an example.


Vigor3300 series
MultiService Security
VIGOROUS BROADBAND ACCESS
Quick Setup System Network Advanced Firewall QoS VPN VoIP
4:03:00 P.M.

Quick Setup - WAN

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

Downstream Rate : 102400 (kbps)

Upstream Rate : 102400 (kbps)

Type : Fast Ethernet

Physical Mode : Auto Negotiation

IP Mode : ○ Static ○ DHCP ○ PPPoE ● PPTP

Static/DHCP Configuration | PPPoE/PPTP Configuration

User Name : 88996666@hinet.net

Password : ●●●●●●●●●●●

Authentication : PAP

Service Name : hinet

PPTP Local Address : 10.66.99.88

PPTP Subnet Mask : 255.225.225.0

PPTP Remote Address : 172.66.99.88

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

Figure 3-5. The PPTP configuration

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.

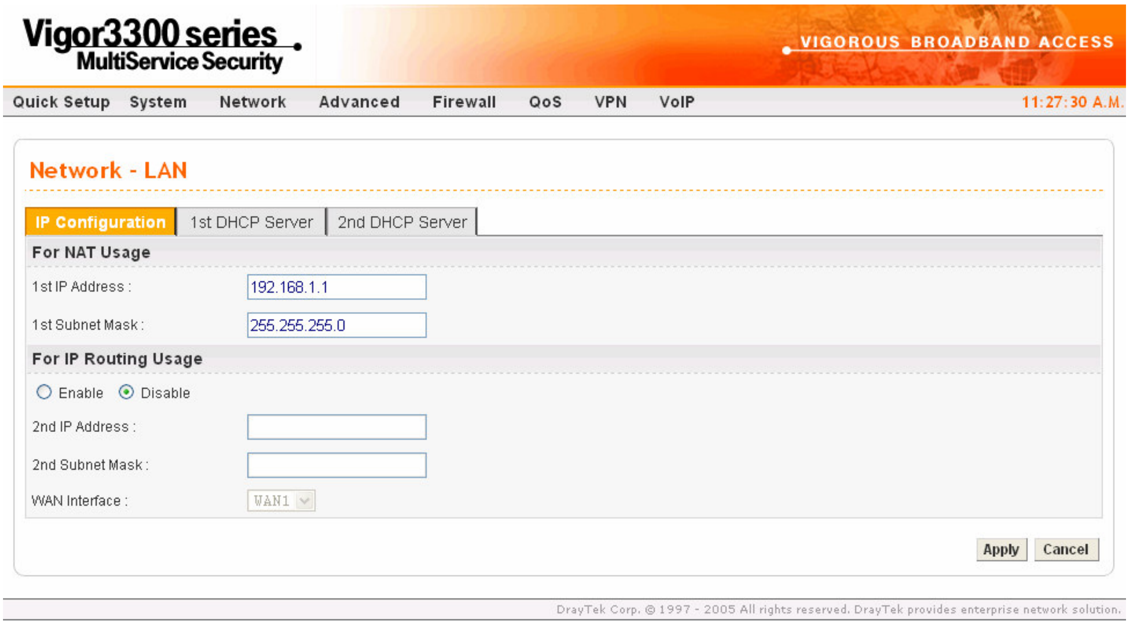
3.2 The LAN Interface Configuration

The LAN interface on the Vigor3300 series has one IP address. There are three options available to the user:

***IP Configuration**
***1st DHCP Server**
***2nd DHCP Server**

3.2.1 IP Configuration

There are some IP address settings for the LAN interface as described below. The IP address/subnet mask is for private users or NAT users. In general, the LAN IP address is 192.168.1.X. Other local PCs should set the default gateway to be the LAN IP address of the Vigor3300. When the connection to the ISP is established, each local PC will directly route to the Internet. Also, you could use the IP address/subnet mask to connect to other private PCs users. On the following web page, you will see the private IP address defined in RFC-1918. Usually, we use the 192.168.1.0/24 subnet for the router. To allow public users, you need to have subscribed to a globally reachable subnet from your ISP. After clicking the IP Configuration option, you will see the following web page. Figure 3-6 illustrates the web page as an example.



For NAT Usage

1st IP Address : 192.168.1.1

1st Subnet Mask : 255.255.255.0

For IP Routing Usage

○ Enable ● Disable

2nd IP Address :

2nd Subnet Mask :

WAN Interface : WAN1

Figure 3-6. The LAN interface configuration

NAT Usage	
1st IP Address	The first private IP address for connecting to a local private network. The default value is 192.168.1.1.
1st Subnet Mask	The first subnet mask of the local private network. The default value is 255.255.255.0.
IP Routing Usage	
Status	Click "**Enable**" to enable this function. Click "**Disable**" to disable this function.
2nd IP Address	Assign an IP address belongs to the subnet of the WAN selected in WAN Interface field.
2nd Subnet Mask	Assign the value of subnet mask.
WAN Interface	Select a WAN interface to be applied in IP Routing Usage.

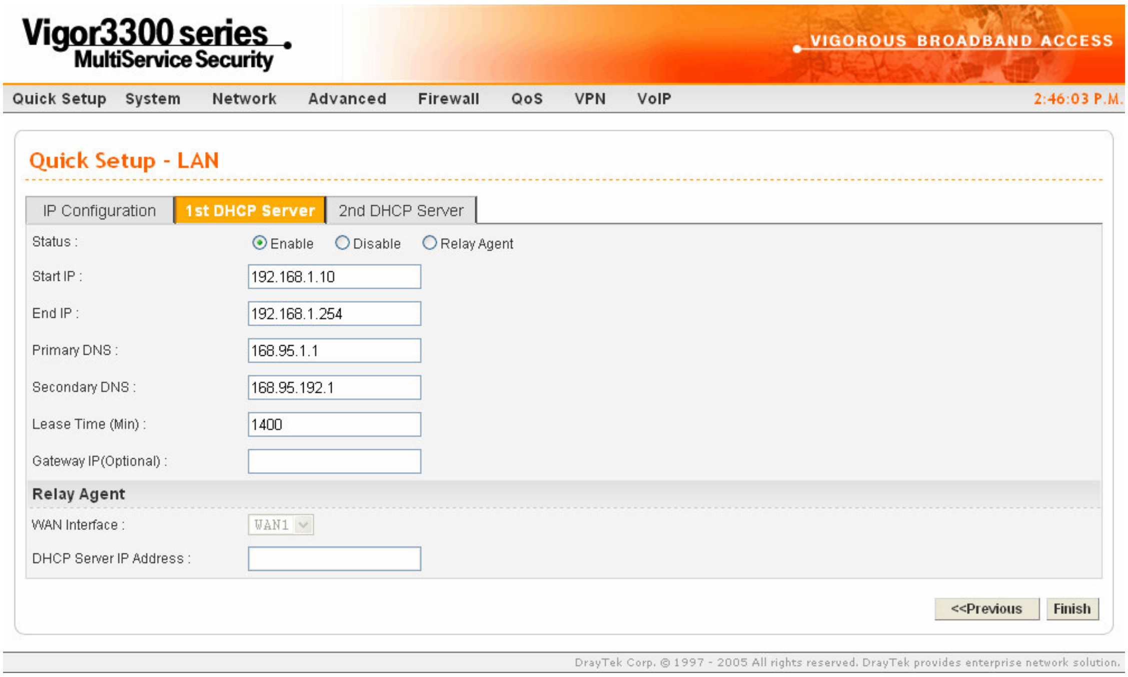
Click the **Finish** option, and the user will be prompted to reboot. Reboot the system to save your settings.

3.2.2 DHCP Server Configuration

DHCP stands for Dynamic Host Configuration Protocol. It can automatically dispatch related IP settings to any local user configured as a DHCP client. Please refer to the following figure for DHCP server configuration.

3.2.2.1 The 1st DHCP Server Setting

After clicking the 1st DHCP Server option, you will see the following web page. Figure 3-7 illustrates the web page as an example.



Quick Setup - LAN

Status : ● Enable ○ Disable ○ Relay Agent

Start IP : 192.168.1.10

End IP : 192.168.1.254

Primary DNS : 168.95.1.1

Secondary DNS : 168.95.192.1

Lease Time (Min) : 1400

Gateway IP(Optional) :

Relay Agent

WAN Interface : WAN1

DHCP Server IP Address :

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

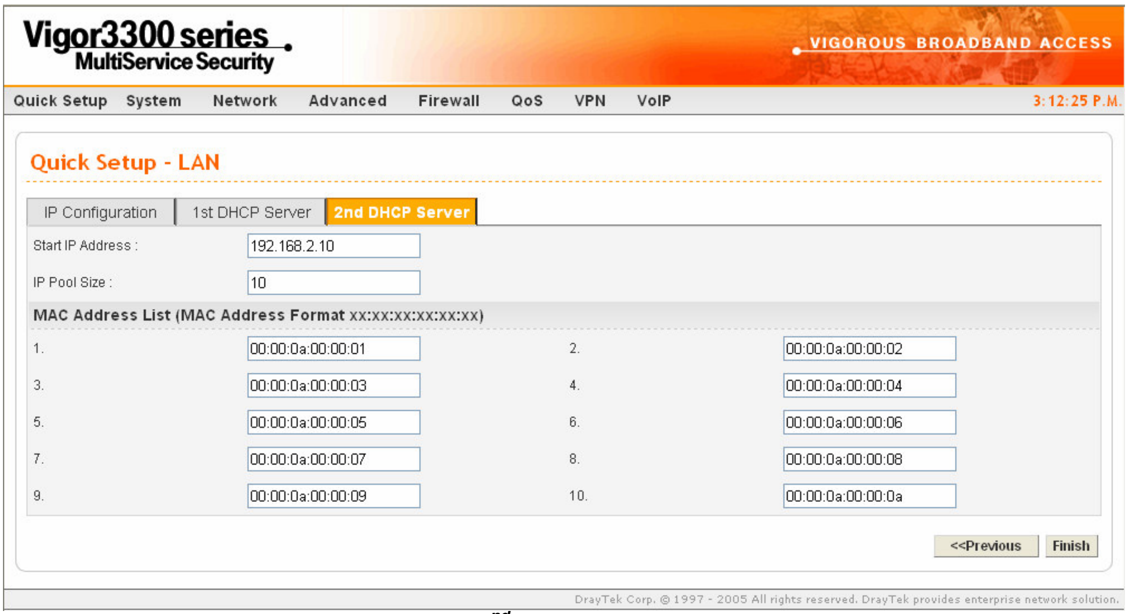
Figure 3-7. The 1st DHCP server configuration

Status	Click "**Enable**" to enable this function. Click "**Disable**" to disable this function. Click "**Relay Agent**" to apply this function.
Start IP	Set the starting IP address of the IP address pool.
End IP	Set the ending IP address of the IP address pool.
Primary DNS	Assign the IP address of the primary DNS.
Secondary DNS	Assign the IP address of the secondary DNS.
Lease Time (Min)	Assign the lease time of DHCP server to client.
Gateway IP(Optional)	Assign a new gateway IP address to DHCP client.
Relay Agent	
WAN Interface	Select a WAN interface which the other DHCP server is from.
DHCP Server IP Address	Assign an IP address of the other DHCP server.

Click the **Finish** option, and the user will be prompted to reboot. Reboot the system to save your settings.

3.2.2.2 The 2nd DHCP Server Setting

The Vigor3300 series routers support a second DHCP server. Click the 2nd DHCP Server option to bring up the following web page. Figure 3-8 illustrates the web page as an example.



Start IP Address : 192.168.2.10

IP Pool Size : 10

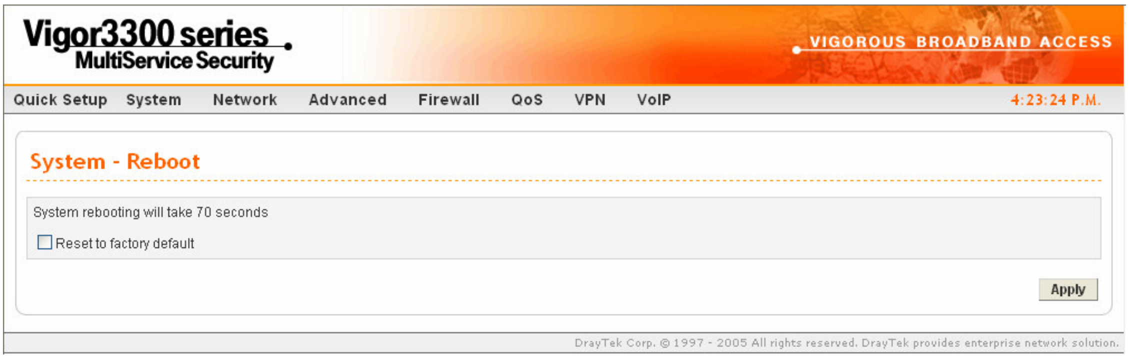
MAC Address List (MAC Address Format xx:xx:xx:xx:xx:xx)

1.	00:00:0a:00:00:01	2.	00:00:0a:00:00:02
3.	00:00:0a:00:00:03	4.	00:00:0a:00:00:04
5.	00:00:0a:00:00:05	6.	00:00:0a:00:00:06
7.	00:00:0a:00:00:07	8.	00:00:0a:00:00:08
9.	00:00:0a:00:00:09	10.	00:00:0a:00:00:0a

Figure 3-8. The 2nd DHCP server configuration

Start IP Address	Set the starting IP address of the IP address pool.
IP Pool Size	Assign the number how many IP addresses in the pool.
Mac Address List	Assign up to 10 MAC addresses to be served. Once a MAC address is matched in this table, the corresponding IP address and associated information will be returned.

Click the **Finish** option, and the user will be prompted to reboot. Reboot the system to save your settings. Figure 3-9 illustrates the web page after clicking **Finish**.


Vigor3300 series
MultiService Security
VIGOROUS BROADBAND ACCESS
Quick Setup
System
Network
Advanced
Firewall
QoS
VPN
VoIP
4:23:24 P.M.
Apply
DrayTek Corp. © 1997 - 2005 All rights reserved. DrayTek provides enterprise network solution.

System - Reboot

System rebooting will take 70 seconds

□ Reset to factory default

Figure 3-9. System reboot

Click the **Apply** option to reboot the Vigor3300 with the new configurations.

CHAPTER 4

System Setup

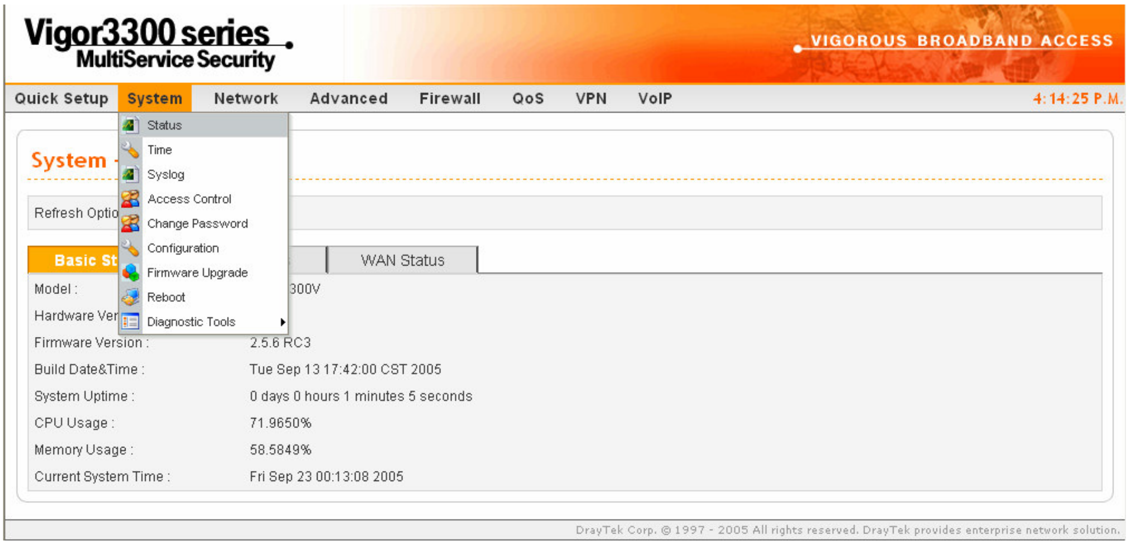
This chapter shows how to configure the System.

This chapter is divided into the following sections.

- Section 4.1: Status.
- Section 4.2: Time Setup
- Section 4.3: Syslog Setup
- Section 4.4: Access Control Setup
- Section 4.5: Reboot and Firmware Upgrade Setup
- Section 4.6: Diagnostic Tools
- Section 4.7: Configuration Setup

4.1 Status

The online **Status** function provides some useful system information on the current status of the Vigor3300 series. A user can also observe the system status on this Web page. In the **System** group, click the **Status** option. The online **Status** Web page contains three parts: **Basic Status, LAN Status, and WAN Status.** Figure 4-1 shows the location of the **Status** option.



System -

Refresh Optio

Model : 300V

Hardware Ver

Firmware Version : 2.5.6 RC3

Build Date&Time : Tue Sep 13 17:42:00 CST 2005

System Uptime : 0 days 0 hours 1 minutes 5 seconds

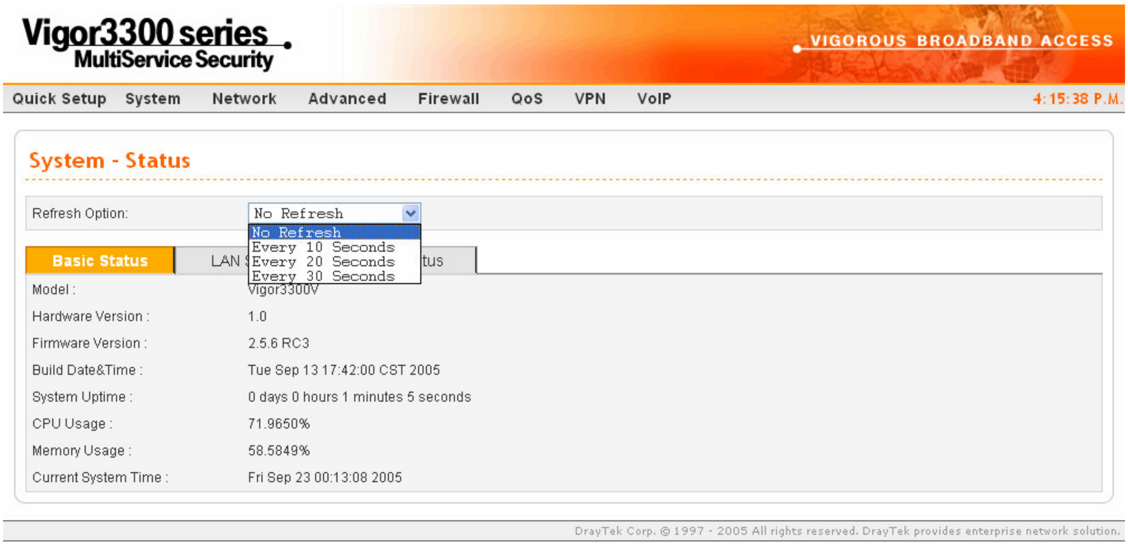
CPU Usage : 71.9650%

Memory Usage : 58.5849%

Current System Time : Fri Sep 23 00:13:08 2005

Figure 4-1. Status option

Figure 4-2 illustrates the status Web page as an example.



System - Status

Refresh Option: No Refresh

Model : Vigor3300V

Hardware Version : 1.0

Firmware Version : 2.5.6 RC3

Build Date&Time : Tue Sep 13 17:42:00 CST 2005

System Uptime : 0 days 0 hours 1 minutes 5 seconds

CPU Usage : 71.9650%

Memory Usage : 58.5849%

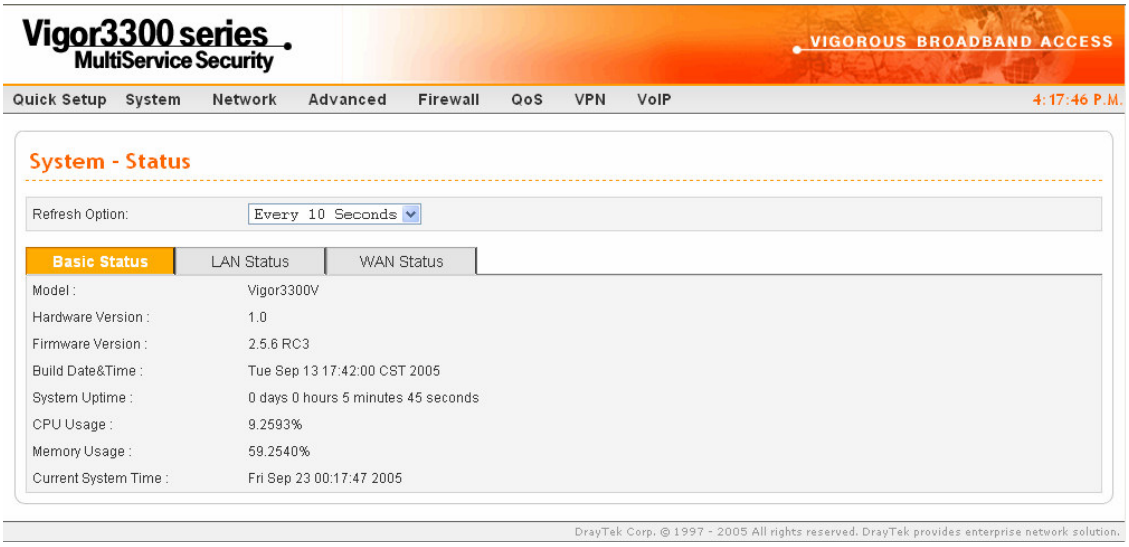
Current System Time : Fri Sep 23 00:13:08 2005

Figure 4-2. The system 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**: Refresh page every 10 seconds. ● **Every 20 Seconds**: Refresh page every 20 seconds. ● **Every 30 Seconds**: Refresh page every 30 seconds.

4.1.1 Basic Status

Click the **Basic Status** option to see the following Web page as shown in Figure 4-3.



Refresh Option: Every 10 Seconds

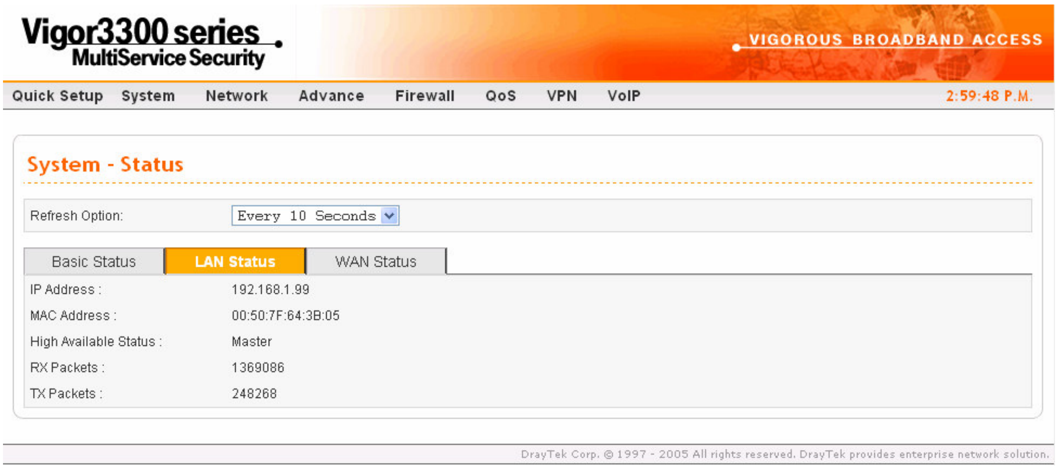
Model :	Vigor3300V
Hardware Version :	1.0
Firmware Version :	2.5.6 RC3
Build Date&Time :	Tue Sep 13 17:42:00 CST 2005
System Uptime :	0 days 0 hours 5 minutes 45 seconds
CPU Usage :	9.2593%
Memory Usage :	59.2540%
Current System Time :	Fri Sep 23 00:17:47 2005

Figure 4-3. The basic status

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

4.1.2 LAN Status

Click the **LAN Status** option to bring up the following Web page as shown in Figure 4-4.



System - Status

Refresh Option: Every 10 Seconds

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

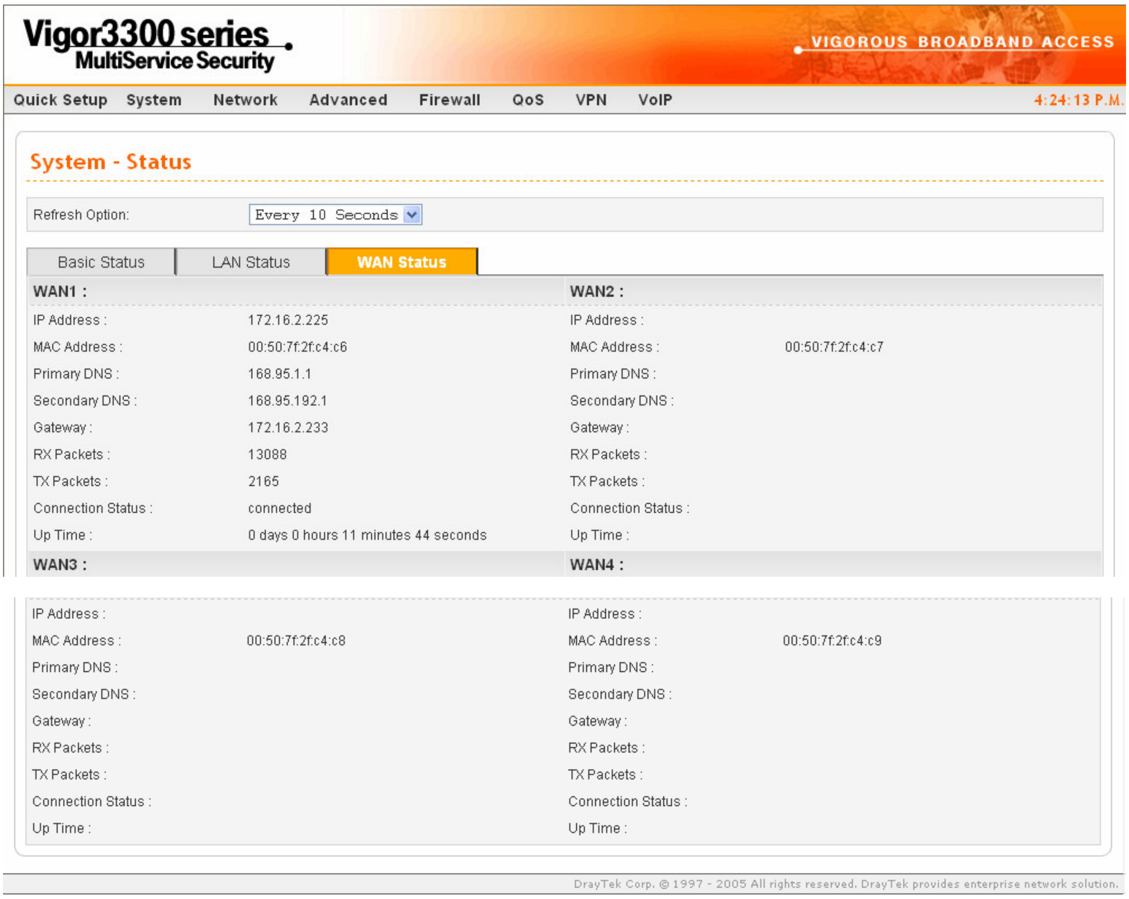
DrayTek Corp. © 1997 - 2005 All rights reserved. DrayTek provides enterprise network solution.

Figure 4-4. The LAN status

IP Address	IP address of the LAN interface.
MAC Address	MAC address of the LAN Interface.
High Available Status	The High Available Status is shown when the function is enabled. There are two options shown as follows. ● Master: Vigor3300 plays the Master role in high availability feature. ● Slave: Vigor3300 plays the Slave role in high availability feature.
RX Packets	Number of total number of received packets at the LAN interface.
TX Packets	Number of total transmitted packets at the LAN interface.

4.1.3 WAN Status

Click the **WAN Status** option to bring up the following Web page as shown in Figure 4-5. There is some basic information displayed for all the four WAN interfaces.



System - Status

Refresh Option: Every 10 Seconds

WAN1 :		WAN2 :	
IP Address :	172.16.2.225	IP Address :	
MAC Address :	00:50:7f:2f:c4:c6	MAC Address :	00:50:7f:2f:c4:c7
Primary DNS :	168.95.1.1	Primary DNS :	
Secondary DNS :	168.95.192.1	Secondary DNS :	
Gateway :	172.16.2.233	Gateway :	
RX Packets :	13088	RX Packets :	
TX Packets :	2165	TX Packets :	
Connection Status :	connected	Connection Status :	
Up Time :	0 days 0 hours 11 minutes 44 seconds	Up Time :	
WAN3 :		**WAN4 :**	
IP Address :		IP Address :	
MAC Address :	00:50:7f:2f:c4:c8	MAC Address :	00:50:7f:2f:c4:c9
Primary DNS :		Primary DNS :	
Secondary DNS :		Secondary DNS :	
Gateway :		Gateway :	
RX Packets :		RX Packets :	
TX Packets :		TX Packets :	
Connection Status :		Connection Status :	
Up Time :		Up Time :	

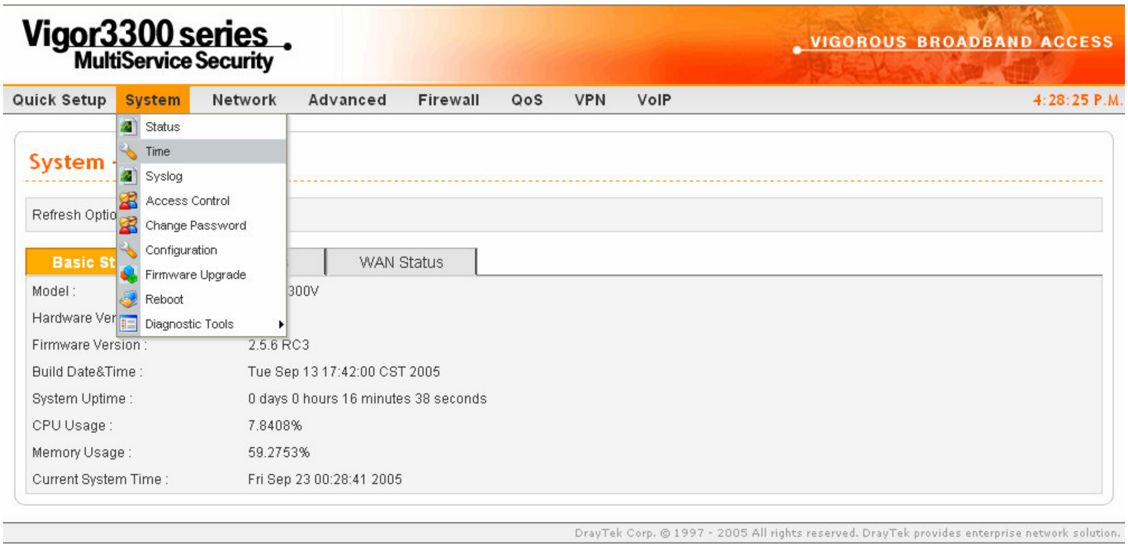
Figure 4-5. The WAN status

IP Address	The IP address of the WAN interface.
MAC Address	The MAC address of the WAN Interface.
Primary DNS	The assigned IP address of the primary DNS.
Secondary DNS	The assigned IP address of the secondary DNS.
Gateway	The assigned IP address of the default gateway.
RX Packets	The number of total received packets for each WAN interface.
TX Packets	The number of total transmitted packets for each WAN interface.
Connection Status	Display the detecting status of the WAN interface ***Connected***: The WAN port is working.
Up Time	The total system uptime of the interface.

4.2 Time Setup

As an NTP (Network Time Protocol) client, the router gets standard time from the time server. Some time-based functions, which are Call Schedule and URL Content filtering, cannot work properly until 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. Figure 4-6 illustrates the location of the **Time** option.

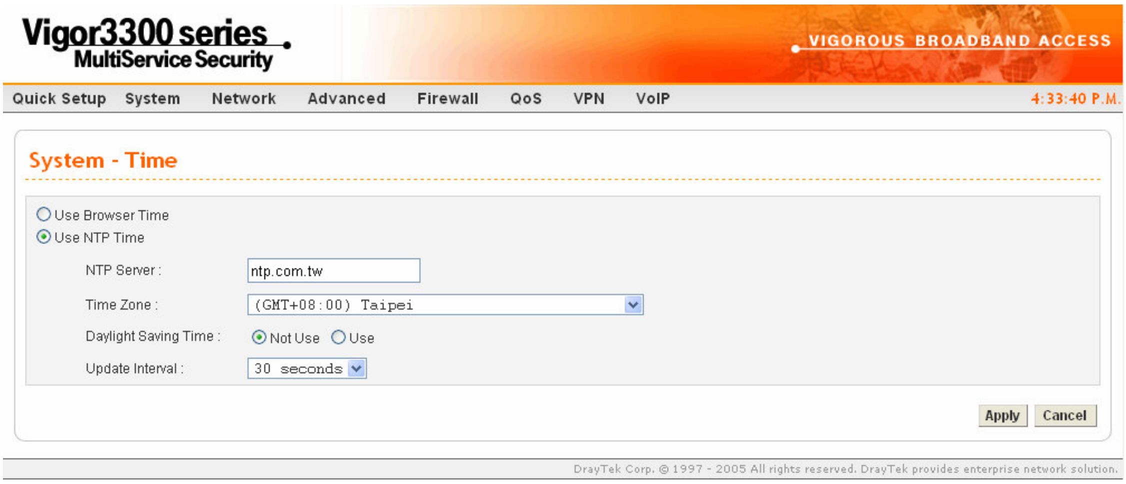


Model : 300V
Hardware Ver
Firmware Version : 2.5.6 RC3
Build Date&Time : Tue Sep 13 17:42:00 CST 2005
System Uptime : 0 days 0 hours 16 minutes 38 seconds
CPU Usage : 7.8408%
Memory Usage : 59.2753%
Current System Time : Fri Sep 23 00:28:41 2005

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

Figure 4-6. The Time option under the system group

After clicking **Time** option, you will see the following Web page as shown in Figure 4-7.


Vigor3300 series
MultiService Security
VIGOROUS BROADBAND ACCESS
Quick Setup
System
Network
Advanced
Firewall
QoS
VPN
VoIP
4:33:40 P.M.
Apply
Cancel
DrayTek Corp. © 1997 - 2005 All rights reserved. DrayTek provides enterprise network solution.

System - Time

○ Use Browser Time
● Use NTP Time

NTP Server : ntp.com.tw

Time Zone : (GMT+08:00) Taipei

Daylight Saving Time : ● Not Use ○ Use

Update Interval : 30 seconds

Figure 4-7. The Time configuration

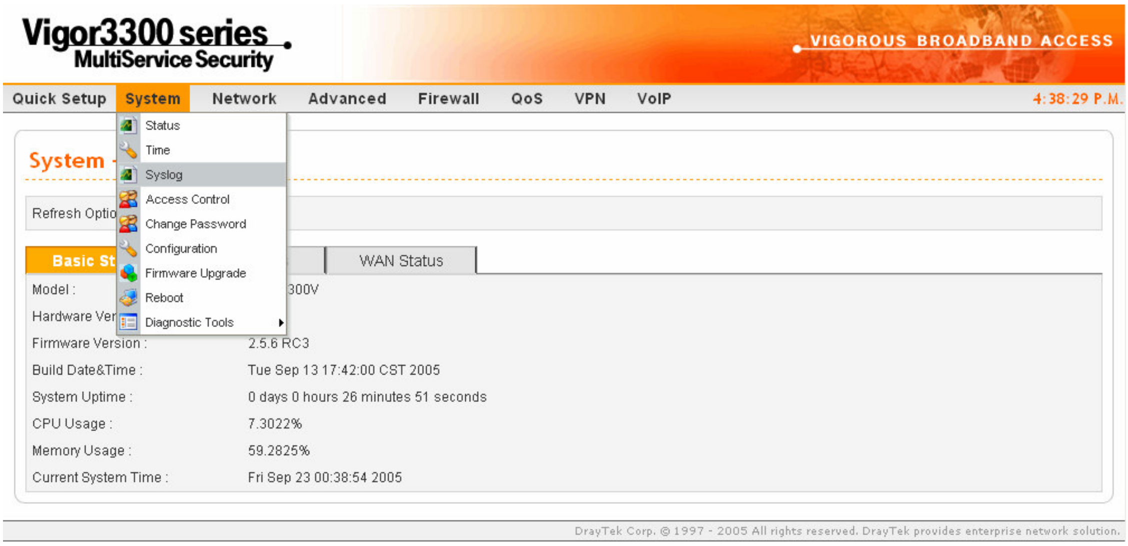
Use Browser Time	Click this option to use the browser time from the remote administrator PC host as 3300 system time.
Use NTP Time	Click this option to use the time from an NTP server as 3300 system time.
NTP Server	Assign a public IP address or domain name of the NTP server.
Time Zone	Select the time zone where the Vigor3300 is located.
Daylight Savings Time	Select "**Use**" to activate this function.
Update Interval	Select a time interval for updating from the NTP server.

Click **Apply** to save these settings.

4.3 Syslog Setup

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 on the Vigor3300.

In the **System** group, the click **Syslog** option. Figure 4-8 illustrates shows the location of this option.

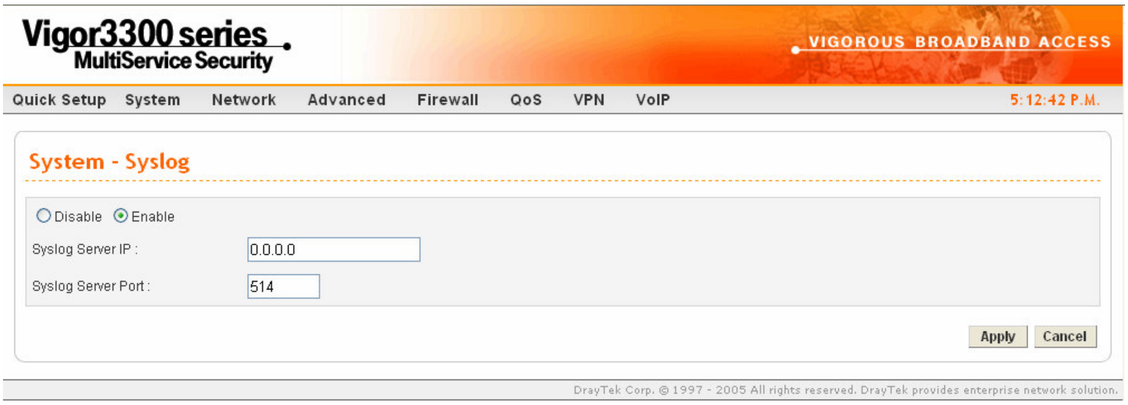


Model : 300V
Hardware Ver
Firmware Version : 2.5.6 RC3
Build Date&Time : Tue Sep 13 17:42:00 CST 2005
System Uptime : 0 days 0 hours 26 minutes 51 seconds
CPU Usage : 7.3022%
Memory Usage : 59.2825%
Current System Time : Fri Sep 23 00:38:54 2005

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

Figure 4-8. The Syslog option

After clicking the **Syslog** option, you will see the following Web page as shown in Figure 4-9.


Vigor3300 series
MultiService Security
VIGOROUS BROADBAND ACCESS
Quick Setup
System
Network
Advanced
Firewall
QoS
VPN
VoIP
5:12:42 P.M.
Apply
Cancel
DrayTek Corp. © 1997 - 2005 All rights reserved. DrayTek provides enterprise network solution.

System - Syslog

○ Disable ● Enable

Syslog Server IP : 0.0.0.0

Syslog Server Port : 514

Figure 4-9. The Syslog configuration

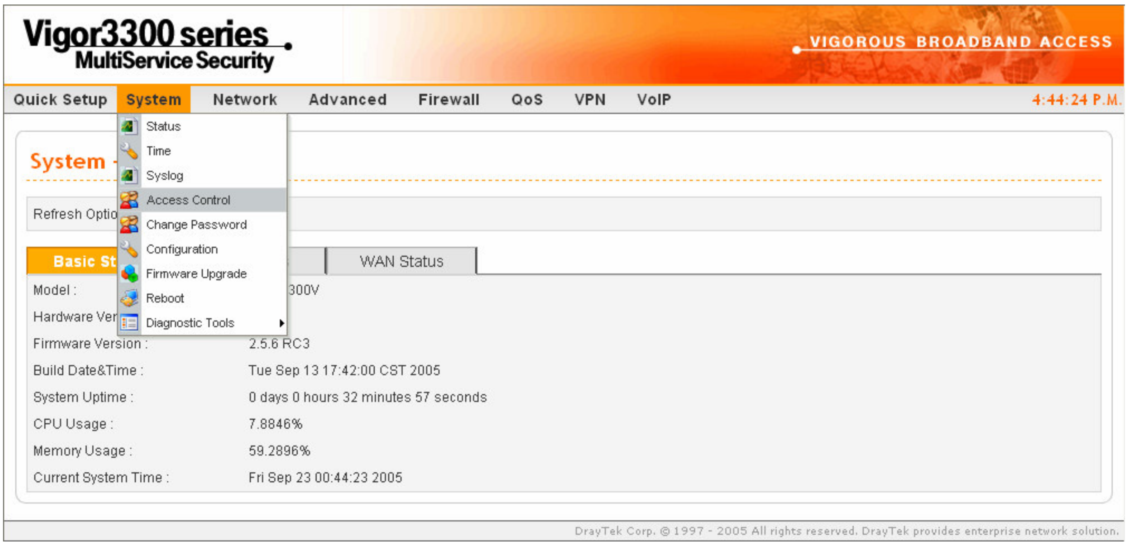
Status	Click "**Enable**" to activate this function.
Syslog Server IP	The IP address of the Syslog server. If the user assigns an IP address of "0.0.0.0", the Syslog function will be disabled Vigor3300 will not send Syslog packets to the Syslog server.
Syslog Server Port	Assign a port for the Syslog protocol.

Click **Apply** to save these settings.

4.4 Access Control Setup

Access control protects the user from ICMP attacking from virus-launched routers. You can disable the ping function from the LAN side when there are worm-type viruses on your LAN network to prevent the virus from spreading. However, such a configuration is not suggested under normal circumstances because it will also block normal query packets.

In the **System** group, click the **Access Control** option to bring up the following Web page as shown in Figure 4-10.



Model : 300V

Hardware Ver

Firmware Version : 2.5.6 RC3

Build Date&Time : Tue Sep 13 17:42:00 CST 2005

System Uptime : 0 days 0 hours 32 minutes 57 seconds

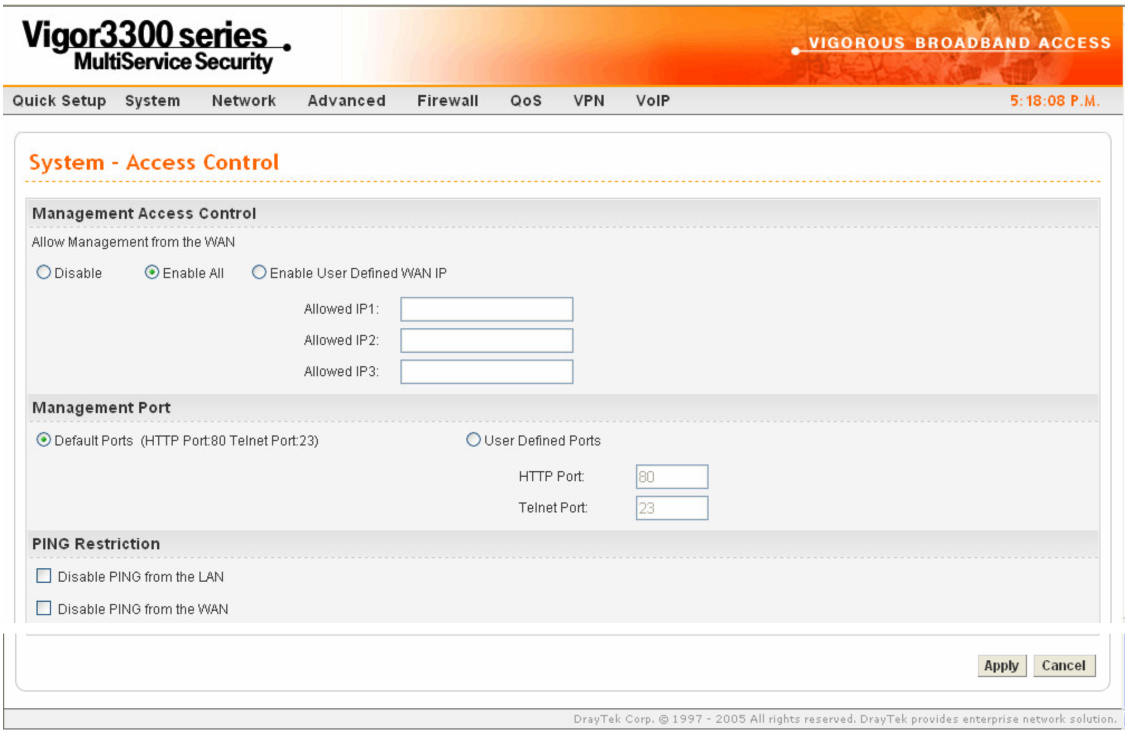
CPU Usage : 7.8846%

Memory Usage : 59.2896%

Current System Time : Fri Sep 23 00:44:23 2005

Figure 4-10. The access control option

After clicking the **Access Control** option**,** you will see the following setup Web page as shown in Figure 4-11.



Vigor3300 series
MultiService Security
VIGOROUS BROADBAND ACCESS
Quick Setup System Network Advanced Firewall QoS VPN VoIP
5:18:08 P.M.
Apply
Cancel
DrayTek Corp. © 1997 - 2005 All rights reserved. DrayTek provides enterprise network solution.

System - Access Control

Management Access Control

Allow Management from the WAN

○ Disable ● Enable All ○ Enable User Defined WAN IP

Allowed IP1:

Allowed IP2:

Allowed IP3:

Management Port

● Default Ports (HTTP Port:80 Telnet Port:23) ○ User Defined Ports

HTTP Port: 80

Telnet Port: 23

PING Restriction

□ Disable PING from the LAN

□ Disable PING from the WAN

Figure 4-11. The access control configuration

The **Management Port** function allows the user to set a port number or to use the default port number in the Vigor3300 series. An administrator can allow three dedicated IP addresses to manage the system via WAN.

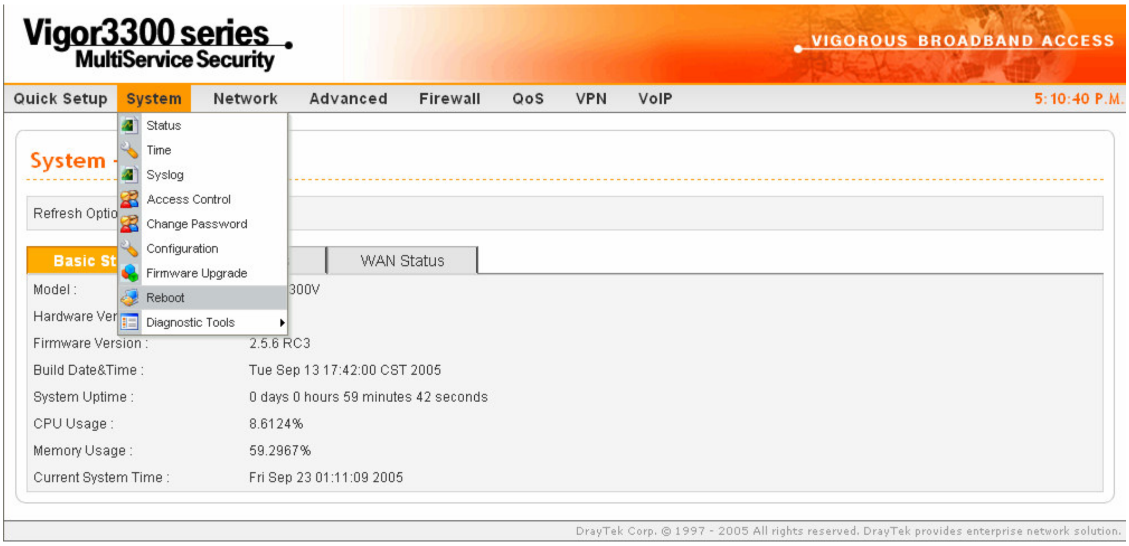
Management Access From WAN	
Disable All	Disable all management functions from the WAN interface.
Enable All	Enable all management functions from the WAN interface.
Enable User Defined WAN IP	System can be managed by these three IP addresses via WAN.
Management Port	
Default Ports (Http Port:80 Telnet Port:23)	Use the default ports for HTTP and Telnet
User Defined Ports	User can assign the new port numbers for HTTP and Telnet.
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.

Click **Apply** to save these settings.

4.5 Reboot and Firmware Upgrade Setup

4.5.1 Reboot Setup

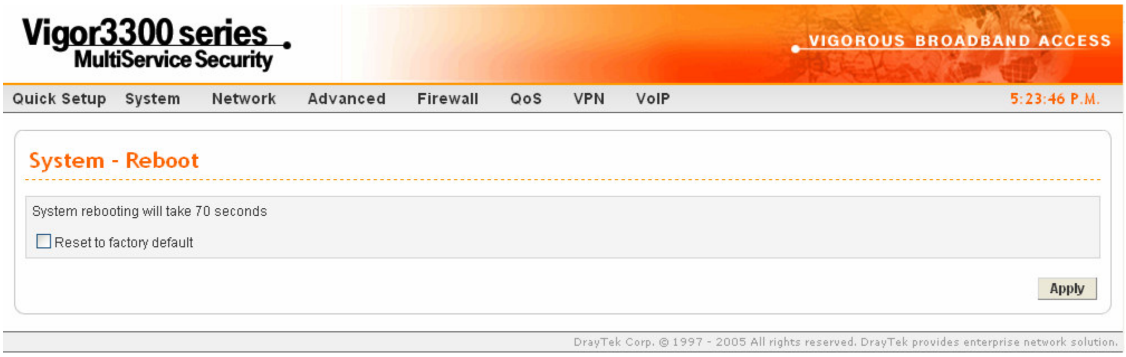
The Vigor3300 system can be restarted from a Web browser. In the **System** group, click the **Reboot** option. Figure 4-12 illustrates the location of the Reboot option.



Model : 300V
Hardware Ver
Firmware Version : 2.5.6 RC3
Build Date&Time : Tue Sep 13 17:42:00 CST 2005
System Uptime : 0 days 0 hours 59 minutes 42 seconds
CPU Usage : 8.6124%
Memory Usage : 59.2967%
Current System Time : Fri Sep 23 01:11:09 2005

Figure 4-12. The reboot option

After clicking the **Reboot** option, you will see the following Web page as shown in Figure 4-13. The user should choose to either keep the current configuration settings or use the default configuration after the Vigor3300 system has been rebooted.


Vigor3300 series
MultiService Security
VIGOROUS BROADBAND ACCESS
Quick Setup
System
Network
Advanced
Firewall
QoS
VPN
VoIP
5:23:46 P.M.
Apply
DrayTek Corp. © 1997 - 2005 All rights reserved. DrayTek provides enterprise network solution.

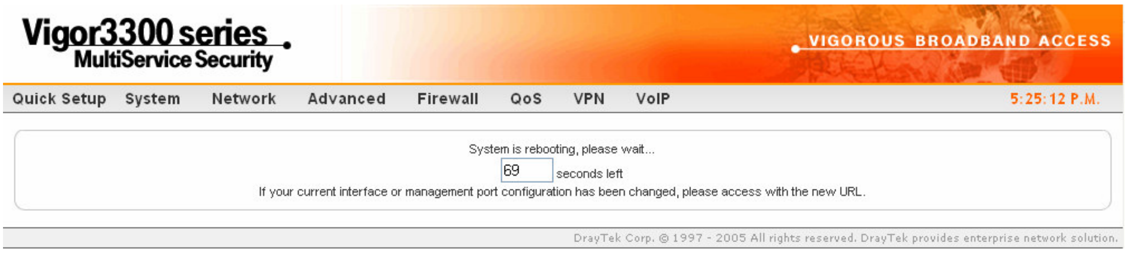
System - Reboot

System rebooting will take 70 seconds

□ Reset to factory default

Figure 4-13. The reboot configuration

Click **Apply** to reboot the whole system. The rebooting procedure usually takes 70 or more seconds. Figure 4-14 illustrates the reboot screen.


Vigor3300 series
MultiService Security
VIGOROUS BROADBAND ACCESS
Quick Setup
System
Network
Advanced
Firewall
QoS
VPN
VoIP
5:25:12 P.M.

System is rebooting, please wait...

69 seconds left

If your current interface or management port configuration has been changed, please access with the new URL.

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

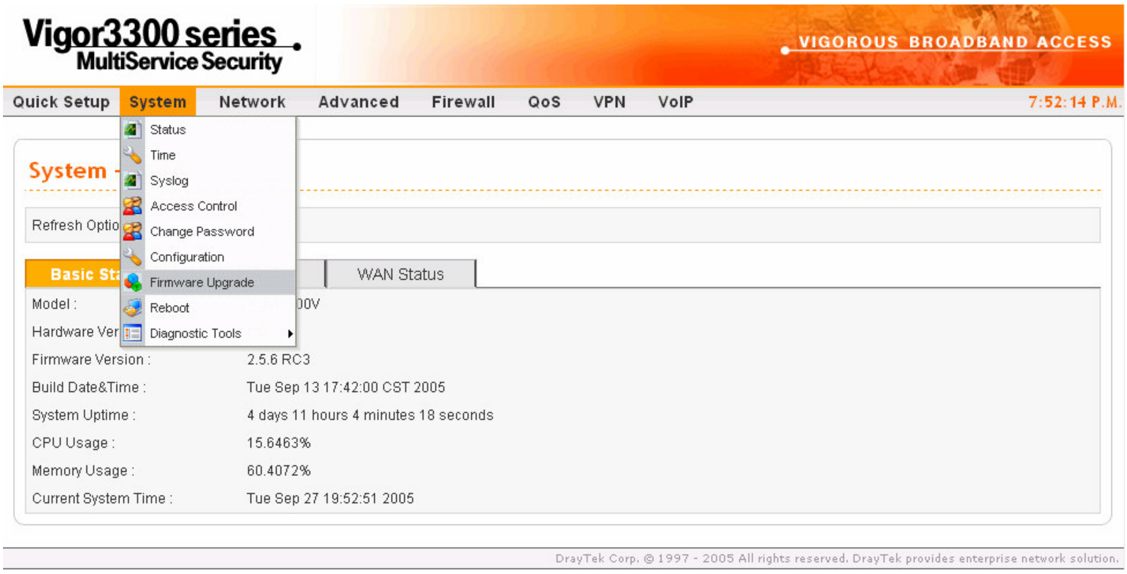
Figure 4-14. Reboot countdown

4.5.2 Firmware Upgrade by TFTP Server

Before upgrading your router firmware, you need to install the router tools on your local PC, which contains the Firmware Upgrade Utility. The following outlines the methods for upgrading the firmware on your router.

4.5.2.1 Firmware Upgrade from Web

Vigor3300 supports the function to upgrade firmware through a Web interface. In the **System** group, click the **Firmware Upgrade** option to bring up the following Web page as shown in Figure 4-15.

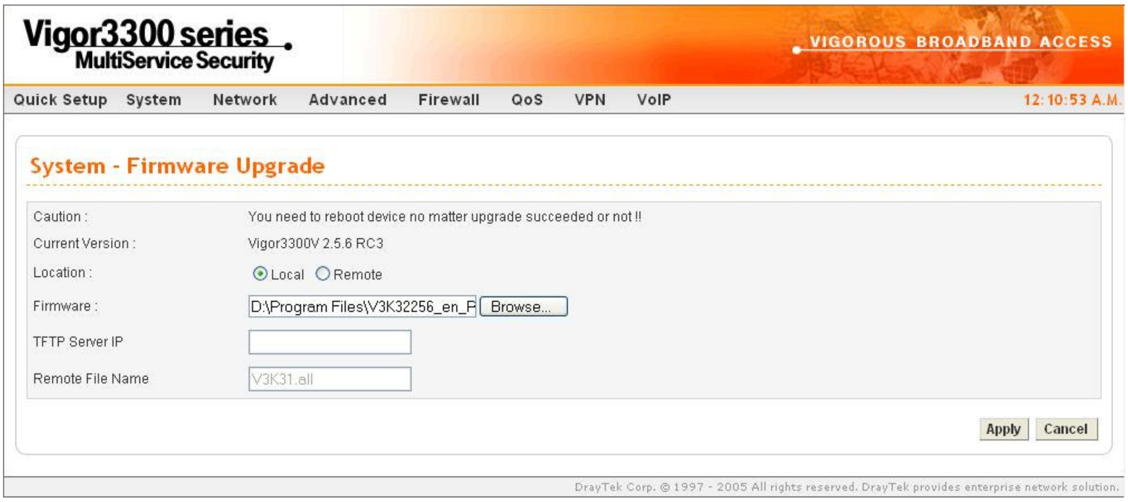


Model :	00V
Hardware Ver	
Firmware Version :	2.5.6 RC3
Build Date&Time :	Tue Sep 13 17:42:00 CST 2005
System Uptime :	4 days 11 hours 4 minutes 18 seconds
CPU Usage :	15.6463%
Memory Usage :	60.4072%
Current System Time :	Tue Sep 27 19:52:51 2005

Figure 4-15. The firmware upgrade option

After clicking the **Firmware Upgrade**, you will see the following Web page.

Figure 4-16 illustrates an example of this Web page running on a Windows environment.


Vigor3300 series
MultiService Security
VIGOROUS BROADBAND ACCESS
Quick Setup
System
Network
Advanced
Firewall
QoS
VPN
VoIP
12:10:53 A.M.

System - Firmware Upgrade

Caution :	You need to reboot device no matter upgrade succeeded or not !!
Current Version :	Vigor3300V 2.5.6 RC3
Location :	● Local ○ Remote
Firmware :	D:\Program Files\V3K32256_en_F Browse...
TFTP Server IP	
Remote File Name	V3K31.all

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

Figure 4-16. The firmware upgrade configuration

Location	**Local:** Upgrade firmware from a local TFTP server. **Remote:** Upgrade firmware from a remote TFTP server.
Firmware	If upgrading locally, select the location of the firmware file.
TFTP Server IP	If upgrading remotely, enter the IP address of the TFTP server.

To upload new firmware to your router:

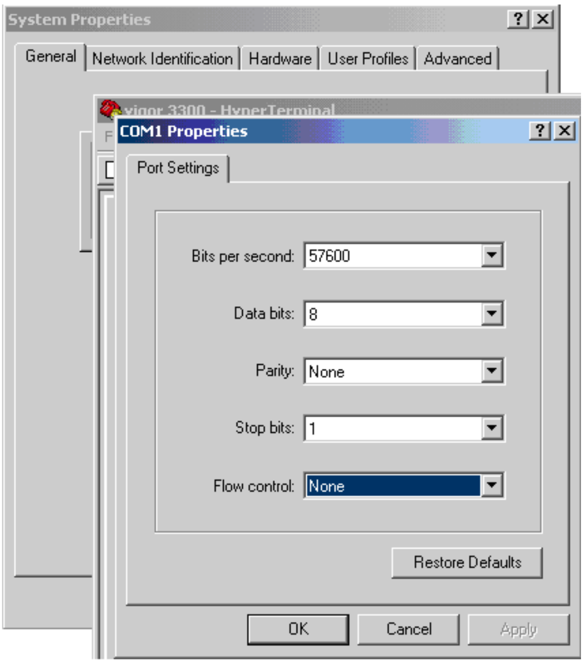
1. Download the newest firmware from the DrayTek's Website (**www.draytek.com.tw**) or FTP site (**ftp.draytek.com**).
2. Click the **Browse** button to locate the new firmware file and click **Apply**. The firmware will be prepared for upgrading and the status will be shown on the progress bar.
3. Click **Apply** to start the upgrading procedure. This process takes 3-5 minutes, and the router will reboot automatically once the upgrade is complete.

4.5.2.2 Firmware Upgrade from a Console Port

This section outlines how to perform a firmware upgrade from a console port. 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**).

2. Use the console management cable to connect the RJ45 connector to a console port on the Vigor3300 and the DB9 connector to an 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." Figure 4-17 illustrates an example of the console setup on a PC.



COM1 Properties

Port Settings

Bits per second: 57600

Data bits: 8

Parity: None

Stop bits: 1

Flow control: None

Figure 4-17. The console setup

3. Power on the Vigor3300, then press **ENTER** on the PC before the system reboots completely. The Vigor3300 can now 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.

4. Type the path name of the firmware image and start 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]*

5. After upgrading is finished, the system will automatically reboot.

4.6 Diagnostic Tools

In some cases, a user may need to know some information the router, such as some static or dynamic databases, or other routing information. The Vigor3300 series supports four functions for the user to review this information.

The Vigor3300 series diagnostic tool has four functions:

* Routing Table

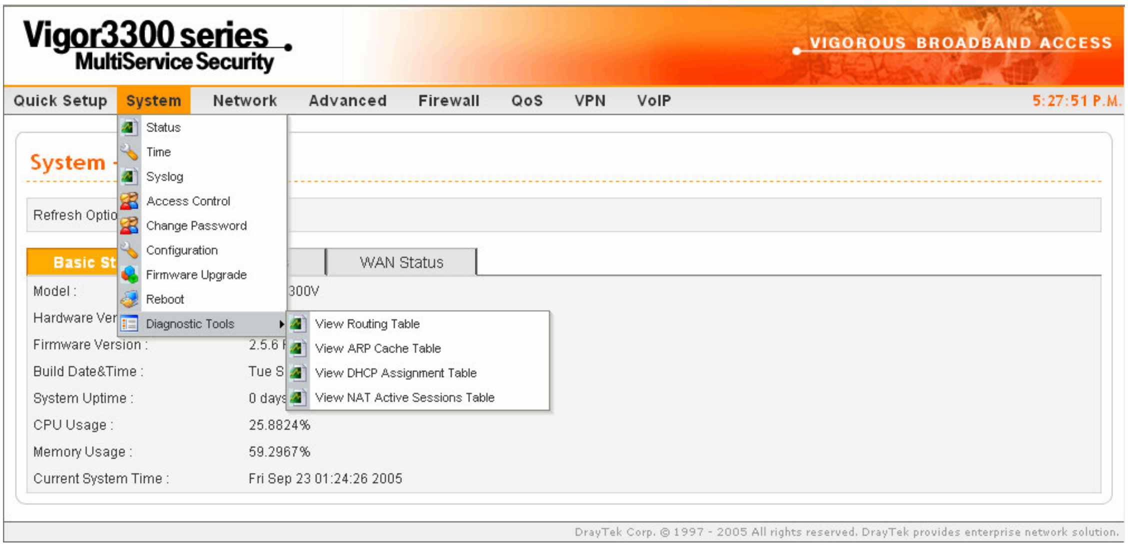
* ARP Cache Table

* DHCP Assignment Table

* NAT Active Sessions Table

We will give more detailed descriptions in following sections.

In the **System** group, click the **Diagnostic Tools** option, and then you will see the following Web page as shown in Figure 4-18.



Model : 300V

Hardware Ver

Firmware Version : 2.5.6 F

Build Date&Time : Tue S

System Uptime : 0 days

CPU Usage : 25.8824%

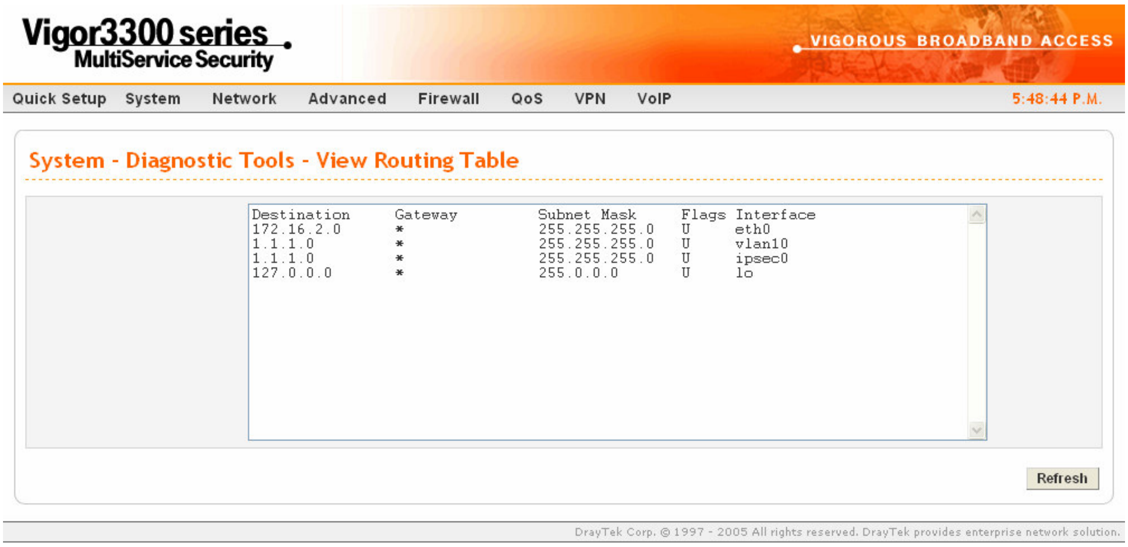
Memory Usage : 59.2967%

Current System Time : Fri Sep 23 01:24:26 2005

Figure 4-18. Functions of the diagnostic tools

4.6.1 The View Routing Table

After clicking the **View Routing Table** option, you will see the following Web page as shown in Figure 4-19.



Vigor3300 series
MultiService Security
VIGOROUS BROADBAND ACCESS
Quick Setup
System
Network
Advanced
Firewall
QoS
VPN
VoIP
5:48:44 P.M.
Refresh
DrayTek Corp. © 1997 - 2005 All rights reserved. DrayTek provides enterprise network solution.

System - Diagnostic Tools - View Routing Table

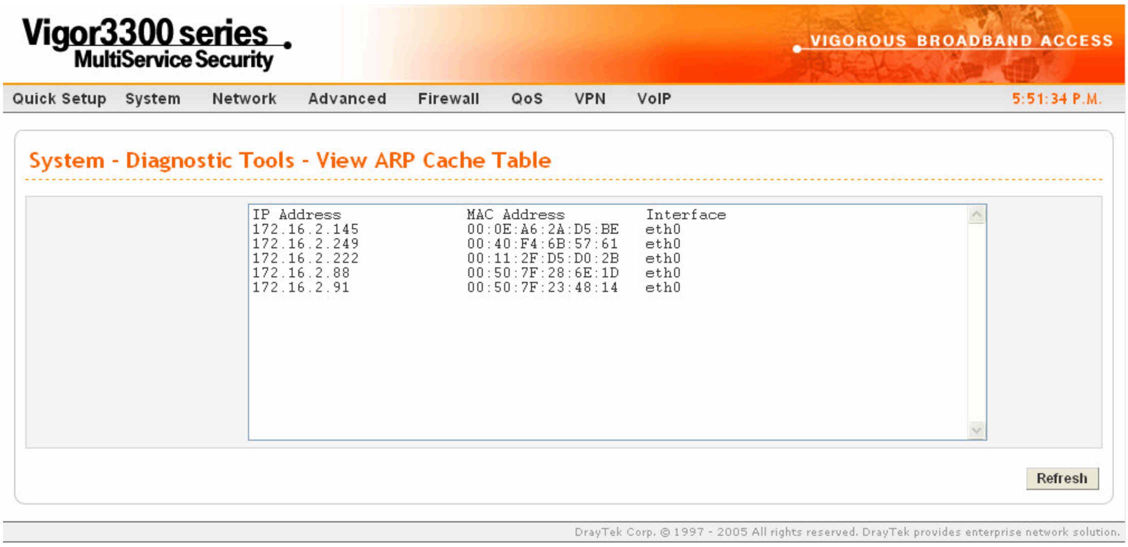
```
Destination     Gateway         Subnet Mask     Flags Interface
172.16.2.0      *               255.255.255.0   U     eth0
1.1.1.0         *               255.255.255.0   U     vlan10
1.1.1.0         *               255.255.255.0   U     ipsec0
127.0.0.0       *               255.0.0.0       U  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

Figure 4-19. The view routing table

In Figure 4-19, “Destination” stands for “destination IP address” and “Gateway” stands for “default gateway”. The “Flags” field describes the status of the routing entries. An interface will be denoted by eth0 if it is a LAN interface and eth1 if it is a WAN interface.

4.6.2 View ARP Cache Table

After clicking the **View ARP Cache Table** option, you will see the following Web page as shown in Figure 4-20.


Vigor3300 series
MultiService Security
VIGOROUS BROADBAND ACCESS
Quick Setup
System
Network
Advanced
Firewall
QoS
VPN
VoIP
5:51:34 P.M.
Refresh
DrayTek Corp. © 1997 - 2005 All rights reserved. DrayTek provides enterprise network solution.

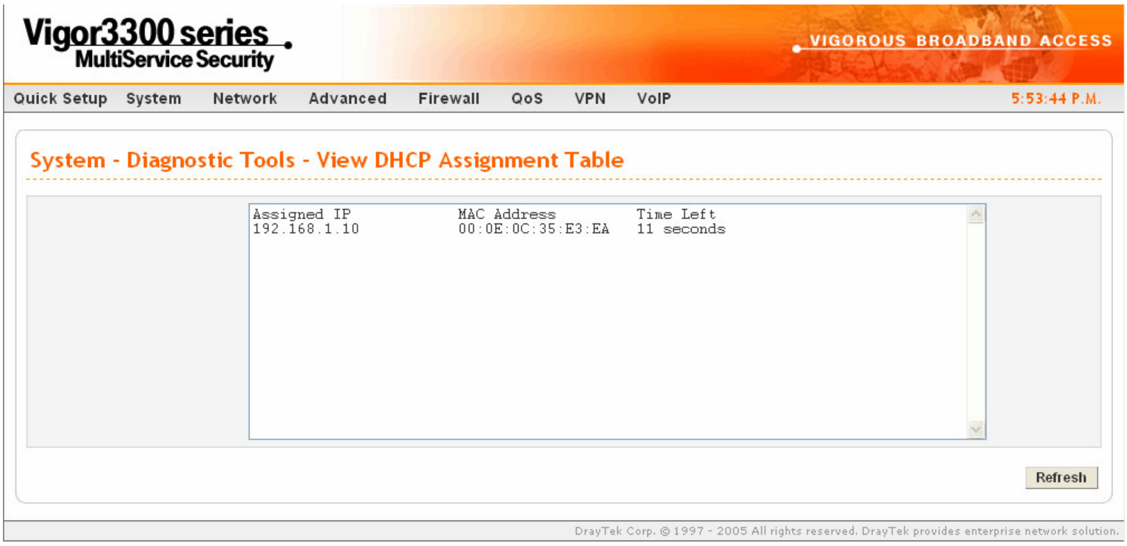
System - Diagnostic Tools - View ARP Cache Table

```
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
```

Figure 4-20. The view ARP cache table option

4.6.3 View DHCP Assignment Table

After clicking the **View DHCP Assignment Table** option, you will see the following Web page as shown in Figure 4-21.


Vigor3300 series
MultiService Security
VIGOROUS BROADBAND ACCESS
Quick Setup
System
Network
Advanced
Firewall
QoS
VPN
VoIP
5:53:44 P.M.
Refresh
DrayTek Corp. © 1997 - 2005 All rights reserved. DrayTek provides enterprise network solution.

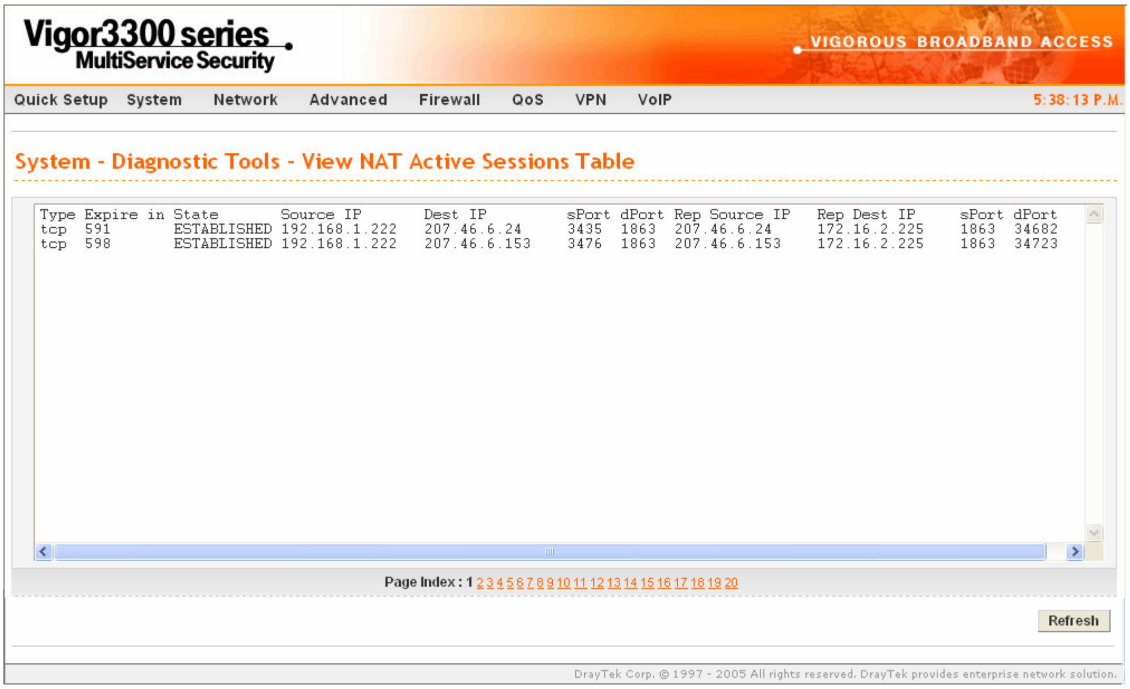
System - Diagnostic Tools - View DHCP Assignment Table

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

Figure 4-21. The view DHCP assignment table option

4.6.4 View NAT Active Sessions Table

After clicking the **View NAT Active Sessions Table** option, you will see the following Web page as shown in Figure 4-22.



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
```

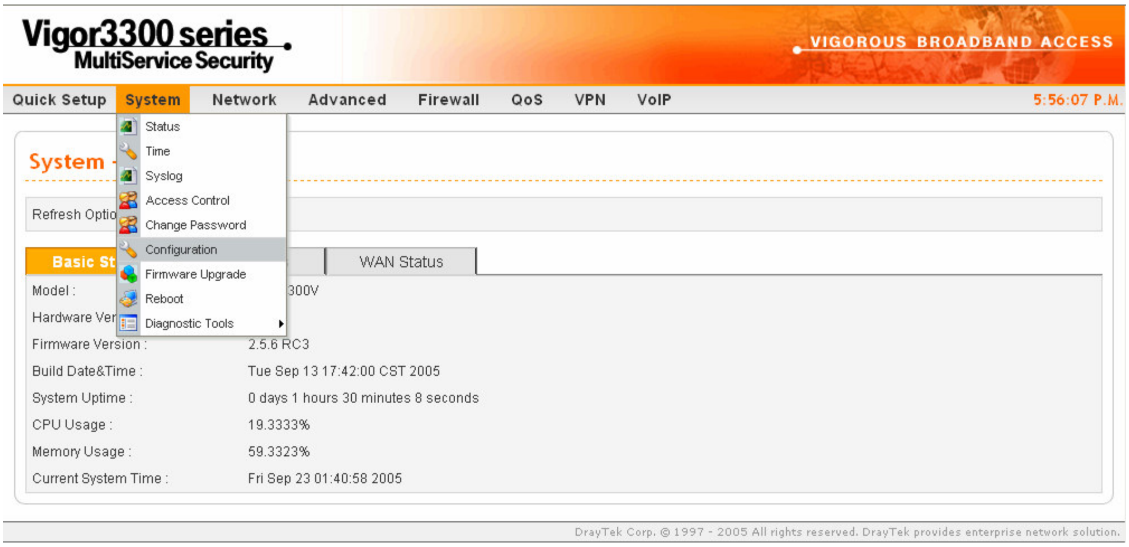
Page Index : 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20

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

Figure 4-22. The view NAT active sessions table option

4.7 Configuration Setup

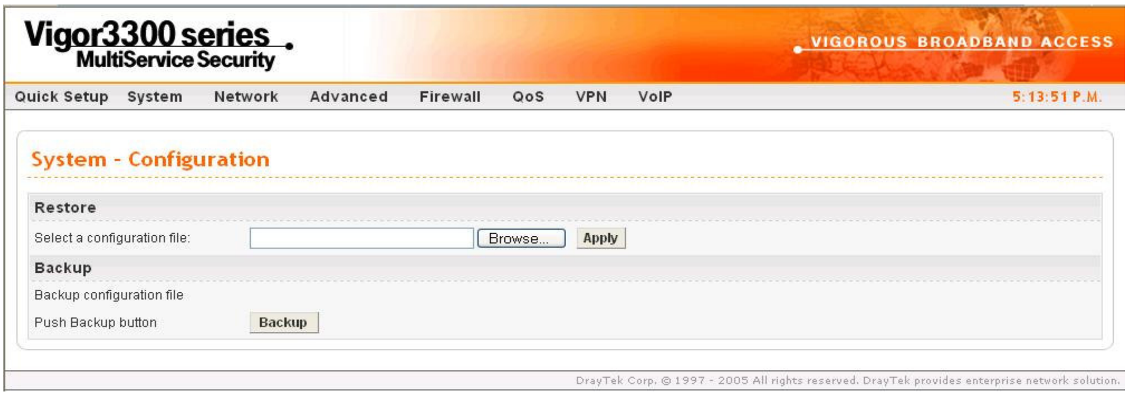
Most of the settings can be saved locally as a configuration file, which can be applied to another router. The Vigor3300 series supports the restore and upload functions of **configuration files.** In the System group, click the **Configuration Setup** option to bring up the following Web page as shown in Figure 4-23.



Model : 300V
Hardware Ver
Firmware Version : 2.5.6 RC3
Build Date&Time : Tue Sep 13 17:42:00 CST 2005
System Uptime : 0 days 1 hours 30 minutes 8 seconds
CPU Usage : 19.3333%
Memory Usage : 59.3323%
Current System Time : Fri Sep 23 01:40:58 2005

Figure 4-23. The configuration setup option

After clicking the **Configuration** option, you will see the following setup Web page as shown in Figure 4-24.



System - Configuration

Restore

Select a configuration file:

Backup

Backup configuration file

Push Backup button

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

Figure 4-24. The configuration file function

Upload	
Select a Configuration File	The location of the configuration file to be uploaded to the router.
Download	
Download Configuration File Push Download Button	Download the configuration file to a local host. The default file name is "**v3300.cfg**".

CHAPTER 5

Network Setup

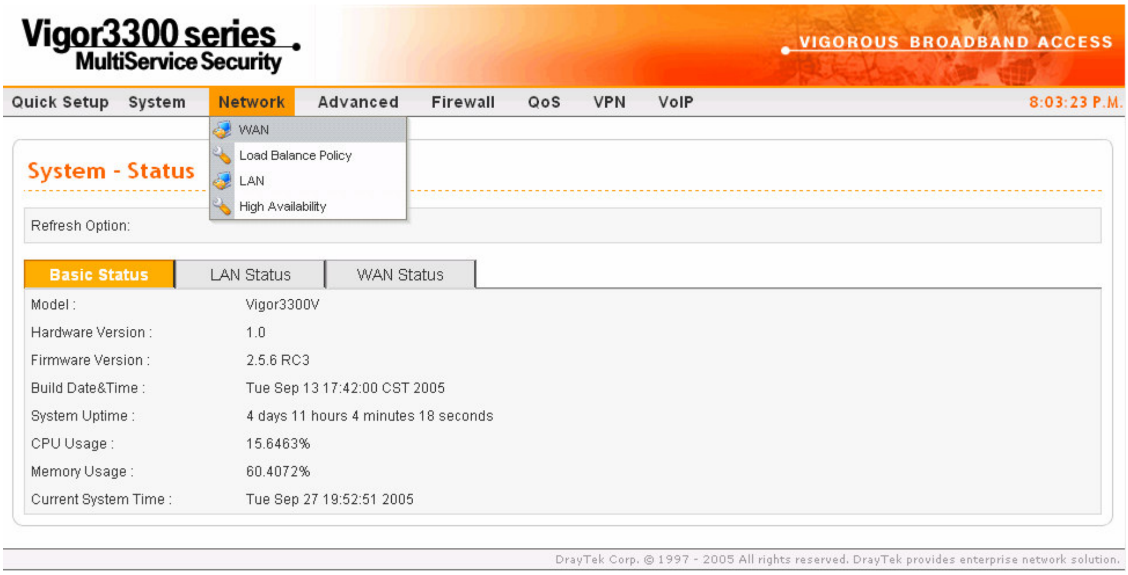
This chapter shows how to setup the router to access the Internet in **WAN** and **LAN** interfaces.

This chapter is divided into the following sections.

- Section 5.1: WAN and Internet Access Setup
- Section 5.2: LAN Setup
- Section 5.3: Load Balance Policy
- Section 5.4: High Availability Setup

5.1 WAN and Internet Access Setup

The Vigor3300 series supports four WAN interfaces, which share the same setting page. These WAN interfaces need to be configured for Internet access. In the **Network** group, click the **WAN** option as shown in Figure 5.1.



System - Status

Refresh Option:

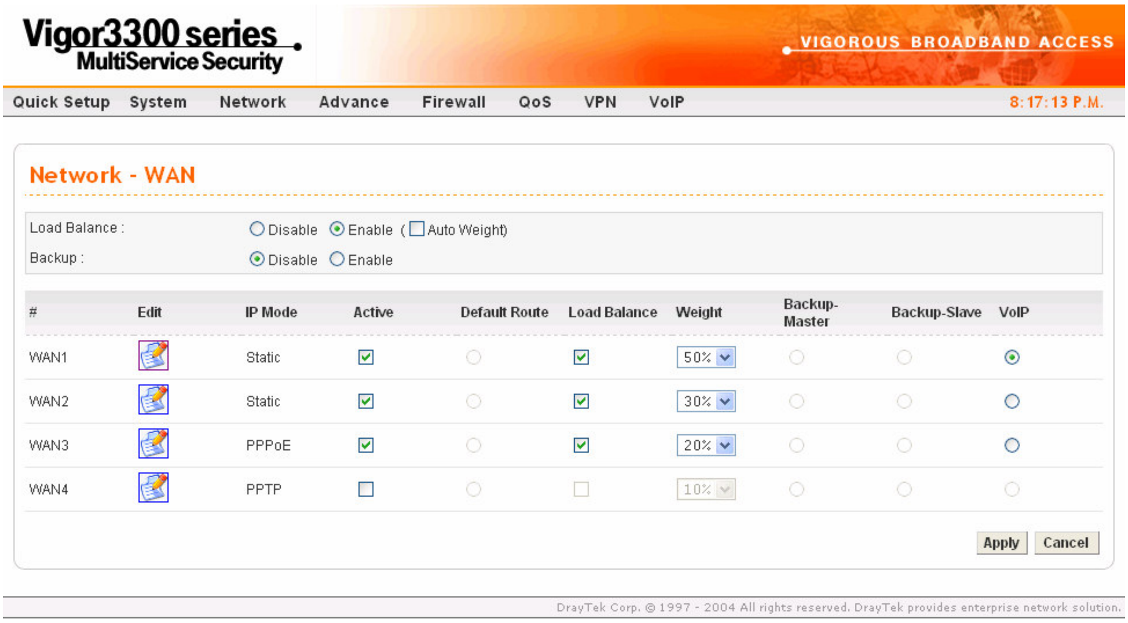
Basic Status | LAN Status | WAN Status

Model :	Vigor3300V
Hardware Version :	1.0
Firmware Version :	2.5.6 RC3
Build Date&Time :	Tue Sep 13 17:42:00 CST 2005
System Uptime :	4 days 11 hours 4 minutes 18 seconds
CPU Usage :	15.6463%
Memory Usage :	60.4072%
Current System Time :	Tue Sep 27 19:52:51 2005

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

Figure 5-1. The WAN option

After clicking the **WAN** option, you will see the following page as shown in Figure 5-2.



Network - WAN

Load Balance : ○ Disable ● Enable (□ Auto Weight)

Backup : ● Disable ○ Enable

#	Edit	IP Mode	Active	Default Route	Load Balance	Weight	Backup-Master	Backup-Slave	VoIP
WAN1		Static	☑	○	☑	50%	○	○	●
WAN2		Static	☑	○	☑	30%	○	○	○
WAN3		PPPoE	☑	○	☑	20%	○	○	○
WAN4		PPTP	□	○	□	10%	○	○	○

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

Figure 5-2. WAN interfaces

Load Balance	"**Enable**" or "**Disable**" the WAN load balance function. The **Auto Weight** option becomes available if "**Enable**" mode is selected.
Backup	**"Enable"** or **"Disable"** backup function for WAN interfaces.
Edit	Link to configuration page of this WAN interface.
IP Mode	The current mode of this WAN interface. There are four options: ● Static ● DHCP ● PPPoE ● PPTP
Active	Activate/deactivate this WAN interface.
Default Route	Set this WAN interface as default route interface.
Load Balance	Add this WAN interface to the load balance group.

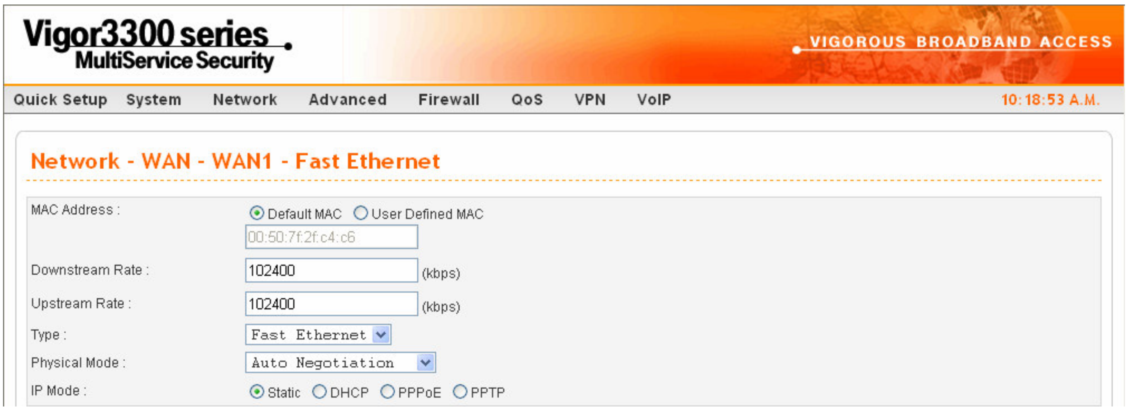
Weight	Set the weight load (10-90%) for this WAN interface for load balance.
Backup-Master	Set this WAN interface as a master interface.
Backup-Slave	Set this WAN interface as a slave interface.
VoIP	Set this WAN interface as VoIP default interface.

Note:

If user enables backup function, user has to assign the WAN1 as Master interface absolutely.

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 on Figure 5-3.



Network - WAN - WAN1 - Fast Ethernet

MAC Address :	● Default MAC ○ User Defined MAC 00:50:7f:2f:c4:c6
Downstream Rate :	102400 (kbps)
Upstream Rate :	102400 (kbps)
Type :	Fast Ethernet
Physical Mode :	Auto Negotiation
IP Mode :	● Static ○ DHCP ○ PPPoE ○ PPTP

Figure 5-3. WAN interface configuration

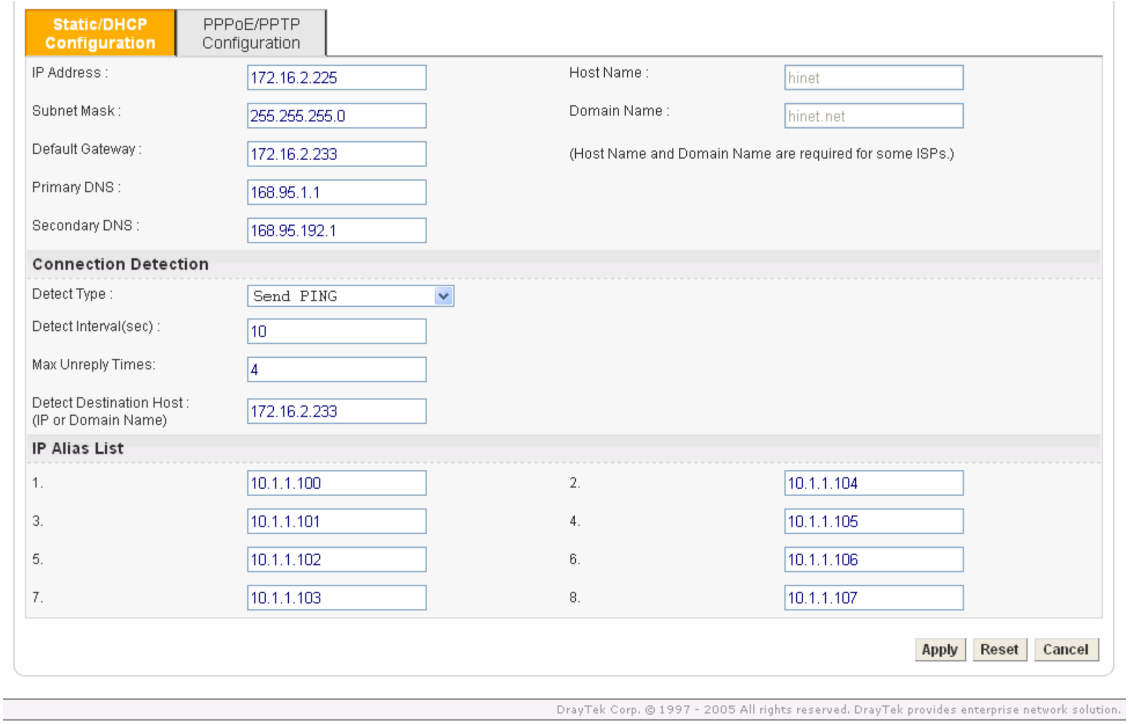
MAC Address	
Default MAC	Select the default Mac address.
User Defined MAC	Select a MAC address defined by user.

Downstream Rate	Set downstream rate for this WAN interface. The default value is 102400 kbps (100 Megabit).
Upstream Rate	Set transmission rate for this WAN interface. The default value is 102400 kbps (100 Megabit).
Type	Set connection type for this WAN interface.
Physical Mode	Set connection speed mode. There are five options for **Auto negotiation**, **full duplex**, **and half duplex,** 10M or 100M.
IP Mode	Set IP Mode to **Static (fixed IP**), **DHCP (dynamic IP address), PPPoE,** or **PPTP** and creates IP group information. Most cable modem users use DHCP to get a globally reachable IP address from the cable head-end system.

Before you connect a broadband access device e.g. a DSL/Cable modem to the router, 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 and **DHCP** for Cable modem. In most cases, you will get a DSL or cable modem from the broadband access service provider. The router is connected behind the broadband device i.e. DSL/cable modem and works as a NAT or IP router for broadband connections.

5.1.1 Static IP Setup

The IP group information for each WAN interface can be manually assigned by the user and shown in Figure 5-4.



IP Address :	172.16.2.225	Host Name :	hinet
Subnet Mask :	255.255.255.0	Domain Name :	hinet.net
Default Gateway :	172.16.2.233	(Host Name and Domain Name are required for some ISPs.)	
Primary DNS :	168.95.1.1		
Secondary DNS :	168.95.192.1		

Connection Detection

Detect Type :	Send PING
Detect Interval(sec) :	10
Max Unreply Times:	4
Detect Destination Host : (IP or Domain Name)	172.16.2.233

IP Alias List

1.	10.1.1.100	2.	10.1.1.104
3.	10.1.1.101	4.	10.1.1.105
5.	10.1.1.102	6.	10.1.1.106
7.	10.1.1.103	8.	10.1.1.107

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

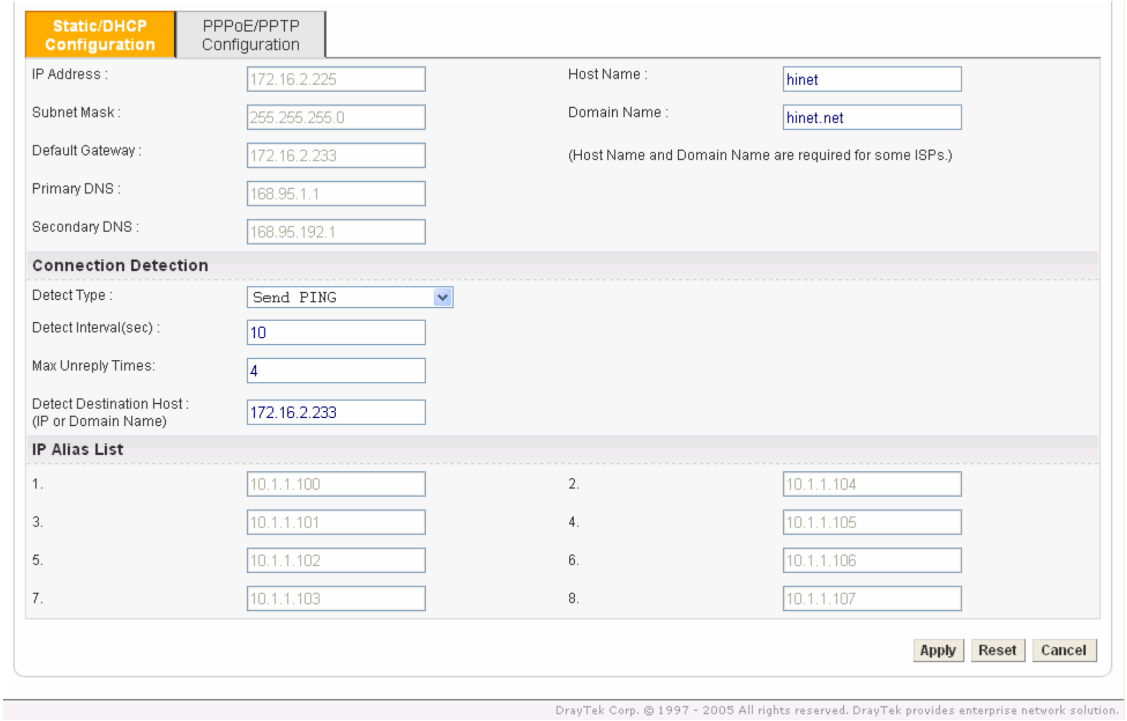
Figure 5-4. Static IP configuration

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.
Connection Detection	
Detect Type	Select a detecting type for this WAN interface. There are three ways "**ARP**", "**PING**" and "**HTTP**" supported in 3300.
Detect Interval(sec)	Assign an interval period of time for each detecting.
Max Unreply Times	Assign detecting times to ensure the connection of the WAN.
Detect Destination Host (IP or Domain Name)	Assign an IP address or Domain name as a destination to be detected.
IP Alias List	Sets other IP addresses binding in this interface.

Click **Apply** to go back to the WAN Interface Configuration page as shown in Figure 5-3. To apply all settings, click **Apply** on the WAN Interface Configuration page and reboot your router when prompted.

5.1.2 DHCP Client Setup

If the WAN interface is set as a DHCP client, the Vigor3300 will ask for IP network settings from the DHCP server or DSL modem automatically. It is not necessary for the user to manually configure the router on Figure 5-5.



IP Address :	172.16.2.225	Host Name :	hinet
Subnet Mask :	255.255.255.0	Domain Name :	hinet.net
Default Gateway :	172.16.2.233	(Host Name and Domain Name are required for some ISPs.)	
Primary DNS :	168.95.1.1		
Secondary DNS :	168.95.192.1		

Connection Detection

Detect Type :	Send PING
Detect Interval(sec) :	10
Max Unreply Times:	4
Detect Destination Host : (IP or Domain Name)	172.16.2.233

IP Alias List

1.	10.1.1.100	2.	10.1.1.104
3.	10.1.1.101	4.	10.1.1.105
5.	10.1.1.102	6.	10.1.1.106
7.	10.1.1.103	8.	10.1.1.107

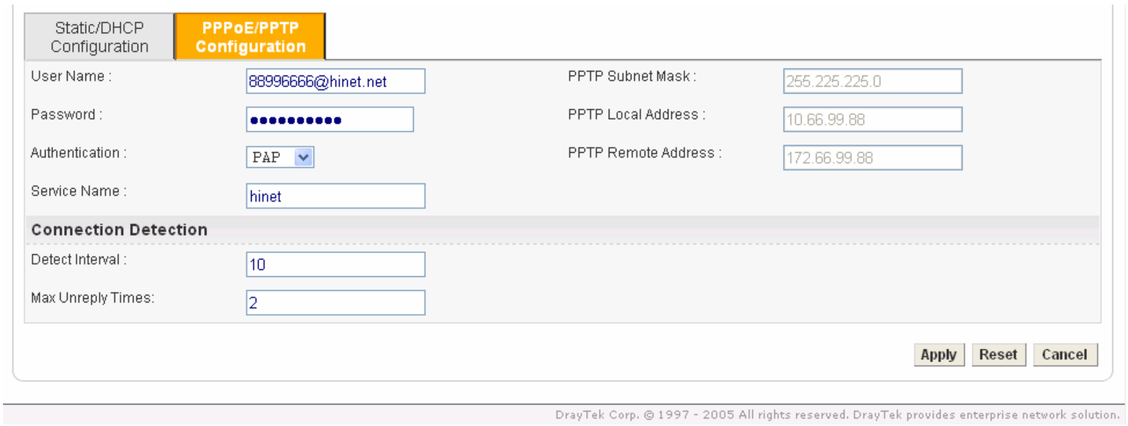
DrayTek Corp. © 1997 - 2005 All rights reserved. DrayTek provides enterprise network solution.

Figure 5-5. DHCP configuration

Click **Apply** to go back to the WAN Interface Configuration page as shown in Figure 5-3. To apply all settings, click **Apply** on the WAN Interface Configuration page and reboot your router when prompted.

5.1.3 PPPoE with a DSL Modem Setup

Most DSL modem users use this mode. All local users can share one PPPoE connection to access the Internet as shown in Figure 5-6.



User Name : 88996666@hinet.net

Password : ●●●●●●●●●●

Authentication : PAP

Service Name : hinet

PPTP Subnet Mask : 255.225.225.0

PPTP Local Address : 10.66.99.88

PPTP Remote Address : 172.66.99.88

Connection Detection

Detect Interval : 10

Max Unreply Times: 2

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

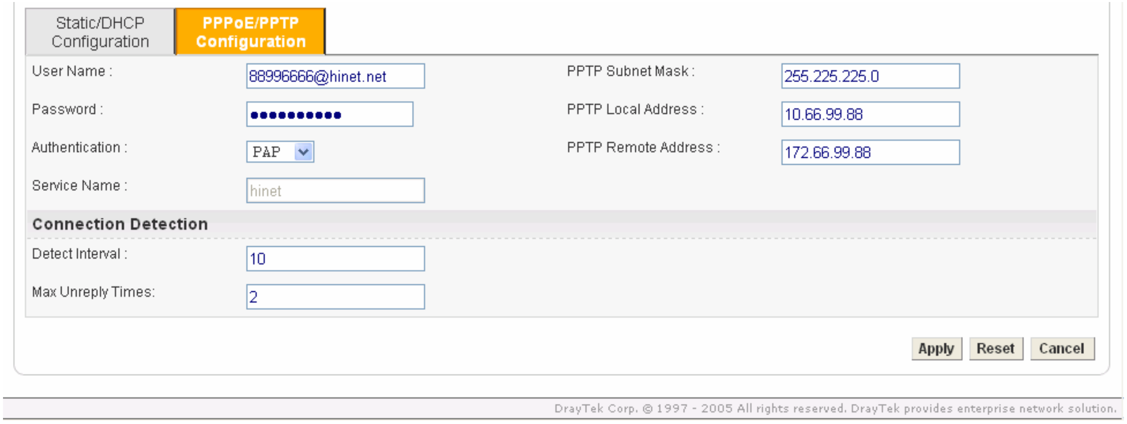
Figure 5-6. PPPoE configuration

User Name	Assign a specific valid user name provided from a local ISP.
Password	Assign a valid password provided from a local ISP.
Authentication	Select **PAP** or **CHAP** protocol for widest compatibility. The default value is **PAP**.
Service Name	Assign a service name required from ISP service.
Connection Detection	
Detect Interval	Assign an interval time for detecting.
Max Unreply Times	Assign detecting times to ensure the connection of WAN.

Click **Apply** to go back to the WAN interface configuration page as shown in Figure 5-3. To apply all settings, click **Apply** on the WAN interface configuration page and reboot your router when prompted.

5.1.4 PPTP with a DSL Modem Setup

The following setup page is just an example on Figure 5-7. Your service provider should provide the exact settings.



User Name :	88996666@hinet.net	PPTP Subnet Mask :	255.225.225.0
Password :	●●●●●●●●●●●	PPTP Local Address :	10.66.99.88
Authentication :	PAP	PPTP Remote Address :	172.66.99.88
Service Name :	hinet		

Connection Detection

Detect Interval :	10
Max Unreply Times:	2

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

Figure 5-7. PPTP configuration

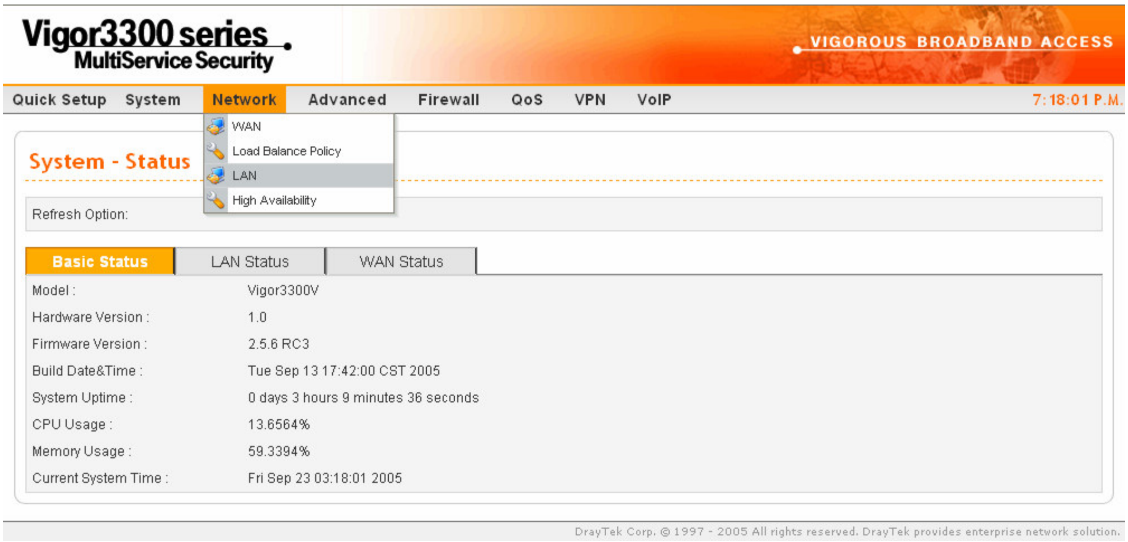
PPTP Local Address	Assign a local IP address.
PPTP Subnet Mask	Assign a subnet mask value of IP address.
PPTP Remote Address	Assign a remote IP address of PPTP server.

Click **Apply** to go back to the WAN Interface Configuration page as shown in Figure 5-3. To apply all settings, click **Apply** on the WAN Interface Configuration page and reboot your router when prompted.

5.2 LAN Setup

In this section, we will explain more details on the **LAN** interface setup.

In the **Network** group, click **LAN** option as shown in Figure 5-8.

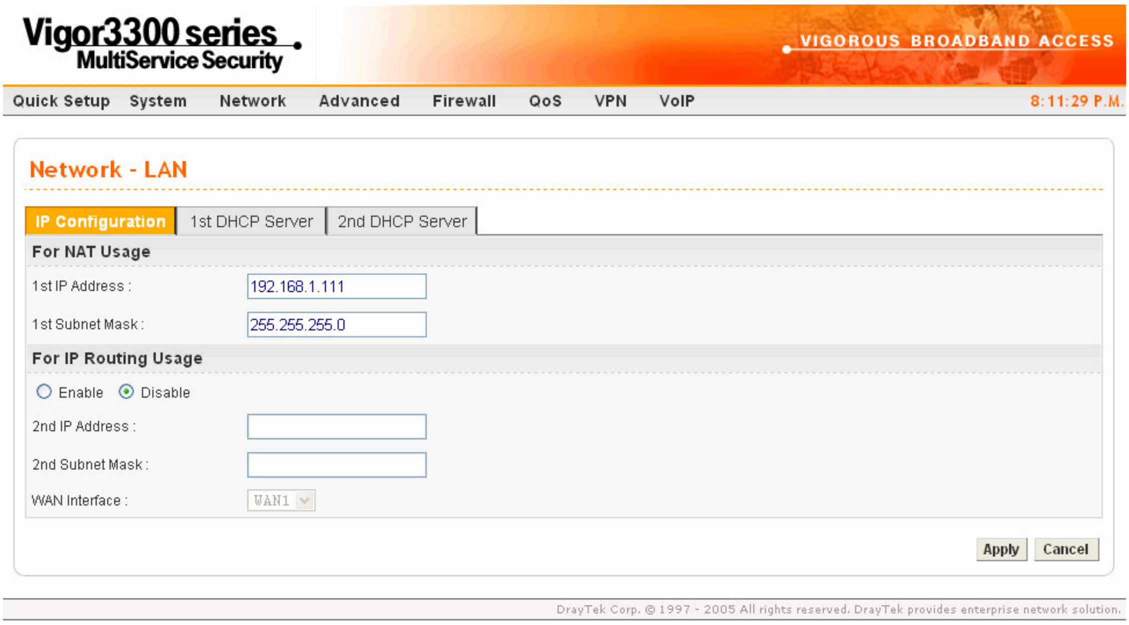


Model :	Vigor3300V
Hardware Version :	1.0
Firmware Version :	2.5.6 RC3
Build Date&Time :	Tue Sep 13 17:42:00 CST 2005
System Uptime :	0 days 3 hours 9 minutes 36 seconds
CPU Usage :	13.6564%
Memory Usage :	59.3394%
Current System Time :	Fri Sep 23 03:18:01 2005

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

Figure 5-8. The LAN option

After clicking the **LAN** option, you will see the following page as shown in Figure 5-9.



Network - LAN

For NAT Usage

1st IP Address : 192.168.1.111

1st Subnet Mask : 255.255.255.0

For IP Routing Usage

○ Enable ● Disable

2nd IP Address :

2nd Subnet Mask :

WAN Interface : WAN1

Figure 5-9. LAN configuration

There are three options:

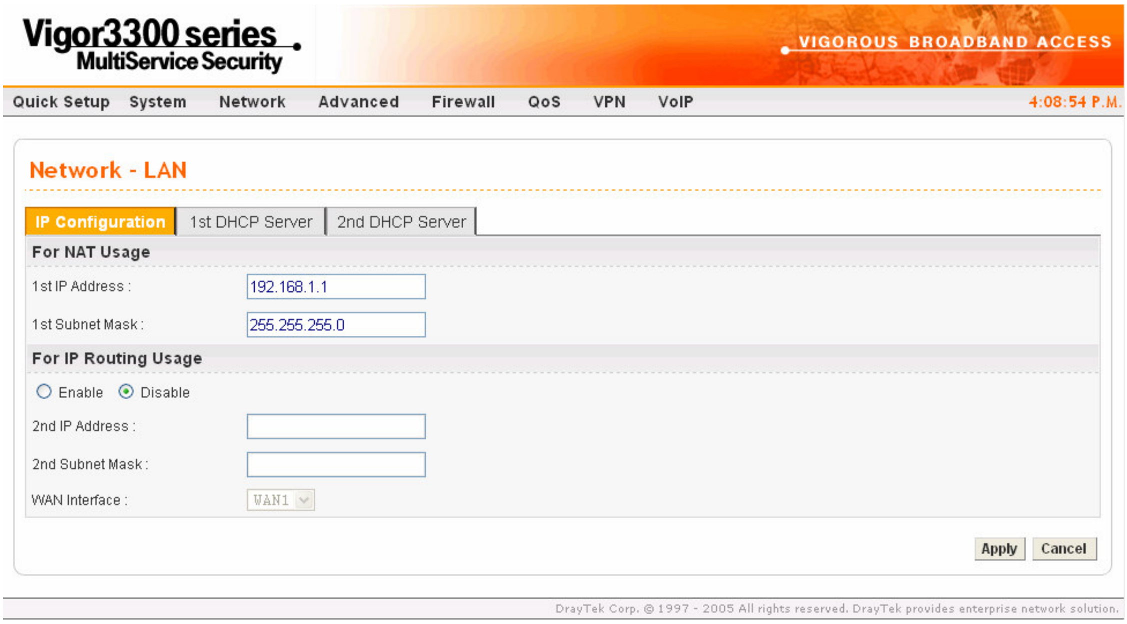
IP Configuration

1st DHCP Server

2nd DHCP Server

5.2.1 IP Configuration

After clicking **IP Configuration**, you will see the following page as shown in Figure 5-10.


Vigor3300 series
MultiService Security
VIGOROUS BROADBAND ACCESS
Quick Setup System Network Advanced Firewall QoS VPN VoIP
4:08:54 P.M.
Network - LAN
IP Configuration | 1st DHCP Server | 2nd DHCP Server
Apply Cancel
DrayTek Corp. © 1997 - 2005 All rights reserved. DrayTek provides enterprise network solution.

For NAT Usage

1st IP Address : 192.168.1.1

1st Subnet Mask : 255.255.255.0

For IP Routing Usage

○ Enable ● Disable

2nd IP Address :

2nd Subnet Mask :

WAN Interface : WAN1

Figure 5-10. IP configuration

In the Vigor3300 router, there are some IP address settings for the LAN interface as shown below. The IP address/subnet mask is for private users or NAT users. To allow public users, you need to subscribe to a globally reachable subnet from your ISP. The IP address of the default gateway on other local PCs should be set as the Vigor3300's 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 the 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.

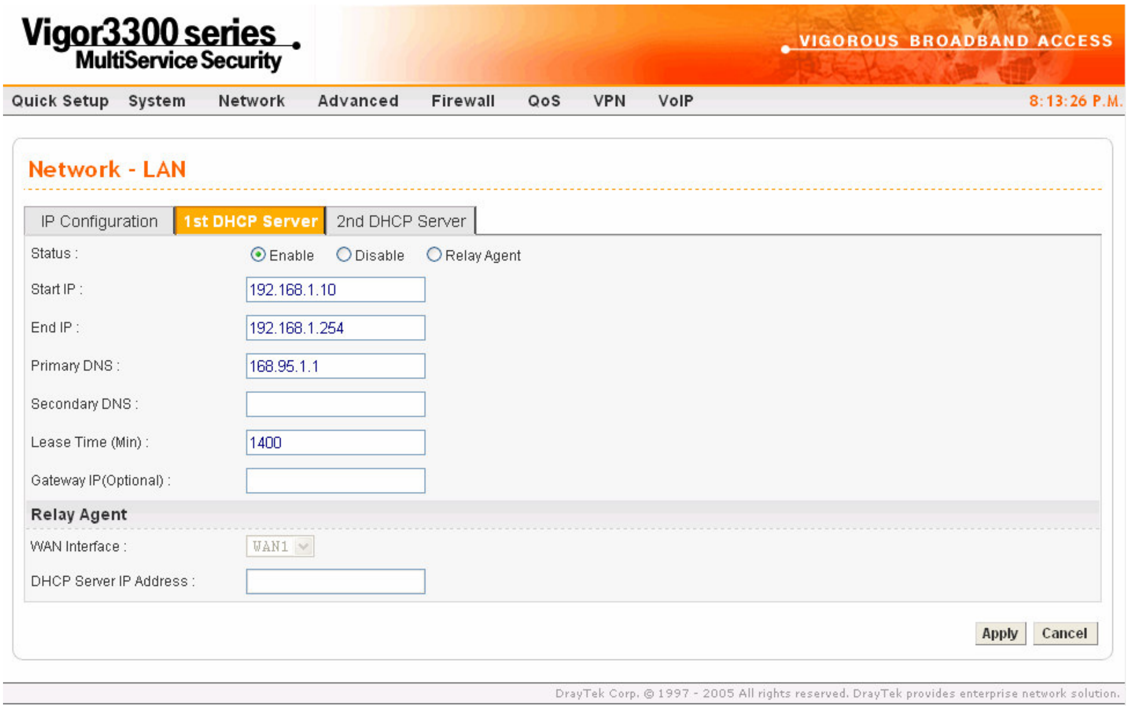
NAT Usage	
1st IP Address	The first private IP address connecting to a local private network. The default value is 192.168.1.1.
1st Subnet Mask	The subnet mask value of the first private IP address connecting to a local private network. The default value is 255.255.255.0.
IP Routing Usage	
Status	"**Enable**" IP Routing Usage. "**Disable**" IP Routing Usage.
2nd IP Address	Assign an IP address belongs to the subnet of the WAN selected in WAN Interface field.
2nd Subnet Mask	The value of subnet mask.
WAN Interface	Select a WAN interface to be applied in IP Routing Usage.

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

5.2.2 1st DHCP Server Configuration

The Vigor3300 series supports two DHCP servers.
DHCP stands for Dynamic Host Configuration Protocol. It acts as DHCP client and can automatically dispatch related IP settings from DHCP server. Please refer to the following picture for DHCP server configuration.

After clicking the **1st DHCP Server** option, you will see the following page as shown in Figure 5-11.



Network - LAN

Status :	● Enable ○ Disable ○ Relay Agent
Start IP :	192.168.1.10
End IP :	192.168.1.254
Primary DNS :	168.95.1.1
Secondary DNS :	
Lease Time (Min) :	1400
Gateway IP(Optional) :	
Relay Agent	
WAN Interface :	WAN1
DHCP Server IP Address :	

Figure 5-11. 1st DHCP server configuration

Status	"**Enable**" the first DHCP server. "**Disable**" the first DHCP server.
Start IP	Set the starting IP address of the IP address pool.
End IP	Set the ending IP address of the IP address pool.
Primary DNS	Sets the private IP address of the primary DNS.
Secondary DNS	Sets the private IP address of the secondary DNS.

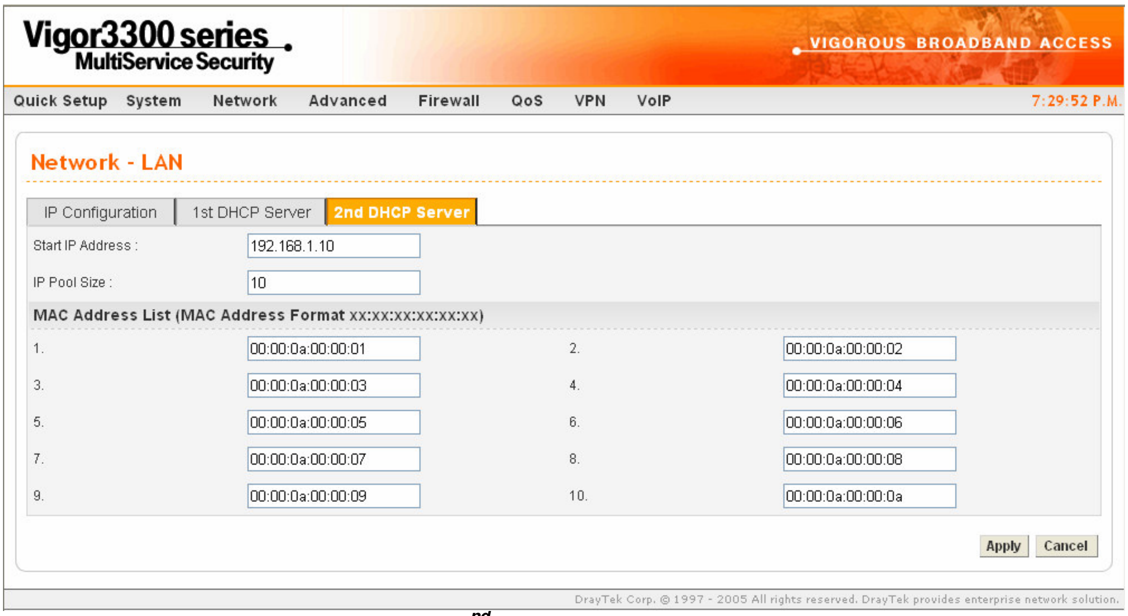
Click **Apply** to reboot the system and apply the settings.

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.

5.2.3 2nd DHCP Server Configuration

The Vigor3300 supports a second DHCP server function for users. After clicking the **2nd DHCP Server** option, you will see the following web page on Figure 5-12. Users can the 2nd DHCP feature to assign a specific PC to related IP in the IP address pool.



Network - LAN

Start IP Address : 192.168.1.10

IP Pool Size : 10

MAC Address List (MAC Address Format xx:xx:xx:xx:xx:xx)

1.	00:00:0a:00:00:01	2.	00:00:0a:00:00:02
3.	00:00:0a:00:00:03	4.	00:00:0a:00:00:04
5.	00:00:0a:00:00:05	6.	00:00:0a:00:00:06
7.	00:00:0a:00:00:07	8.	00:00:0a:00:00:08
9.	00:00:0a:00:00:09	10.	00:00:0a:00:00:0a

Figure 5-12. 2nd DHCP server configuration

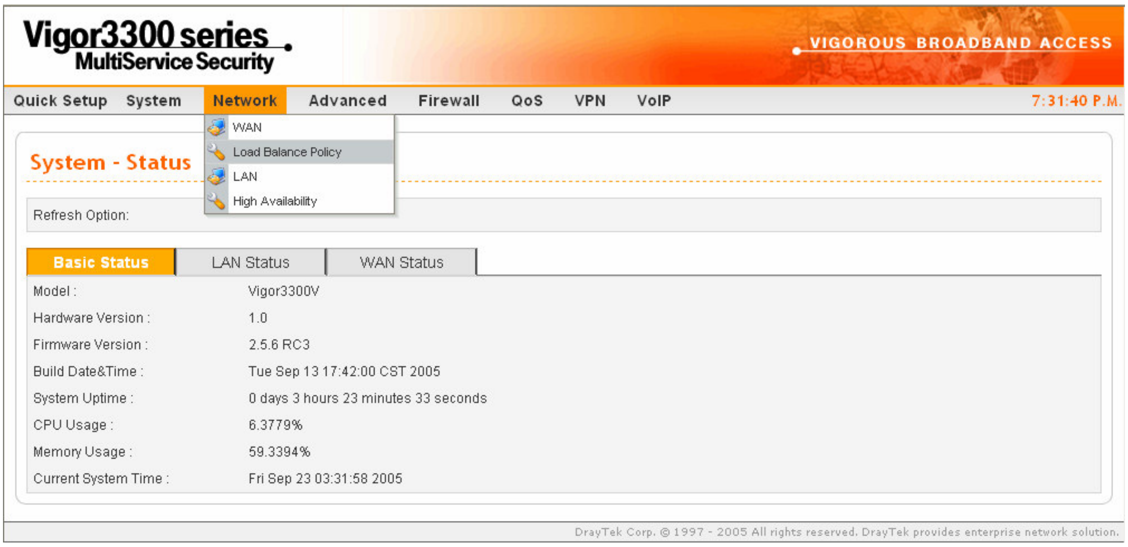
Start IP Address	Set the starting IP address of the IP address pool.
IP Pool Size	Assign the number how many IP addresses in the pool.
Mac Address List	Sets 10 Mac addresses to be served. Once the Mac address is matched in this table, the router can get IP address group information.

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

5.3 Load Balance Policy

The Vigor3300 supports a load balancing function. This function 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 these traffic 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 as shown in Figure 5-13.



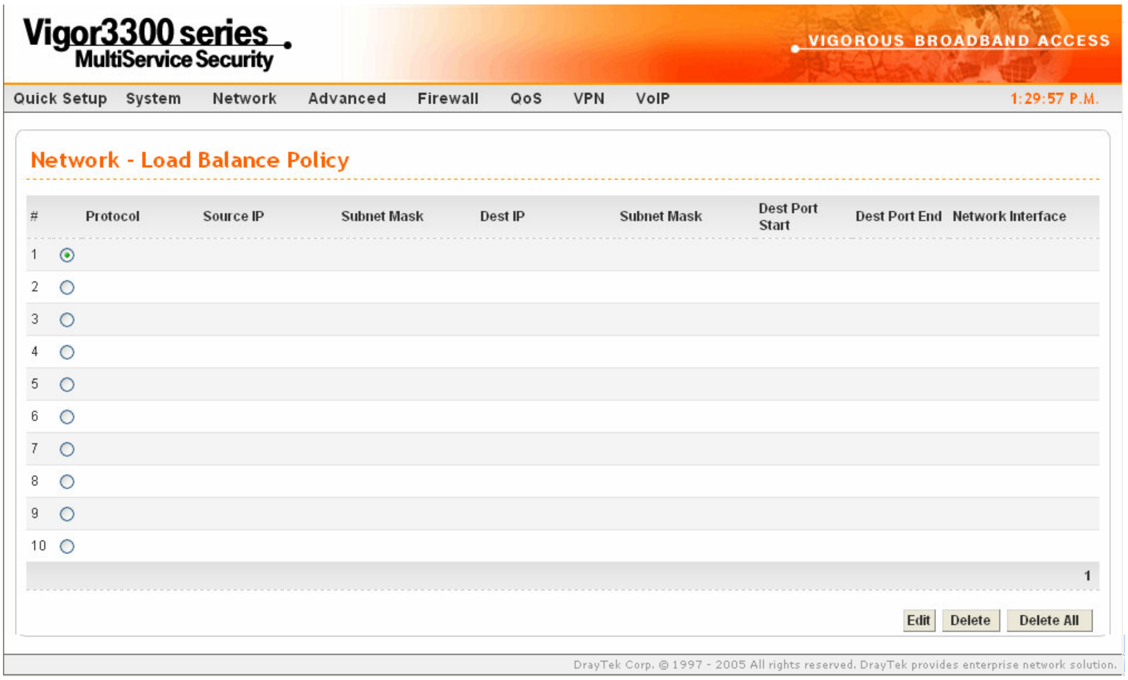
System - Status

Refresh Option:

Model :	Vigor3300V
Hardware Version :	1.0
Firmware Version :	2.5.6 RC3
Build Date&Time :	Tue Sep 13 17:42:00 CST 2005
System Uptime :	0 days 3 hours 23 minutes 33 seconds
CPU Usage :	6.3779%
Memory Usage :	59.3394%
Current System Time :	Fri Sep 23 03:31:58 2005

Figure 5-13. The load balance policy option

After clicking the **Load Balance Policy** option, you will see the following web page as shown in Figure 5-14.



Network - Load Balance Policy

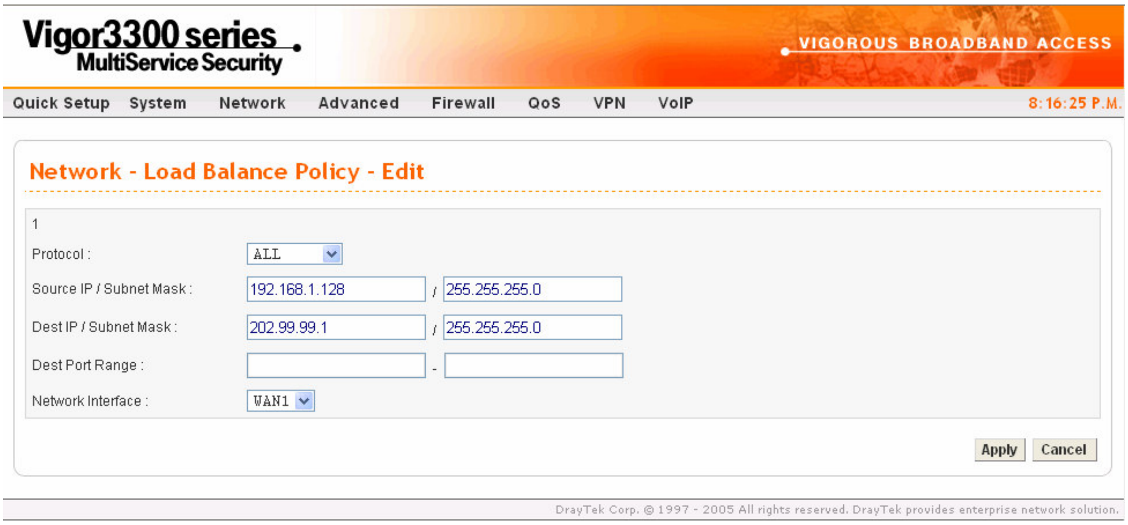
#		Protocol	Source IP	Subnet Mask	Dest IP	Subnet Mask	Dest Port Start	Dest Port End	Network Interface
1	●								
2	○								
3	○								
4	○								
5	○								
6	○								
7	○								
8	○								
9	○								
10	○								

1

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

Figure 5-14. Load balance policy table

To edit an entry, select it by clicking the radio button. Then click the **Edit** option to bring up the following Web page as shown in Figure 5-15.


Vigor3300 series
MultiService Security
VIGOROUS BROADBAND ACCESS
Quick Setup
System
Network
Advanced
Firewall
QoS
VPN
VoIP
8:16:25 P.M.

Network - Load Balance Policy - Edit

1

Protocol : ALL

Source IP / Subnet Mask : 192.168.1.128 / 255.255.255.0

Dest IP / Subnet Mask : 202.99.99.1 / 255.255.255.0

Dest Port Range : -

Network Interface : WAN1

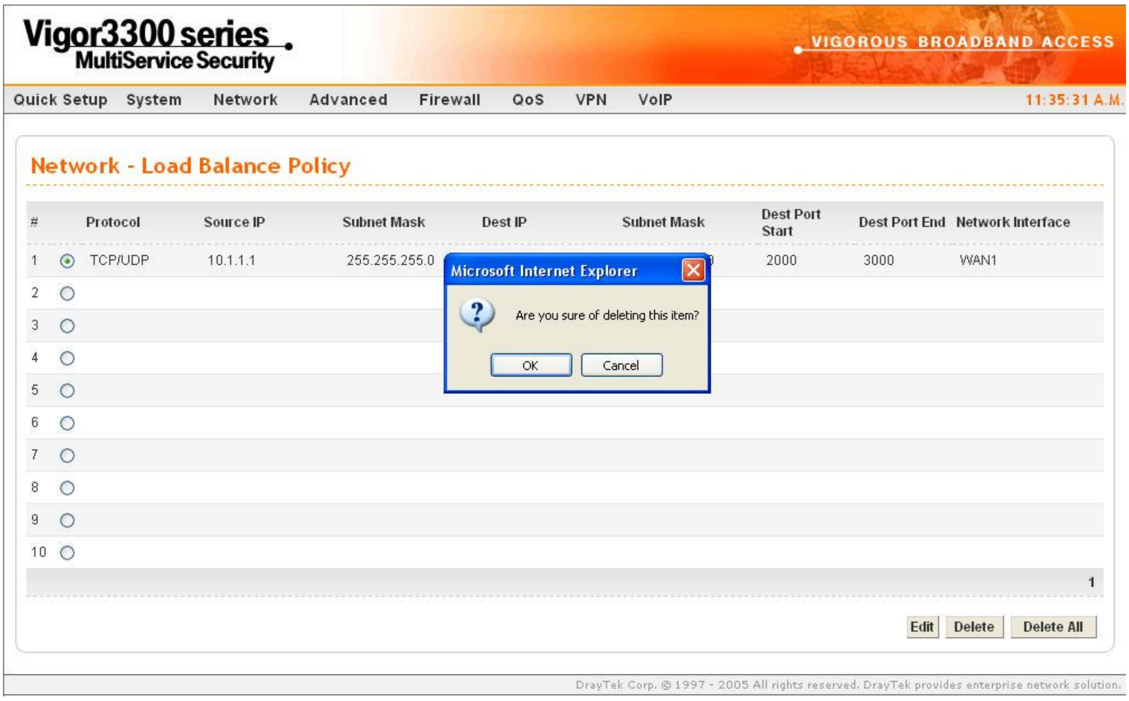
Apply
Cancel
DrayTek Corp. © 1997 - 2005 All rights reserved. DrayTek provides enterprise network solution.

Figure 5-15. Edit load balance policy entry

Protocol	Select the desired protocol.
Source IP/Subnet Mask	Assign a source IP address or a subnet.
Dest IP/Subnet Mask	Assign a destination IP address or a subnet.
Dest Port Range	Assign a destination port number range.
Network Interface	Select an interface to be forwarded to.

Click **Apply** to add or modify this entry into the Load Balance Policy table.

To delete an entry, select by clicking the radio button. Then click the **Delete** option to bring up the following Web page as shown in Figure 5-16.



Network - Load Balance Policy

#		Protocol	Source IP	Subnet Mask	Dest IP	Subnet Mask	Dest Port Start	Dest Port End	Network Interface
1	●	TCP/UDP	10.1.1.1	255.255.255.0		0	2000	3000	WAN1
2	○								
3	○								
4	○								
5	○								
6	○								
7	○								
8	○								
9	○								
10	○								

1

Microsoft Internet Explorer

Are you sure of deleting this item?

OK Cancel

Figure 5-16. Delete load balance policy entry

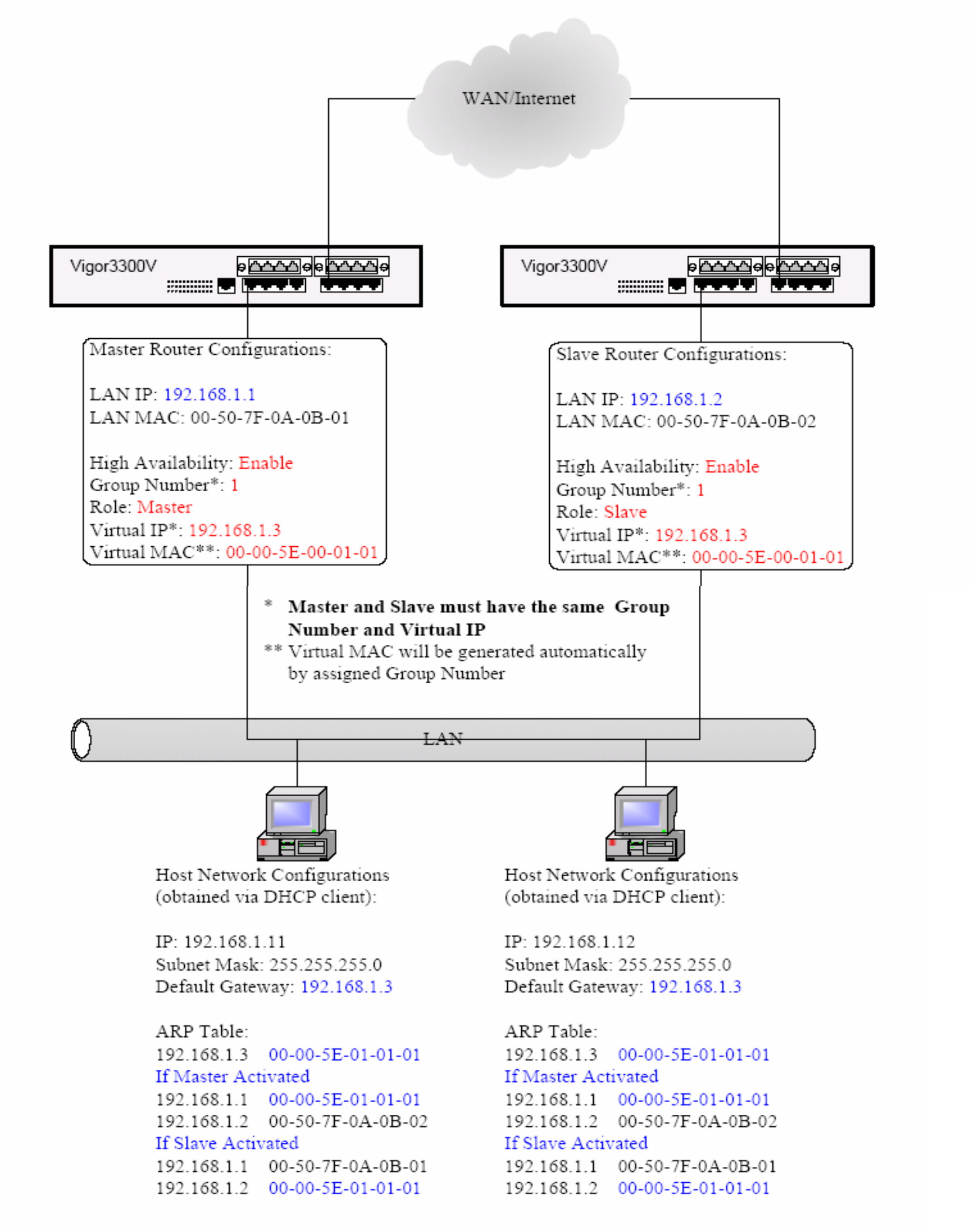
Click **Delete** to delete this entry from the Load Balance Policy table.

Click **Delete All** in the Load Balance Policy page (Figure 5-14) to delete all 10 entries on the page.

5.4 High Availability Setup

The High Availability (HA) feature refers to the availability of resources in the wake of component failures in the system. The complexity of a high availability solution to provide constant service is determined by a company's availability needs and by the amount of system interruptions that can be tolerated by a business. Any hardware or software components in the system will fail to have a redundant component to backup. Systems that can provide 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 is Master, the right V3300 is Slave. When Master V3300 is broken down, the Slave V3300 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.



Master Router Configurations:

LAN IP: 192.168.1.1
LAN MAC: 00-50-7F-0A-0B-01

High Availability: Enable
Group Number*: 1
Role: Master
Virtual IP*: 192.168.1.3
Virtual MAC**: 00-00-5E-00-01-01

Slave Router Configurations:

LAN IP: 192.168.1.2
LAN MAC: 00-50-7F-0A-0B-02

High Availability: Enable
Group Number*: 1
Role: Slave
Virtual IP*: 192.168.1.3
Virtual MAC**: 00-00-5E-00-01-01

* **Master and Slave must have the same Group Number and Virtual IP**

** Virtual MAC will be generated automatically by assigned Group Number

Host Network Configurations
(obtained via DHCP client):

IP: 192.168.1.11
Subnet Mask: 255.255.255.0
Default Gateway: 192.168.1.3

ARP Table:
192.168.1.3 00-00-5E-01-01-01
If Master Activated
192.168.1.1 00-00-5E-01-01-01
192.168.1.2 00-50-7F-0A-0B-02
If Slave Activated
192.168.1.1 00-50-7F-0A-0B-01
192.168.1.2 00-00-5E-01-01-01

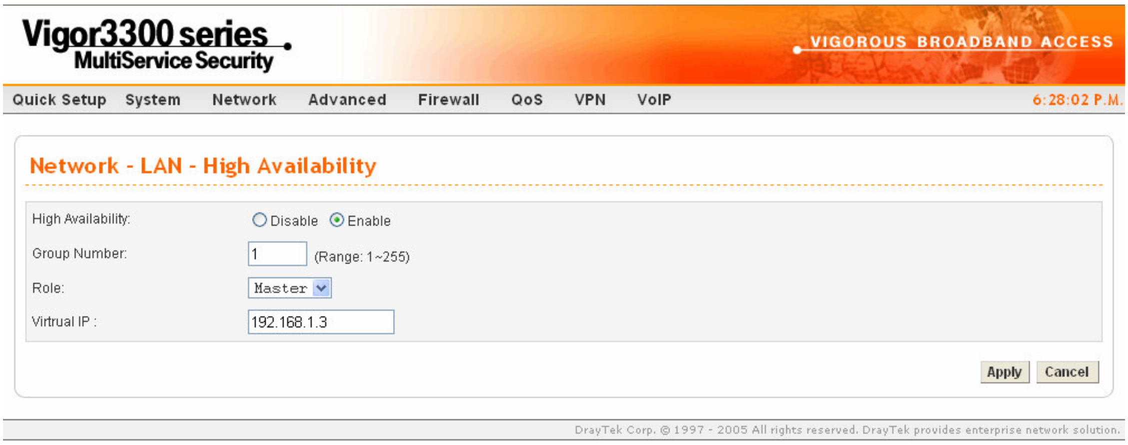
Host Network Configurations
(obtained via DHCP client):

IP: 192.168.1.12
Subnet Mask: 255.255.255.0
Default Gateway: 192.168.1.3

ARP Table:
192.168.1.3 00-00-5E-01-01-01
If Master Activated
192.168.1.1 00-00-5E-01-01-01
192.168.1.2 00-50-7F-0A-0B-02
If Slave Activated
192.168.1.1 00-50-7F-0A-0B-01
192.168.1.2 00-00-5E-01-01-01

Figure 5-17. High availability application scenario

Please refer to the following web page in Figure 5-18.


Vigor3300 series
MultiService Security
VIGOROUS BROADBAND ACCESS
Quick Setup
System
Network
Advanced
Firewall
QoS
VPN
VoIP
6:28:02 P.M.
Apply
Cancel
DrayTek Corp. © 1997 - 2005 All rights reserved. DrayTek provides enterprise network solution.

Network - LAN - High Availability

High Availability: ○ Disable ● Enable

Group Number: 1 (Range: 1~255)

Role: Master

Virtual IP : 192.168.1.3

Figure 5-18. High availability configuration

High Availability	"**Disable**" or "**Enable**" this function.
Group Number	Assign a group number, the range is from 1 to 255.
Role	Select a role as Master or Slave.
Virtual IP	Assigns an IP address as a virtual IP.

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

CHAPTER 6

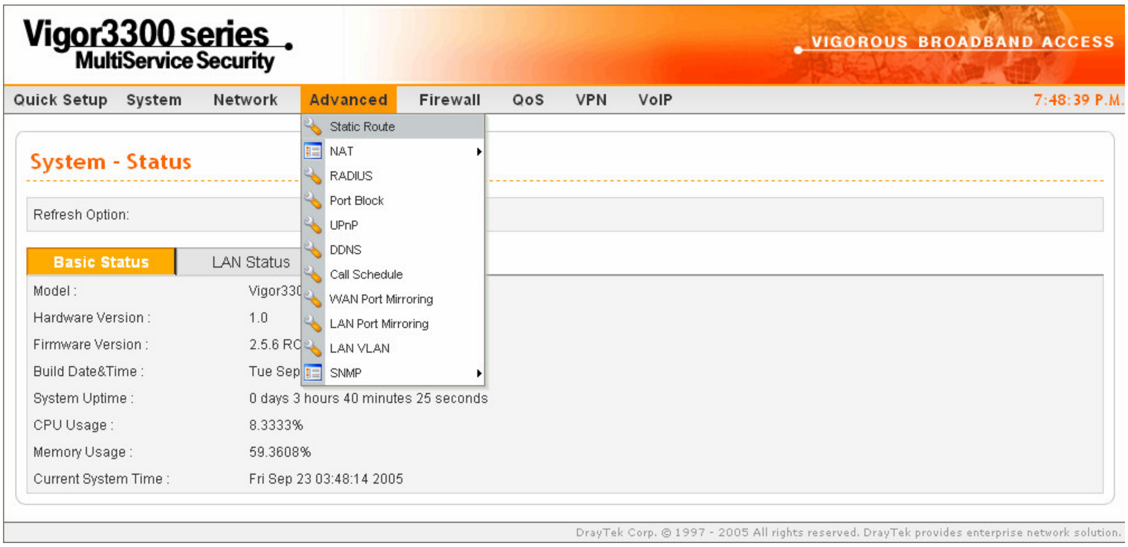
Advanced Setup

This chapter shows how to configure Advanced functions.

This chapter is divided into the following sections:

6.1 Static Route Setup

The **Static Route** function allows users to assign static routing information. In the **Advanced** group, click the **Static Route** option as shown in Figure 6-1.



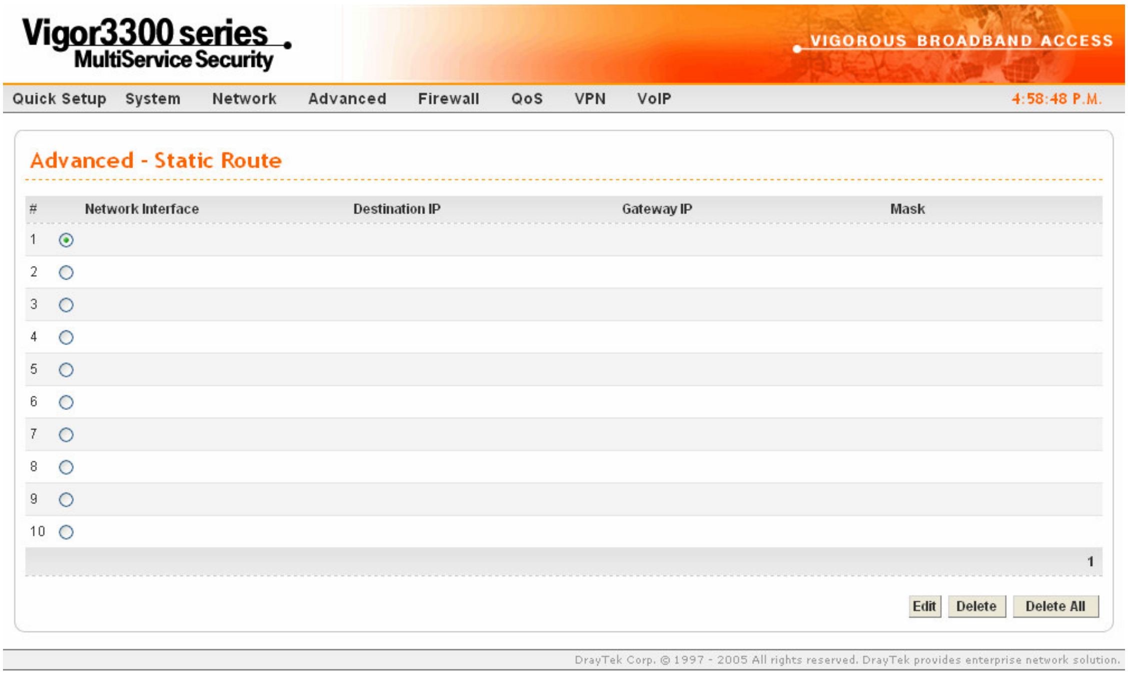
System - Status

Refresh Option:

Model :	Vigor330
Hardware Version :	1.0
Firmware Version :	2.5.6 RC
Build Date&Time :	Tue Sep
System Uptime :	0 days 3 hours 40 minutes 25 seconds
CPU Usage :	8.3333%
Memory Usage :	59.3608%
Current System Time :	Fri Sep 23 03:48:14 2005

Figure 6-1. The static route option

After clicking the **Static Route** option**,** you will see the following web page as shown in Figure 6-2.


Vigor3300 series
MultiService Security
VIGOROUS BROADBAND ACCESS
Quick Setup
System
Network
Advanced
Firewall
QoS
VPN
VoIP
4:58:48 P.M.
Edit
Delete
Delete All
DrayTek Corp. © 1997 - 2005 All rights reserved. DrayTek provides enterprise network solution.

Advanced - Static Route

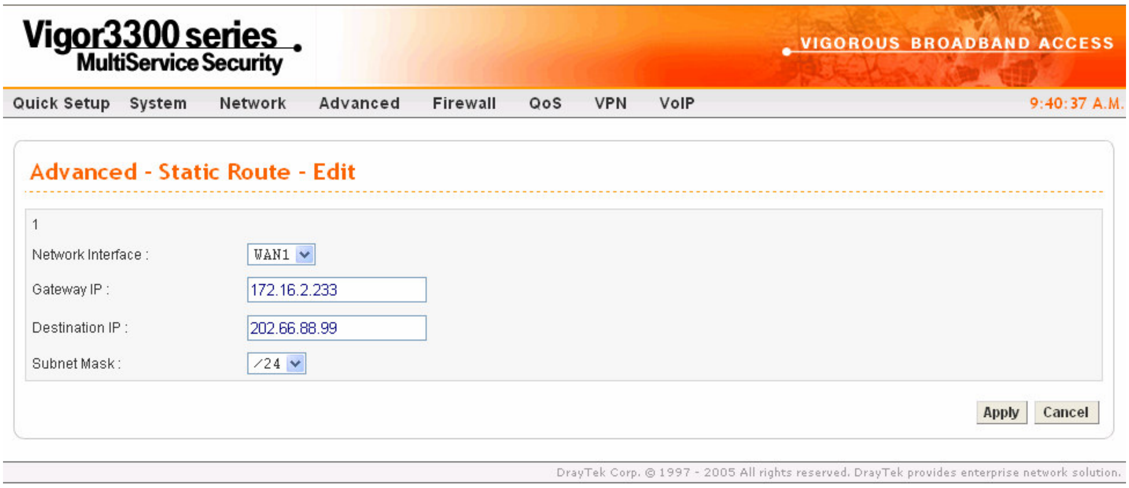
#		Network Interface	Destination IP	Gateway IP	Mask
1	●				
2	○				
3	○				
4	○				
5	○				
6	○				
7	○				
8	○				
9	○				
10	○				

1

Figure 6-2. Static route table

6.1.1 Edit Option

Click **Edit** to add or edit an entry in the static route table as shown in Figure 6-3.


Vigor3300 series
MultiService Security
VIGOROUS BROADBAND ACCESS
Quick Setup
System
Network
Advanced
Firewall
QoS
VPN
VoIP
9:40:37 A.M.
Apply
Cancel
DrayTek Corp. © 1997 - 2005 All rights reserved. DrayTek provides enterprise network solution.

Advanced - Static Route - Edit

1

Network Interface :	WAN1
Gateway IP :	172.16.2.233
Destination IP :	202.66.88.99
Subnet Mask :	/24

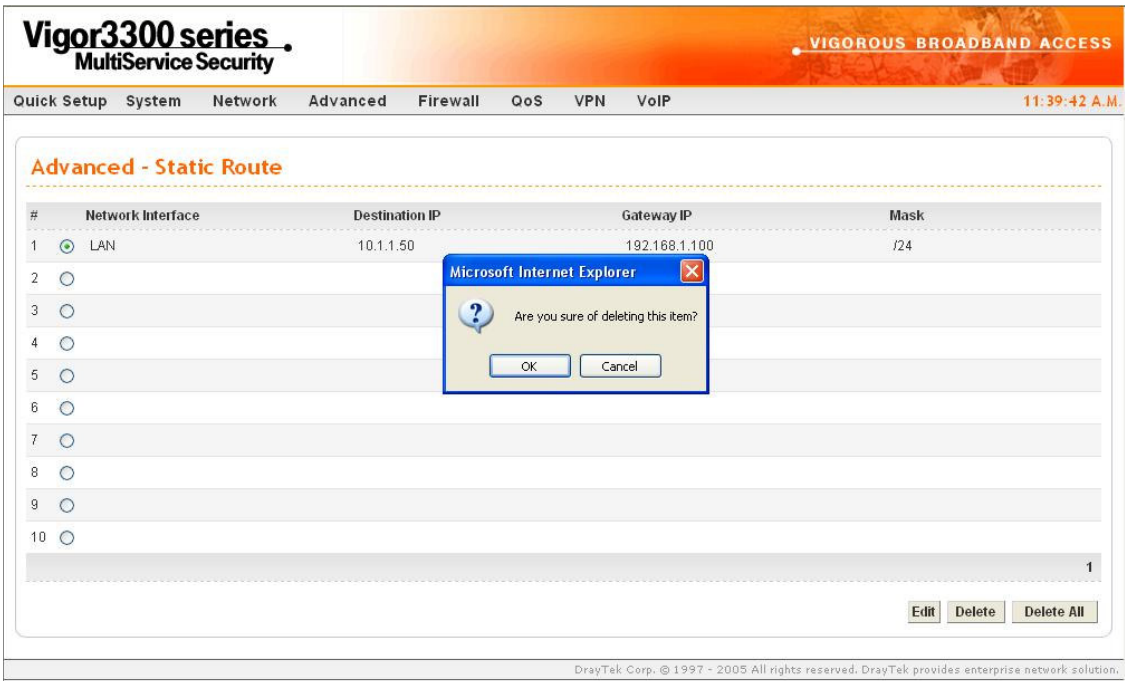
Figure 6-3. Edit option

Network Interface	Select a network interface as a destination to be sent. It includes **LAN**, **WAN1~WAN4**.
Gateway IP	Assign an IP address of the gateway within the interface selected in **Network Interface field**.
Destination IP	Assign the destination IP address to be checked.
Mask	Assign a value of subnet mask for destination IP address.

Click **Apply** to finish settings.

6.1.2 Delete option

Click **Delete** button to remove an entry in the static route table then the following window will be popped-up as shown in Figure 6-4.



Advanced - Static Route

#		Network Interface	Destination IP	Gateway IP	Mask
1	●	LAN	10.1.1.50	192.168.1.100	/24
2	○				
3	○				
4	○				
5	○				
6	○				
7	○				
8	○				
9	○				
10	○				

Microsoft Internet Explorer

Are you sure of deleting this item?

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

Figure 6-4. Delete option

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

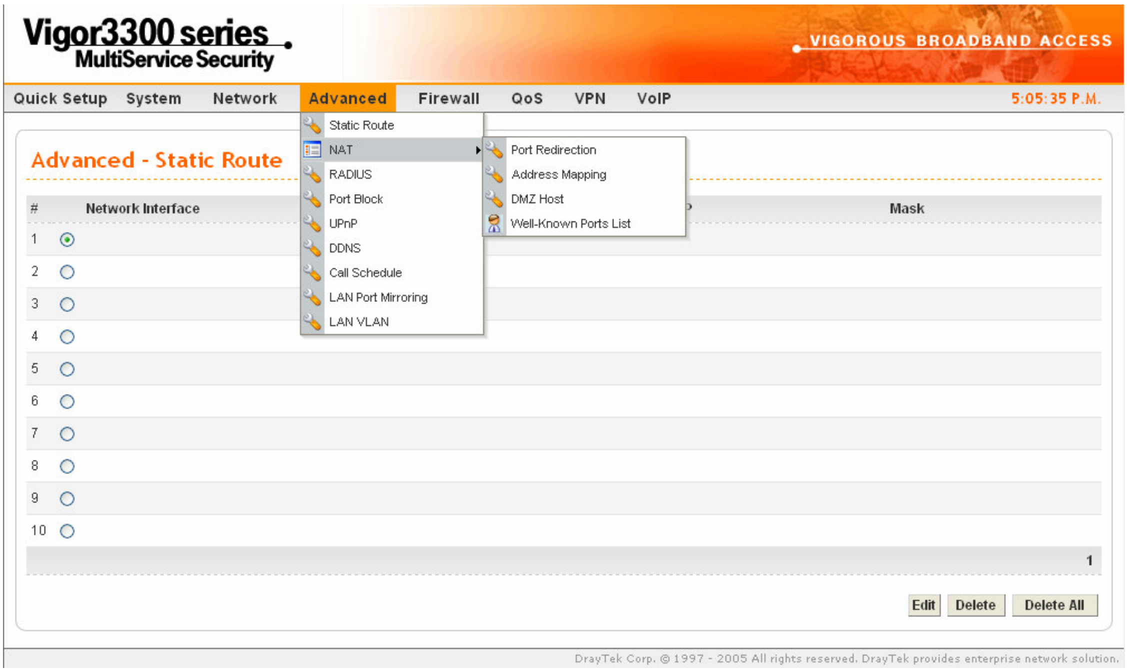
Before execute the **Edit** or **Delete** options, the user has to click the radio box belonging to each index number.

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

6.2 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 on 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 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 will translate 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 to bring up the following setup page as shown in Figure 6-5.



Advanced - Static Route

#		Network Interface	Mask
1	●		
2	○		
3	○		
4	○		
5	○		
6	○		
7	○		
8	○		
9	○		
10	○		

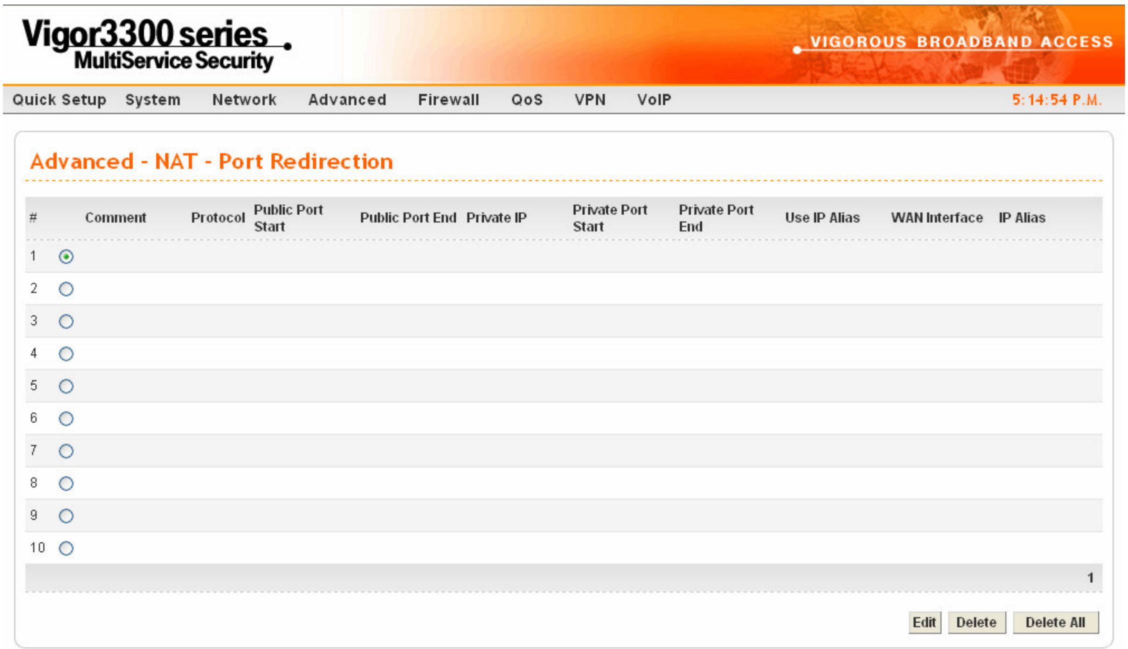
1

Figure 6-5. NAT functions

6.2.1 Port Redirection Table Setup

The **Port Redirection Table** 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, etc. The following example shows how an internal FTP server is exposed to the public domain. The internal FTP server is running on the local host addressed as 192.168.1.2. A user can also translate the port to another port by configuration. The packet is forwarded to a specific local host if the port number matches that defined in the table.

Click **Port Redirection** option, and then you will see the following setup page. Figure 6-6 illustrates the web page as an example.



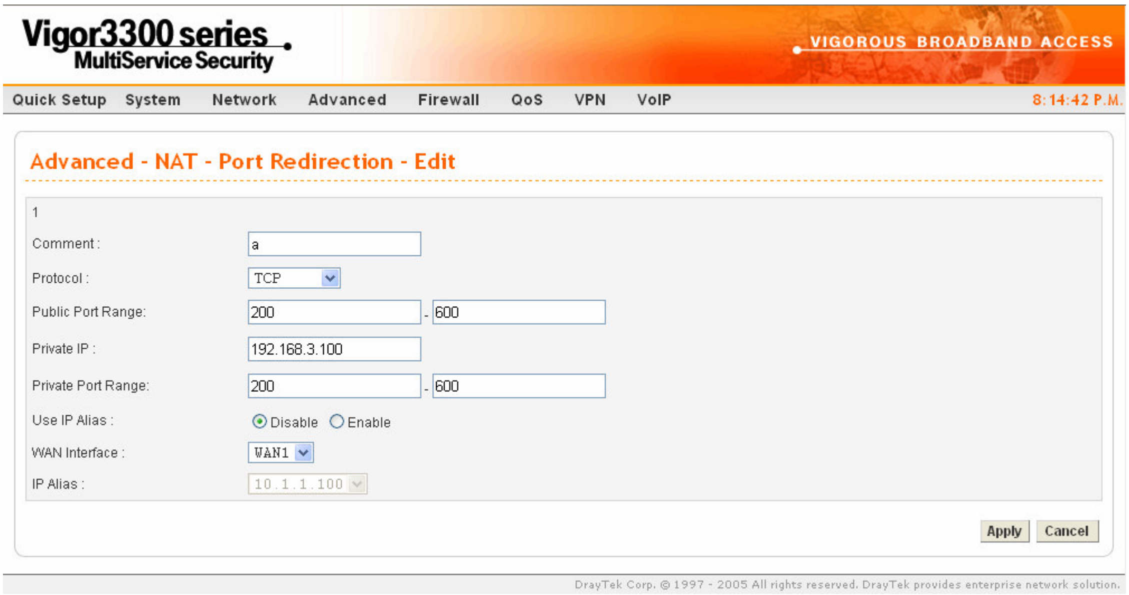
Advanced - NAT - Port Redirection

#		Comment	Protocol	Public Port Start	Public Port End	Private IP	Private Port Start	Private Port End	Use IP Alias	WAN Interface	IP Alias
1	●										
2	○										
3	○										
4	○										
5	○										
6	○										
7	○										
8	○										
9	○										
10	○										

1

Figure 6-6. NAT-Port redirection information page

Click **Edit** to add a new rule entry or modify an existed rule entry. Figure 6-7 illustrates the web page as an example.


Vigor3300 series
MultiService Security
VIGOROUS BROADBAND ACCESS
Quick Setup
System
Network
Advanced
Firewall
QoS
VPN
VoIP
8:14:42 P.M.
Apply
Cancel
DrayTek Corp. © 1997 - 2005 All rights reserved. DrayTek provides enterprise network solution.

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

Figure 6-7. Edit a new entry

Comment	Assign a name of this entry.
Protocol	Assign the transport layer protocol with **TCP** or **UDP**.
Public Port Range ***Private IP***	Assign a port range from starting to end public port number. 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 finish this setting.

Note:

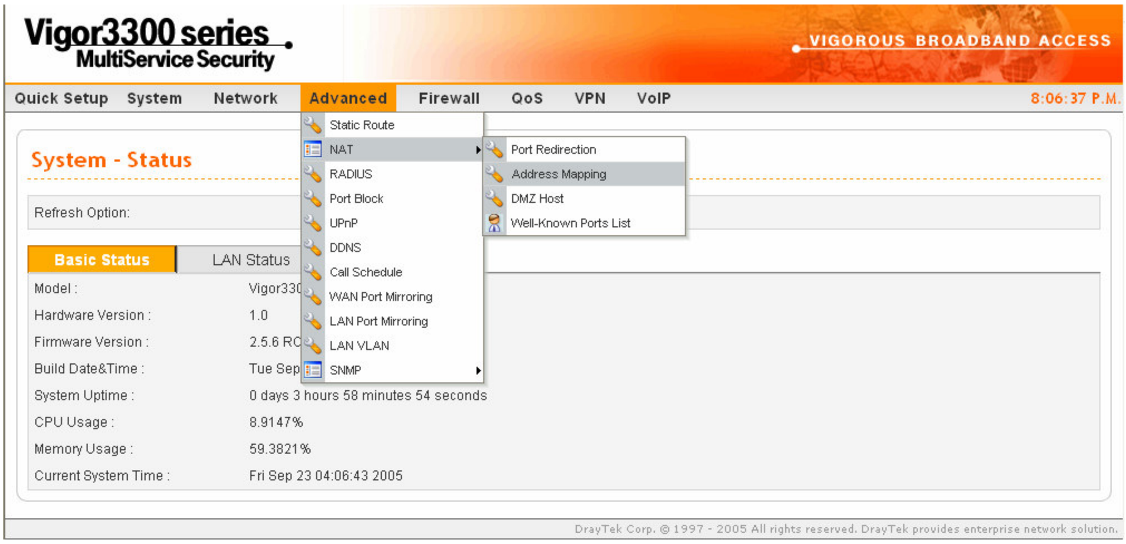
The port forwarding function could redirect the Internet traffic, which has the destination port within the public port range and has the same IP address as "WAN Interface" or "IP Alias" you set. Please redirect only the ports you know you have to forward rather than forward all ports. Otherwise, the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

By the way, user can click **Delete** to remove one current existed NAT entry and click **Delete All** to remove all entries.

6.2.2 Address Mapping Setup

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 **Advance** group, click **NAT** option. Then you will see the following setup page. Figure 6-8 illustrates the location of **Address Mapping** option.



System - Status

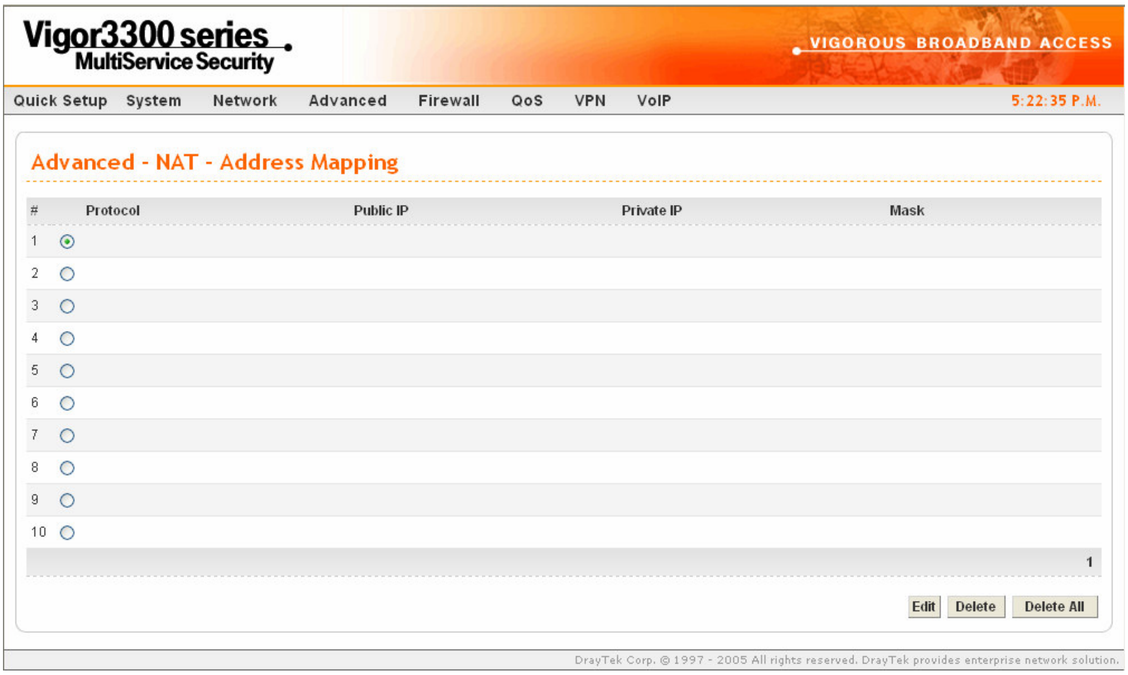
Refresh Option:

Basic Status | LAN Status

Model :	Vigor330
Hardware Version :	1.0
Firmware Version :	2.5.6 RC
Build Date&Time :	Tue Sep
System Uptime :	0 days 3 hours 58 minutes 54 seconds
CPU Usage :	8.9147%
Memory Usage :	59.3821%
Current System Time :	Fri Sep 23 04:06:43 2005

Figure 6-8. NAT-Address mapping option

Click **Address Mapping** option, then you will see the following web page. Figure 6-9 illustrates the web page as an example.


Vigor3300 series
MultiService Security
VIGOROUS BROADBAND ACCESS
Quick Setup
System
Network
Advanced
Firewall
QoS
VPN
VoIP
5:22:35 P.M.
Edit
Delete
Delete All
DrayTek Corp. © 1997 - 2005 All rights reserved. DrayTek provides enterprise network solution.

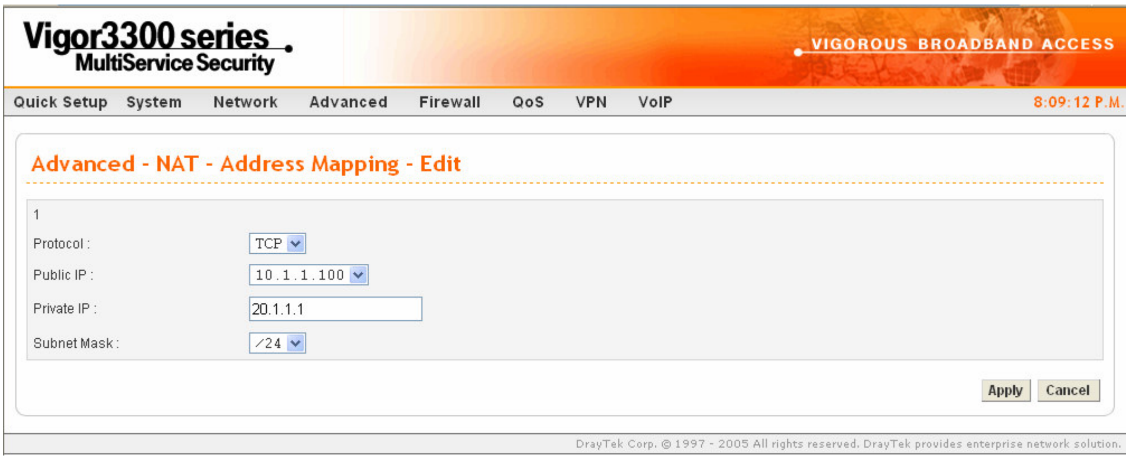
Advanced - NAT - Address Mapping

#	Protocol	Public IP	Private IP	Mask
1	●			
2	○			
3	○			
4	○			
5	○			
6	○			
7	○			
8	○			
9	○			
10	○			

1

Figure 6-9. NAT-Address mapping information page

Click **Edit** to add a new rule entry or modify an existed rule entry. Figure 6-10 illustrates the web page as an example.


Vigor3300 series
MultiService Security
VIGOROUS BROADBAND ACCESS
Quick Setup
System
Network
Advanced
Firewall
QoS
VPN
VoIP
8:09:12 P.M.
Apply
Cancel
DrayTek Corp. © 1997 - 2005 All rights reserved. DrayTek provides enterprise network solution.

Advanced - NAT - Address Mapping - Edit

1

Protocol :	TCP
Public IP :	10.1.1.100
Private IP :	20.1.1.1
Subnet Mask :	/24

Figure 6-10. Edit a new entry in address mapping

Protocol	Select the transport layer protocol. It could be TCP, UDP, or All for selection.
Public IP	Select an IP address from IP Alias in WAN interface. Local host can use this IP to connect to the Internet.
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.

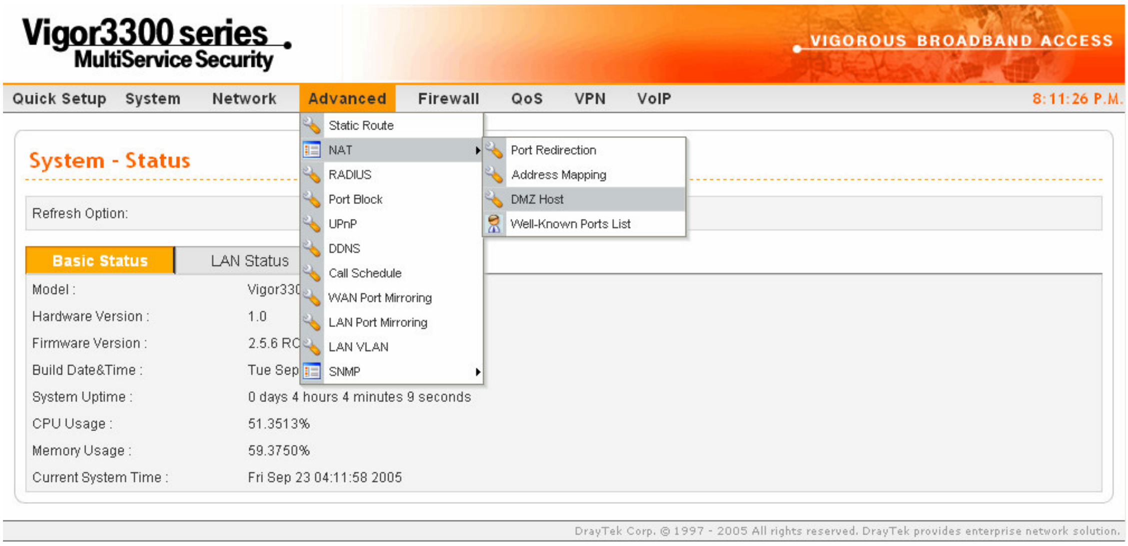
Click **Apply** to finish this setting.

By the way, user can click **Delete** to remove a current existed NAT entry and click **Delete All** to remove all entries.

6.2.3 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 might be corrupted but other company information would not be exposed.

In the **Advanced** group, click **NAT** option. Then you will see the following page. Figure 6-11 illustrates the location of **DMZ Host** option.



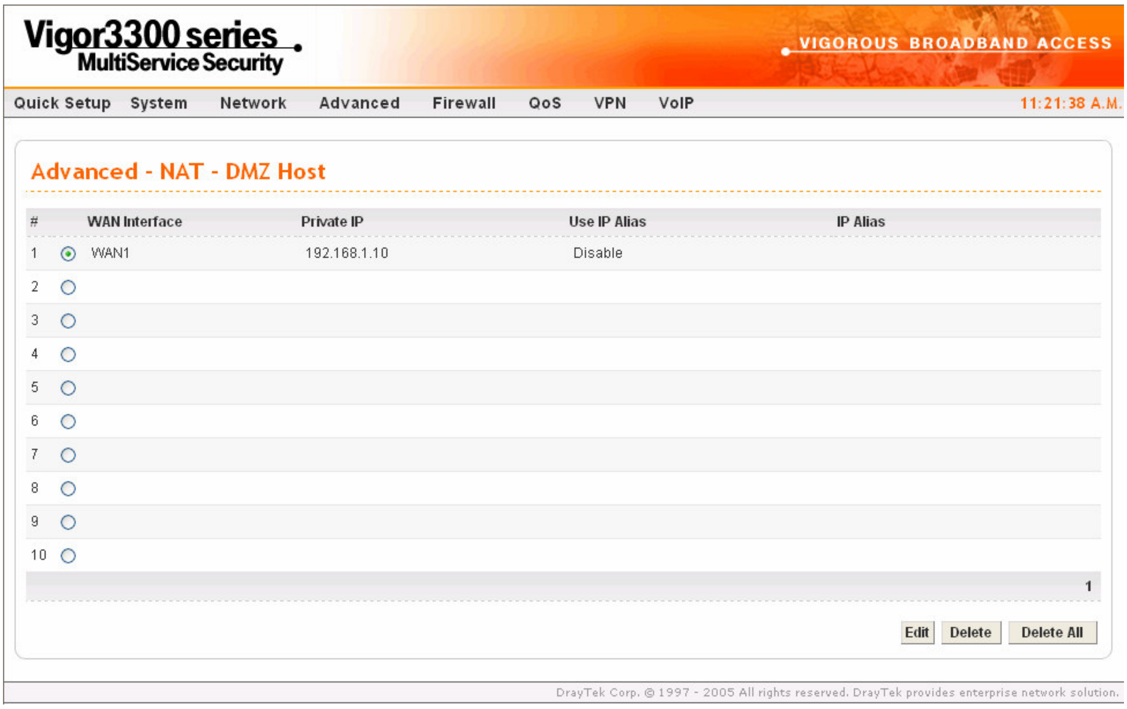
System - Status

Refresh Option:

Model :	Vigor330
Hardware Version :	1.0
Firmware Version :	2.5.6 RC
Build Date&Time :	Tue Sep
System Uptime :	0 days 4 hours 4 minutes 9 seconds
CPU Usage :	51.3513%
Memory Usage :	59.3750%
Current System Time :	Fri Sep 23 04:11:58 2005

Figure 6-11. DMZ host option

Click **DMZ Host**, and then you will see the following page. Figure 6-12 illustrates the web page as an example.


Vigor3300 series
MultiService Security
VIGOROUS BROADBAND ACCESS
Quick Setup System Network Advanced Firewall QoS VPN VoIP
11:21:38 A.M.
Edit
Delete
Delete All
DrayTek Corp. © 1997 - 2005 All rights reserved. DrayTek provides enterprise network solution.

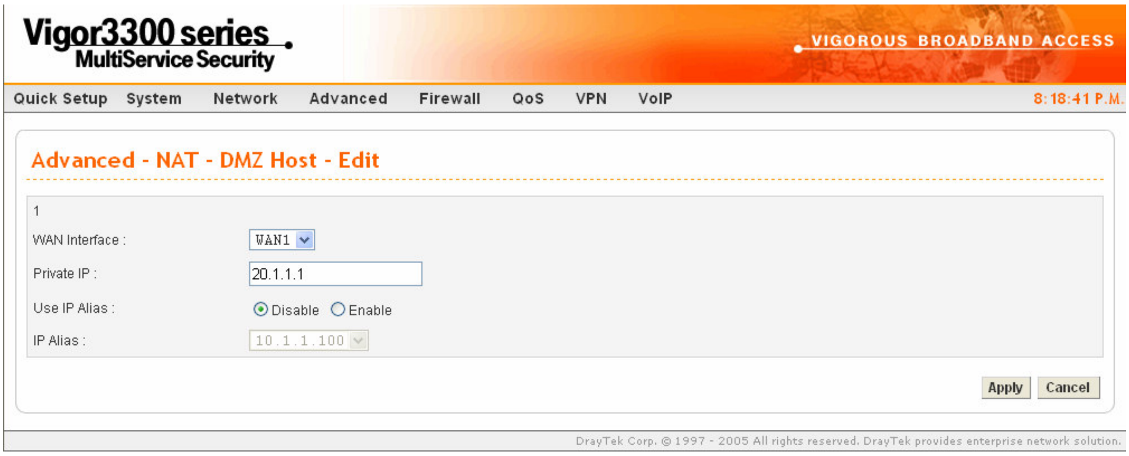
Advanced - NAT - DMZ Host

#		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	○				

1

Figure 6-12. DMZ host table

Click **Edit** to add a new entry in DMZ Host table. Figure 6-13 illustrates the web page as an example.


Vigor3300 series
MultiService Security
VIGOROUS BROADBAND ACCESS
Quick Setup System Network Advanced Firewall QoS VPN VoIP
8:18:41 P.M.

Advanced - NAT - DMZ Host - Edit

1

WAN Interface : WAN1

Private IP : 20.1.1.1

Use IP Alias : ● Disable ○ Enable

IP Alias : 10.1.1.100

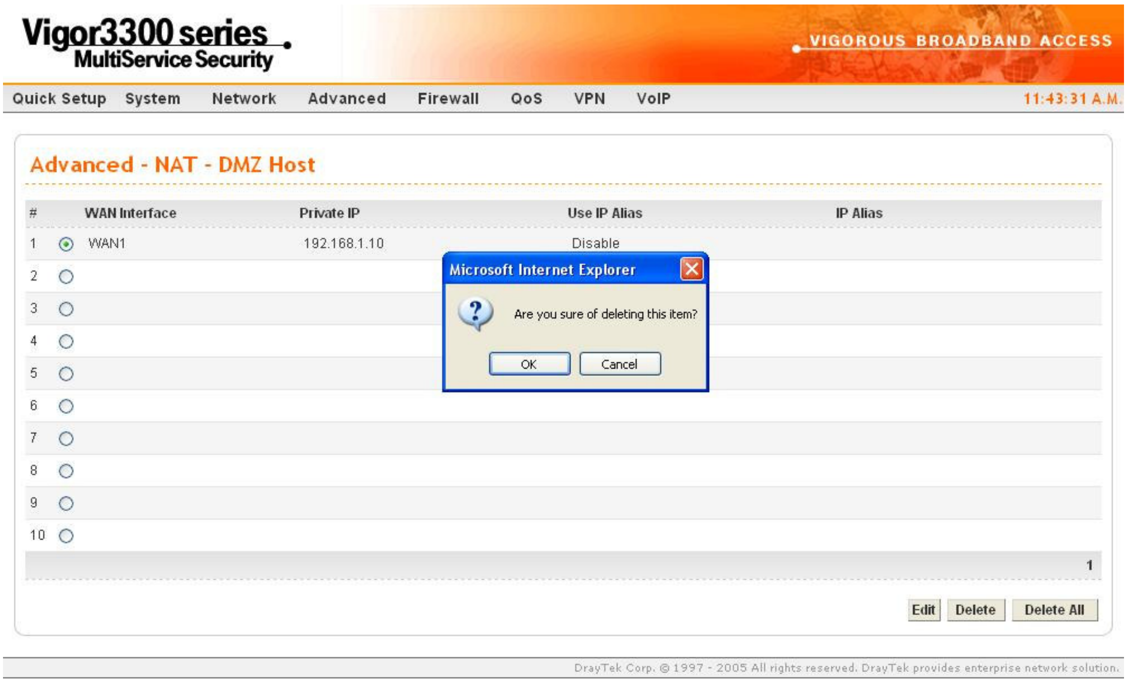
Apply
Cancel
DrayTek Corp. © 1997 - 2005 All rights reserved. DrayTek provides enterprise network solution.

Figure 6-13. DMZ host – edit

WAN Interface	Select a WAN interface
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 within the list of IP Alias configured in WAN interface.

Click **Apply** to finish this setting.

Click **Delete** to remove an existed entry in DMZ Host table. Figure 6-14 illustrates the web page as an example.



Advanced - NAT - DMZ Host

#		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	○				

1

Microsoft Internet Explorer

Are you sure of deleting this item?

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

Figure 6-14. DMZ host – delete

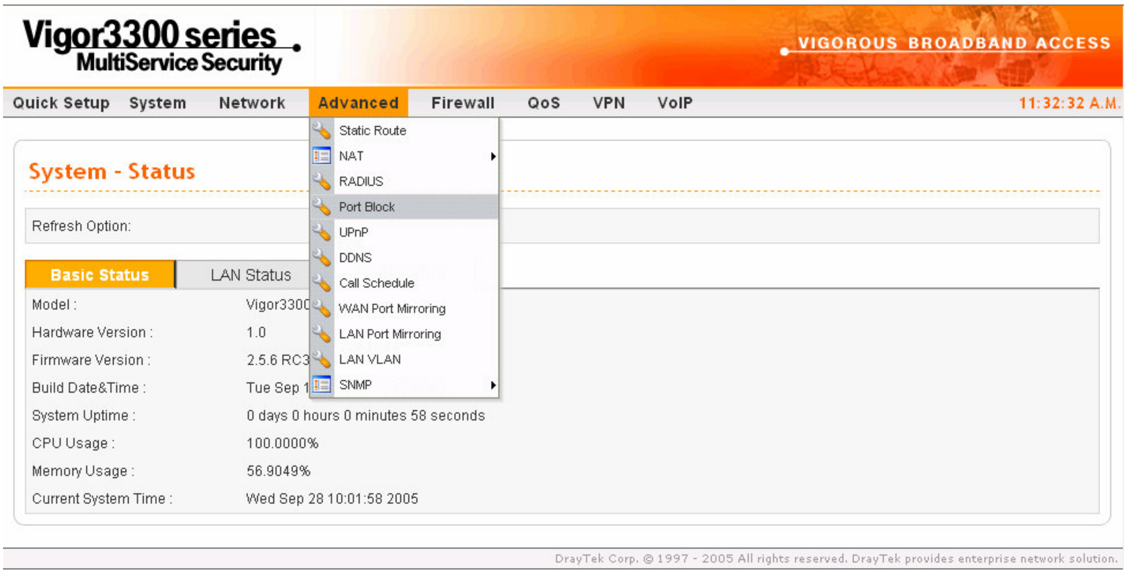
Click **Apply** to finish this setting.

User can click **Delete All** to remove all entries in the table.

6.3 Port Block Setup

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 both on WAN and LAN. The advantage of this feature is to filter some unnecessary packets or attacking packets on Internet environment or LAN network. The Vigor3300 series supports ten port numbers[1] to be blocked.

In the **Advanced** group, click **Port Block** option. Figure 6-15 illustrates the location of the **Port Block** option.



System - Status

Refresh Option:

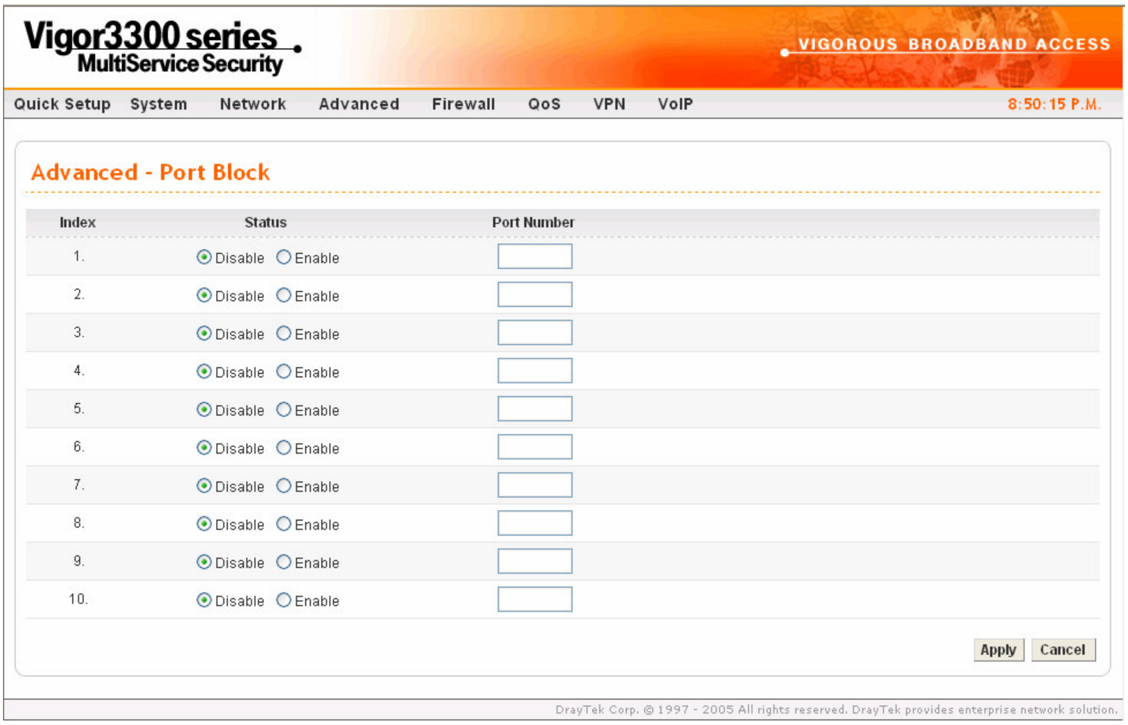
Model :	Vigor330(
Hardware Version :	1.0
Firmware Version :	2.5.6 RC3
Build Date&Time :	Tue Sep 1
System Uptime :	0 days 0 hours 0 minutes 58 seconds
CPU Usage :	100.0000%
Memory Usage :	56.9049%
Current System Time :	Wed Sep 28 10:01:58 2005

Figure 6-15. Port block option

Click the **Port Block** option, and then you will see the following web page.

[1] **Vigor3300V model does not support default values.**

Figure 6-16 illustrates the web page as an example.



Advanced - Port Block

Index	Status	Port Number
1.	● Disable ○ Enable	
2.	● Disable ○ Enable	
3.	● Disable ○ Enable	
4.	● Disable ○ Enable	
5.	● Disable ○ Enable	
6.	● Disable ○ Enable	
7.	● Disable ○ Enable	
8.	● Disable ○ Enable	
9.	● Disable ○ Enable	
10.	● Disable ○ Enable	

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

Figure 6-16. Port block configuration

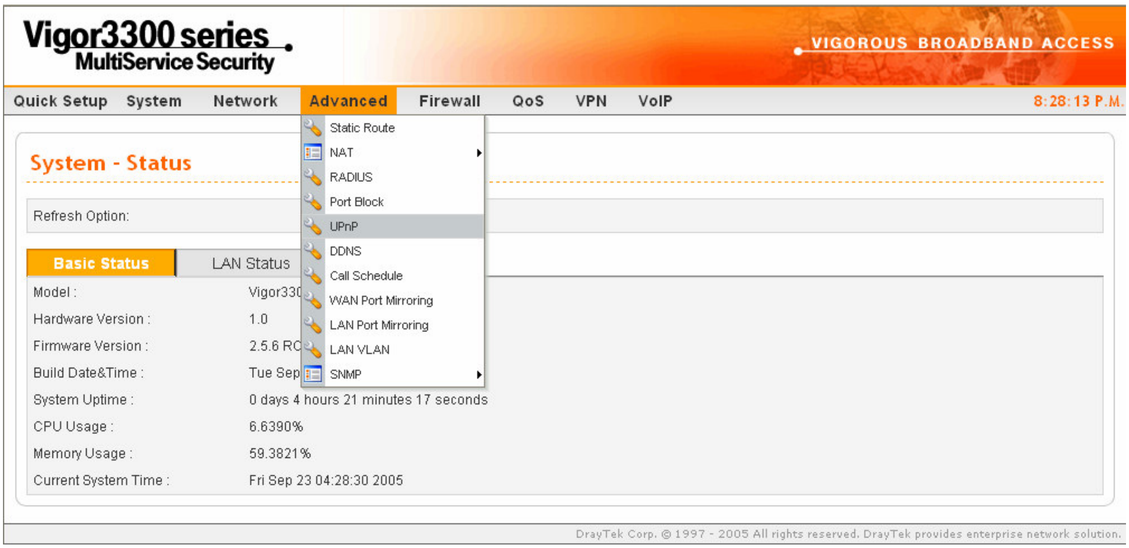
Index	The number of each entry.
Status	User can "**Disable**" or "**Enable**" this port to be blocked
Port Number	Assign a port number to be blocked in system.

Click **Apply** to finish this setting. The default port setting for V3300B, 3300B+ is 135, 137, 138, 139, and 445.

6.4 UPnP Setup

The UPnP (Universal Plug and Play) protocol aims at the plug and play of network devices. Such a feature is already available for directly connected PC peripherals in Windows 'Plug and Play' system. For NAT routers, the major feature of UPnP on the Vigor3300 router is “NAT Traversal”, which means that applications inside firewall could open ports to penetrate router automatically. Such a mechanism is more feasible than relying on the router to allocate open ports by itself. Further, the user does not have to manually setup port mappings or a DMZ.

In the **Advanced** group, click **UPnP** option. Figure 6-17 illustrates the location of **UPnP** option.



System - Status

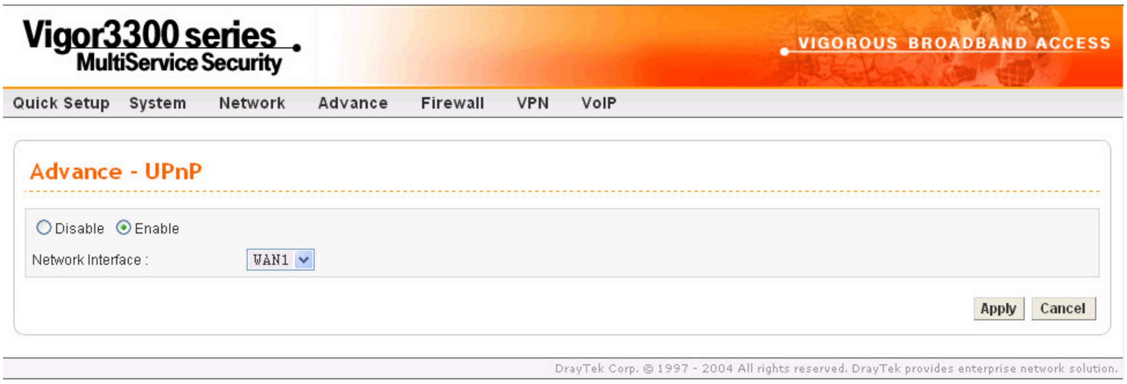
Refresh Option:

Model :	Vigor330
Hardware Version :	1.0
Firmware Version :	2.5.6 RC
Build Date&Time :	Tue Sep
System Uptime :	0 days 4 hours 21 minutes 17 seconds
CPU Usage :	6.6390%
Memory Usage :	59.3821%
Current System Time :	Fri Sep 23 04:28:30 2005

Figure 6-17. UPnP option

With the UPnP feature employed, the Vigor3300 series provide voice, video and messaging communication of MSN Messenger for user on Windows XP.

Click **UPnP option**, and then you will see the following web page. Figure 6-18 illustrates the web page as an example.


Vigor3300 series
MultiService Security
VIGOROUS BROADBAND ACCESS
Quick Setup System Network Advance Firewall VPN VoIP
Apply
Cancel
DrayTek Corp. © 1997 - 2004 All rights reserved. DrayTek provides enterprise network solution.

Advance - UPnP

○ Disable ● Enable

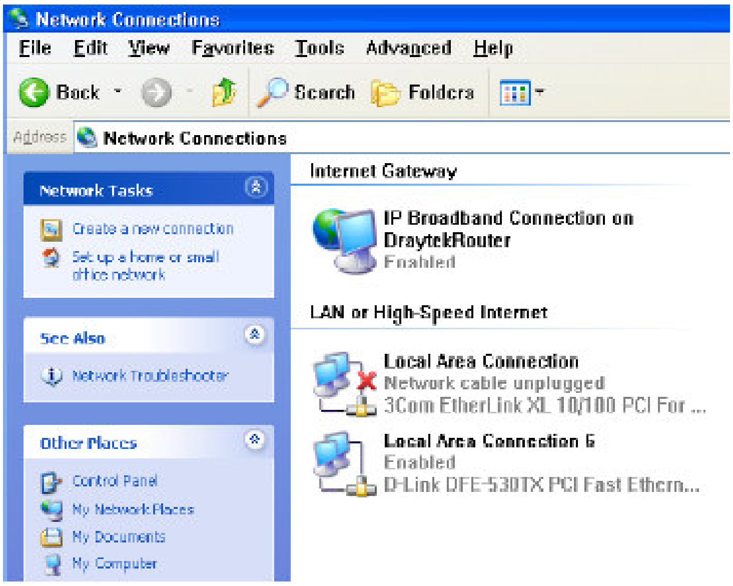
Network Interface : WAN1

Figure 6-18. UPnP configuration

Enable/Disable	Click the round box to **Disable** or **Enable** UPnP function.
Network Interfaces	Select a specific WAN interface for UPnP.

Click **Apply** to finish this setting.

Click the **IP Broadband Connection on DrayTek Router** on Windows XP/Network Connections, as shown as Figure 6-19. The connection status and control status will be able to be activated.



Internet Gateway

IP Broadband Connection on DraytekRouter
Enabled

LAN or High-Speed Internet

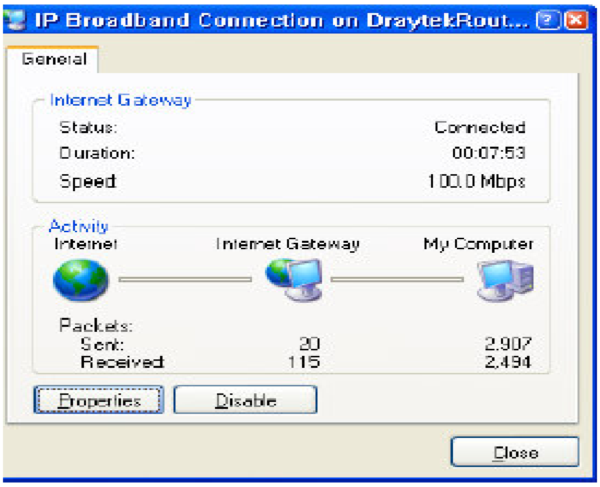
Local Area Connection
Network cable unplugged
3Com EtherLink XL 10/100 PCI For ...

Local Area Connection 5
Enabled
D-Link DFE-530TX PCI Fast Ethern...

Figure 6-19. Windows network connection

The NAT Traversal feature of UPnP enables multimedia feature of your applications. Without UPnP, you will have to set up port mappings or do some similarly configurations manually.

Figure 6-20, 6-21 illustrate the web page as an example.



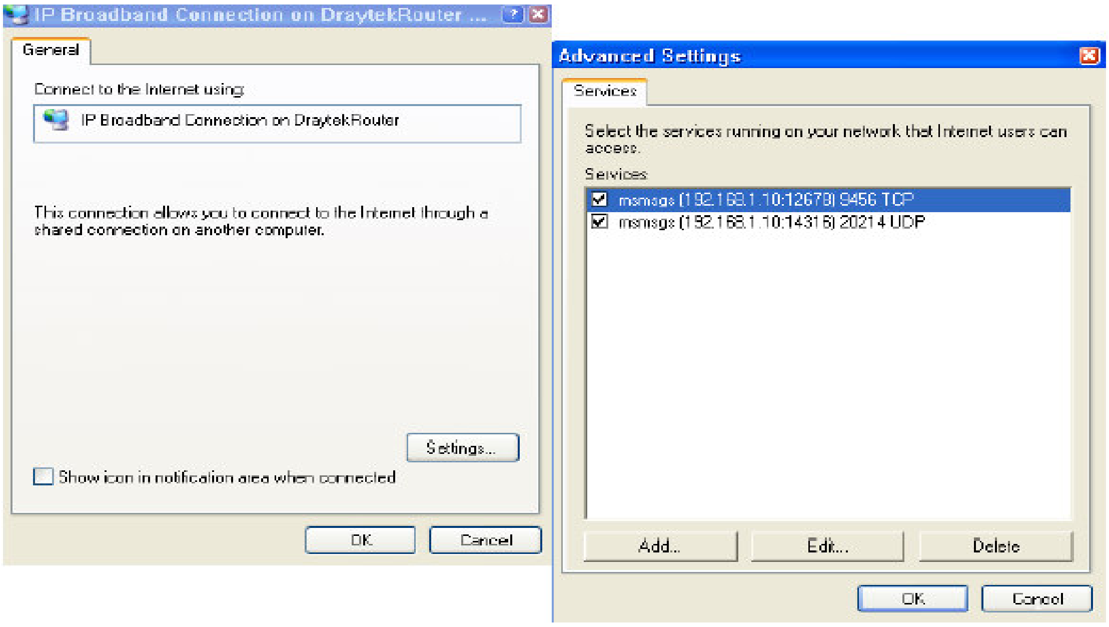
Internet Gateway

Status:	Connected
Duration:	00:07:53
Speed:	100.0 Mbps

Activity

	Internet	Internet Gateway	My Computer
Packets:			
Sent:		20	2,907
Received:		115	2,494

Figure 6-20. Connection status



Connect to the Internet using:

IP Broadband Connection on DraytekRouter

This connection allows you to connect to the Internet through a shared connection on another computer.

□ Show icon in notification area when connected

Select the services running on your network that Internet users can access.

Services

☑ msmsgs (192.168.1.10:12678) 9456 TCP
☑ msmsgs (192.168.1.10:14316) 20214 UDP

Figure 6-21. UPnP configuration

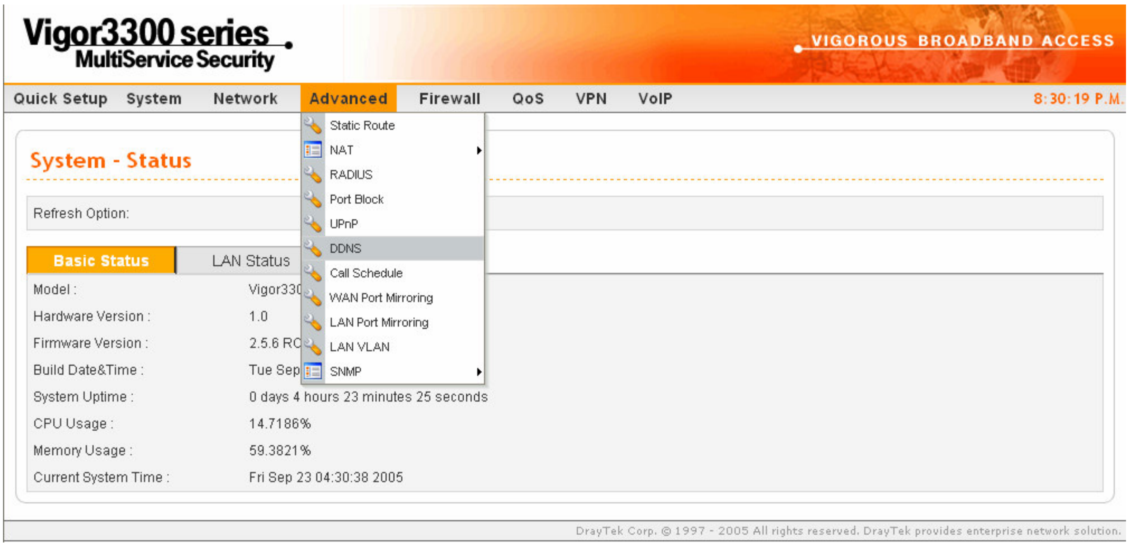
The Vigor3300 UPnP facility triggers UPnP-sensitive applications inside NAT such as MSN Messenger to discover the external IP address and configure port mappings on router. As a result, router with UPnP facility will redirect packets from the external ports to the internal ports according to application's requirement.

6.5 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. Figure 6-22 illustrates the location of **DDNS** option.



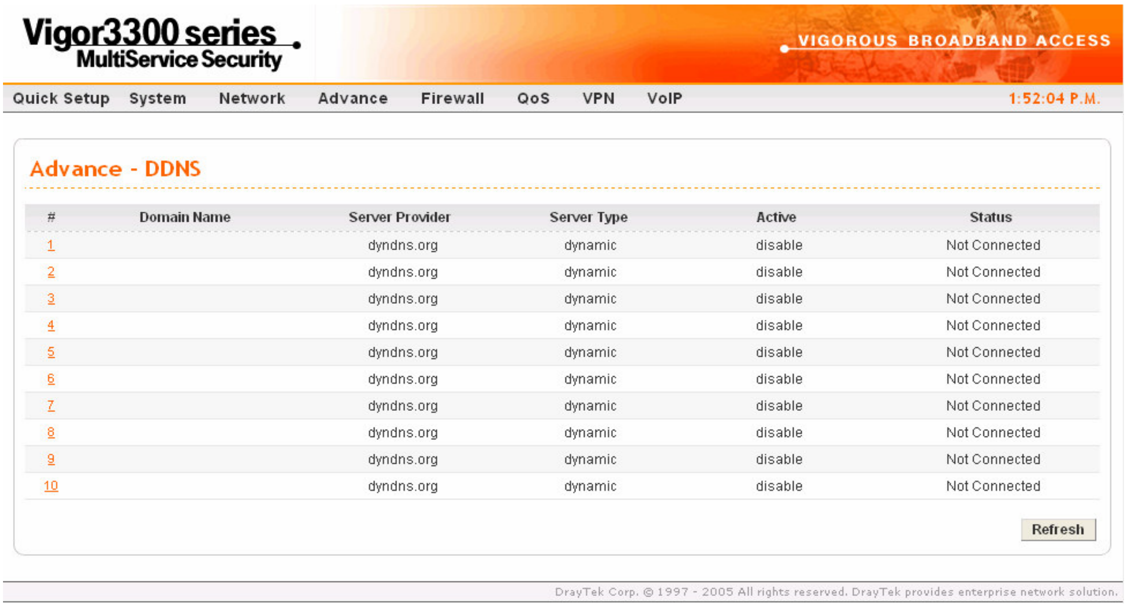
System - Status

Refresh Option:

Model :	Vigor330
Hardware Version :	1.0
Firmware Version :	2.5.6 RC
Build Date&Time :	Tue Sep
System Uptime :	0 days 4 hours 23 minutes 25 seconds
CPU Usage :	14.7186%
Memory Usage :	59.3821%
Current System Time :	Fri Sep 23 04:30:38 2005

Figure 6-22. DDNS option

Click the **DDNS** option, and then you will see the following web page. Figure 6-23 illustrates the web page as an example.

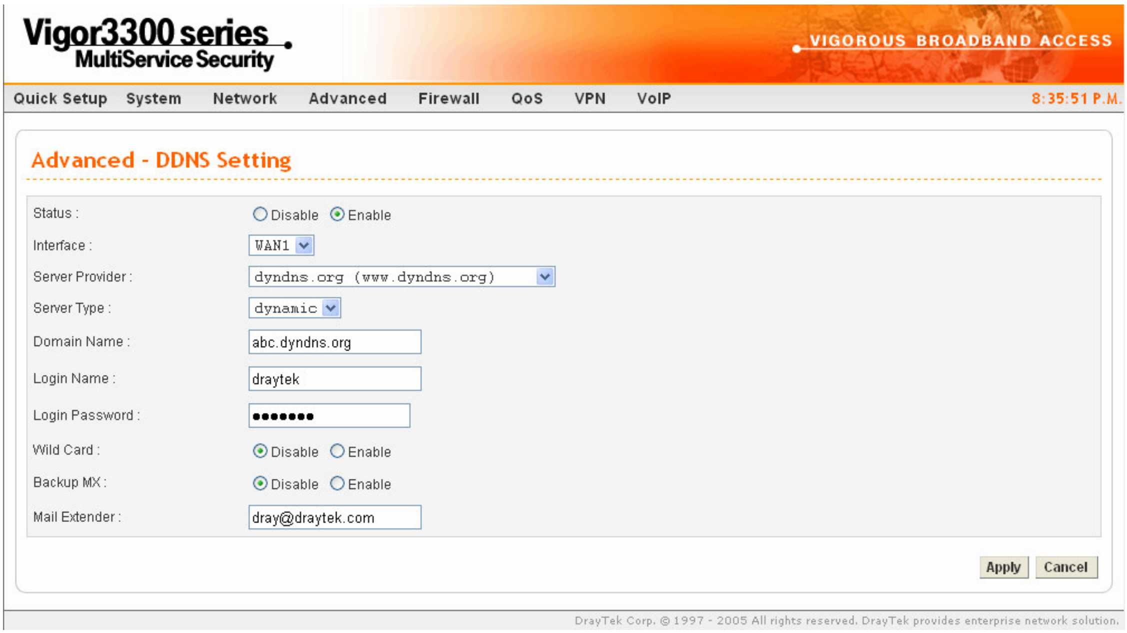

Vigor3300 series
MultiService Security
VIGOROUS BROADBAND ACCESS
Quick Setup
System
Network
Advance
Firewall
QoS
VPN
VoIP
1:52:04 P.M.
Refresh
DrayTek Corp. © 1997 - 2005 All rights reserved. DrayTek provides enterprise network solution.

Advance - DDNS

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

Figure 6-23. DDNS table

Click **Refresh** to re-display the whole page information. Click **#number** into edit mode to modify an entry in DDNS table. Figure 6-24 illustrates the web page as an example.


Vigor3300 series
MultiService Security
VIGOROUS BROADBAND ACCESS
Quick Setup
System
Network
Advanced
Firewall
QoS
VPN
VoIP
8:35:51 P.M.
Apply
Cancel
DrayTek Corp. © 1997 - 2005 All rights reserved. DrayTek provides enterprise network solution.

Advanced - DDNS Setting

Status :	○ Disable ● Enable
Interface :	WAN1
Server Provider :	dyndns.org (www.dyndns.org)
Server Type :	dynamic
Domain Name :	abc.dyndns.org
Login Name :	draytek
Login Password :	•••••••
Wild Card :	● Disable ○ Enable
Backup MX :	● Disable ○ Enable
Mail Extender :	dray@draytek.com

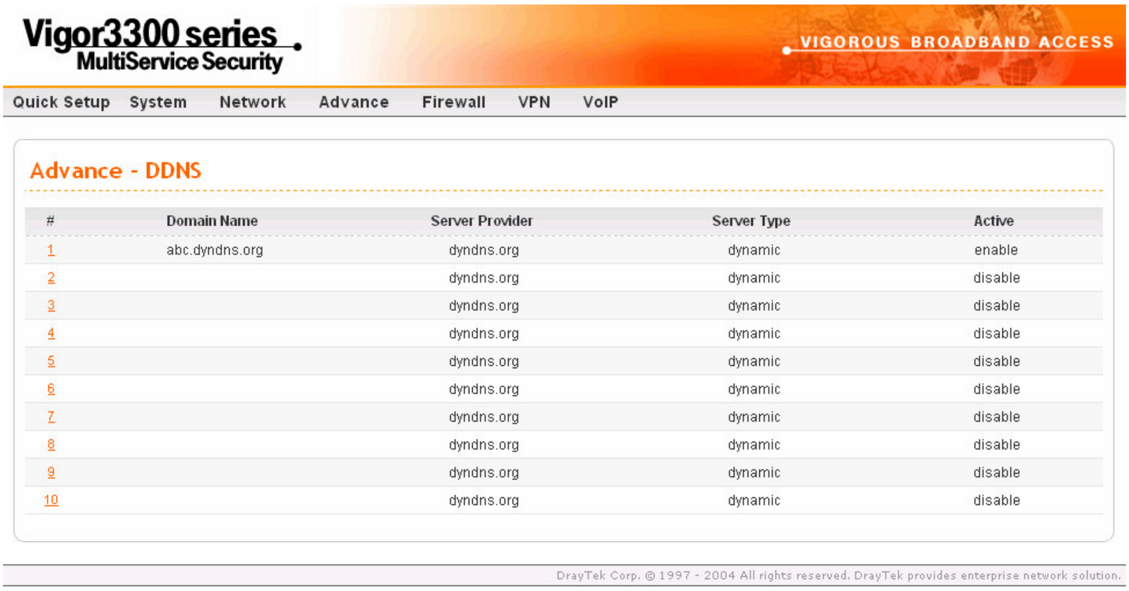
Figure 6-24. DDNS configuration

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 4 domain server providers as default.
Server Type	Select **Static**, **Dynamic** or **Custom** type.
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[3]	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 this setting. Figure 6-25 illustrates the web page as an example.

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

[3] 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.


Vigor3300 series
MultiService Security
VIGOROUS BROADBAND ACCESS
Quick Setup
System
Network
Advance
Firewall
VPN
VoIP
DrayTek Corp. © 1997 - 2004 All rights reserved. DrayTek provides enterprise network solution.

Advance - DDNS

#	Domain Name	Server Provider	Server Type	Active
1	abc.dyndns.org	dyndns.org	dynamic	enable
2		dyndns.org	dynamic	disable
3		dyndns.org	dynamic	disable
4		dyndns.org	dynamic	disable
5		dyndns.org	dynamic	disable
6		dyndns.org	dynamic	disable
7		dyndns.org	dynamic	disable
8		dyndns.org	dynamic	disable
9		dyndns.org	dynamic	disable
10		dyndns.org	dynamic	disable

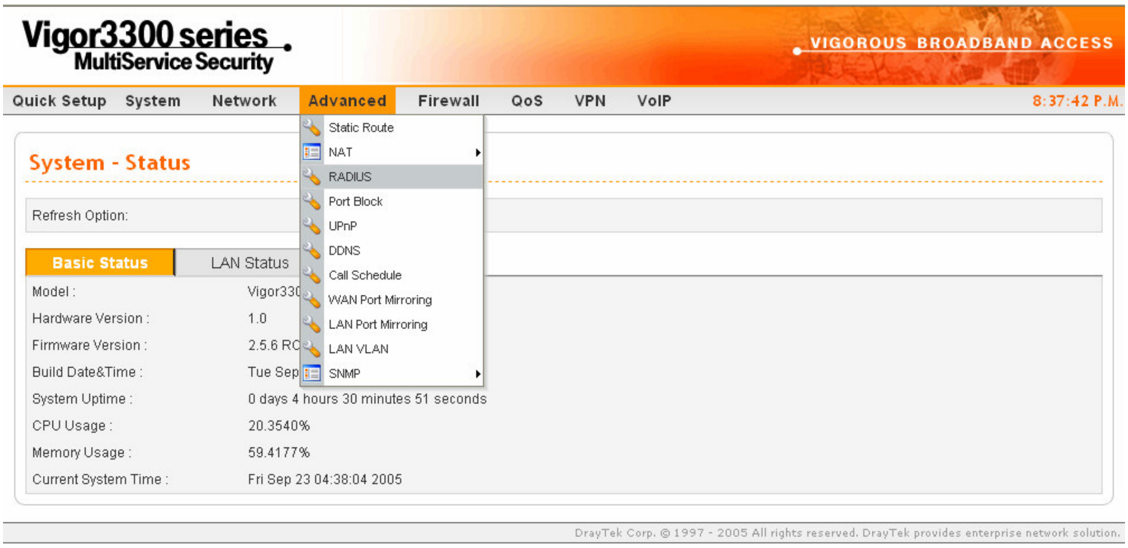
Figure 6-25. DDNS table

6.6 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. 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 server obtains the user’s personal data from one of the following places.

The Vigor 3300 series of routers support Radius client function. A user can configure some authentication information to do an authentication with Radius server. In the Vigor 3300, it is only used in VPN->PPTP function.

In the **Advanced** group, click the **Radius** option. Figure 6-26 illustrates the location of the **Radius** option.



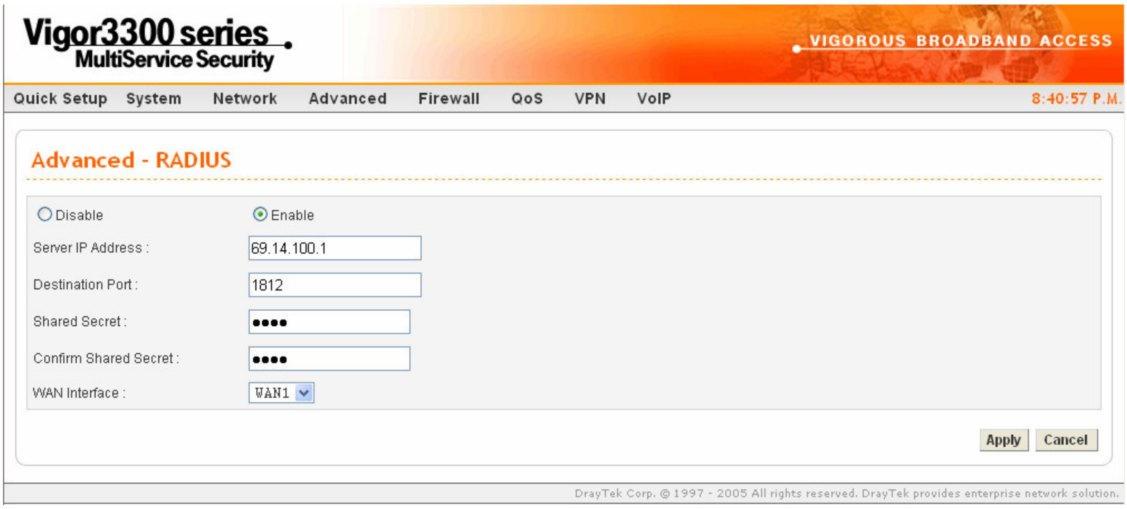
System - Status

Refresh Option:

Model :	Vigor330
Hardware Version :	1.0
Firmware Version :	2.5.6 RC
Build Date&Time :	Tue Sep
System Uptime :	0 days 4 hours 30 minutes 51 seconds
CPU Usage :	20.3540%
Memory Usage :	59.4177%
Current System Time :	Fri Sep 23 04:38:04 2005

Figure 6-26. Radius option

Click **Radius** option, and then you will see the following web page. Figure 6-27 illustrates the web page as an example.


Vigor3300 series
MultiService Security
VIGOROUS BROADBAND ACCESS
Quick Setup System Network Advanced Firewall QoS VPN VoIP
8:40:57 P.M.
Advanced - RADIUS
Apply
Cancel
DrayTek Corp. © 1997 - 2005 All rights reserved. DrayTek provides enterprise network solution.

○ Disable ● Enable

Server IP Address : 69.14.100.1

Destination Port : 1812

Shared Secret : ●●●●

Confirm Shared Secret : ●●●●

WAN Interface : WAN1

Figure 6-27. Radius configuration

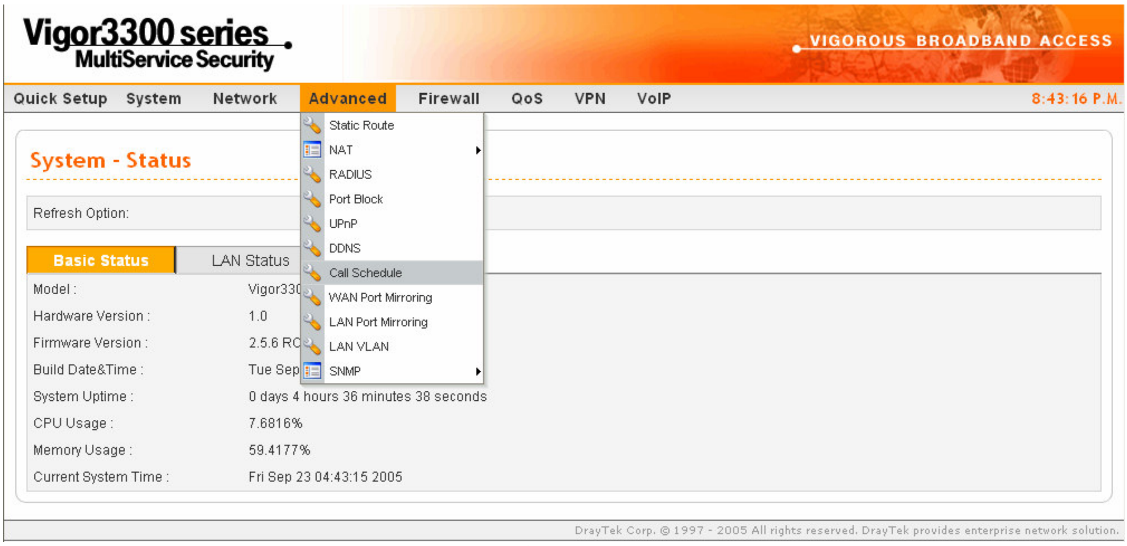
Enable/Disable	Click "**Disable**" to disable this function. Click "**Enable**" to activate this function.
Server IP Address	Assign an IP address of a Radius server.
Destination Port	Assign a destination port number used for Radius function.
Shared Secret	Assign a code for authentication to server.
Confirm Shared Secret	Confirm the code assigned in Shared Secret field.
WAN Interface	Select one specific WAN interface to be used.

Click **Apply** to finish this setting.

6.7 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. The Vigor 3300 series of routers support lots of profiles for call schedule usage.

In the **Advanced** group, click the **Call Schedule** option. Figure 6-28 illustrates the location of the **Call Schedule** option.



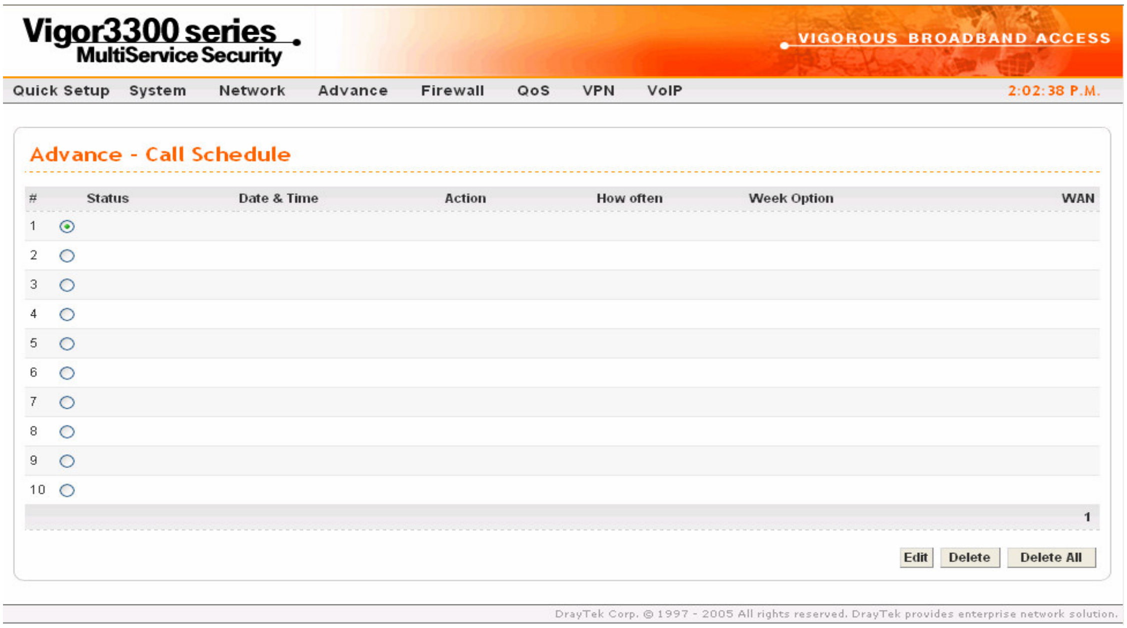
System - Status

Refresh Option:

Model :	Vigor330
Hardware Version :	1.0
Firmware Version :	2.5.6 RC
Build Date&Time :	Tue Sep
System Uptime :	0 days 4 hours 36 minutes 38 seconds
CPU Usage :	7.6816%
Memory Usage :	59.4177%
Current System Time :	Fri Sep 23 04:43:15 2005

Figure 6-28. Call schedule option

Click the **Call Schedule** option, and then you will see the following web page. Figure 6-29 illustrates the web page as an example.


Vigor3300 series
MultiService Security
VIGOROUS BROADBAND ACCESS
Quick Setup
System
Network
Advance
Firewall
QoS
VPN
VoIP
2:02:38 P.M.
1
Edit
Delete
Delete All
DrayTek Corp. © 1997 - 2005 All rights reserved. DrayTek provides enterprise network solution.

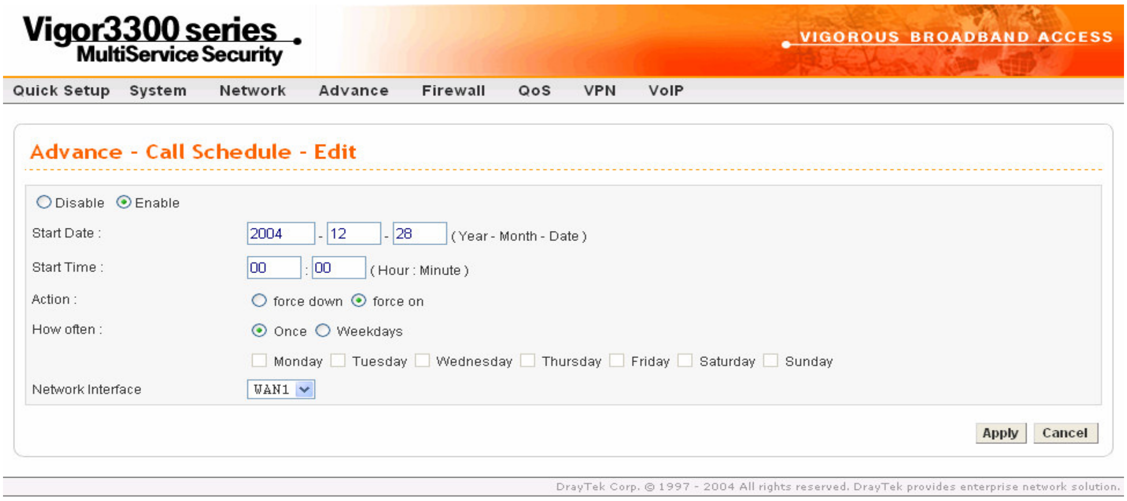
Advance - Call Schedule

#	Status	Date & Time	Action	How often	Week Option	WAN
1	●					
2	○					
3	○					
4	○					
5	○					
6	○					
7	○					
8	○					
9	○					
10	○					

Figure 6-29. Call schedule configuration

6.7.1 Edit Option

Click **Edit** to add or edit one entry in call schedule table. Figure 6-30 illustrates the web page as an example.



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

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

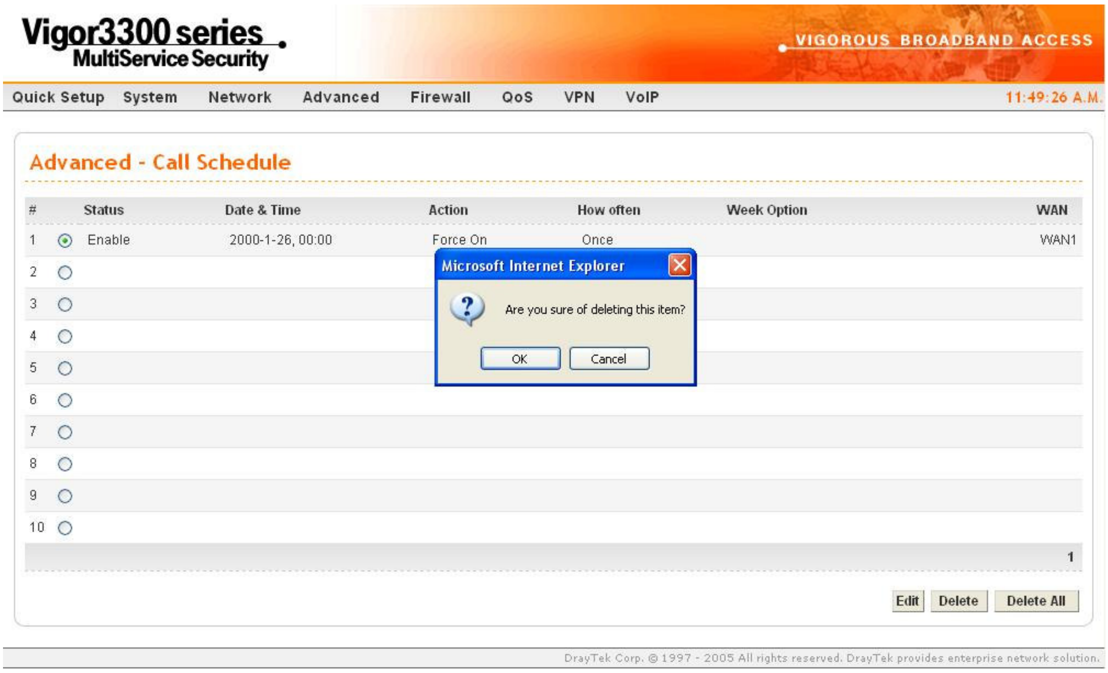
Figure 6-30. Edit call schedule table

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.

6.7.2 Delete Option

Click **Delete** to remove a profile entry in call schedule table. Figure 6-31 illustrates the web page as an example.



Advanced - Call Schedule

#		Status	Date & Time	Action	How often	Week Option	WAN
1	●	Enable	2000-1-26, 00:00	Force On	Once		WAN1
2	○						
3	○						
4	○						
5	○						
6	○						
7	○						
8	○						
9	○						
10	○						

1

Microsoft Internet Explorer

Are you sure of deleting this item?

OK Cancel

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

Figure 6-31. Call schedule - delete

Click **Apply** to finish this setting.

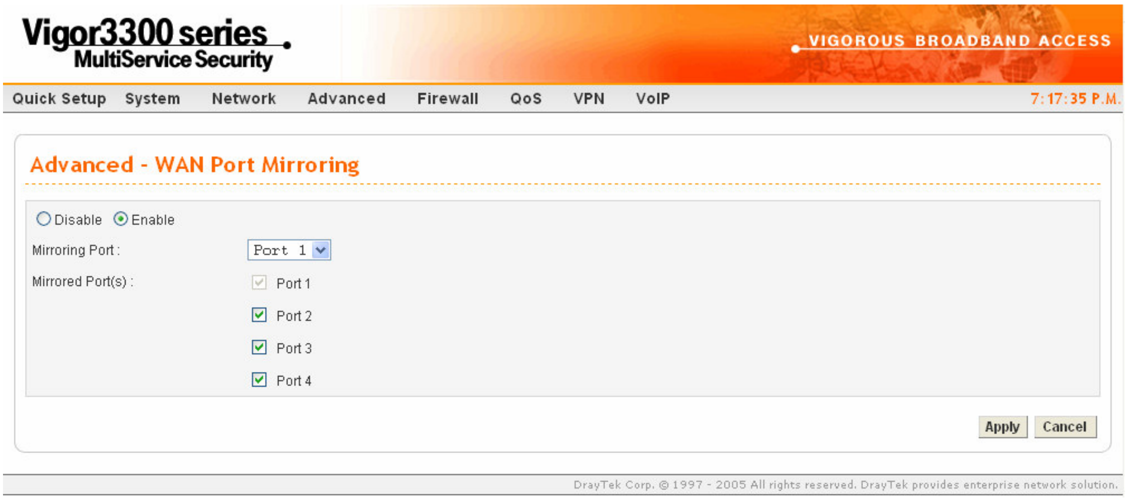
User can click **Delete All** to remove all entries in the table.

6.8 WAN Port Mirroring Setup

3300V supports port mirroring function in four 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 interface.

In the **Advanced** group, click the **WAN Port Mirroring** option as shown in Figure 6-32.


Vigor3300 series
MultiService Security
VIGOROUS BROADBAND ACCESS
Quick Setup
System
Network
Advanced
Firewall
QoS
VPN
VoIP
7:17:35 P.M.
Apply
Cancel
DrayTek Corp. © 1997 - 2005 All rights reserved. DrayTek provides enterprise network solution.

Advanced - WAN Port Mirroring

○ Disable ● Enable

Mirroring Port : Port 1

Mirrored Port(s) :
☑ Port 1
☑ Port 2
☑ Port 3
☑ Port 4

Figure 6-32. WAN port mirroring configuration

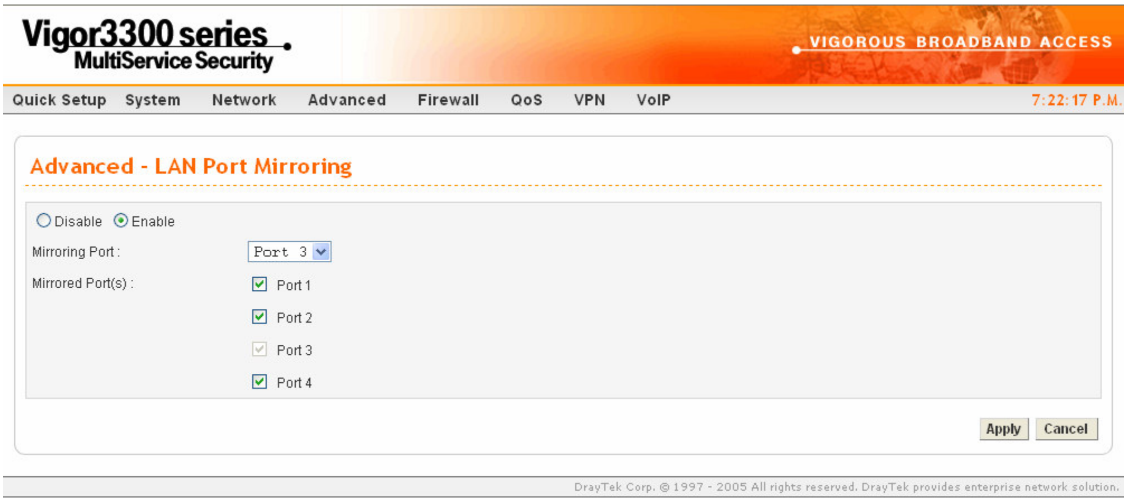
Click **Apply** to finish this setting.

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.

6.9 LAN Port Mirroring Setup

We still support the port mirroring function in LAN site not only in WAN site. It has the same mechanism like WAN port mirroring.

In the **Advanced** group, click the **LAN Port Mirroring** option as shown in Figure 6-33.


Vigor3300 series
MultiService Security
VIGOROUS BROADBAND ACCESS
Quick Setup
System
Network
Advanced
Firewall
QoS
VPN
VoIP
7:22:17 P.M.
Apply
Cancel
DrayTek Corp. © 1997 - 2005 All rights reserved. DrayTek provides enterprise network solution.

Advanced - LAN Port Mirroring

○ Disable ● Enable

Mirroring Port : Port 3

Mirrored Port(s) :
☑ Port 1
☑ Port 2
☑ Port 3
☑ Port 4

Figure 6-33. LAN port mirroring configuration

Click **Apply** to finish this setting.

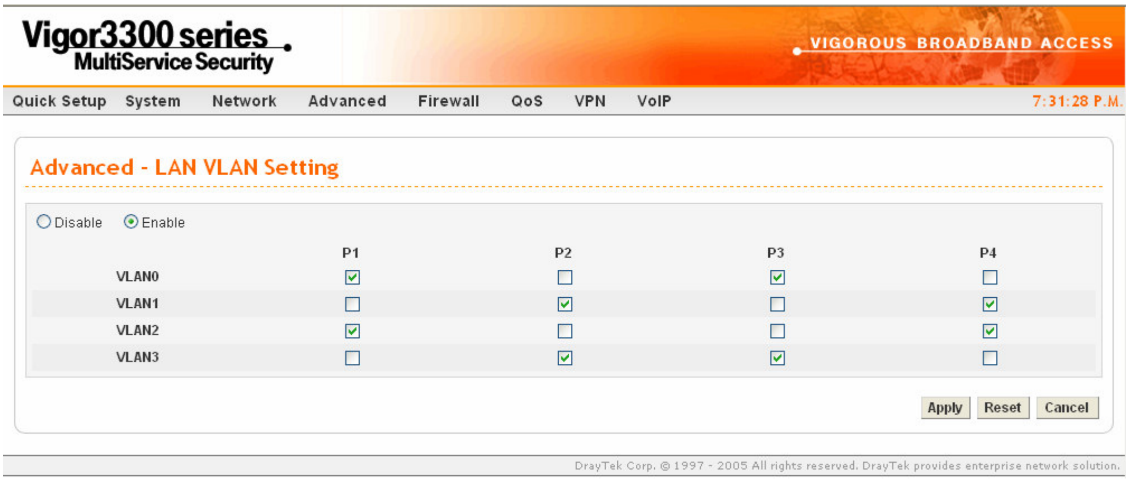
Enable/Disable	Click "**Disable**" to disable this function. Click "**Enable**" to activate this function.
Mirroring Port	Select a port to view traffic sent from mirrored ports.
Mirrored Port(s)	Click which ports are necessary to be mirrored.

6.10 LAN VLAN Setup

3300 supports VLAN function in only in LAN site. Basically, it is only implemented by port-based. 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.

In the **Advanced** group, click the **LAN VLAN** option as shown in Figure 6-34.


Vigor3300 series
MultiService Security
VIGOROUS BROADBAND ACCESS
Quick Setup
System
Network
Advanced
Firewall
QoS
VPN
VoIP
7:31:28 P.M.
Apply
Reset
Cancel
DrayTek Corp. © 1997 - 2005 All rights reserved. DrayTek provides enterprise network solution.

Advanced - LAN VLAN Setting

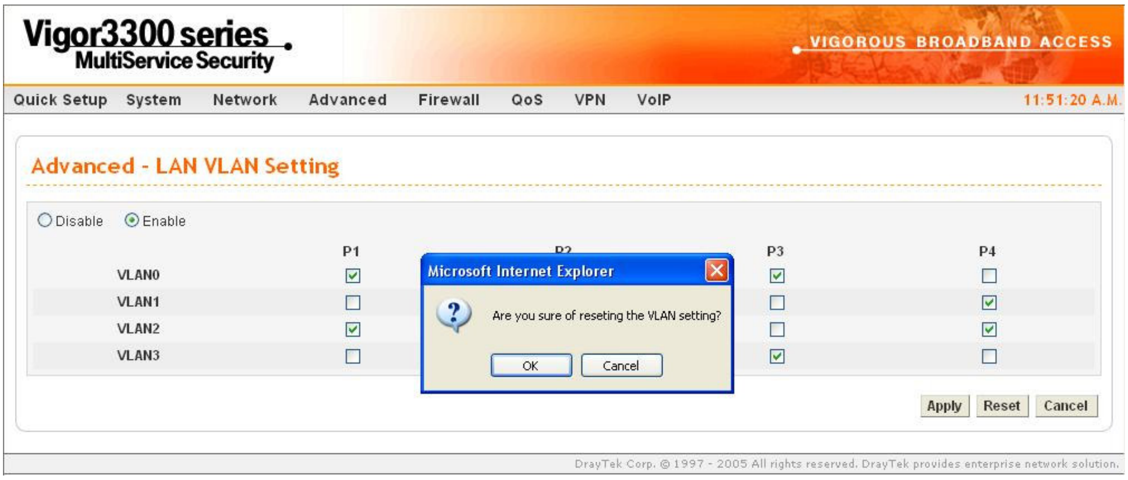
○ Disable ● Enable

	P1	P2	P3	P4
VLAN0	☑	□	☑	□
VLAN1	□	☑	□	☑
VLAN2	☑	□	□	☑
VLAN3	□	☑	☑	□

Figure 6-34. LAN VLAN configuration

Click **Apply** to finish this setting.

Click **Reset** to reset the VLAN setting as default.


Vigor3300 series
MultiService Security
VIGOROUS BROADBAND ACCESS
Quick Setup System Network Advanced Firewall QoS VPN VoIP
11:51:20 A.M.

Advanced - LAN VLAN Setting

○ Disable ● Enable

	P1	P2	P3	P4
VLAN0	☑		☑	□
VLAN1	□		□	☑
VLAN2	☑		□	☑
VLAN3	□		☑	□

Microsoft Internet Explorer

Are you sure of reseting the VLAN setting?

OK Cancel

Apply Reset Cancel

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

Figure 6-35. LAN VLAN configuration-Reset

6.11 SNMP Configuration

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.

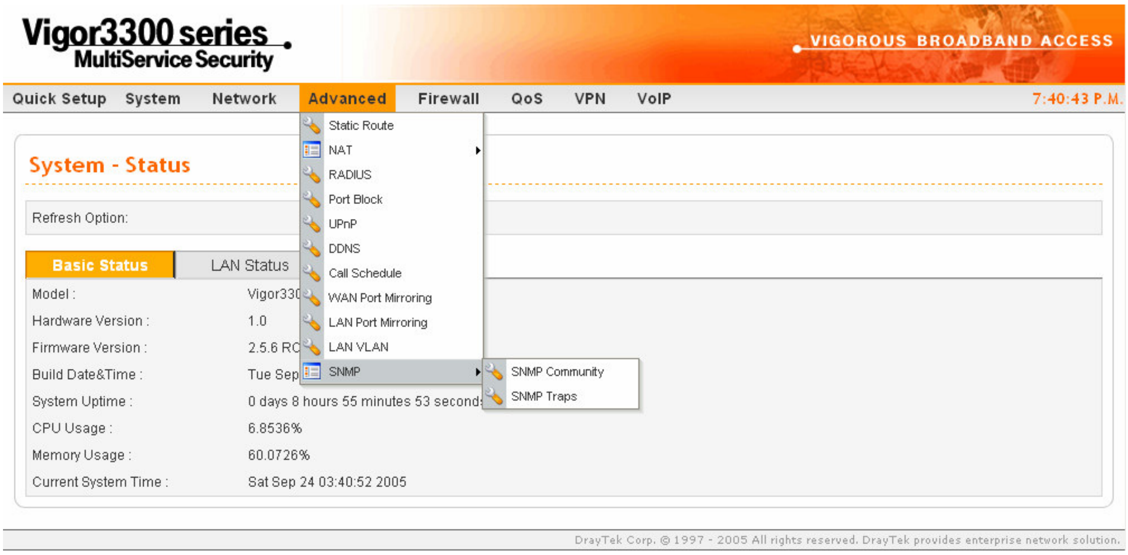
A SNMP-managed network consists of three key components, managed devices, agents, and network-management systems (NMSs).

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

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.

A 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 as shown in Figure 6-36.



Refresh Option:

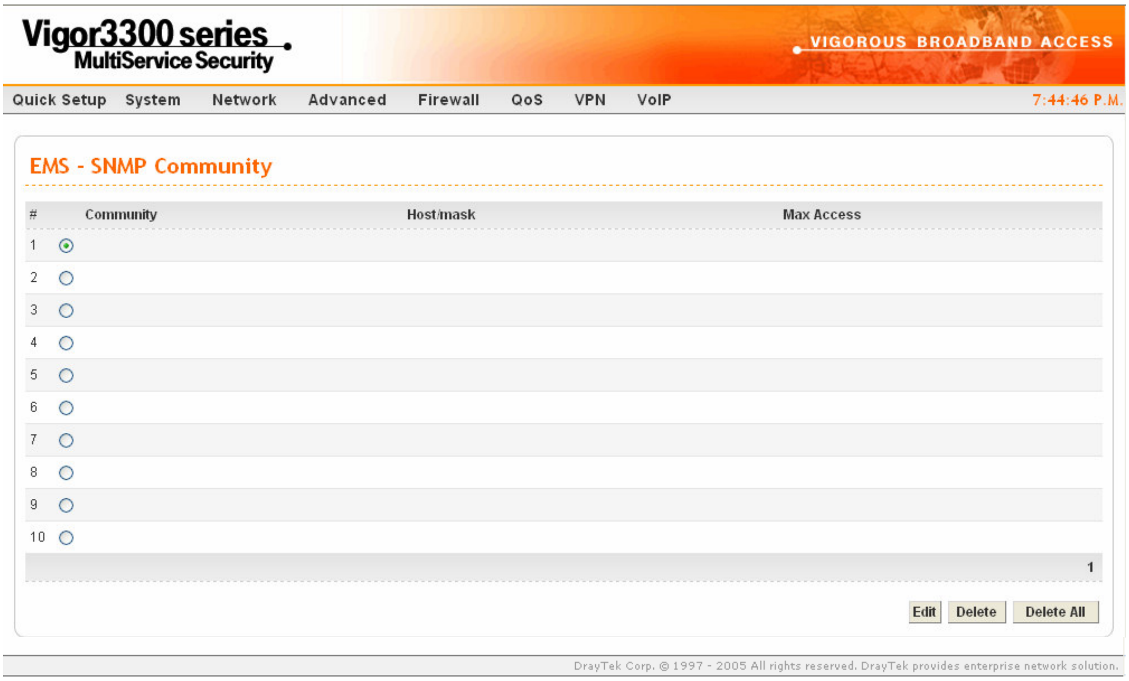
Model :	Vigor330
Hardware Version :	1.0
Firmware Version :	2.5.6 RC
Build Date&Time :	Tue Sep
System Uptime :	0 days 8 hours 55 minutes 53 second
CPU Usage :	6.8536%
Memory Usage :	60.0726%
Current System Time :	Sat Sep 24 03:40:52 2005

Figure 6-36. The location of SNMP

6.11.1 SNMP Community

This function is to define a community string name. Generally speaking, NMSs which is within the community are said to exist within the same administrative domain. Community names serve as a weak form of authentication because devices that do not know the proper community name are precluded from SNMP operations.

Click **SNMP Community** option, the page is shown as Figure 6-37.


Vigor3300 series
MultiService Security
VIGOROUS BROADBAND ACCESS
Quick Setup
System
Network
Advanced
Firewall
QoS
VPN
VoIP
7:44:46 P.M.
Edit
Delete
Delete All
DrayTek Corp. © 1997 - 2005 All rights reserved. DrayTek provides enterprise network solution.

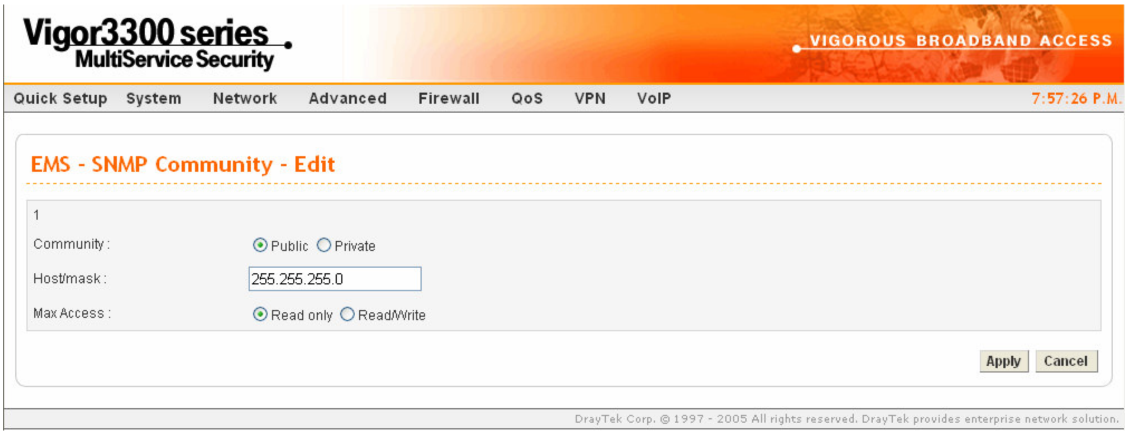
EMS - SNMP Community

#		Community	Host/mask	Max Access
1	●			
2	○			
3	○			
4	○			
5	○			
6	○			
7	○			
8	○			
9	○			
10	○			

1

Figure 6-37. SNMP community configuration

Click **Edit** button, the page is shown in Figure 6-38.


Vigor3300 series
MultiService Security
VIGOROUS BROADBAND ACCESS
Quick Setup
System
Network
Advanced
Firewall
QoS
VPN
VoIP
7:57:26 P.M.

EMS - SNMP Community - Edit

1

Community : ● Public ○ Private

Host/mask : 255.255.255.0

Max Access : ● Read only ○ Read/Write

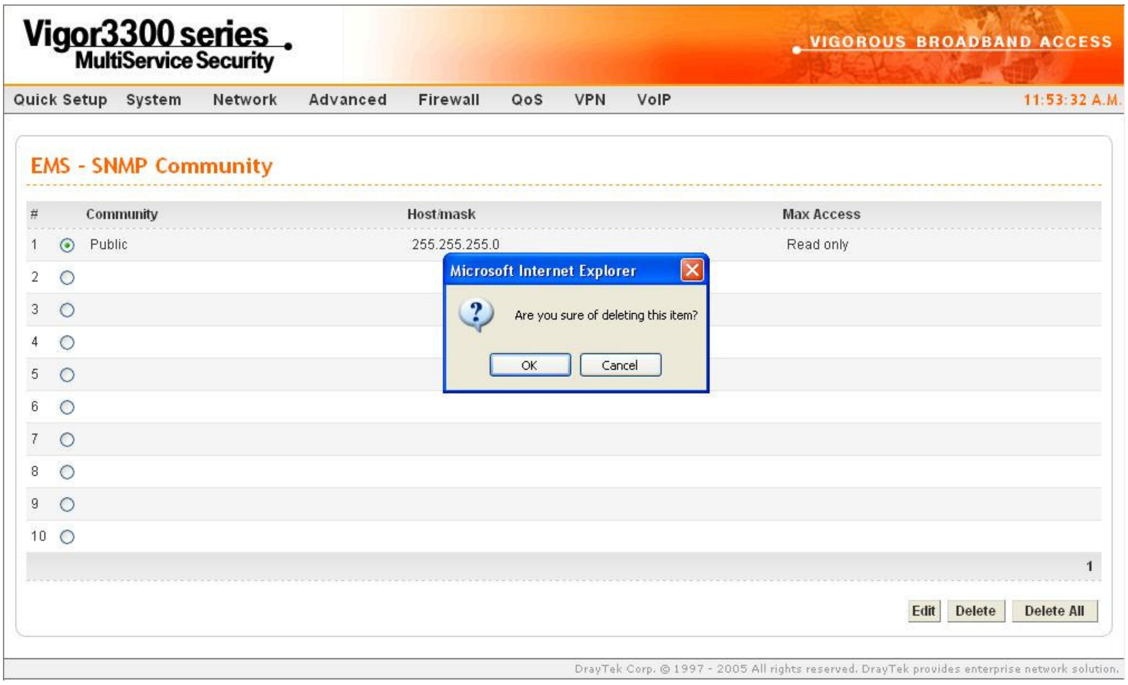
DrayTek Corp. © 1997 - 2005 All rights reserved. DrayTek provides enterprise network solution.

Figure 6-38. SNMP community-edit

Community	Click "**Public**" as the community string in SNMP protocol. Click "**Private**" as the community string in SNMP protocol.
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.

Click **Apply** to finish this setting.

Click **Delete** to remove this entry. The page is shown as Figure 6-39.


Vigor3300 series
MultiService Security
VIGOROUS BROADBAND ACCESS
Quick Setup System Network Advanced Firewall QoS VPN VoIP
11:53:32 A.M.

EMS - SNMP Community

#		Community	Host/mask	Max Access
1	●	Public	255.255.255.0	Read only
2	○			
3	○			
4	○			
5	○			
6	○			
7	○			
8	○			
9	○			
10	○			

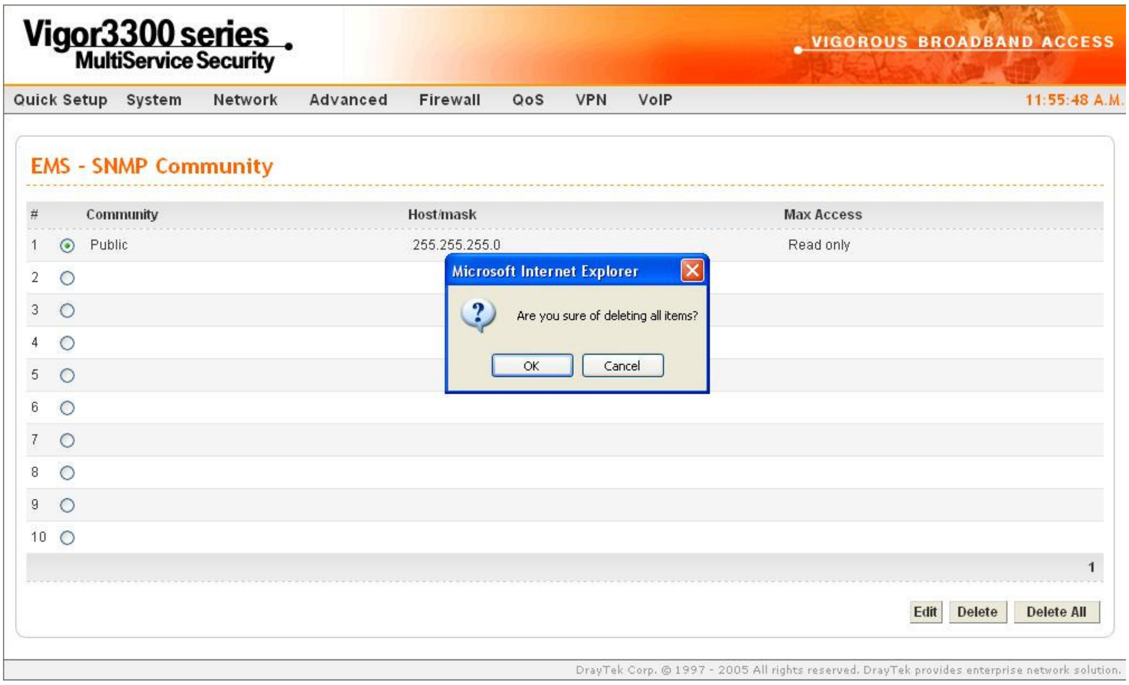
Microsoft Internet Explorer

Are you sure of deleting this item?

OK
Cancel
1
Edit
Delete
Delete All
DrayTek Corp. © 1997 - 2005 All rights reserved. DrayTek provides enterprise network solution.

Figure 6-39. SNMP community-delete

Click **Delete All** to remove all entries in the table. The page is shown as Figure 6-40.



Vigor3300 series
MultiService Security
VIGOROUS BROADBAND ACCESS
Quick Setup System Network Advanced Firewall QoS VPN VoIP
11:55:48 A.M.

EMS - SNMP Community

#		Community	Host/mask	Max Access
1	●	Public	255.255.255.0	Read only
2	○			
3	○			
4	○			
5	○			
6	○			
7	○			
8	○			
9	○			
10	○			

1

Microsoft Internet Explorer

Are you sure of deleting all items?

OK
Cancel
Edit
Delete
Delete All

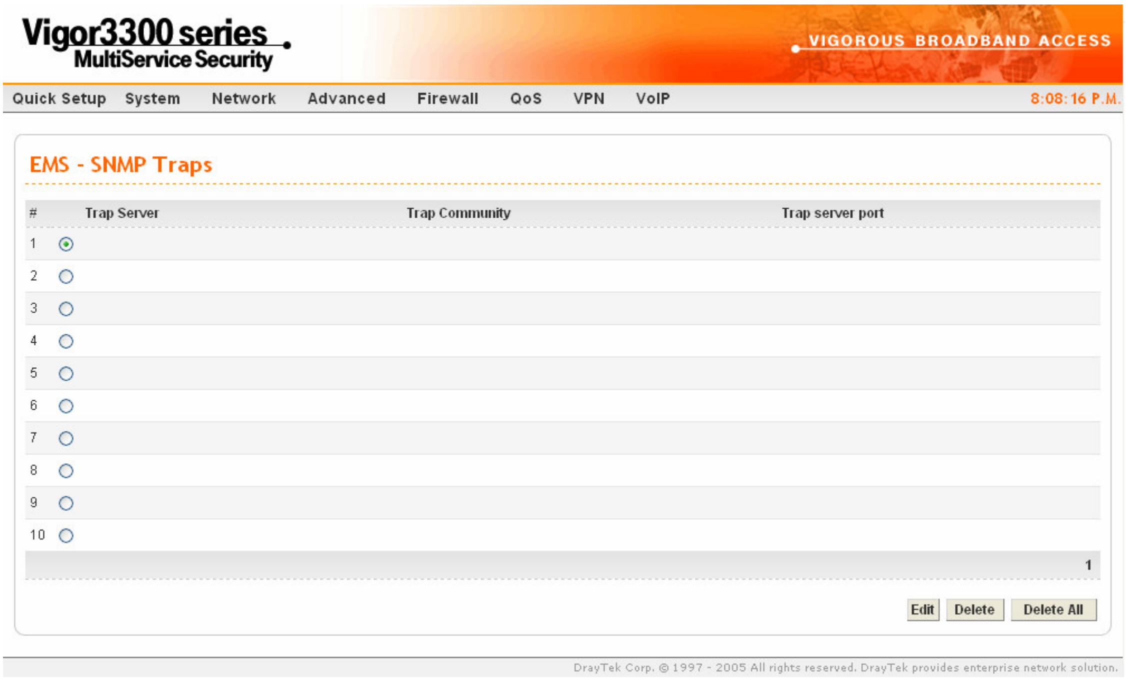
DrayTek Corp. © 1997 - 2005 All rights reserved. DrayTek provides enterprise network solution.

Figure 6-40. SNMP community-delete all

6.11.2 SNMP Traps

In managed network by SNMP protocol, agent will send a specific packet as an attention for administrator; it is called “**Trap**”. Trap is the only PDU 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).

Click **SNMP Traps** option, the page is shown as Figure 6-41.



EMS - SNMP Traps

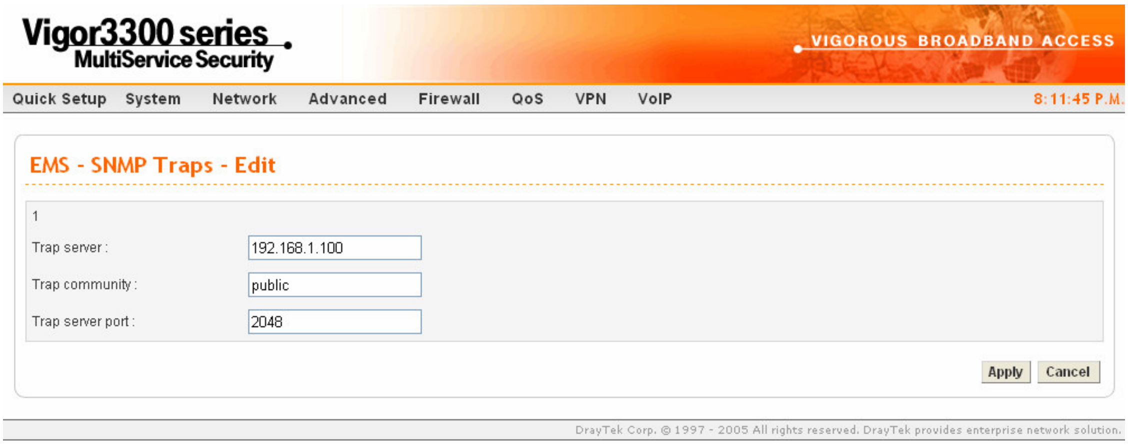
#		Trap Server	Trap Community	Trap server port
1	●			
2	○			
3	○			
4	○			
5	○			
6	○			
7	○			
8	○			
9	○			
10	○			

1

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

Figure 6-41. SNMP traps configuration

Click **Edit** button, the page is shown as Figure 6-42.


Vigor3300 series
MultiService Security
VIGOROUS BROADBAND ACCESS
Quick Setup
System
Network
Advanced
Firewall
QoS
VPN
VoIP
8:11:45 P.M.
Apply
Cancel
DrayTek Corp. © 1997 - 2005 All rights reserved. DrayTek provides enterprise network solution.

EMS - SNMP Traps - Edit

1

Trap server : 192.168.1.100

Trap community : public

Trap server port : 2048

Figure 6-42. SNMP Traps-Edit

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.

Click **Delete** option to remove this entry.

Click **Delete All** option to remove all the entries in the table.

CHAPTER 7

Firewall Setup

This chapter shows how to configure your router's firewall feature. The firewall controls which packets to allow or deny into or out of the router.

This chapter is divided into the following sections.

- Section 7.1: Introduction
- Section 7.2: An Overview of the Firewall Setup
- Section 7.3: IP Filter Setup
- Section 7.4: Denial of Service Attacks Setup
- Section 7.5: URL Filter Setup

7.1 Introduction

The **Firewall Setup** in the Vigor 3300 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 an unexpected outgoing connection such as a Trojan.

There is group, filter definition on the firewall Web page as follows. A group contains filter rules, and a filter is a member of a particular group. Before IP filter rules are set, a group should be created to arrange and maintain filer rules. One group should be selected as the starting group to enable the firewall function.

In the next group setting, the order of groups can be arranged. A filter rule can also link to another group for advanced properties. An example is shown in Figure 7-1.

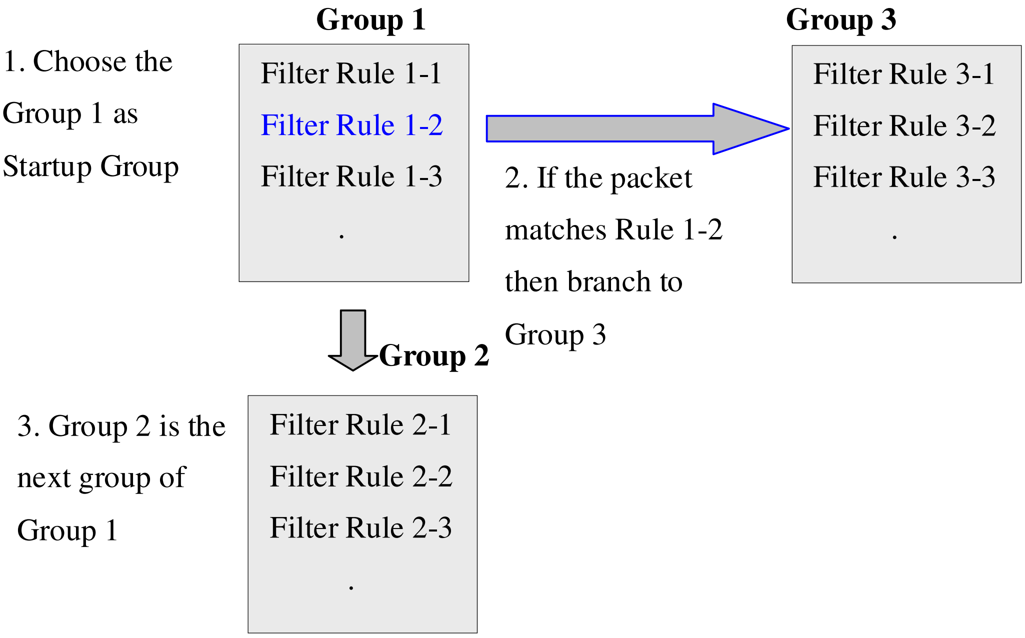
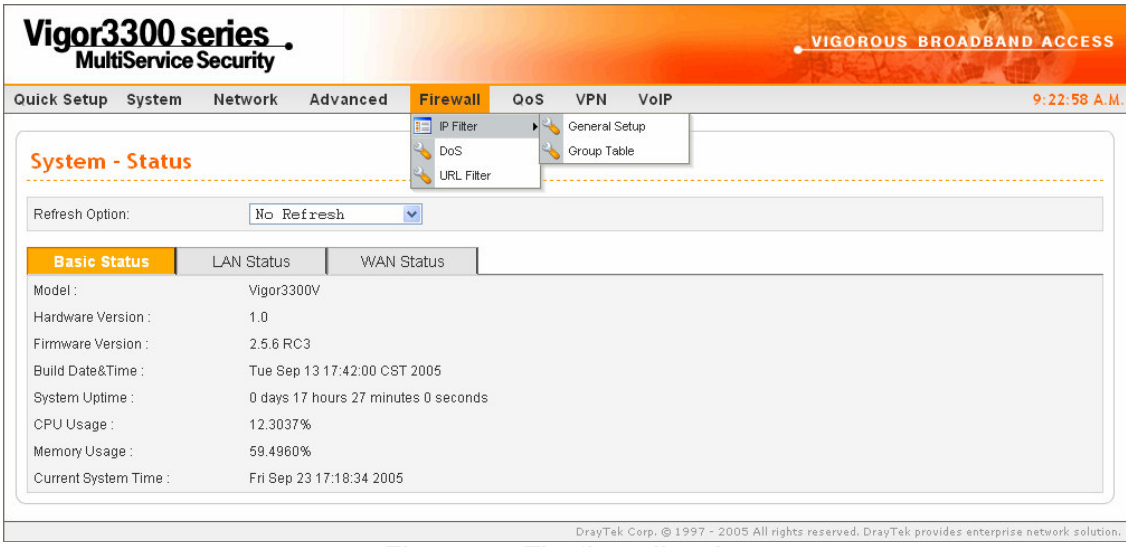


Figure 7-1. Concept of filter rules group

7.2 An Overview of the Firewall Setup

The following sections will explain how to configure the **Firewall**. User can select the **Firewall** option in the menu to find the **General Setup**, **IP Filter**, **DoS** and **URL Filter** options.

The **DoS** facility can detect and mitigate the DoS attacks. The **URL Filter** can block inappropriate websites for SME. The setting is shown in Figure 7-2.



System - Status

Refresh Option: No Refresh

Model :	Vigor3300V
Hardware Version :	1.0
Firmware Version :	2.5.6 RC3
Build Date&Time :	Tue Sep 13 17:42:00 CST 2005
System Uptime :	0 days 17 hours 27 minutes 0 seconds
CPU Usage :	12.3037%
Memory Usage :	59.4960%
Current System Time :	Fri Sep 23 17:18:34 2005

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

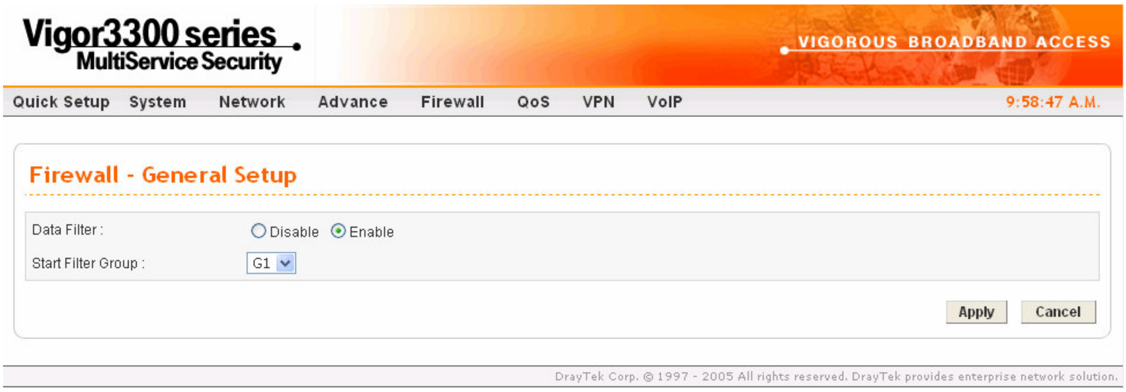
Figure 7-2. The firewall option

7.3 IP Filter Setup

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.

7.3.1 General Setup

Click the **General Setup** option to bring up the following Web page as shown in Figure 7-3.


Vigor3300 series
MultiService Security
VIGOROUS BROADBAND ACCESS
Quick Setup
System
Network
Advance
Firewall
QoS
VPN
VoIP
9:58:47 A.M.
Apply
Cancel
DrayTek Corp. © 1997 - 2005 All rights reserved. DrayTek provides enterprise network solution.

Firewall - General Setup

Data Filter : ○ Disable ● Enable

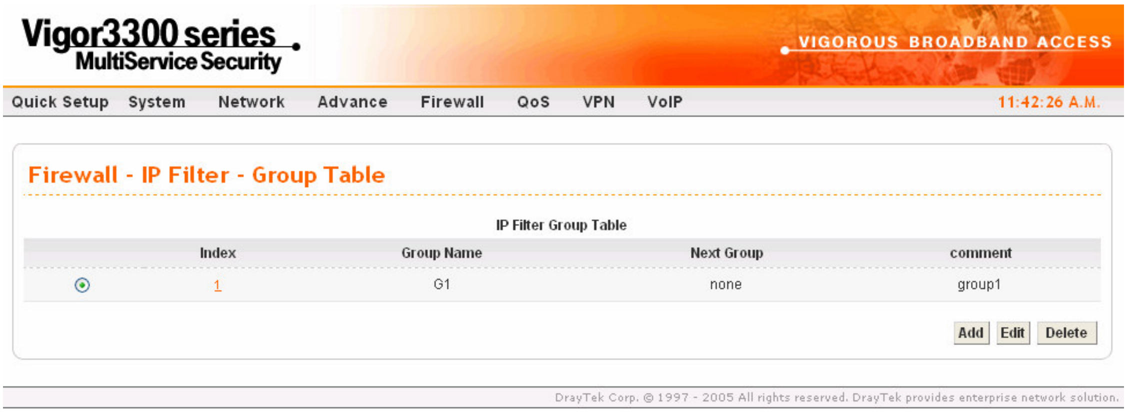
Start Filter Group : G1

Figure 7-3. General configuration

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	Select the first filter group to begin filtering mechanism. The group in this list must exist and had been pre-configured.

7.3.2 Group Table Setup

Click the **Group Table** option to bring up the following Web page and shown in Figure 7-4.


Vigor3300 series
MultiService Security
VIGOROUS BROADBAND ACCESS
Quick Setup
System
Network
Advance
Firewall
QoS
VPN
VoIP
11:42:26 A.M.
Add
Edit
Delete
DrayTek Corp. © 1997 - 2005 All rights reserved. DrayTek provides enterprise network solution.

Firewall - IP Filter - Group Table

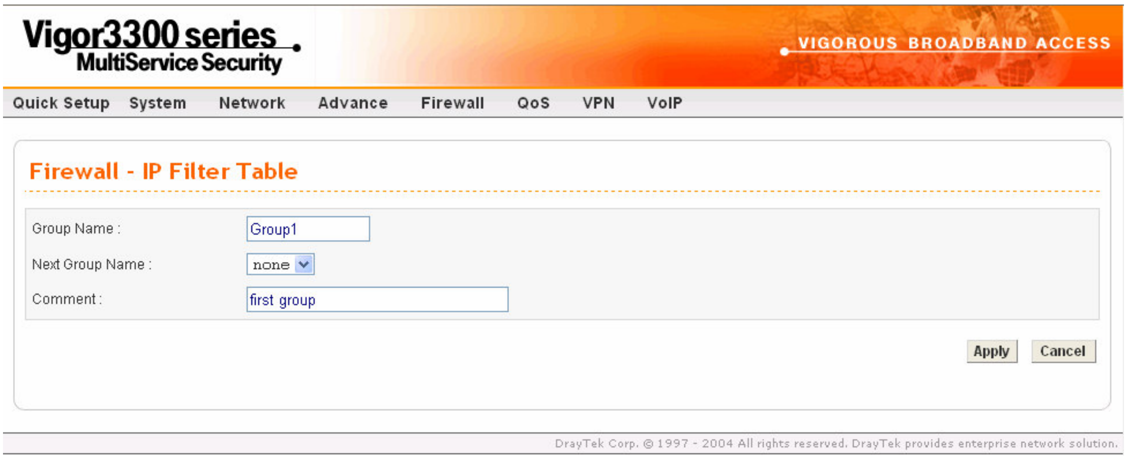
IP Filter Group Table

	Index	Group Name	Next Group	comment
●	1	G1	none	group1

Figure 7-4. Group table configuration

Click **Delete**[1] to remove a group from the IP Filter table configuration.
Click **Add** to add a new Group. The Web page is shown in Figure 7-5.

[1] *If this entry is assigned as the started filter group already, it cannot be deleted unless the Data Filter function is disabled in General Setup page in Figure 7-7.*


Vigor3300 series
MultiService Security
VIGOROUS BROADBAND ACCESS
Quick Setup
System
Network
Advance
Firewall
QoS
VPN
VoIP
Apply
Cancel
DrayTek Corp. © 1997 - 2004 All rights reserved. DrayTek provides enterprise network solution.

Firewall - IP Filter Table

Group Name : Group1

Next Group Name : none

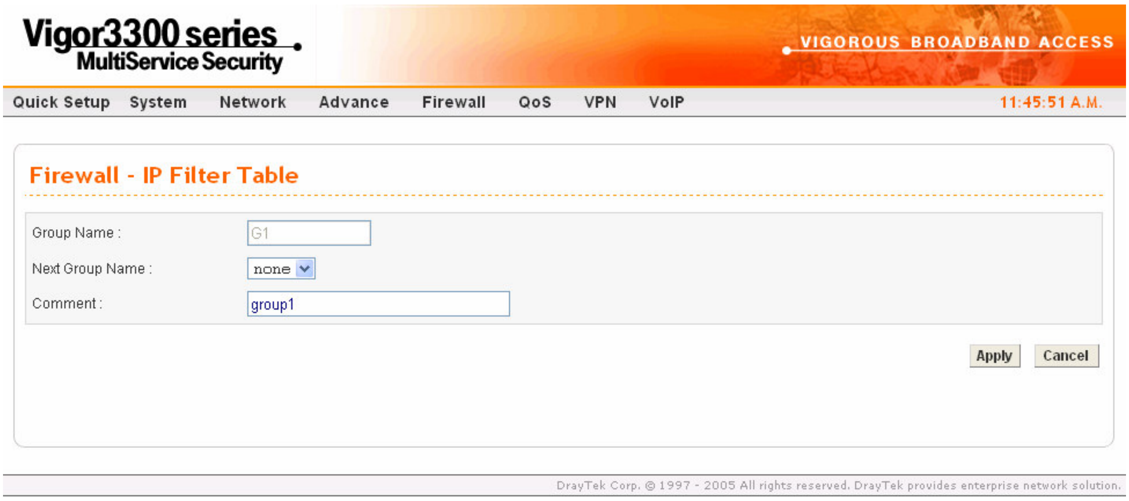
Comment : first group

Figure 7-5. Add IP filter group

Group Name	The name of the group.
Next Group Name	The next group to filter packets.
Comment	A comment or description for the group.

Fill out the **Group Name**, **Next Group Name** and **Comment** fields. Click **Apply** when you are finished to apply the settings, or click **Cancel** to go back without saving the settings. Users should change any setting on the same screen by clicking **Edit**[2] to modify an IP Filter table configuration as Figure 7-6.

[2] ***In Edit mode, the Group Name field cannot be modified.***

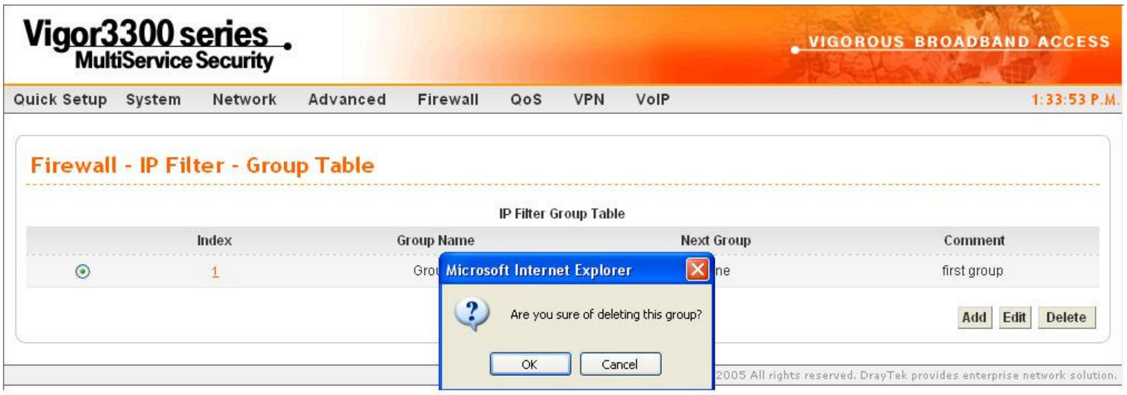

Vigor3300 series
MultiService Security
VIGOROUS BROADBAND ACCESS
Quick Setup
System
Network
Advance
Firewall
QoS
VPN
VoIP
11:45:51 A.M.
Apply
Cancel
DrayTek Corp. © 1997 - 2005 All rights reserved. DrayTek provides enterprise network solution.

Firewall - IP Filter Table

Group Name :	G1
Next Group Name :	none
Comment :	group1

Figure 7-6. Edit IP filter table entry

Click **Apply** to apply the settings.


Vigor3300 series
MultiService Security
VIGOROUS BROADBAND ACCESS
Quick Setup
System
Network
Advanced
Firewall
QoS
VPN
VoIP
1:33:53 P.M.
Add
Edit
Delete
Microsoft Internet Explorer
OK
Cancel
2005 All rights reserved. DrayTek provides enterprise network solution.

Firewall - IP Filter - Group Table

IP Filter Group Table

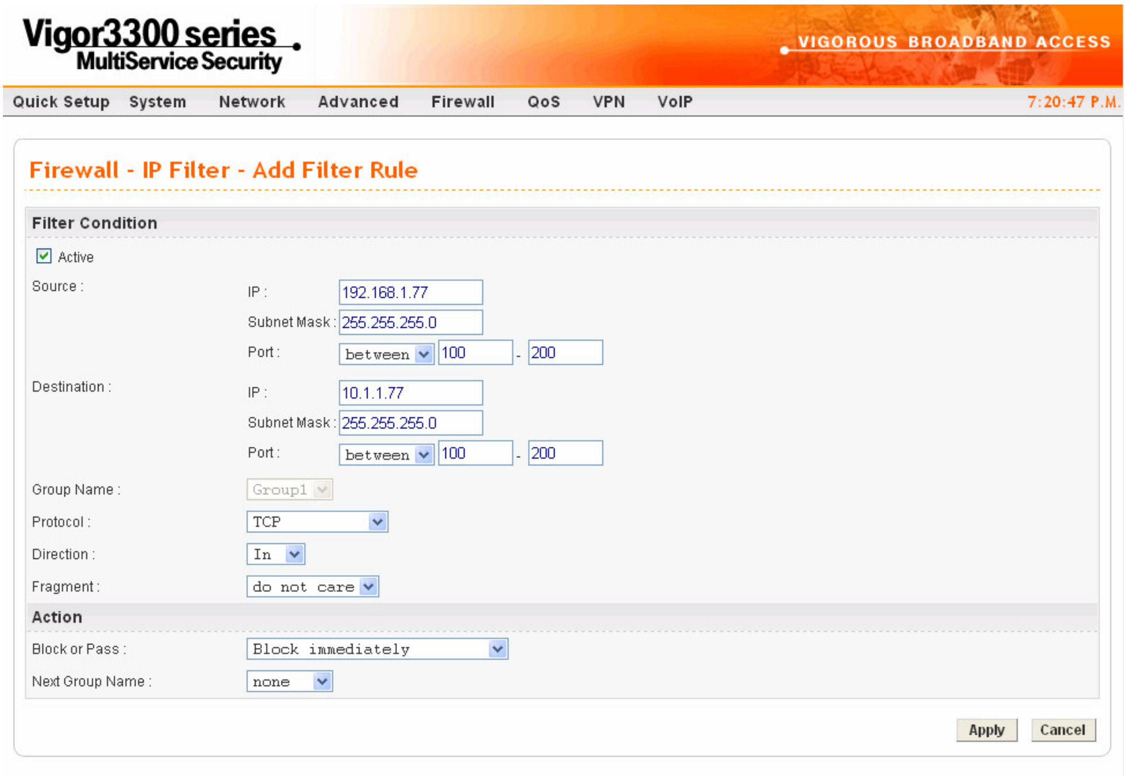
	Index	Group Name	Next Group	Comment
●	1	Grou	ne	first group

Are you sure of deleting this group?

Figure 7-7. Delete IP filter table

7.3.3 Add Filter Rule

Click **Add Rule** icon **under Firewall->IP Filter Table** to add a new rule as following Web page **in** Figure 7-8[3].



Firewall - IP Filter - Add Filter Rule

Filter Condition

☑ Active

Source :	IP :	192.168.1.77
	Subnet Mask :	255.255.255.0
	Port :	between 100 - 200
Destination :	IP :	10.1.1.77
	Subnet Mask :	255.255.255.0
	Port :	between 100 - 200
Group Name :		Group1
Protocol :		TCP
Direction :		In
Fragment :		do not care

Action

Block or Pass :	Block immediately
Next Group Name :	none

Figure 7-8. IP filter configuration

[3] *Don't forget to click the Active checkbox to activate this rule.*

Source IP	It is 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 is the subnet mask for the source IP.
Source Port	It is the port for the source IP
Destination IP	It is 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 is the subnet mask for the destination IP.
Destination Port	It is the port for the destination IP.
Group Name	It is the filter group for the current rule.
Direction	The direction of packet flow **IN** is for incoming packets. **OUT is** for outgoing packets, and **Any** is for both directions.
Protocol	It is the protocol(s) for this filter rule.
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.
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**.

(Operator)

The operator column specifies the port number settings. 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***.

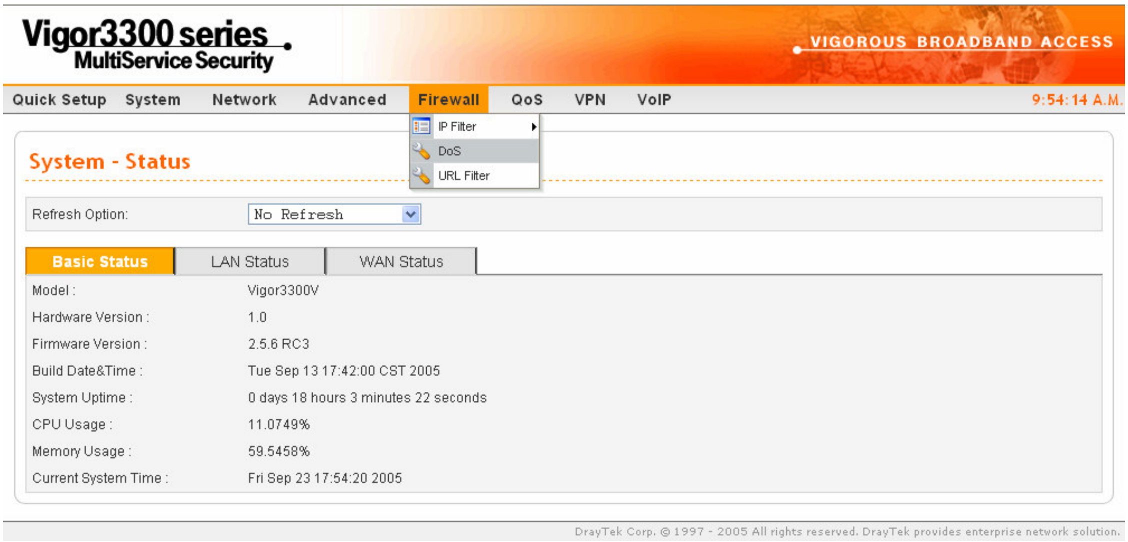
!=: If the ***End Port*** column is empty, the port number is not equal to the value of the ***Start Port*** column**.** Otherwise, this port number is not between the ***Start Port*** and the ***End Port*** including the ***Start Port*** and ***End Port***.

>: 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***.

7.4 Denial of Service Attacks Setup

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. Click the **DoS** option under the **Firewall** menu in Figure 7-8 and to set up the **DoS** function in Figure 7-9.

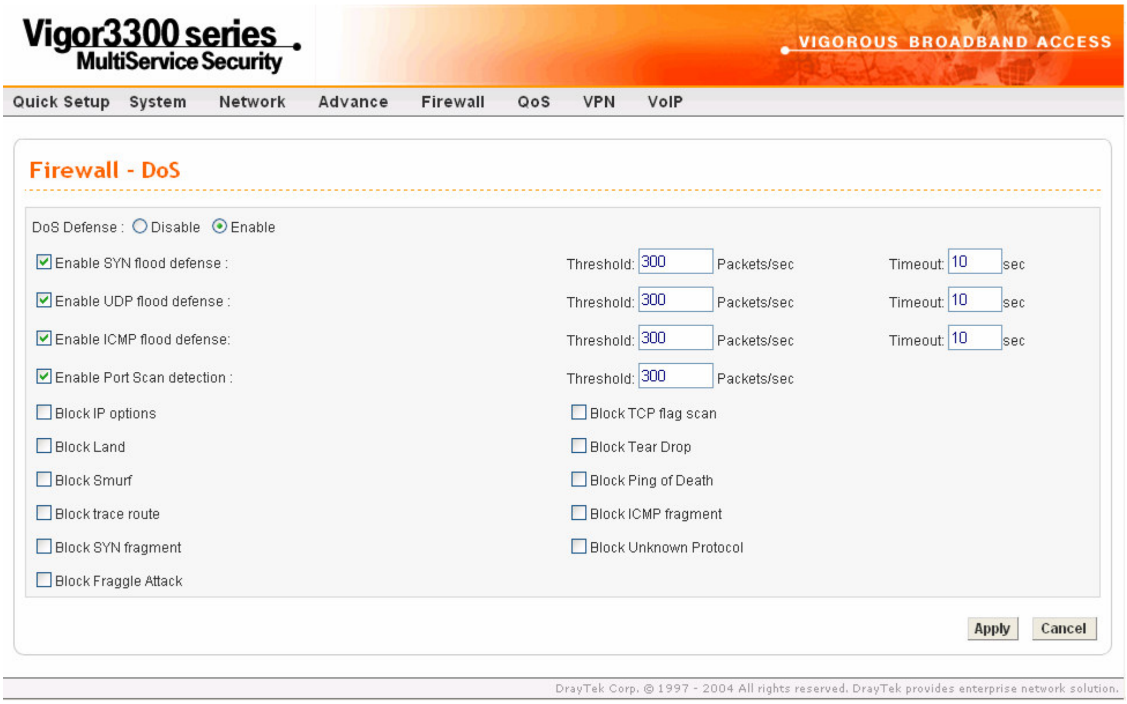


System - Status

Refresh Option: No Refresh

Model :	Vigor3300V
Hardware Version :	1.0
Firmware Version :	2.5.6 RC3
Build Date&Time :	Tue Sep 13 17:42:00 CST 2005
System Uptime :	0 days 18 hours 3 minutes 22 seconds
CPU Usage :	11.0749%
Memory Usage :	59.5458%
Current System Time :	Fri Sep 23 17:54:20 2005

Figure 7-8. The DoS option


Vigor3300 series
MultiService Security
VIGOROUS BROADBAND ACCESS
Quick Setup
System
Network
Advance
Firewall
QoS
VPN
VoIP
Apply
Cancel
DrayTek Corp. © 1997 - 2004 All rights reserved. DrayTek provides enterprise network solution.

Firewall - DoS

DoS Defense : ○ Disable ● Enable

☑ Enable SYN flood defense :	Threshold: 300 Packets/sec	Timeout: 10 sec
☑ Enable UDP flood defense :	Threshold: 300 Packets/sec	Timeout: 10 sec
☑ Enable ICMP flood defense:	Threshold: 300 Packets/sec	Timeout: 10 sec
☑ Enable Port Scan detection :	Threshold: 300 Packets/sec	
□ Block IP options	□ Block TCP flag scan	
□ Block Land	□ Block Tear Drop	
□ Block Smurf	□ Block Ping of Death	
□ Block trace route	□ Block ICMP fragment	
□ Block SYN fragment	□ Block Unknown Protocol	
□ Block Fraggle Attack		

Figure 7-9. DoS configuration

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 corresponding defense function is executed to mitigate the attack.

The following section will explains the DoS Defense Setup in more detail. It is a sub-functionality of the IP filter. There are 15 kinds of defense functions for the DoS Defense Setup. A brief description for each function is shown below.

DoS Defense	**Enables** or **Disables** the DoS Defense function. 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.

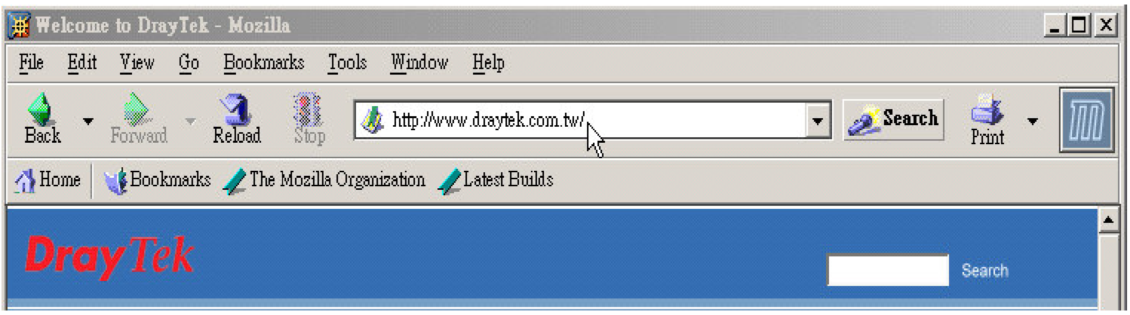
7.5 URL Filter Setup

7.5.1 Introduction

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.

7.5.2 An Overview of URL Content Filtering



Welcome to DrayTek - Mozilla
File Edit View Go Bookmarks Tools Window Help
Back
Forward
Reload
Stop
http://www.draytek.com.tw/
Search
Print
Home
Bookmarks
The Mozilla Organization
Latest Builds
DrayTek
Search

Figure 7-10. URL filtering example

The URL content filter in the series of broadband security routers inspects every URL string in the HTTP request initiated inside against the keyword list. If the entire or part of the URL string (for instance, http://www.draytek.com, as shown as Figure 7-11) matches any activated keyword, 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.

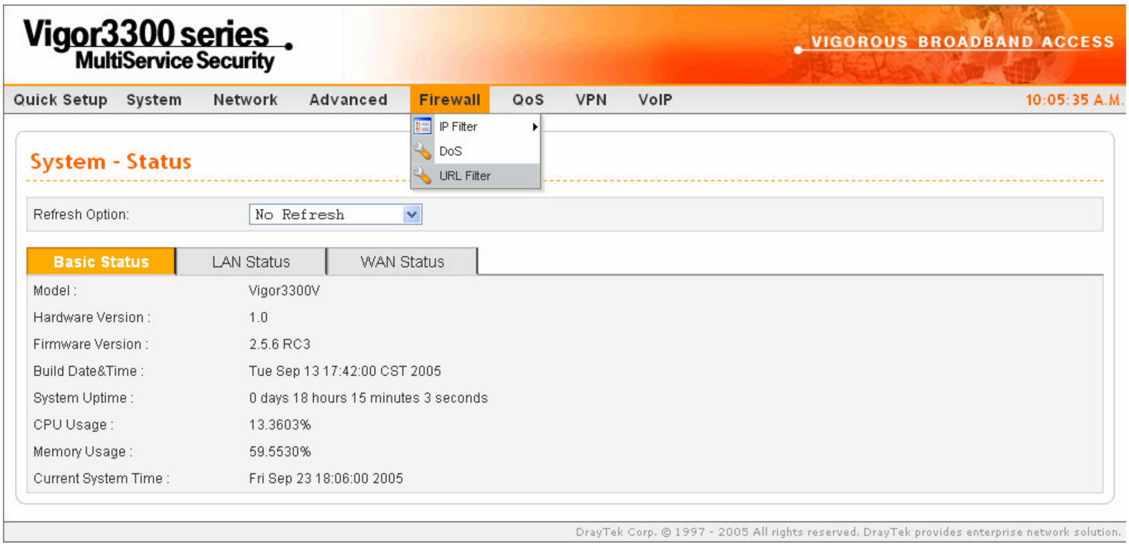
7.5.3 URL Content Filter Configuration

The following sections describe the Web configuration for setting up the URL content filter, including specific configuration information and limitations.

The URL content filter consists of the following functions: **URL Access Control**, **Block Web access by IP address**, **Restrict Web Feature**, **Excepting Subnets**, and **Filter Schedule**. The **URL Access Control** controls Web site access by inspecting the URL string against user-defined keywords. The **Restrict Web Feature** control blocks malicious codes hidden in Web pages, such as Java Applet, Active X, Cookies, Proxy, compressed files, and executable files. It is also able to block all downloads of multimedia files from Web pages in order to control the bandwidth usage.

The **Block Web access by IP address** function is used to avoid inappropriate Web sites that can be accessed directly using the IP address in the URL locator. The **Excepting Subnets** function allows the administrator to specify a group of hosts that are free from the URL Access Control. This group of hosts can be defined as a set of IP addresses or subnets. Finally, the **Filter Schedule** function controls what times the URL content filter should be active.

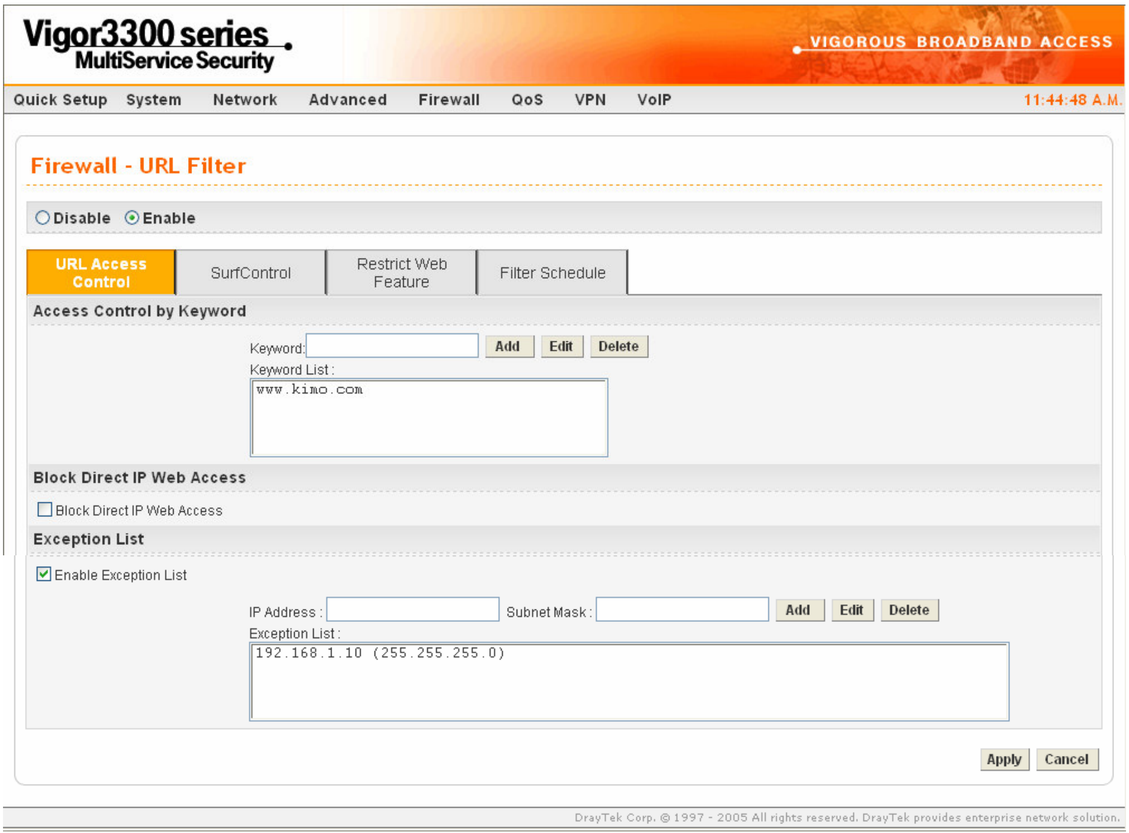
Click the **URL Filter** option in the **Firewall** menu in Figure 7-11 and to configure the **URL Filter** in Figure 7-12.



Refresh Option: No Refresh

Model :	Vigor3300V
Hardware Version :	1.0
Firmware Version :	2.5.6 RC3
Build Date&Time :	Tue Sep 13 17:42:00 CST 2005
System Uptime :	0 days 18 hours 15 minutes 3 seconds
CPU Usage :	13.3603%
Memory Usage :	59.5530%
Current System Time :	Fri Sep 23 18:06:00 2005

Figure 7-11. The URL filter option



Firewall - URL Filter

○ Disable ● Enable

Access Control by Keyword

Keyword:

Keyword List :

```
www.kimo.com
```

Block Direct IP Web Access

□ Block Direct IP Web Access

Exception List

☑ Enable Exception List

IP Address : Subnet Mask :

Exception List :

```
192.168.1.10 (255.255.255.0)
```

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

Figure 7-12. URL filter on URL access control

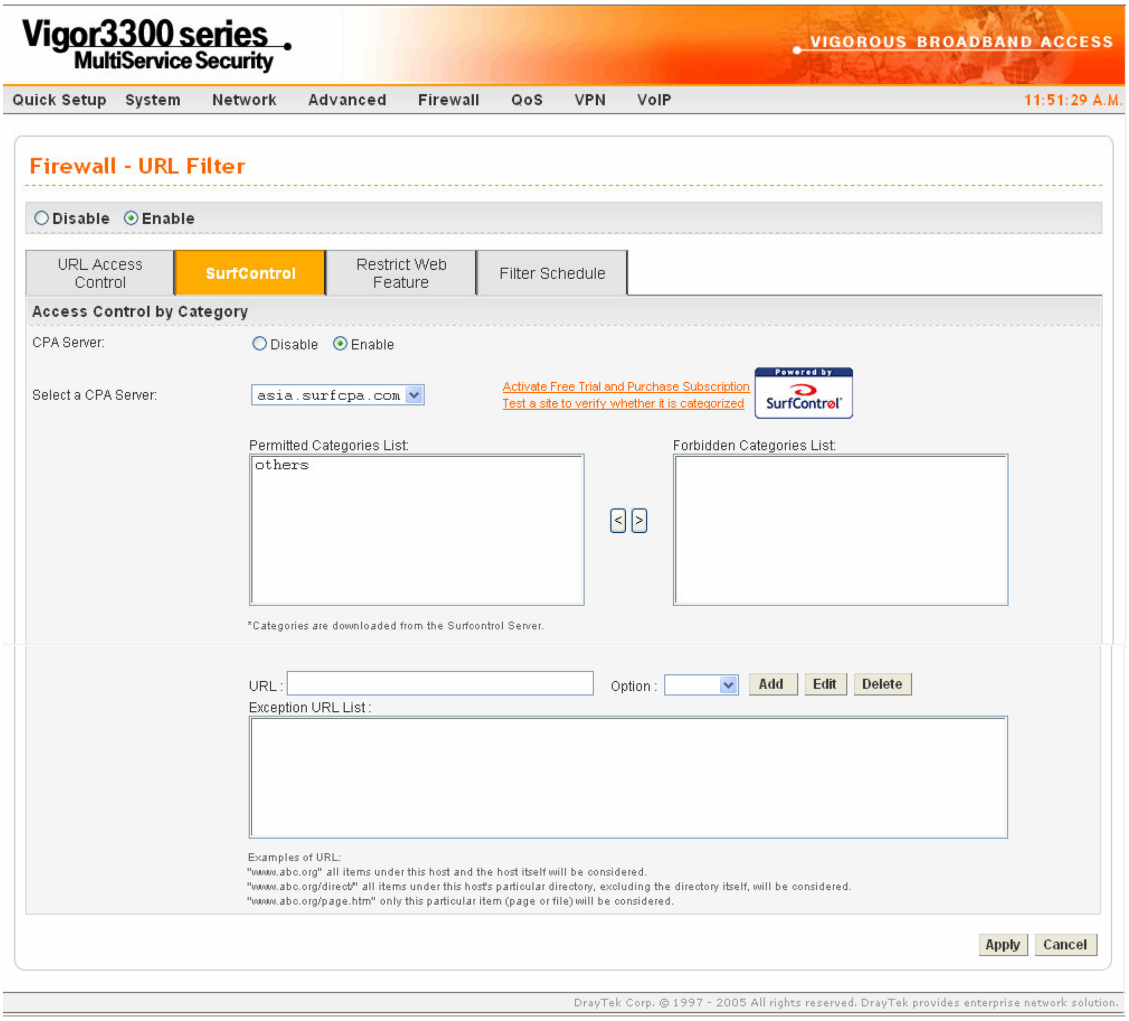
Enable/Disable	"**Disable**" or "**Enable**" URL Filter function.

7.5.3.1 URL Access Control Setup

Access Control by Keyword	
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	
Block Direct IP Web Access	Deny any Web surfing activity that directly uses an IP address.
Exception List	
Enable Excepting 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.

7.5.3.2 SurfControl Setup

Click the **SurfControl** page as Figure 7-13 to set up this function.



Firewall - URL Filter

○ Disable ● Enable

Access Control by Category

CPA Server: ○ Disable ● Enable

Select a CPA Server: asia.surfcpa.com

Activate Free Trial and Purchase Subscription

Test a site to verify whether it is categorized

Permitted Categories List: others

Forbidden Categories List:

*Categories are downloaded from the Surfcontrol Server.

URL :

Option :

Exception URL List :

Examples of URL:
"www.abc.org" all items under this host and the host itself will be considered.
"www.abc.org/direct/" all items under this host's particular directory, excluding the directory itself, will be considered.
"www.abc.org/page.htm" only this particular item (page or file) will be considered.

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

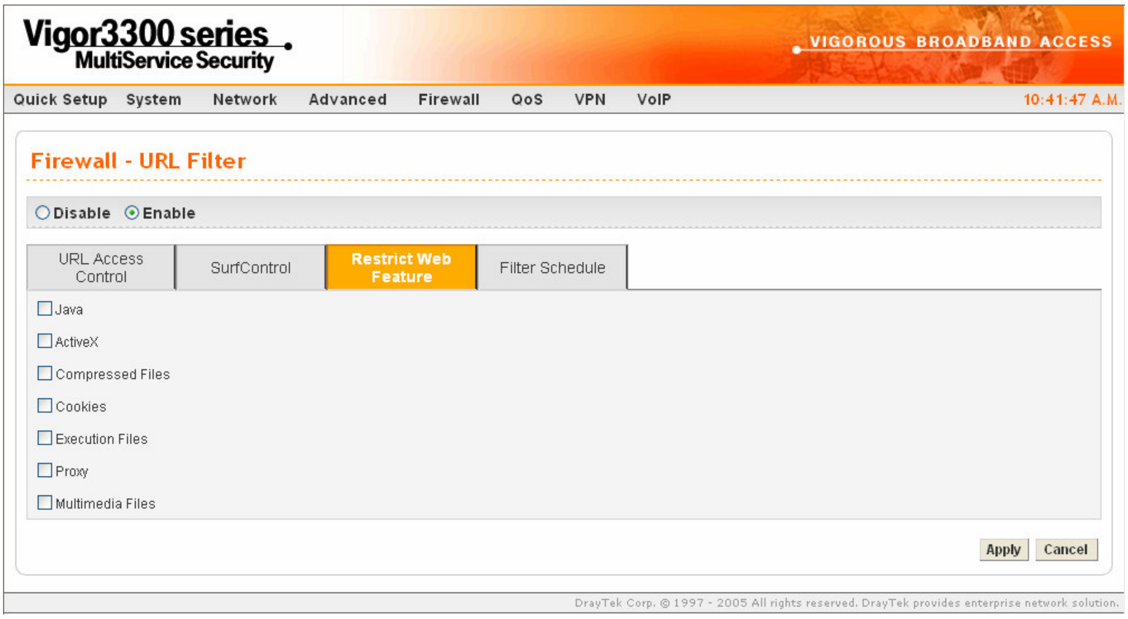
Figure 7-13. URL filter on SurfControl

Access Control by Category	
CPA Server	**Enable** or **Disable** URL Access Control.
Select a CPA Server	The domain name is used to as a CPA server. The name should be filled when enable CPA Server, otherwise it will impact performance.
Permitted Categories List	The permitted categories are from the selected CPA server.
Forbidden Categories List	The forbidden categories are from the selected CPA server.
Category Exception List	
URL	The URL domain name.
Option ***Exception URL List***	**Allow** or **Deny** the selected URL. The list of filtered URLs.

Example - If you want to filter any website whose URL string contains "sex", "gun", or "drug", you should add these words into the keyword frames. Thus, the system will automatically deny any Web surfing with the URL string containing any one of the keywords listed. If the user tries to access www.backdoor.net/images/sex /p_386.html, the router will deny the connection because this website is prohibited. However, the user is still able to access the website www.backdoor.net/firewall/forum/d_123.html. Further, the URL content filtering facility also allows you to specify either a complete URL string (e.g., "www.whitehouse.com" and "www.hotmail.com") or a partial URL string (e.g., "yahoo.com") in the blocking keyword list. Accordingly, the router will identify the forbidden URL and deny the associated connections.

7.5.3.3 Restrict Web Feature Setup

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. Click the **Restrict Web Feature** tab (Figure 7-14) to set up this function.



Firewall - URL Filter

○ Disable ● Enable

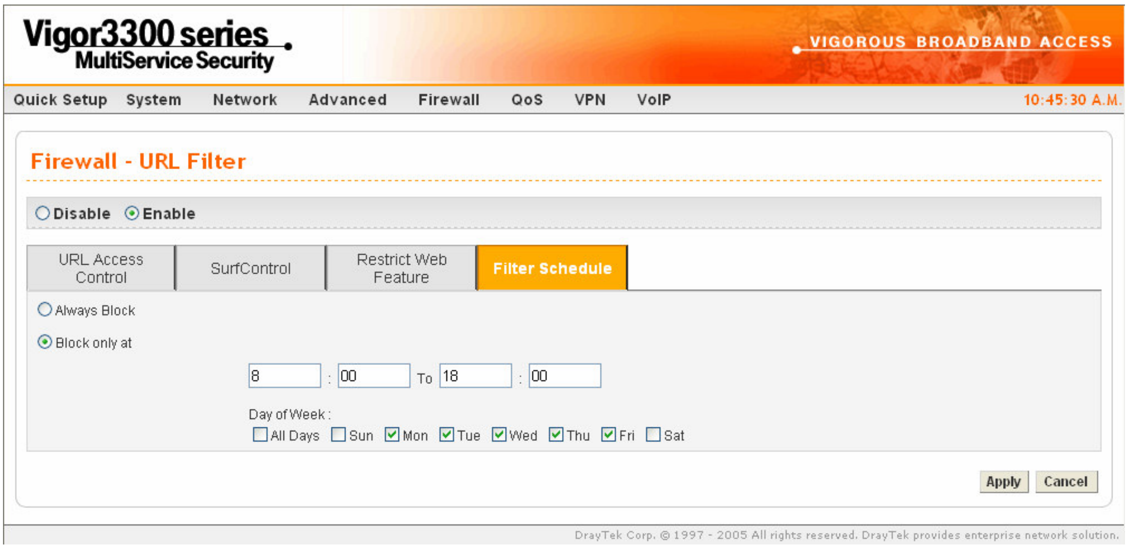
□ Java
□ ActiveX
□ Compressed Files
□ Cookies
□ Execution Files
□ Proxy
□ Multimedia Files

Figure 7-14. URL filter for restrict web feature

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 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 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.

7.5.3.4 Filter Schedule Setup

The Filter Schedule specifies what times the URL content filtering facility should be active in Figure 7-15.



Firewall - URL Filter

○ Disable ● Enable

○ Always Block

● Block only at

8 : 00 To 18 : 00

Day of Week :

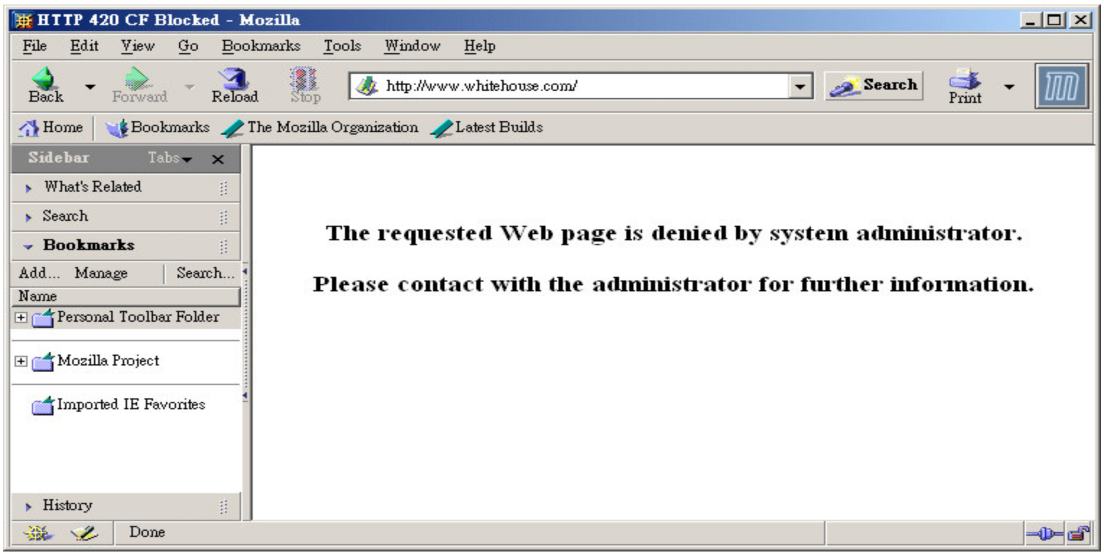
□ All Days □ Sun ☑ Mon ☑ Tue ☑ Wed ☑ Thu ☑ Fri □ Sat

Figure 7-15. URL filter for filter schedule

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.

7.5.4 Warning Message

When an HTTP request is denied, an alert page will appear in your browser, as shown in Figure 7-16.



The requested Web page is denied by system administrator.

Please contact with the administrator for further information.

Figure 7-16. Warning message

CHAPTER 8

VPN (Virtual Private Network) and Remote Access Setup

This chapter shows how to setup the configuration of VPN and Remote Access to let users create a virtual private network for security in the Internet.

This chapter is divided into the following sections.

- Section 8.1: Introduction
- Section 8.2: IPSec Group Setup
- Section 8.3: PPTP Group Setup

8.1 Introduction

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.

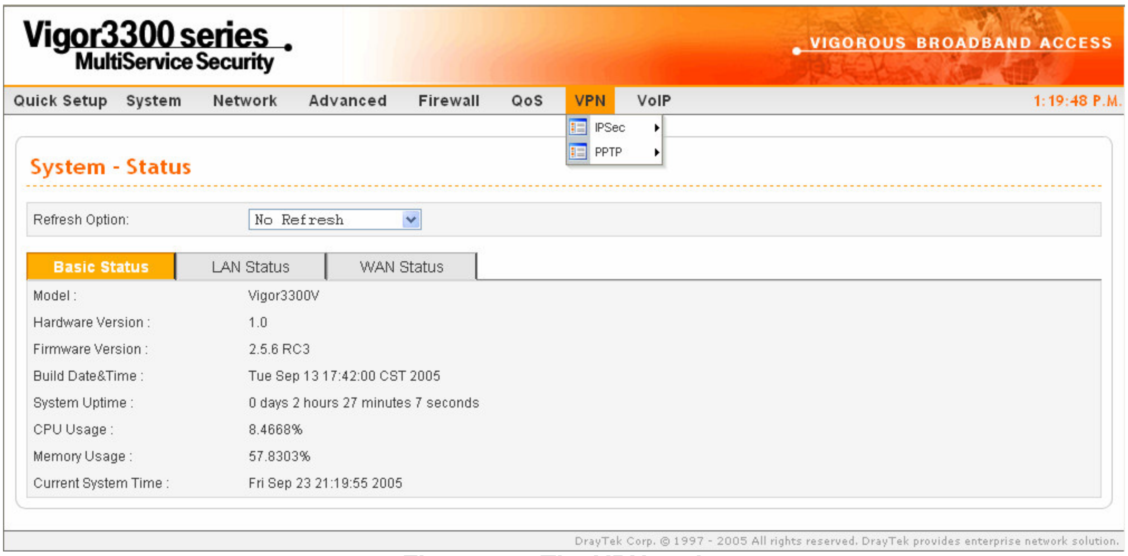
There are two types of VPN connections: remote dial-in access and LAN-to-LAN connection. The “Remote dial-In Access” facility allows a remote access node, a NAT router or a single computer to dial into a VPN router through the Internet to access the network resources of the remote network. The “LAN-to-LAN 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 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.

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.

Click the VPN option to configure the VPN Setup in Figure 8-1.



System - Status

Refresh Option: No Refresh

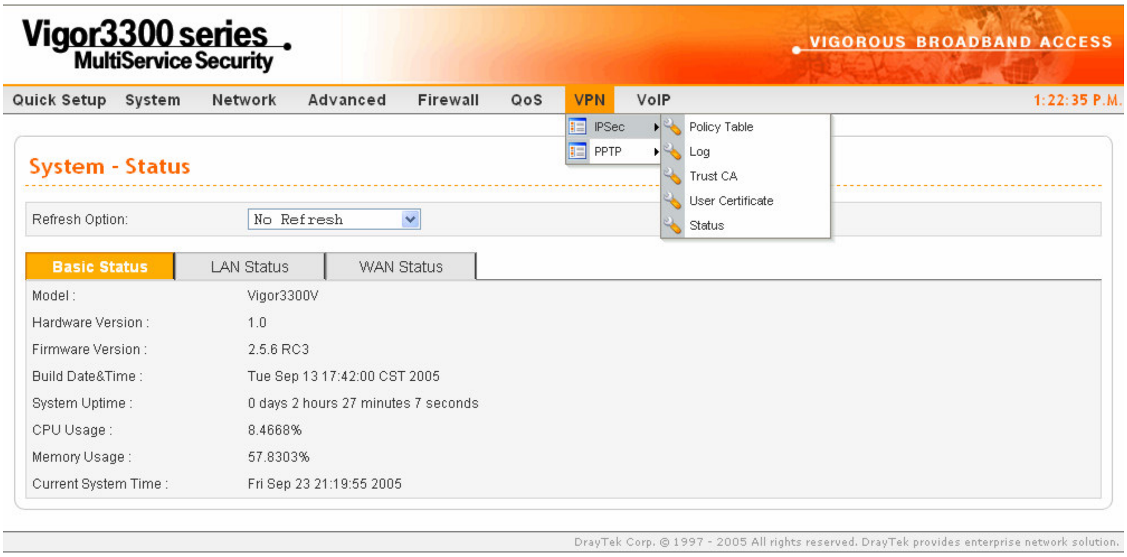
Model :	Vigor3300V
Hardware Version :	1.0
Firmware Version :	2.5.6 RC3
Build Date&Time :	Tue Sep 13 17:42:00 CST 2005
System Uptime :	0 days 2 hours 27 minutes 7 seconds
CPU Usage :	8.4668%
Memory Usage :	57.8303%
Current System Time :	Fri Sep 23 21:19:55 2005

Figure 8-1. The VPN option

8.2 IPSec Group Setup

8.2.1 Policy Table Setup

To create a VPN IPSec policy, click the **Policy Table** option under the **IPSec** menu in Figure 8-2 and bring up the Policy Table Setup in Figure 8-3.

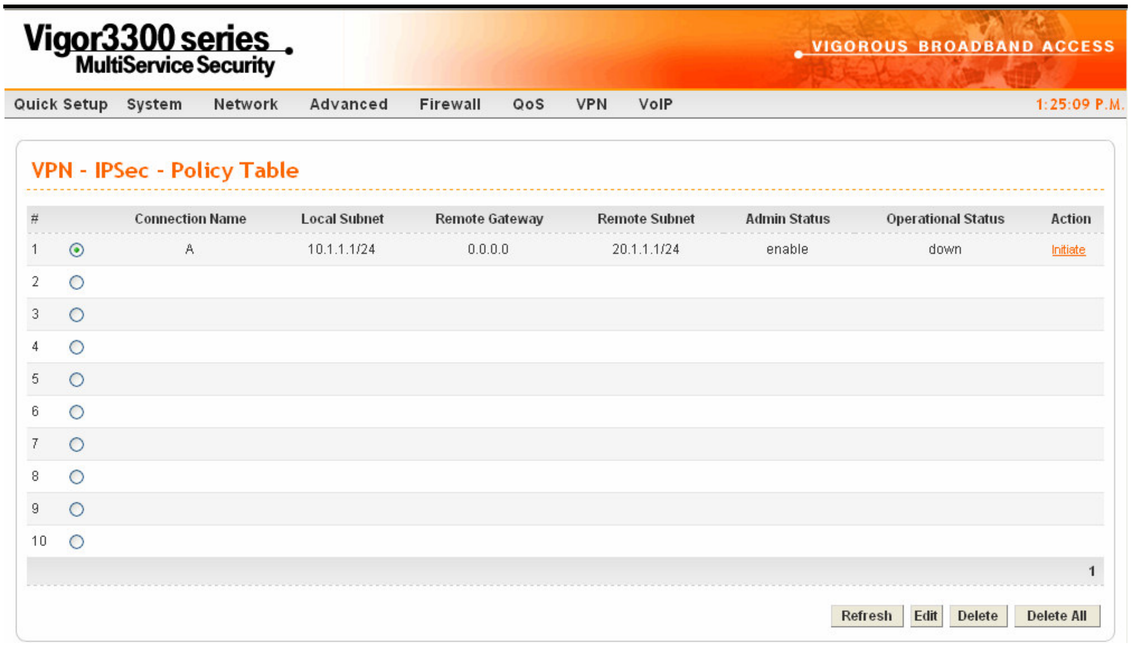


System - Status

Refresh Option: No Refresh

Model : Vigor3300V
Hardware Version : 1.0
Firmware Version : 2.5.6 RC3
Build Date&Time : Tue Sep 13 17:42:00 CST 2005
System Uptime : 0 days 2 hours 27 minutes 7 seconds
CPU Usage : 8.4668%
Memory Usage : 57.8303%
Current System Time : Fri Sep 23 21:19:55 2005

Figure 8-2. The VPN policy table option



VPN - IPSec - Policy Table

#		Connection Name	Local Subnet	Remote Gateway	Remote Subnet	Admin Status	Operational Status	Action
1	●	A	10.1.1.1/24	0.0.0.0	20.1.1.1/24	enable	down	Initiate
2	○							
3	○							
4	○							
5	○							
6	○							
7	○							
8	○							
9	○							
10	○							

1

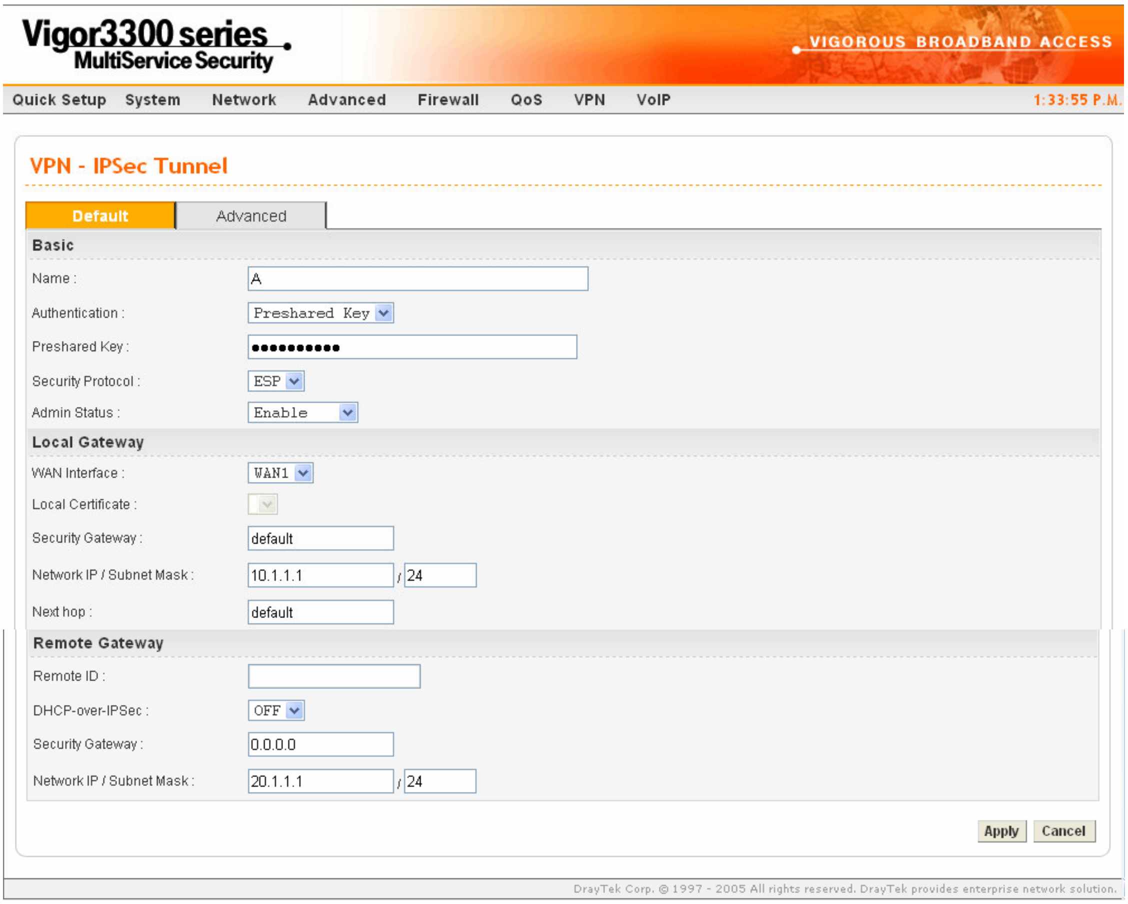
Figure 8-3. VPN policy table setup

There are four options:

Refresh	Refresh the page information.
Edit	Configure an entry.
Delete	Delete a designated entry.
Delete All	Delete all entries in the table.

8.2.2.1 Default Setup

Select an entry and click **Edit** to create a new IPSec Tunnel in Figure 8-4.



Vigor3300 series
MultiService Security
VIGOROUS BROADBAND ACCESS
Quick Setup System Network Advanced Firewall QoS VPN VoIP
1:33:55 P.M.
Default
Advanced
Apply
Cancel
DrayTek Corp. © 1997 - 2005 All rights reserved. DrayTek provides enterprise network solution.

VPN - IPSec Tunnel

Basic

Name : A

Authentication : Preshared Key

Preshared Key : ●●●●●●●●●●●

Security Protocol : ESP

Admin Status : Enable

Local Gateway

WAN Interface : WAN1

Local Certificate :

Security Gateway : default

Network IP / Subnet Mask : 10.1.1.1 / 24

Next hop : default

Remote Gateway

Remote ID :

DHCP-over-IPSec : OFF

Security Gateway : 0.0.0.0

Network IP / Subnet Mask : 20.1.1.1 / 24

Figure 8-4. IPSec tunnel configuration

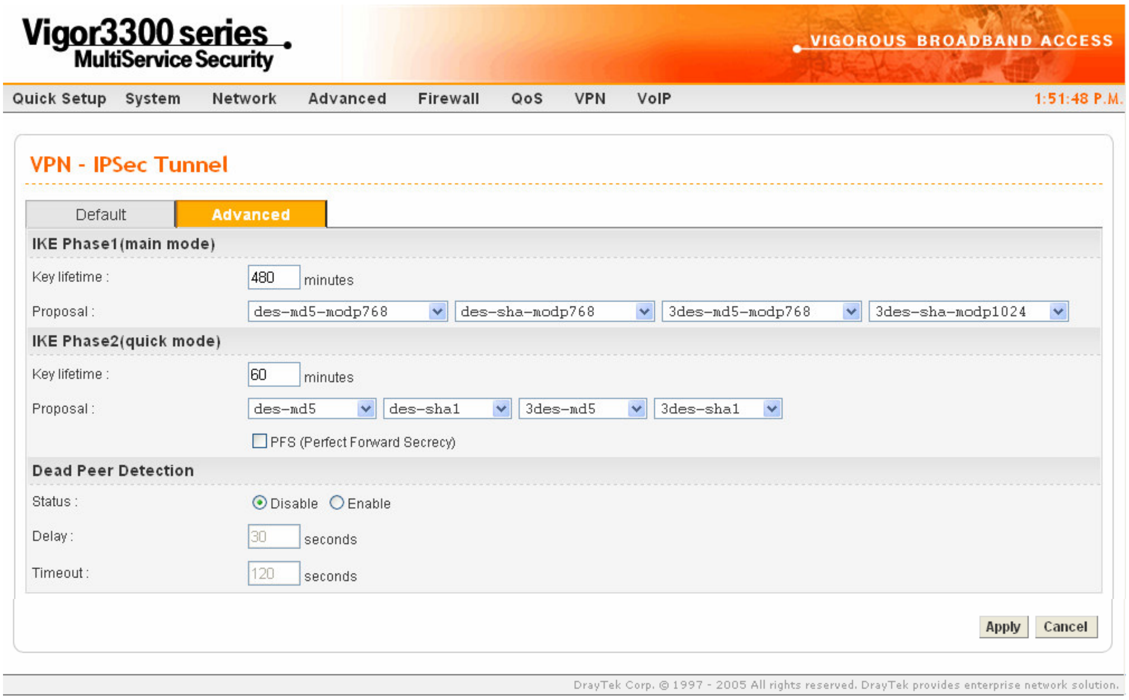
Basic	
Name	The name for VPN connection (ex. "VPN1"). The maximum length of name is 20 characters including spaces.
Authentication	The authentication to be used by PreShared Key or RSA Signature.

PreShared Key	The shared key for peer identification. The maximum length is 40 characters, including spaces.
Security Protocol	AH: Specify the IPSec protocol for the Authentication Header protocol. The data will be authenticated, but not be encrypted. ESP: Specify the IPSec protocol for the Encapsulating Security Payload protocol. The data will be encrypted and authenticated.
Admin Status	The administrative status. **Enable** the policy to wait for a peer to initiate the IKE negotiation. **Disable** the policy to deactivate the VPN connection. The **Always-on** is recommended and automatically activates a VPN connection indefinitely.
Local Gateway	
WAN Interface	The WAN interface to be used.
Local Certificate	The local certificate to be used for authentication if the "RSA Signature" option is selected in the "Authentication" field. These options are from the user certificate file.
Security Gateway	The IP address of the local gateway's public-network interface. The keyword "default" can be used to represent the IP Address of the selected "WAN Interface".
Network IP / Subnet Mask	The subnet behind the local gateway.
Next Hop	The IP address of the next hop. The keyword "default" can be used to represent the gateway IP address of the selected "WAN Interface".
Remote Gateway	
Remote ID	The identification number for the remote gateway.
DHCP-over-IPSEC	Turns this function **ON** or **OFF**.

Security Gateway	The IP address of the remote client/gateway. This field is mandatory. The setting for 0.0.0.0 is used for the road-warrior with a dynamic IP address.
Network IP / Subnet Mask	The subnet behind the remote gateway. If the remote gateway IP address is 0.0.0.0, this field can be omitted, but you can specify it as 0.0.0.0/32 for clarity.

8.2.2.2 Advance Setup

Click the **Advanced** tab to see the Advanced Setup page in Figure 8-5.



VPN - IPSec Tunnel

IKE Phase1(main mode)

Key lifetime : 480 minutes

Proposal : des-md5-modp768 | des-sha-modp768 | 3des-md5-modp768 | 3des-sha-modp1024

IKE Phase2(quick mode)

Key lifetime : 60 minutes

Proposal : des-md5 | des-sha1 | 3des-md5 | 3des-sha1

□ PFS (Perfect Forward Secrecy)

Dead Peer Detection

Status : ● Disable ○ Enable

Delay : 30 seconds

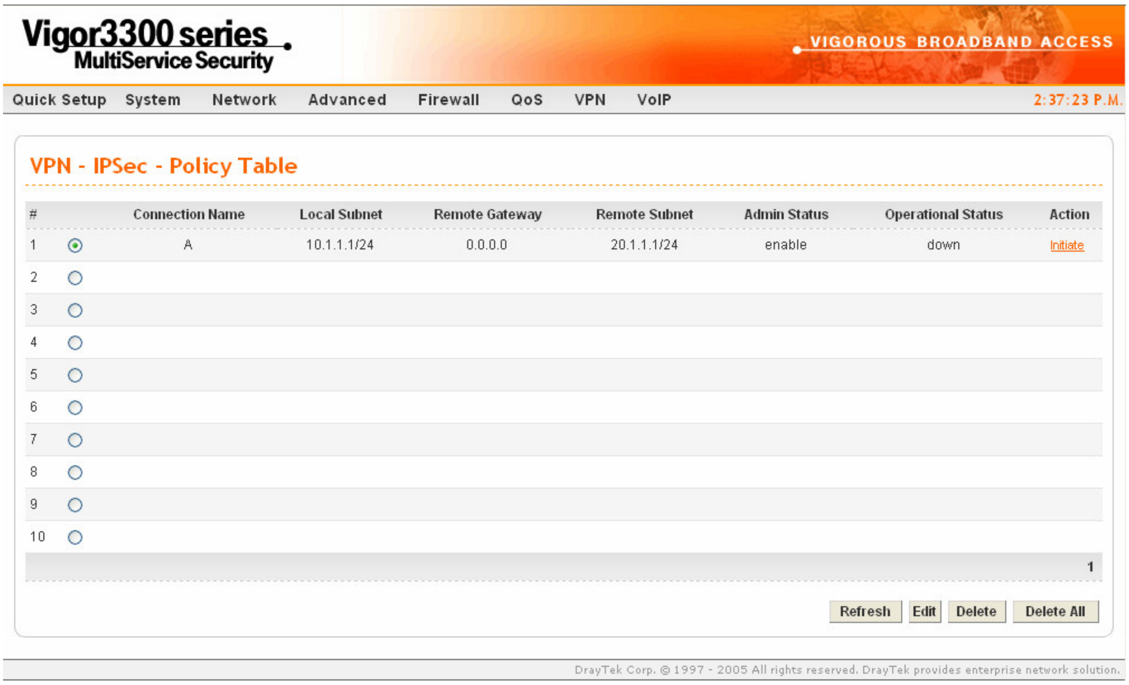
Timeout : 120 seconds

Figure 8-5. VPN advanced configuration

IKE Phase1 Group (Main Mode)	
Key Lifetime	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	The proposed encryption and/or authentication algorithms for IKE Phase1 negotiation. There are 3 options: ***Encryption algorithms* -** DES/3DES/AES ***Authentication algorithms* -** MD5/SHA1 ***DH Group* -** MODP768/MODP1024/MODP1536.
IKE Phase 2(Quick Mode)	
Key Lifetime	The rekey-renegotiated period of the IKE Phase2 keying channel. The acceptable range is from 5 to 1440 minutes (24 hours).
Proposal	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
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.
Dead Peer Detection	
Status	**Enables** or **Disables** the 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.

Click **Apply** to apply the IPSec policy setting and add a new record into the policy table in Figure 8-6.


Vigor3300 series
MultiService Security
VIGOROUS BROADBAND ACCESS
Quick Setup System Network Advanced Firewall QoS VPN VoIP
2:37:23 P.M.

VPN - IPSec - Policy Table

#		Connection Name	Local Subnet	Remote Gateway	Remote Subnet	Admin Status	Operational Status	Action
1	●	A	10.1.1.1/24	0.0.0.0	20.1.1.1/24	enable	down	Initiate
2	○							
3	○							
4	○							
5	○							
6	○							
7	○							
8	○							
9	○							
10	○							

1
Refresh Edit Delete Delete All
DrayTek Corp. © 1997 - 2005 All rights reserved. DrayTek provides enterprise network solution.

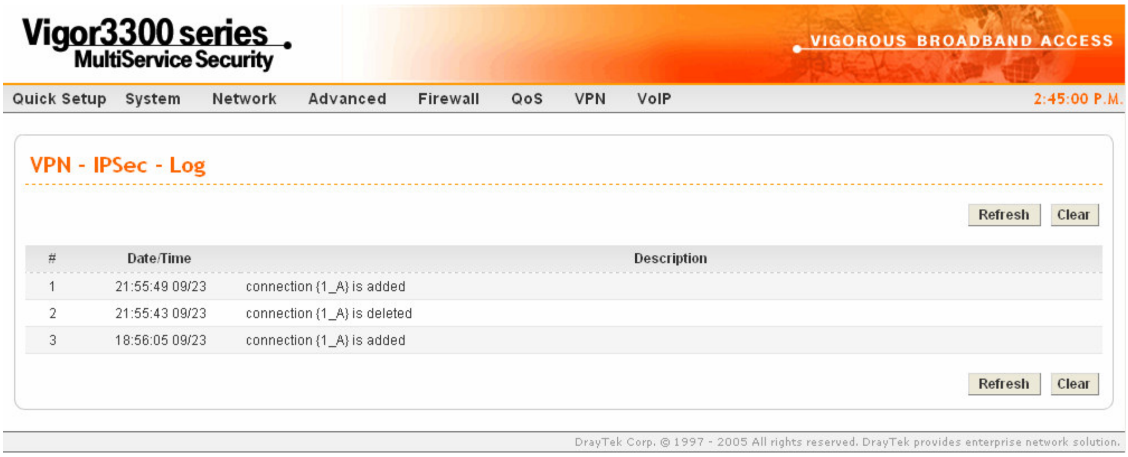
Figure 8-6. VPN policy table list

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.

8.2.2 Log

At any time, you can click **VPN > Log** to monitor the VPN tunnel status (Figure 8-7). The log is helpful for solving some setting problems. The system will keep the 100 most recent messages. Click **Clear** to clear the log.

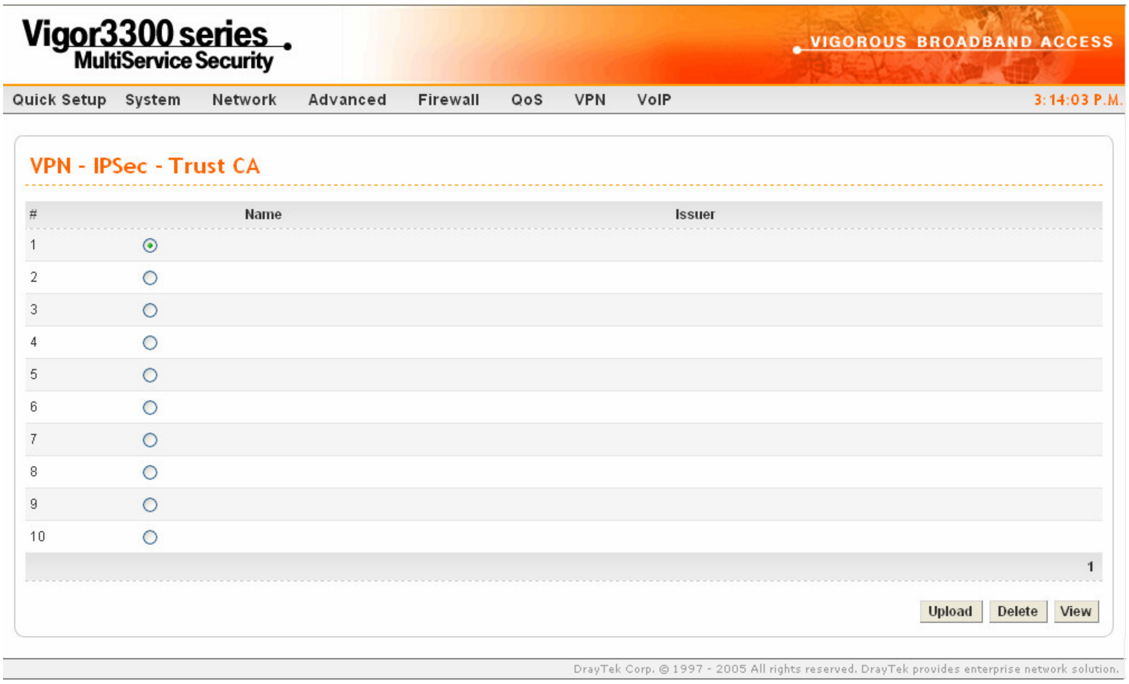


#	Date/Time	Description
1	21:55:49 09/23	connection {1_A} is added
2	21:55:43 09/23	connection {1_A} is deleted
3	18:56:05 09/23	connection {1_A} is added

Figure 8-7. VPN log information

8.2.3 Trust CA Setup

Click the **VPN->IPSec->Trust CA** option to set up the CA configuration in Figure 8-8.

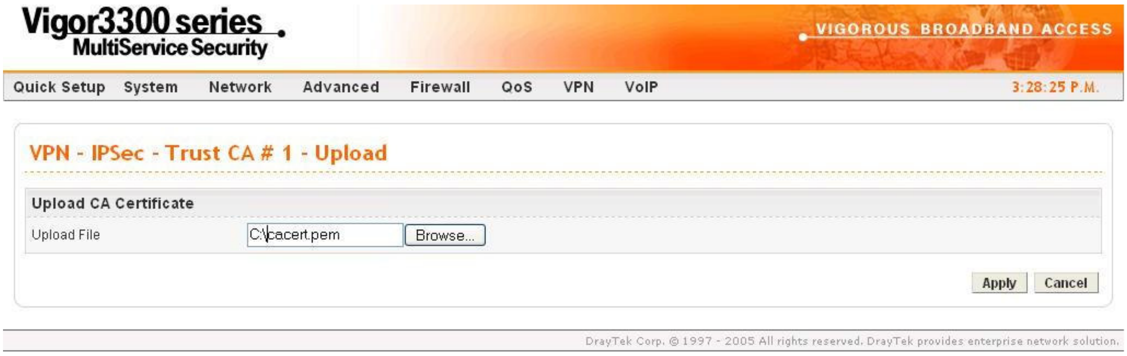

Vigor3300 series
MultiService Security
VIGOROUS BROADBAND ACCESS
Quick Setup
System
Network
Advanced
Firewall
QoS
VPN
VoIP
3:14:03 P.M.
1
Upload
Delete
View
DrayTek Corp. © 1997 - 2005 All rights reserved. DrayTek provides enterprise network solution.

VPN - IPSec - Trust CA

#		Name	Issuer
1	●		
2	○		
3	○		
4	○		
5	○		
6	○		
7	○		
8	○		
9	○		
10	○		

Figure 8-8. VPN IPSec trust CA configuration

Select an entry, and then click the **Upload** option (Figure 8-9).


Vigor3300 series
MultiService Security
VIGOROUS BROADBAND ACCESS
Quick Setup
System
Network
Advanced
Firewall
QoS
VPN
VoIP
3:28:25 P.M.
Browse...
Apply
Cancel
DrayTek Corp. © 1997 - 2005 All rights reserved. DrayTek provides enterprise network solution.

VPN - IPSec - Trust CA # 1 - Upload

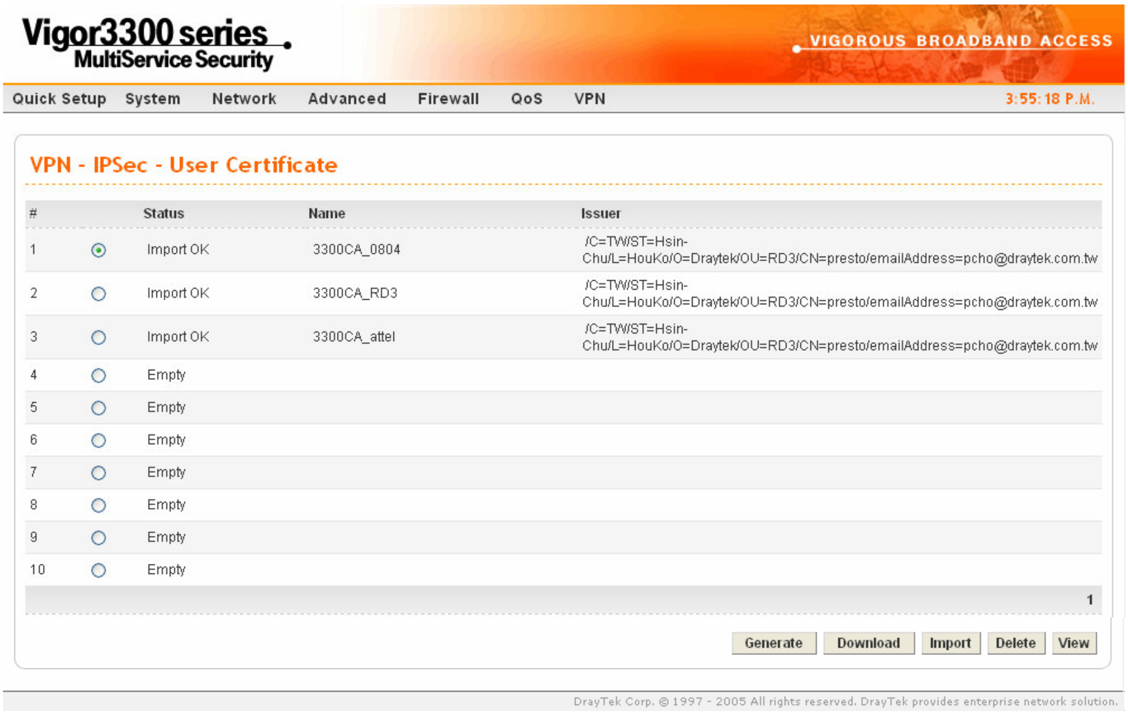
Upload CA Certificate

Upload File: C:\cacert.pem

Figure 8-9. Upload VPN IPSec trust CA

8.2.4 User Certificate

Click the User Certificate option to see the User Certificate page in Figure 8-10.



VPN - IPSec - User Certificate

#		Status	Name	Issuer
1	●	Import OK	3300CA_0804	/C=TW/ST=Hsin-Chu/L=HouKo/O=Draytek/OU=RD3/CN=presto/emailAddress=pcho@draytek.com.tw
2	○	Import OK	3300CA_RD3	/C=TW/ST=Hsin-Chu/L=HouKo/O=Draytek/OU=RD3/CN=presto/emailAddress=pcho@draytek.com.tw
3	○	Import OK	3300CA_attel	/C=TW/ST=Hsin-Chu/L=HouKo/O=Draytek/OU=RD3/CN=presto/emailAddress=pcho@draytek.com.tw
4	○	Empty		
5	○	Empty		
6	○	Empty		
7	○	Empty		
8	○	Empty		
9	○	Empty		
10	○	Empty		

1

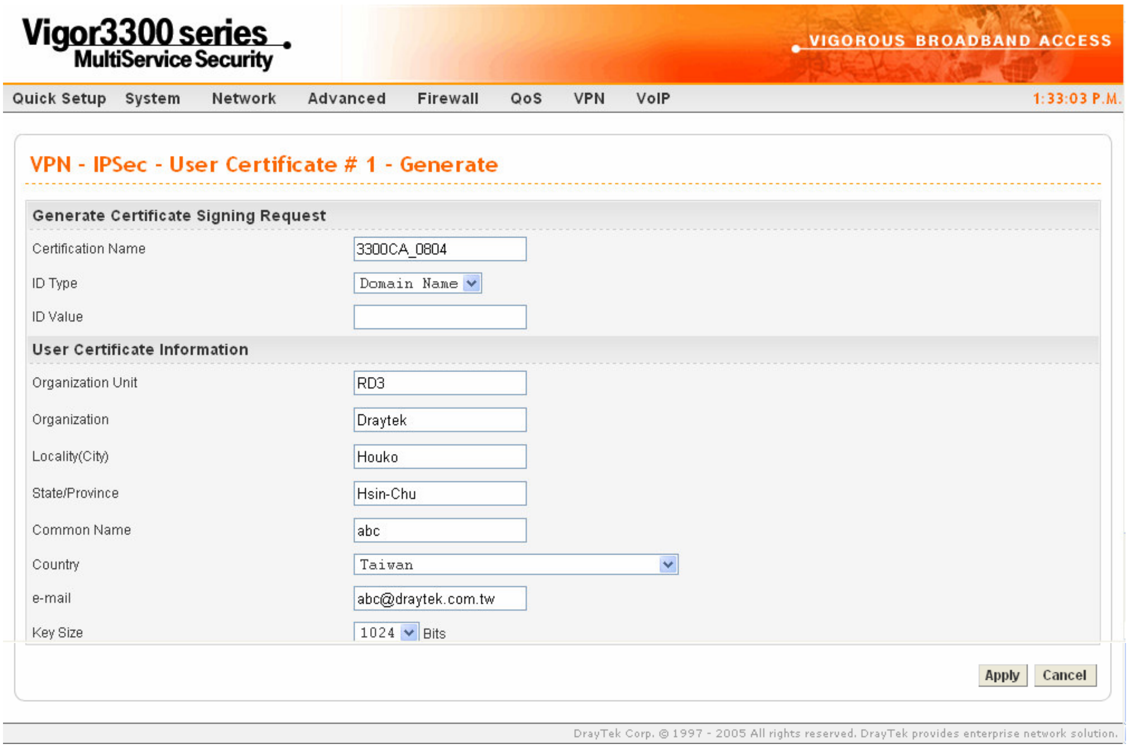
Figure 8-10. VPN IPSec user certificate

There are five options:

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 server.
Delete	Delete an assigned entry.
View	Show configuration of the assigned entry.

8.2.4.1 Generate Setup

Click **Generate** to bring up the following web page in Figure 8-11.


Vigor3300 series
MultiService Security
VIGOROUS BROADBAND ACCESS
Quick Setup
System
Network
Advanced
Firewall
QoS
VPN
VoIP
1:33:03 P.M.
Apply
Cancel
DrayTek Corp. © 1997 - 2005 All rights reserved. DrayTek provides enterprise network solution.

VPN - IPSec - User Certificate # 1 - Generate

Generate Certificate Signing Request

Certification Name	3300CA_0804
ID Type	Domain Name
ID Value	

User Certificate Information

Organization Unit	RD3
Organization	Draytek
Locality(City)	Houko
State/Province	Hsin-Chu
Common Name	abc
Country	Taiwan
e-mail	abc@draytek.com.tw
Key Size	1024 Bits

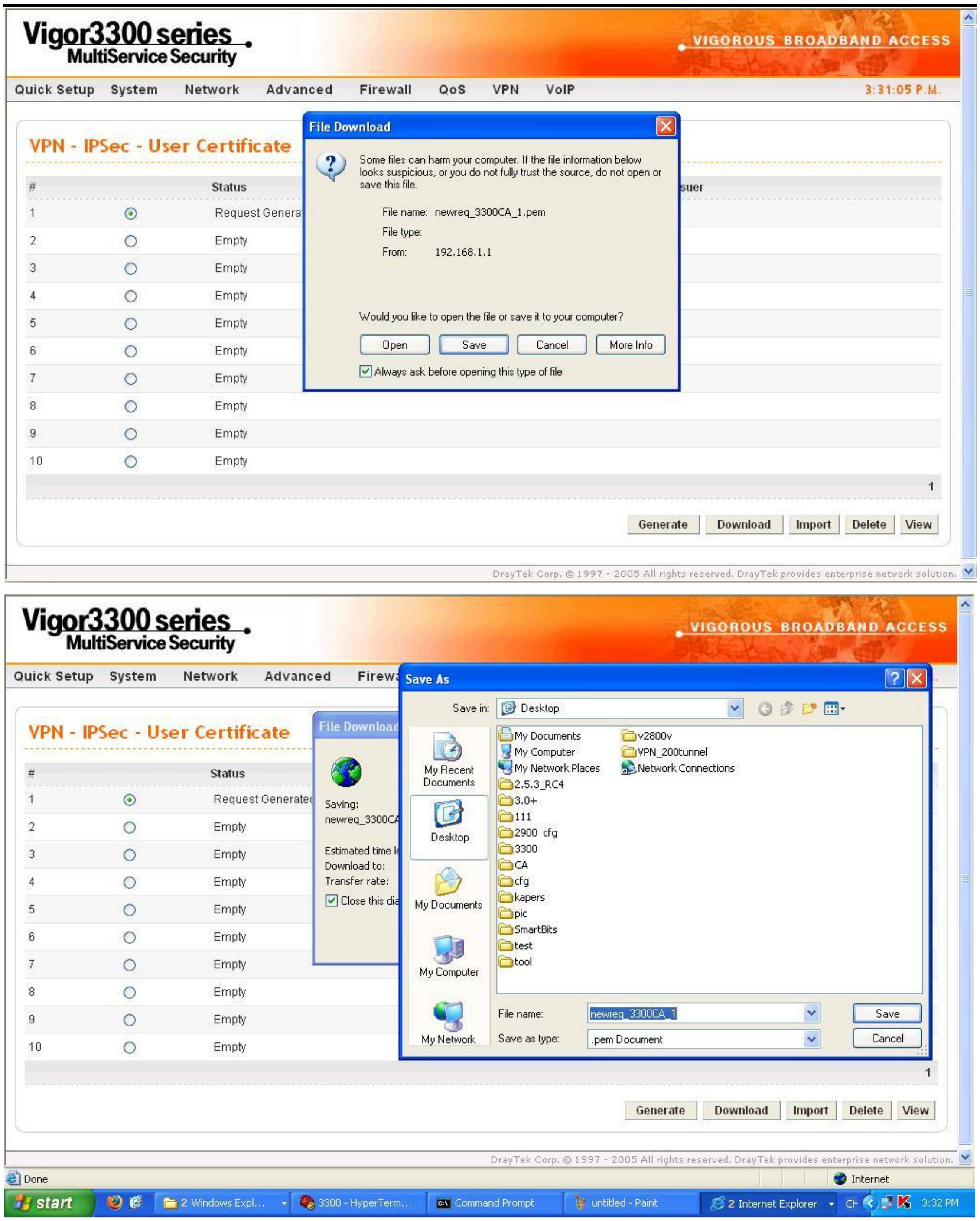
Figure 8-11. Generate VPN IPSec user certificate

Generate Certificate Signing Request	
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.

User Certification Information	
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 ● **2048** Bits

8.2.4.2 Download Setup

This function exports a certification file generated in the router to a local host. This file must be removed to a certification server for certification (Figure 8-12).



Vigor3300 series
MultiService Security
VIGOROUS BROADBAND ACCESS
Quick Setup System Network Advanced Firewall QoS VPN VoIP
3:31:05 P.M.

VPN - IPSec - User Certificate

#		Status
1	●	Request Genera
2	○	Empty
3	○	Empty
4	○	Empty
5	○	Empty
6	○	Empty
7	○	Empty
8	○	Empty
9	○	Empty
10	○	Empty

File Download

Some files can harm your computer. If the file information below looks suspicious, or you do not fully trust the source, do not open or save this file.

File name: newreq_3300CA_1.pem
File type:
From: 192.168.1.1

Would you like to open the file or save it to your computer?

☑ Always ask before opening this type of file

Generate Download Import Delete View
DrayTek Corp. © 1997 - 2005 All rights reserved. DrayTek provides enterprise network solution.

Vigor3300 series
MultiService Security
VIGOROUS BROADBAND ACCESS
Quick Setup System Network Advanced Firewa

VPN - IPSec - User Certificate

#		Status
1	●	Request Generated
2	○	Empty
3	○	Empty
4	○	Empty
5	○	Empty
6	○	Empty
7	○	Empty
8	○	Empty
9	○	Empty
10	○	Empty

File Download

Saving:
newreq_3300CA
Estimated time le
Download to:
Transfer rate:
☑ Close this dia

Save As

Save in: Desktop

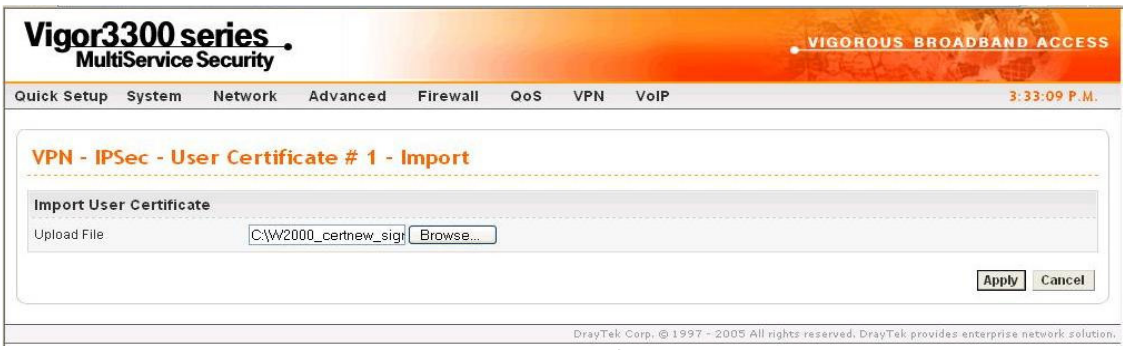
File name: newreq_3300CA_1
Save as type: .pem Document

Save
Cancel
Generate Download Import Delete View
DrayTek Corp. © 1997 - 2005 All rights reserved. DrayTek provides enterprise network solution.
Done
Internet
start
2 Windows Expl...
3300 - HyperTerm...
Command Prompt
untitled - Paint
2 Internet Explorer
3:32 PM

Figure 8-12. Download VPN IPSec user certificate

8.2.4.3 Import Setup

Click **Import** to bring up the following web page in Figure 8-13. Select a certified file from a local host and click **Apply** to import the user certificate.


Vigor3300 series
MultiService Security
VIGOROUS BROADBAND ACCESS
Quick Setup
System
Network
Advanced
Firewall
QoS
VPN
VoIP
3:33:09 P.M.
Browse...
Apply
Cancel
DrayTek Corp. © 1997 - 2005 All rights reserved. DrayTek provides enterprise network solution.

VPN - IPSec - User Certificate # 1 - Import

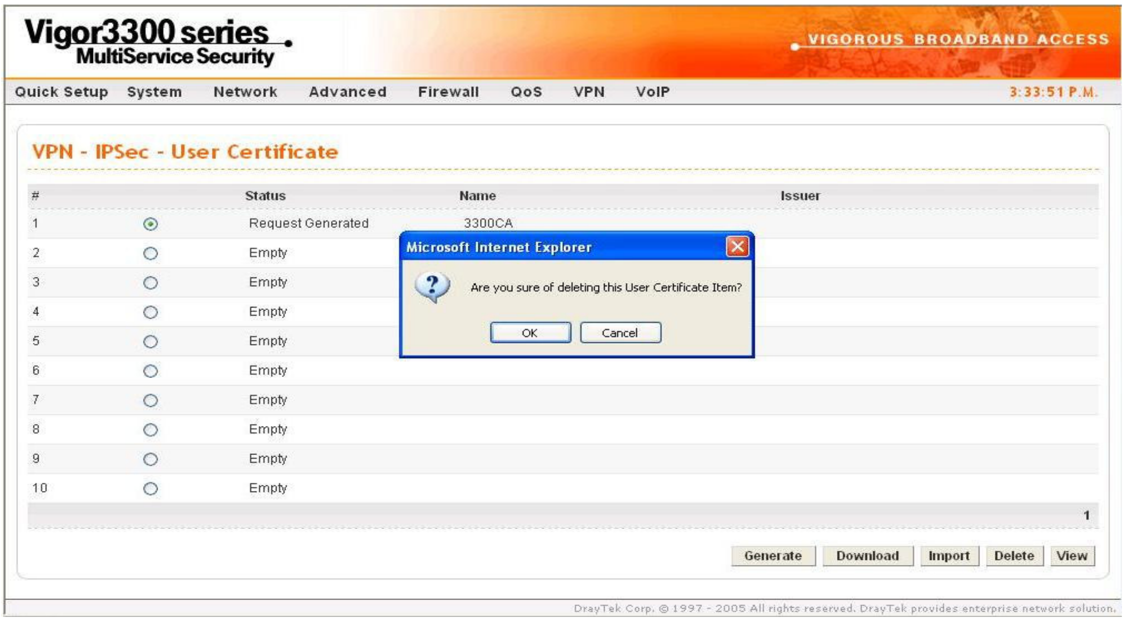
Import User Certificate

Upload File: C:\W2000_certnew_sigr

Figure 8-13. Import VPN IPSec user certificate

8.2.4.4 Delete Setup

Click **Delete** to delete a user certificate in Figure 8-14. Any User Certificate can be deleted from this table.



VPN - IPSec - User Certificate

#		Status	Name	Issuer
1	●	Request Generated	3300CA	
2	○	Empty		
3	○	Empty		
4	○	Empty		
5	○	Empty		
6	○	Empty		
7	○	Empty		
8	○	Empty		
9	○	Empty		
10	○	Empty		

1

Microsoft Internet Explorer

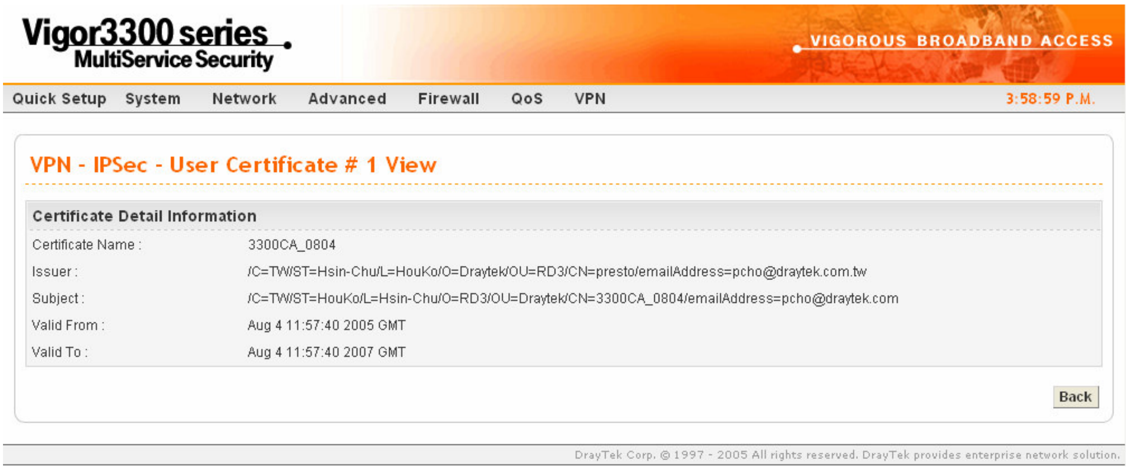
Are you sure of deleting this User Certificate Item?

OK | Cancel

Figure 8-14. Delete VPN IPSec user certificate

8.2.4.5 View

Click **View** to view the certification information in Figure 8-15.


Vigor3300 series
MultiService Security
VIGOROUS BROADBAND ACCESS
Quick Setup System Network Advanced Firewall QoS VPN
3:58:59 P.M.
Back
DrayTek Corp. © 1997 - 2005 All rights reserved. DrayTek provides enterprise network solution.

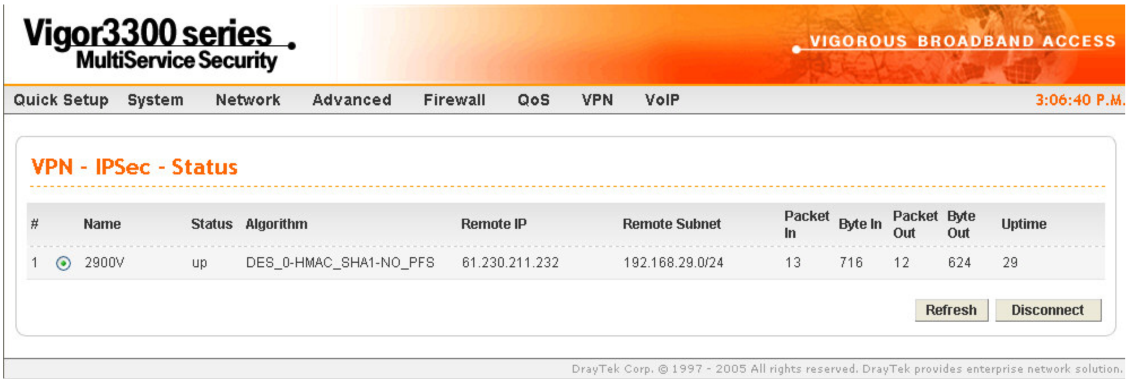
VPN - IPSec - User Certificate # 1 View

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

Figure 8-15. View VPN IPSec user certificate

8.2.5 Status

The **Status** page is shown in Figure 8-16.


Vigor3300 series
MultiService Security
VIGOROUS BROADBAND ACCESS
Quick Setup System Network Advanced Firewall QoS VPN VoIP
3:06:40 P.M.
Refresh
Disconnect
DrayTek Corp. © 1997 - 2005 All rights reserved. DrayTek provides enterprise network solution.

VPN - IPSec - Status

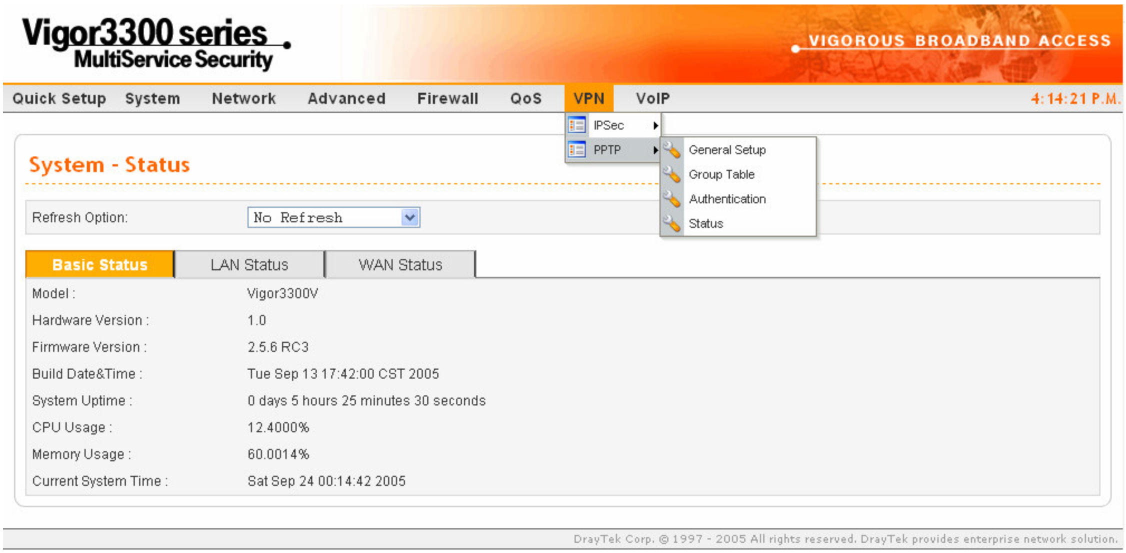
#		Name	Status	Algorithm	Remote IP	Remote Subnet	Packet In	Byte In	Packet Out	Byte Out	Uptime
1	◉	2900V	up	DES_0-HMAC_SHA1-NO_PFS	61.230.211.232	192.168.29.0/24	13	716	12	624	29

Figure. 8-16 VPN connection status

8.3 PPTP Group Setup

8.3.1 General Setup

The Vigor3300 series supports PPTP configuration through the VPN function in Figure 8-17.



System - Status

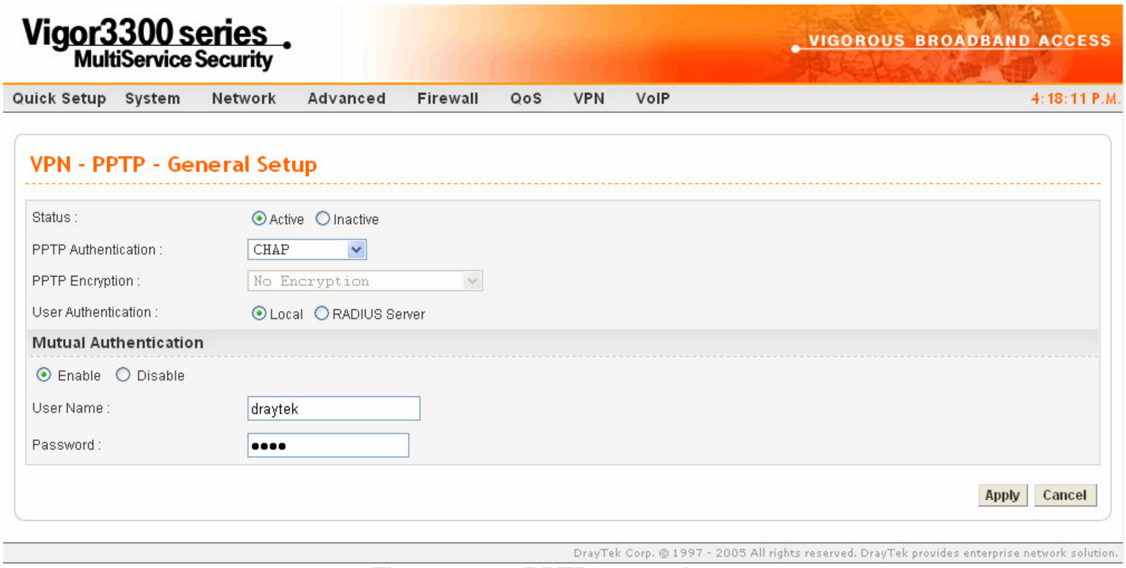
Refresh Option: No Refresh

Model :	Vigor3300V
Hardware Version :	1.0
Firmware Version :	2.5.6 RC3
Build Date&Time :	Tue Sep 13 17:42:00 CST 2005
System Uptime :	0 days 5 hours 25 minutes 30 seconds
CPU Usage :	12.4000%
Memory Usage :	60.0014%
Current System Time :	Sat Sep 24 00:14:42 2005

Figure 8-17. The VPN PPTP option

8.3.1.1 General Setup

Click **VPN -> PPTP->General Setup** to bring up the following web page in Figure 8-18.


Vigor3300 series
MultiService Security
VIGOROUS BROADBAND ACCESS
Quick Setup
System
Network
Advanced
Firewall
QoS
VPN
VoIP
4:18:11 P.M.
Apply
Cancel
DrayTek Corp. © 1997 - 2005 All rights reserved. DrayTek provides enterprise network solution.

VPN - PPTP - General Setup

Status : ● Active ○ Inactive

PPTP Authentication : CHAP

PPTP Encryption : No Encryption

User Authentication : ● Local ○ RADIUS Server

Mutual Authentication

● Enable ○ Disable

User Name : draytek

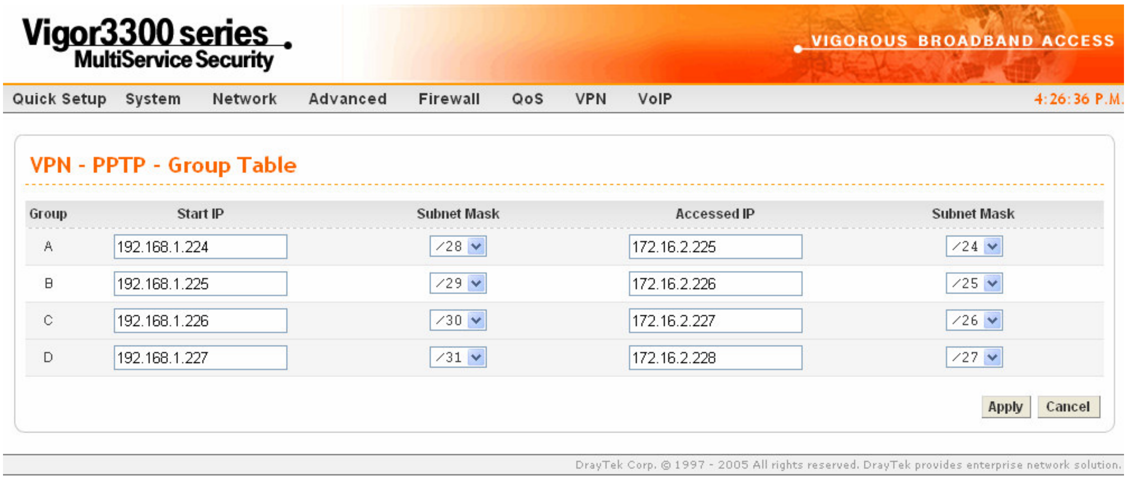
Password : ••••

Figure 8-18. PPTP general setup

Status	Sets the function to **Active** or **Inactive**.
PPTP Authentication	The authentication mode to be used. The default setting is **CHAP**.
PPTP Encryption	The encryption mode to be used. If PPTP authentication mode is set to CHAP or PAP, PPTP Encryption mode does not need to be set.
User Authentication	Sets user authentication to **Local** server or **RADIUS** server.
Mutual Authentication	
Status	**Enables** or **Disables** this function.
User Name	The user name.
Password	The password.

8.3.2.2 Group Setup

The Vigor3300 series provides up to four groups configurations in Figure 8-19.


Vigor3300 series
MultiService Security
VIGOROUS BROADBAND ACCESS
Quick Setup
System
Network
Advanced
Firewall
QoS
VPN
VoIP
4:26:36 P.M.
Apply
Cancel
DrayTek Corp. © 1997 - 2005 All rights reserved. DrayTek provides enterprise network solution.

VPN - PPTP - Group Table

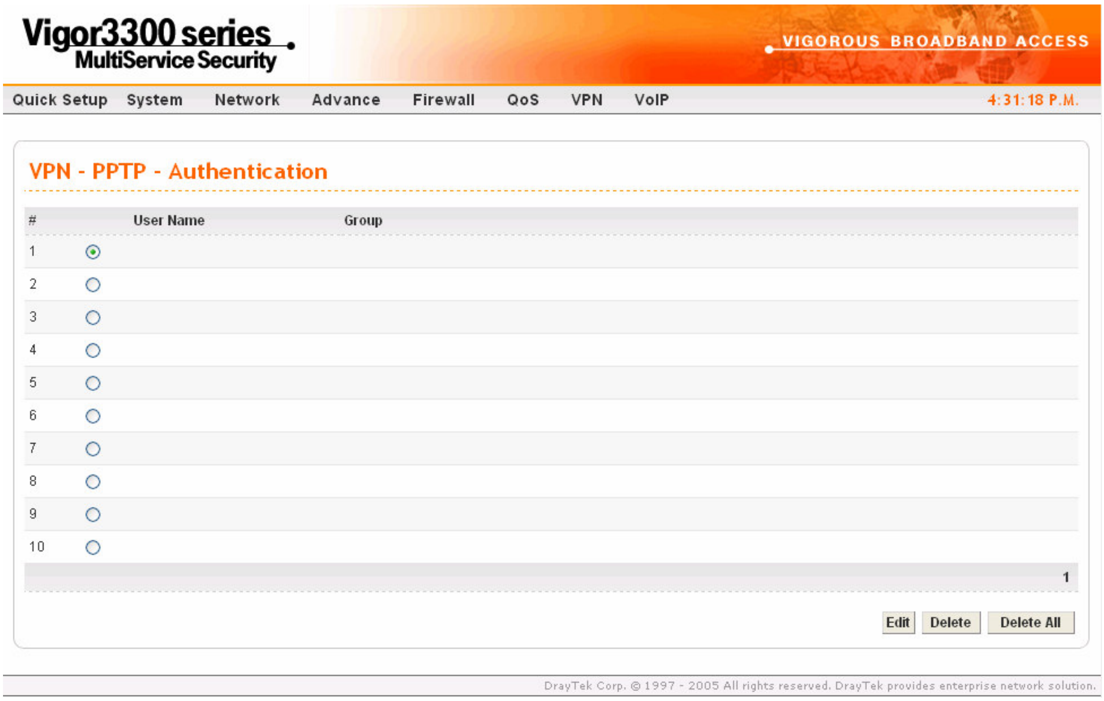
Group	Start IP	Subnet Mask	Accessed IP	Subnet Mask
A	192.168.1.224	/28	172.16.2.225	/24
B	192.168.1.225	/29	172.16.2.226	/25
C	192.168.1.226	/30	172.16.2.227	/26
D	192.168.1.227	/31	172.16.2.228	/27

Figure 8-19. PPTP group configuration

Start IP	The starting IP address. The default group value is 192.168.1.224/28.
Subnet Mask	The value of subnet mask for the Start IP.
Accessed IP	The accessed IP address.
Subnet Mask	The value of subnet mask for the Accessed IP.

8.3.2.3 Authentication Setup

Click the **Authentication** option to bring up the following web page (Figure 8-20). This page will display "**User Name**" and "**Group**" fields. Select an entry and click **Edit** to add a new entry in Figure 8-21.

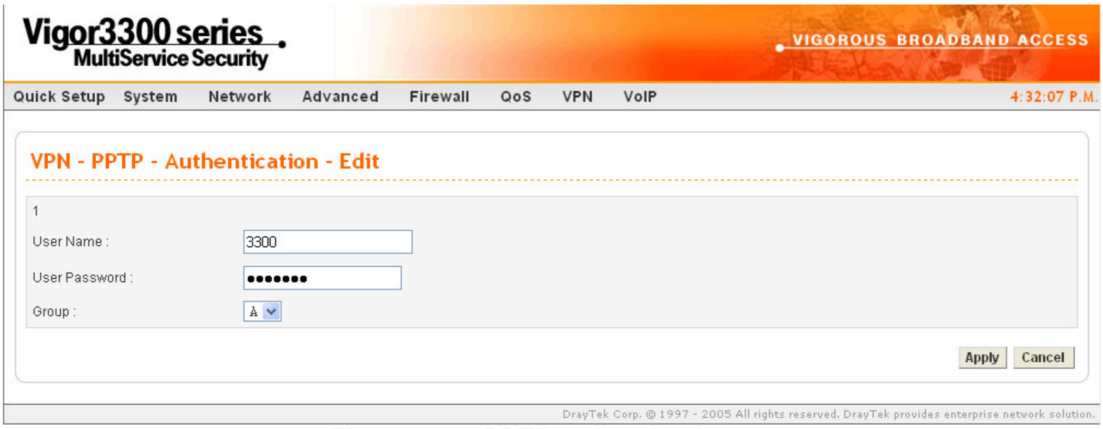

Vigor3300 series
MultiService Security
VIGOROUS BROADBAND ACCESS
Quick Setup System Network Advance Firewall QoS VPN VoIP
4:31:18 P.M.

VPN - PPTP - Authentication

#		User Name	Group
1	●		
2	○		
3	○		
4	○		
5	○		
6	○		
7	○		
8	○		
9	○		
10	○		

1
Edit Delete Delete All
DrayTek Corp. © 1997 - 2005 All rights reserved. DrayTek provides enterprise network solution.

Figure 8-20. PPTP authentication configuration


Vigor3300 series
MultiService Security
VIGOROUS BROADBAND ACCESS
Quick Setup System Network Advanced Firewall QoS VPN VoIP
4:32:07 P.M.

VPN - PPTP - Authentication - Edit

1

User Name : 3300

User Password : •••••••

Group : A

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

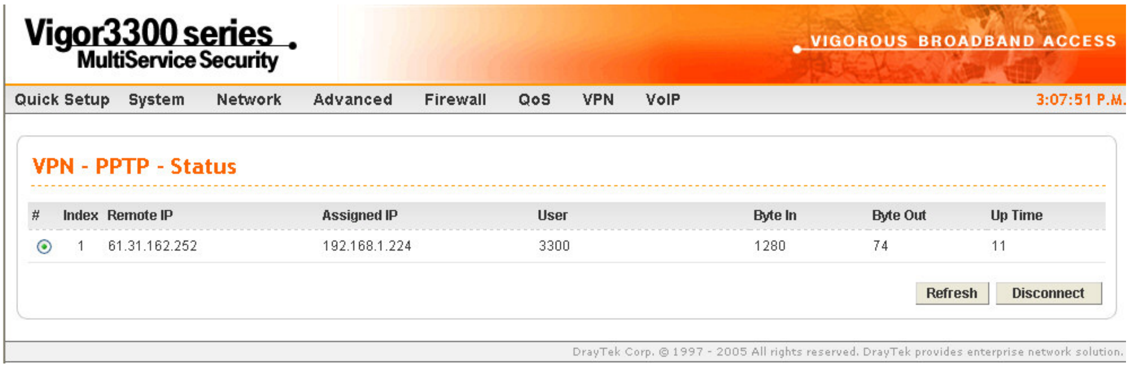
Figure 8-21. PPTP authentication entry

User Name	The user name for this entry.
User Password	The password for this entry.
Group	The group for this entry.

Click **Apply** to apply these settings.

8.3.2.4 Status

Click the **Status** option to bring up the following web in Figure 8-22. This page displays some relevant information about PPTP connection. It will refresh automatically every 10 seconds.



Vigor3300 series
MultiService Security
VIGOROUS BROADBAND ACCESS
Quick Setup
System
Network
Advanced
Firewall
QoS
VPN
VoIP
3:07:51 P.M.

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

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

Figure 8-22. PPTP status

CHAPTER 9

VoIP Setup

This chapter shows how to configure VoIP function.

This chapter is divided into the following sections.

- Section 9.1: Introduction
- Section 9.2: Protocol Setup
- Section 9.3: Port Settings Setup
- Section 9.4: Speed Dial Setup
- Section 9.5: Advanced Speed Dial Setup
- Section 9.6: Miscellaneous Setup
- Section 9.7: Tone Settings Setup
- Section 9.8: QoS Setup
- Section 9.9: NAT Traversal Setup
- Section 9.10: Incoming Call Barring Setup
- Section 9.11: Call History
- Section 9.12: Status

9.1 Introduction

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 provides cost effective voice solution for SME customers in Figure 9-1.

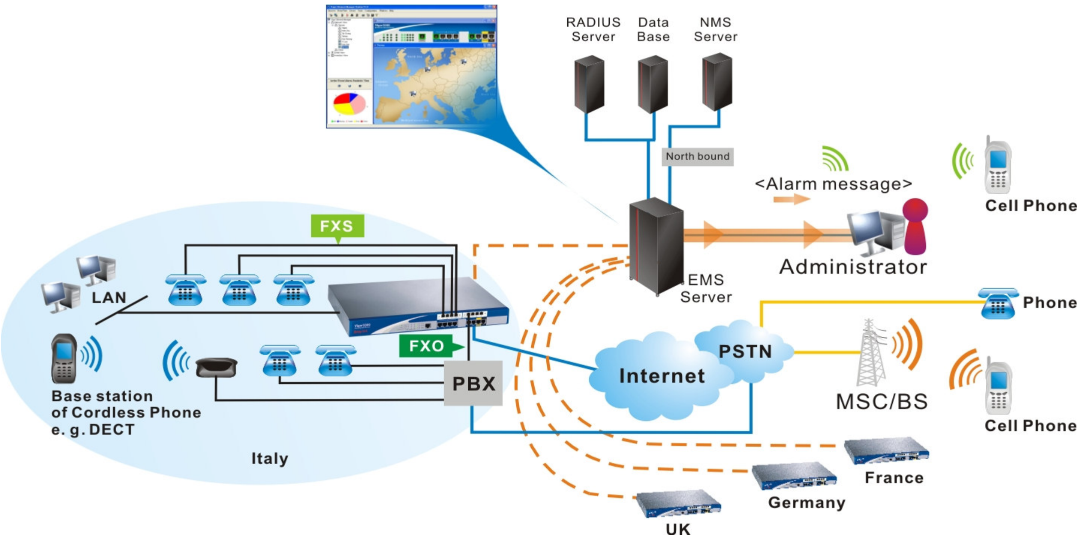
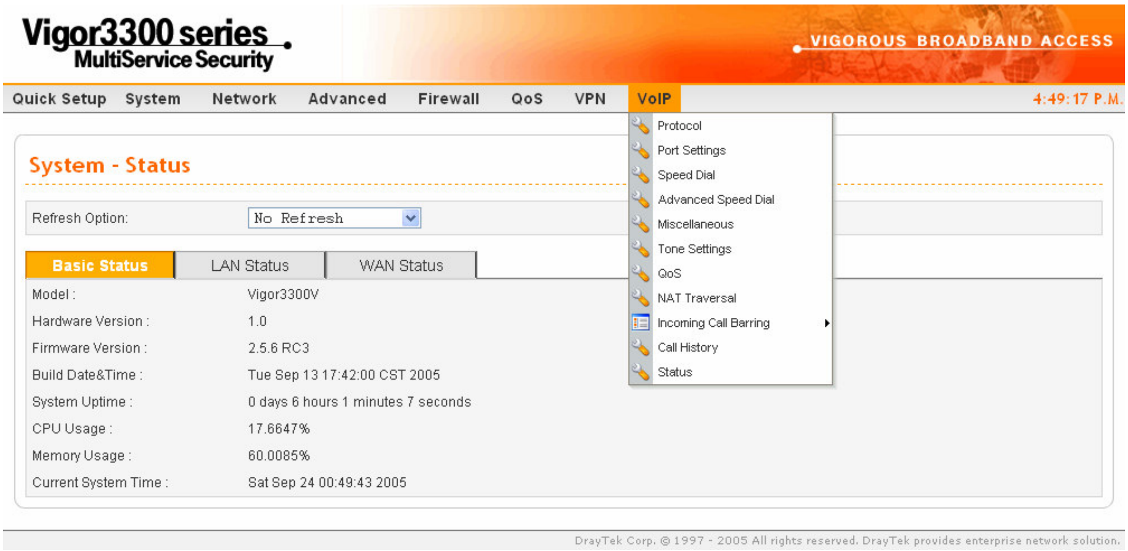


Figure 9-1. Vigor3300 VoIP application scenario

Click the VoIP option to set up VoIP configuration in Figure 9-2.



System - Status

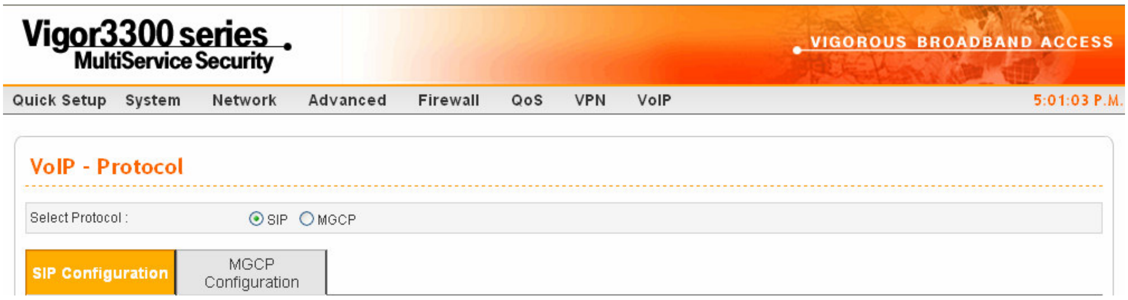
Refresh Option: No Refresh

Model : Vigor3300V
Hardware Version : 1.0
Firmware Version : 2.5.6 RC3
Build Date&Time : Tue Sep 13 17:42:00 CST 2005
System Uptime : 0 days 6 hours 1 minutes 7 seconds
CPU Usage : 17.6647%
Memory Usage : 60.0085%
Current System Time : Sat Sep 24 00:49:43 2005

Figure 9-2. The VoIP menu

9.2 Protocol Setup

Click the **Protocol** option to bring up the following web page in Figure 9-3. There are two protocols in VoIP: **SIP** and **MGCP**.



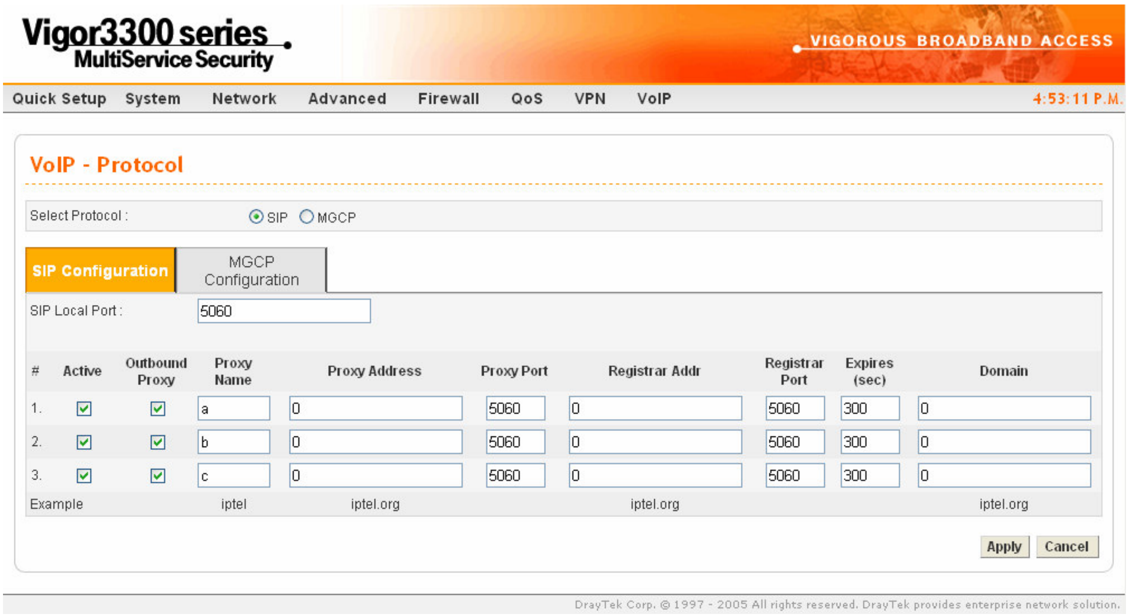
Select Protocol : ● SIP ○ MGCP

Figure 9-3. Protocol configuration

Select Protocol	The protocol to be used. There are two options: **SIP**, and **MGCP**. The default setting is **SIP**.

9.2.1 SIP Configuration

The Vigor 3300V supports three SIP server settings in Figure 9-4.


Vigor3300 series
MultiService Security
VIGOROUS BROADBAND ACCESS
Quick Setup System Network Advanced Firewall QoS VPN VoIP
4:53:11 P.M.
DrayTek Corp. © 1997 - 2005 All rights reserved. DrayTek provides enterprise network solution.

VoIP - Protocol

Select Protocol : ● SIP ○ MGCP

SIP Configuration | MGCP Configuration

SIP Local Port : 5060

#	Active	Outbound Proxy	Proxy Name	Proxy Address	Proxy Port	Registrar Addr	Registrar Port	Expires (sec)	Domain
1.	☑	☑	a	0	5060	0	5060	300	0
2.	☑	☑	b	0	5060	0	5060	300	0
3.	☑	☑	c	0	5060	0	5060	300	0
Example			iptel	iptel.org		iptel.org			iptel.org

Apply Cancel

Figure 9-4. SIP configurations

SIP Local Port –The port number for SIP protocol. The default value is 5060.

SIP Proxy Setting	
Active[1]	Click this square box to activate this SIP proxy server setting.
Outbound Proxy	Enable this function to send SIP protocol packets to an SIP proxy server.

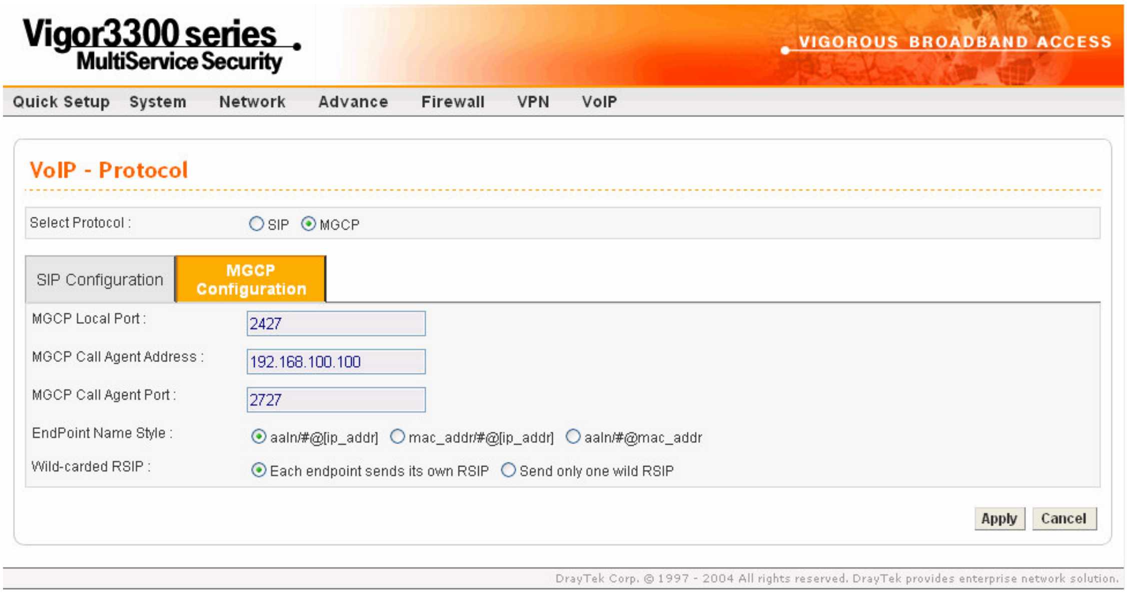
[1] ***If the "LAN/VPN" option is selected in the VoIP IP Address field, it is recommended to keep each SIP proxy entry inactive to keep connections of VoIP applications.***

Proxy Name	The name of the SIP proxy server.
Proxy Address	The IP address of the SIP proxy server.
Proxy Port	The port number of the SIP proxy server.
Registrar Address	The IP address or domain name of the SIP registrar server.
Registrar Port	The port number of the SIP registrar server.
Expires	The timeout value for SIP protocols. The default value is 300.
Domain	The IP address or domain name of the SIP Domain/Realm.

Click **Apply** to apply these settings.

9.2.2 MGCP Configuration

Click **MGCP** to bring up the following web page in Figure 9-5.



VoIP - Protocol

Select Protocol : ○ SIP ● MGCP

MGCP Local Port : 2427

MGCP Call Agent Address : 192.168.100.100

MGCP Call Agent Port : 2727

EndPoint Name Style : ● aaln/#@[ip_addr] ○ mac_addr/#@[ip_addr] ○ aaln/#@mac_addr

Wild-carded RSIP : ● Each endpoint sends its own RSIP ○ Send only one wild RSIP

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

Figure 9-5. MGCP configuration

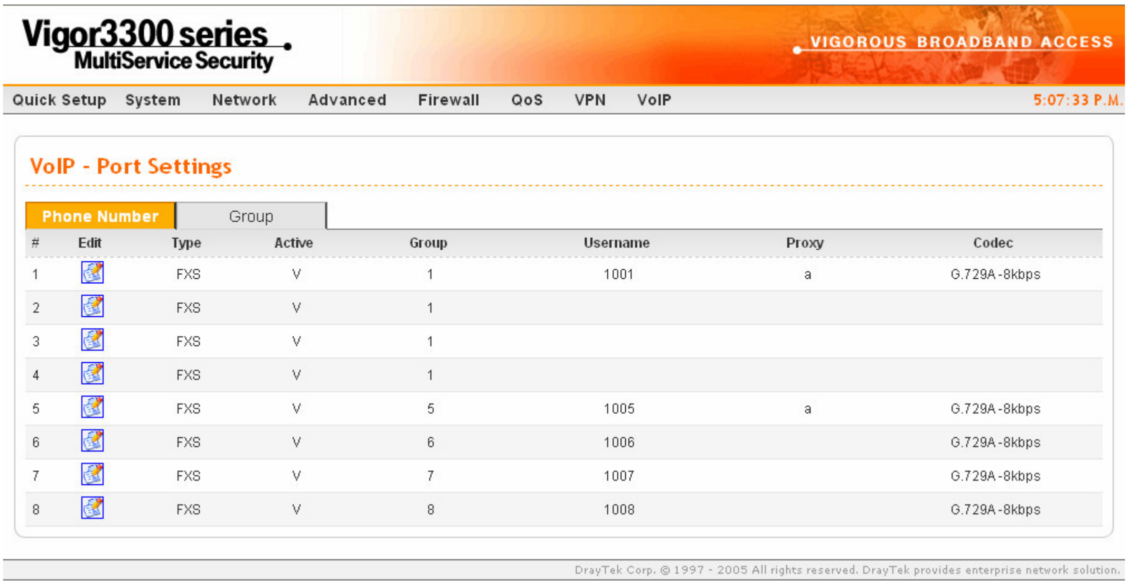
MGCP Local Port	The UDP port number in MGCP local terminal.
MGCP Call Agent Address	The IP address of the Call Agent server in MGCP.
MGCP Call Agent Port	The UDP port number for the Call Agent server.
EndPoint Name Style	There are three options: **aaln/#@[ip_addr] ex: aaln/1@[1.1.1.1]** **mac_addr/#@[ip_addr] ex: 000504030201/1@[1.1.1.1]** **aaln/#@mac_addr ex: aaln/1@000504030201**
Wild-carded RSIP	There are two options: **Each endpoint sends its own RSIP** **Send only one wild RSIP**

9.3 Port Settings Setup

There are two parts to this feature. They are described in greater details as below.

9.3.1 Phone Number Configuration

Click **VoIP -> Port settings** to configure basic information for VoIP in Figure 9-6.

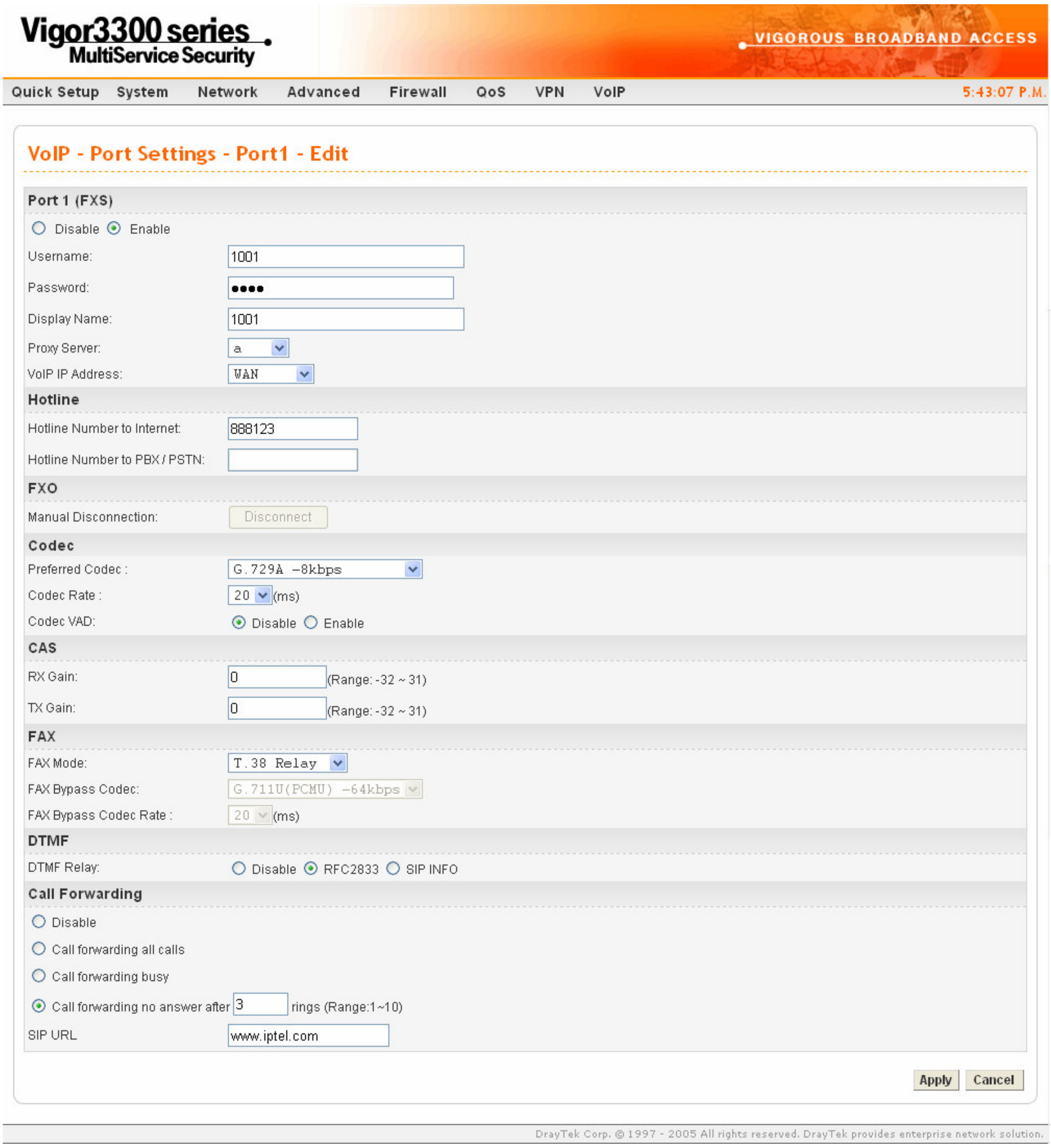

Vigor3300 series
MultiService Security
VIGOROUS BROADBAND ACCESS
Quick Setup
System
Network
Advanced
Firewall
QoS
VPN
VoIP
5:07:33 P.M.
Phone Number
Group
DrayTek Corp. © 1997 - 2005 All rights reserved. DrayTek provides enterprise network solution.

VoIP - Port Settings

#	Edit	Type	Active	Group	Username	Proxy	Codec
1	✎	FXS	V	1	1001	a	G.729A-8kbps
2	✎	FXS	V	1			
3	✎	FXS	V	1			
4	✎	FXS	V	1			
5	✎	FXS	V	5	1005	a	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

Figure 9-6. The port settings configuration

Click **Edit** to bring up the following web page in Figure 9-7.



VoIP - Port Settings - Port1 - Edit

Port 1 (FXS)

○ Disable ● Enable

Username:	1001
Password:	••••
Display Name:	1001
Proxy Server:	a
VoIP IP Address:	WAN

Hotline

Hotline Number to Internet:	888123
Hotline Number to PBX / PSTN:	

FXO

Manual Disconnection:	Disconnect

Codec

Preferred Codec :	G.729A -8kbps
Codec Rate :	20 (ms)
Codec VAD:	● Disable ○ Enable

CAS

RX Gain:	0 (Range: -32 ~ 31)
TX Gain:	0 (Range: -32 ~ 31)

FAX

FAX Mode:	T.38 Relay
FAX Bypass Codec:	G.711U(PCMU) -64kbps
FAX Bypass Codec Rate :	20 (ms)

DTMF

DTMF Relay:	○ Disable ● RFC2833 ○ SIP INFO

Call Forwarding

○ Disable

○ Call forwarding all calls

○ Call forwarding busy

● Call forwarding no answer after 3 rings (Range:1~10)

SIP URL www.iptel.com

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

Figure 9-7. Edit phone number configuration

Port 1 (FXS)	
Selective Box	**Enable** or **Disable** this port.
User Name	The user name (a number) for each phone line.
Password	The user password for each phone line.
Display Name	The user name to be displayed on another phone terminal.
Proxy Server	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 this phone number to make the port dial out to Internet automatically.
Hotline Number to PBX / PSTN	Pre-set this phone number to make the port dial out to PBX/PSTN automatically.

FXO	
Manual Disconnection	Click “Disconnect” button to disconnect this phone line by manual.

Codec	
Preferred Codec	The Codec to be applied on this port. Vigor3300 supports five Codecs.
Codec Rate	The rate value to be applied on this port.
Codec VAD	**Enable** or **Disable** VAD (Voice Activity Detection).

CAS	
RX Gain	The gain value while receiving voice. The default value is 0. The range is from -32 to 31.
TX Gain	The gain value while transmitting 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 to be applied if FAX mode is configured as **Bypass** mode.

DTMF	
DTMF Relay	The DTMF Relay function. There are three options to be supported as below: **Disable** **RFC2833** **SIP INFO**

Call Forwarding	Click "Disable" to disable forwarding function. Click "Call forwarding all calls" to forward all callings. Click "Call forwarding busy" to forward callings when this line is busy. Click "Call forwarding no answer after (Range: 1~10) rings" to forward callings after ringing 1~10 times.
SIP URL	Assign a SIP URL site to be confirmed by call forwarding function.

Click **Apply** to apply these settings.

Note

1. The default internal phone numbers are "01", "02", "03"…"08" for each port. These numbers can be dialed for internal phone line usage.

2. If the FAX function needs to be used, it is advisable to configure the same FAX mode settings between the two VoIP routers.

The FAX mode option will be varied depends on which Codec has been selected (see table).

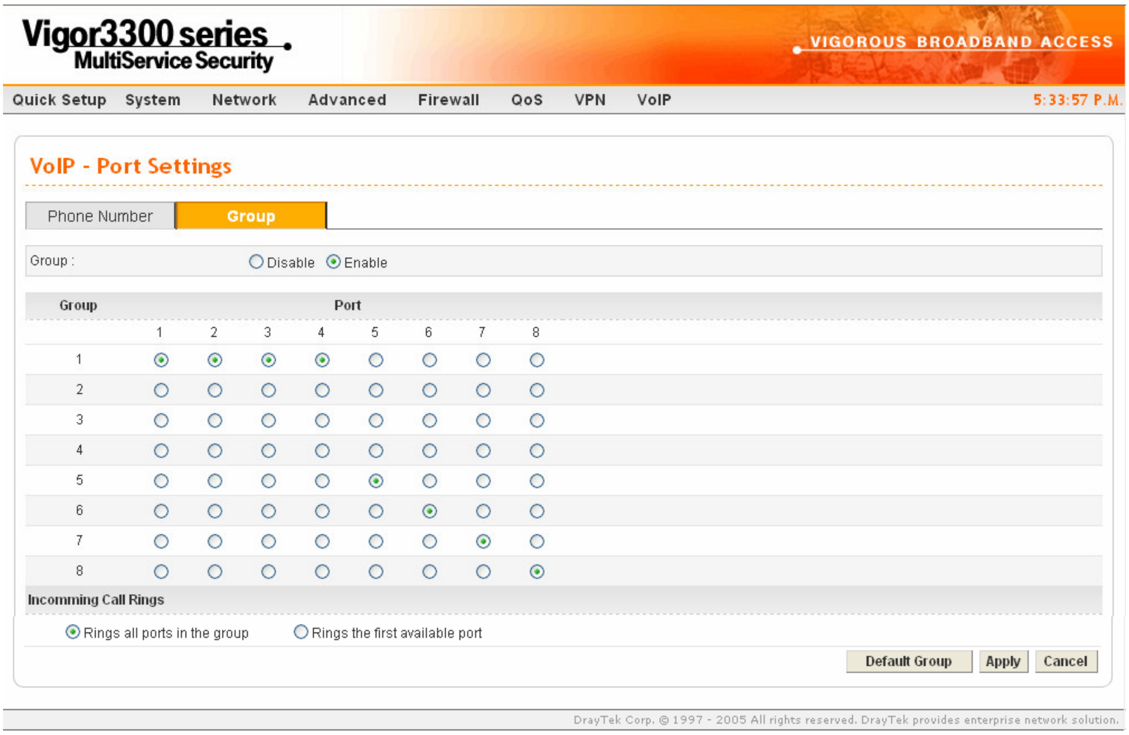
Codec	*Allowed FAX Modes*
G.711U ***G.711A*** ***G.726***	***Transparent, T.38, Bypass***
G.729A ***G.723.1***	***T.38, Bypass***

9.3.2 Group Configuration

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 in Figure 9-8[2].

[2] ***Each group has a default leading port. If this group has more than one port, the settings for all ports have to follow the setting of the leading port.***


Vigor3300 series
MultiService Security
VIGOROUS BROADBAND ACCESS
Quick Setup System Network Advanced Firewall QoS VPN VoIP
5:33:57 P.M.

VoIP - Port Settings

Group : ○ Disable ● Enable

Group	Port							
	1	2	3	4	5	6	7	8
1	●	●	●	●	○	○	○	○
2	○	○	○	○	○	○	○	○
3	○	○	○	○	○	○	○	○
4	○	○	○	○	○	○	○	○
5	○	○	○	○	●	○	○	○
6	○	○	○	○	○	●	○	○
7	○	○	○	○	○	○	●	○
8	○	○	○	○	○	○	○	●

Incomming Call Rings

● Rings all ports in the group ○ Rings the first available port

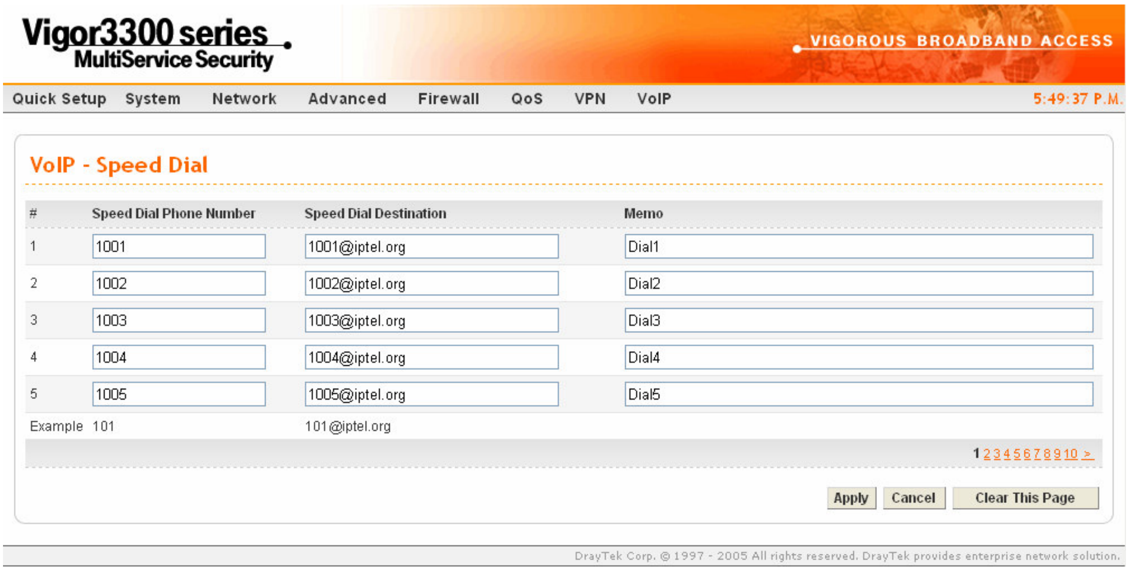
Default Group
Apply
Cancel
DrayTek Corp. © 1997 - 2005 All rights reserved. DrayTek provides enterprise network solution.

Figure 9-8. The group configuration

9.4 Speed Dial Setup

This feature provides a simple way to dial a specific number. Up to 150 numbers can be stored in Vigor3300V.

Click **VoIP -> Speed Dial** to set up dialing entries in Figure 9-9.



VoIP - Speed Dial

#	Speed Dial Phone Number	Speed Dial Destination	Memo
1	1001	1001@iptel.org	Dial1
2	1002	1002@iptel.org	Dial2
3	1003	1003@iptel.org	Dial3
4	1004	1004@iptel.org	Dial4
5	1005	1005@iptel.org	Dial5
Example	101	101@iptel.org	

1 2 3 4 5 6 7 8 9 10 >

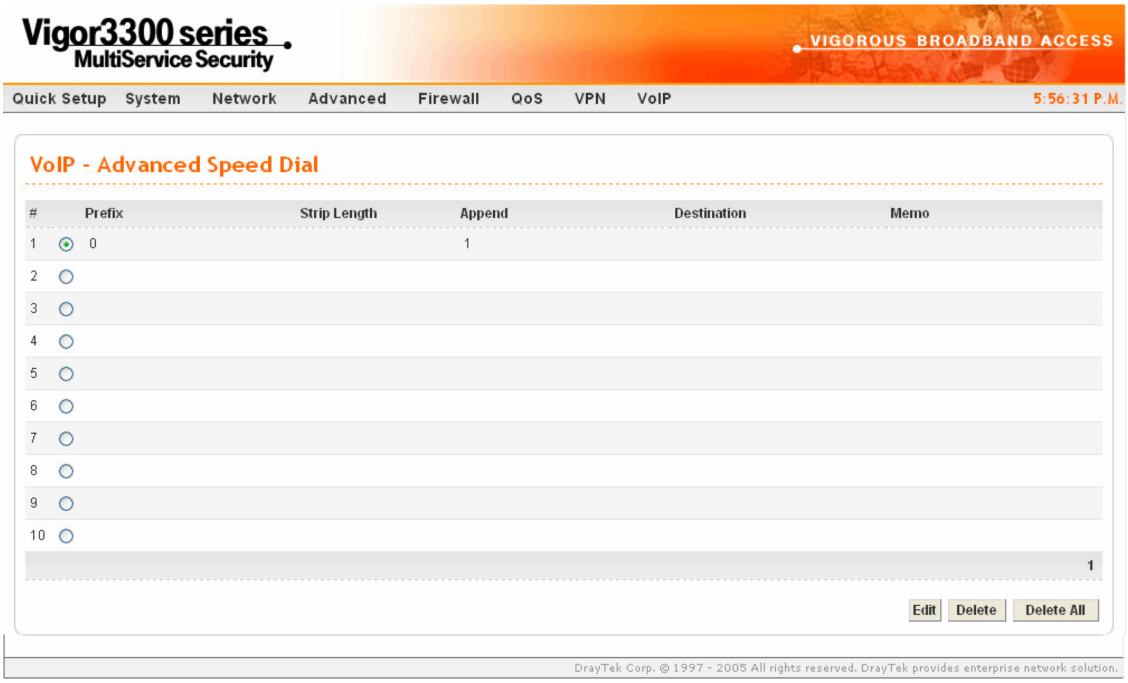
Figure 9-9. The speed dial configuration

Speed Dial Phone Number	The phone number to be dialed.
Speed Dial Destination	The dialing destination address.
Memo	A description for each number.

Click **Apply** to apply these settings.

9.5 Advanced Speed Dial

Click **VoIP ->Advanced Speed Dial** to configure the setting as shown in Figure 9-10.



VoIP - Advanced Speed Dial

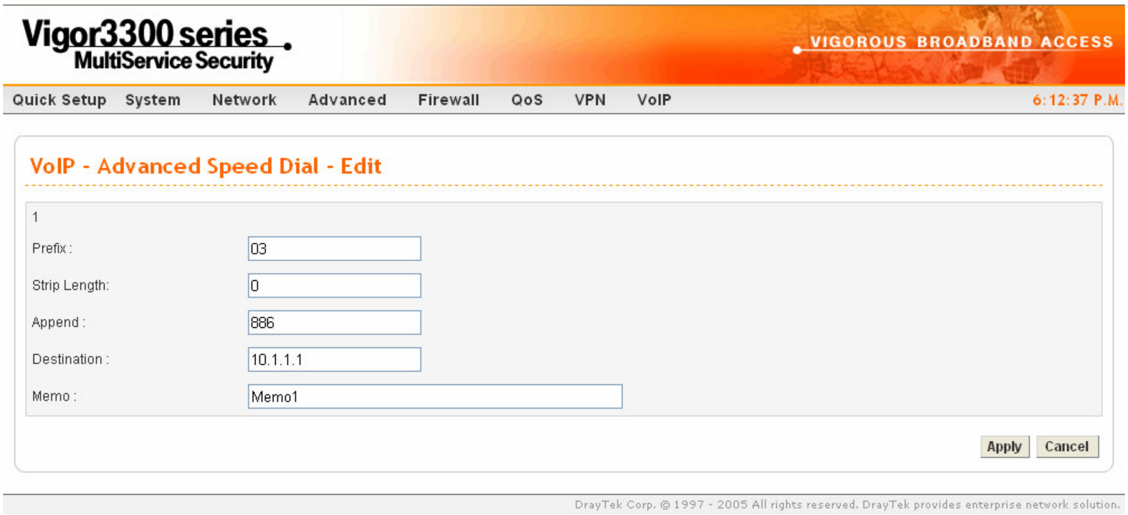
#		Prefix	Strip Length	Append	Destination	Memo
1	●	0		1		
2	○					
3	○					
4	○					
5	○					
6	○					
7	○					
8	○					
9	○					
10	○					

1

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

Figure 9-10. The advanced speed dial configuration

Click **Edit** to configure one entry and the following web page as shown in Figure 9-11.


Vigor3300 series
MultiService Security
VIGOROUS BROADBAND ACCESS
Quick Setup
System
Network
Advanced
Firewall
QoS
VPN
VoIP
6:12:37 P.M.
Apply
Cancel
DrayTek Corp. © 1997 - 2005 All rights reserved. DrayTek provides enterprise network solution.

VoIP - Advanced Speed Dial - Edit

1

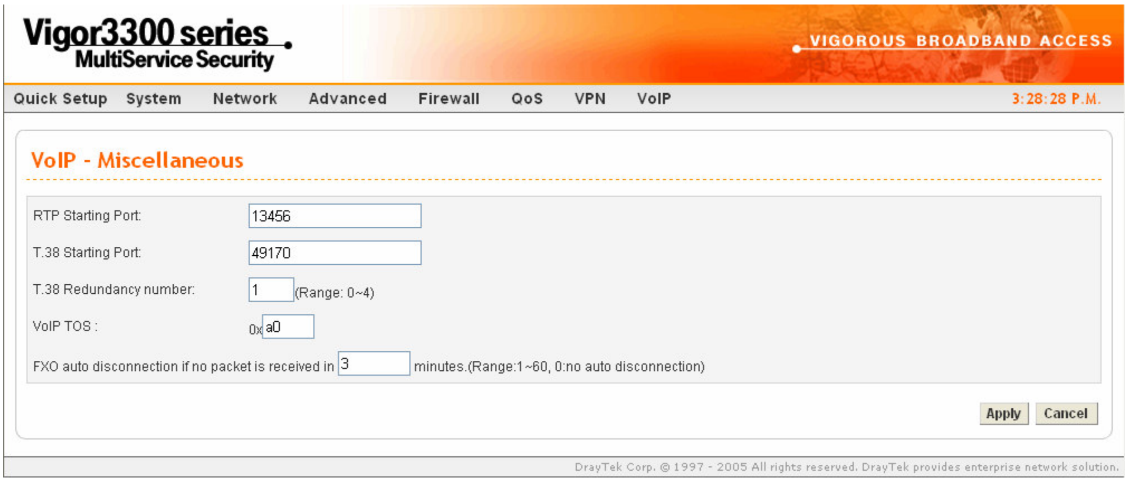
Prefix :	03
Strip Length:	0
Append :	886
Destination :	10.1.1.1
Memo :	Memo1

Figure 9-11. Advanced speed dial edit page

Prefix	Assign a prefix of phone number to be checked.
Strip Length	Assign the length of digit to be removed.
Append	Assign the number to be added before a phone number.
Destination	Assign a destination address to be sent.
Memo	A description for this entry.

9.6 Miscellaneous Setup

Miscellaneous Setup includes **RTP** and **T.38 Starting Port, T.38 Redundancy Number** and **VoIP ToS** settings. Click **VoIP ->Miscellaneous** to configure Miscellaneous Setup in Figure 9-12.


Vigor3300 series
MultiService Security
VIGOROUS BROADBAND ACCESS
Quick Setup
System
Network
Advanced
Firewall
QoS
VPN
VoIP
3:28:28 P.M.
Apply
Cancel
DrayTek Corp. @ 1997 - 2005 All rights reserved. DrayTek provides enterprise network solution.

VoIP - Miscellaneous

RTP Starting Port: 13456

T.38 Starting Port: 49170

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

VoIP TOS : 0x a0

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

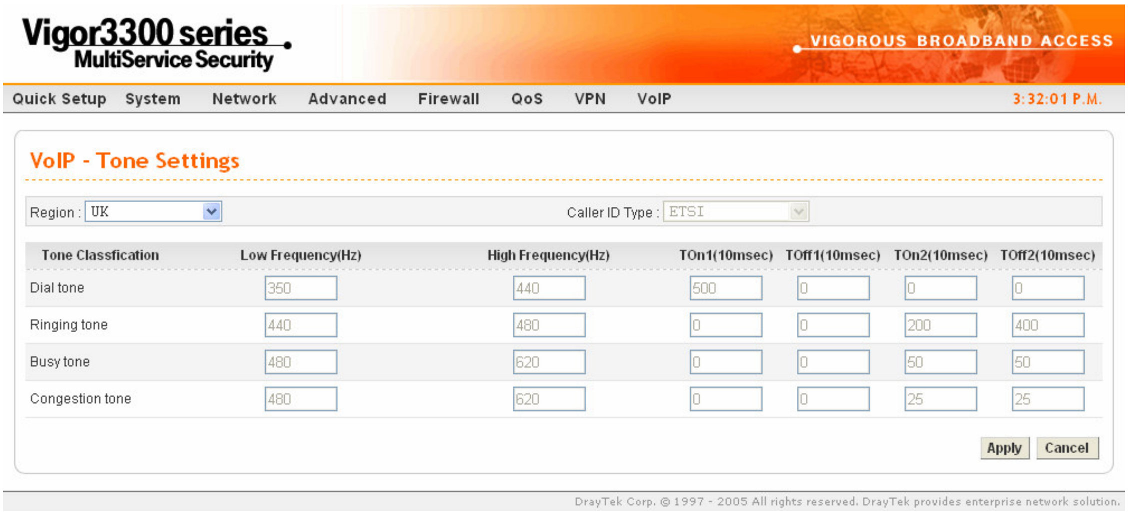
Figure 9-12. Miscellaneous configuration

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 to attach to the tail of the packet) for T.38 protocol. The default value is 1.
VoIP ToS	The ToS value in VoIP protocol packet. The default setting is 0xa0.

Click **Apply** to apply these settings.

9.7 Tone Settings Setup

Click **VoIP->Tone Settings** to configure the **Tone Settings** in Figure 9-13.



Vigor3300 series
MultiService Security
VIGOROUS BROADBAND ACCESS
Quick Setup
System
Network
Advanced
Firewall
QoS
VPN
VoIP
3:32:01 P.M.
Apply
Cancel
DrayTek Corp. © 1997 - 2005 All rights reserved. DrayTek provides enterprise network solution.

VoIP - Tone Settings

Region : UK

Caller ID Type : ETSI

Tone Classfication	Low Frequency(Hz)	High Frequency(Hz)	TOn1(10msec)	TOff1(10msec)	TOn2(10msec)	TOff2(10msec)
Dial tone	350	440	500	0	0	0
Ringing tone	440	480	0	0	200	400
Busy tone	480	620	0	0	50	50
Congestion tone	480	620	0	0	25	25

Figure 9-13. The tone setting configuration

Region	The country area for using VoIP feature. 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.

There are four kinds of tones provided: **Dial tone, Ringing tone, Busy tone and Congestion tone**).

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

Ringing tone –A tone means the call is ringing.

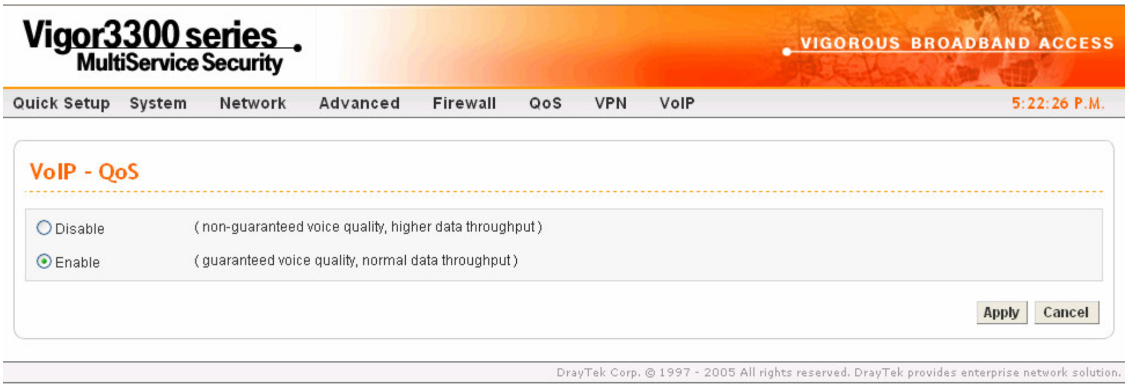
Busy tone – A tone means the phone line is busy.

Congestion tone – A tone means the network is busy.

Low Frequency (Hz)	The low frequency number in Hertz.
High Frequency (Hz)	The high frequency number in Hertz.
Ton1 (10msec)	The duration of the first ring.
TOff1 (10msec)	The silence duration after the first ring.
Ton2 (10msec)	The duration of the next continuous ring.
Toff2 (10msec)	The silence duration after the next continuous ring.

9.8 VoIP QoS[3] Setup

Click **VoIP->QoS** to bring up the following web page as Figure 9-14.


Vigor3300 series
MultiService Security
VIGOROUS BROADBAND ACCESS
Quick Setup System Network Advanced Firewall QoS VPN VoIP
5:22:26 P.M.

VoIP - QoS

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

● Enable (guaranteed voice quality, normal data throughput)

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

Figure 9-14. VoIP QoS configuration

Status	**Enable** or **Disable** QoS function

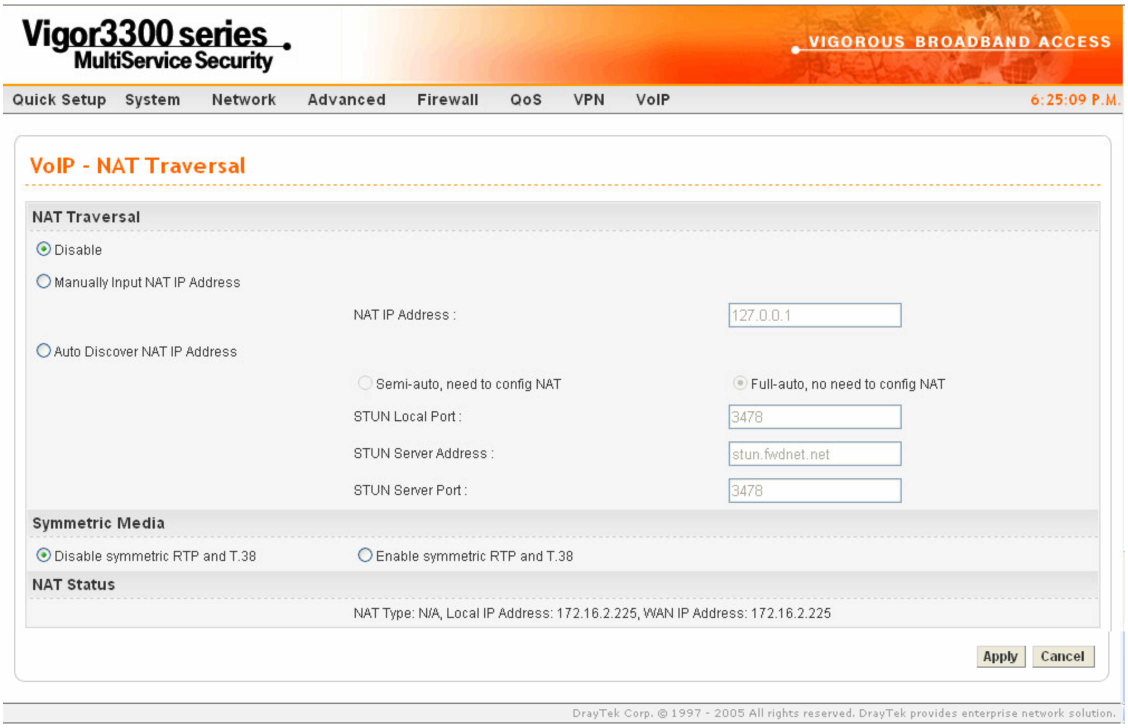
Click **Apply** to apply these settings.

[3] *This Quality of Service (QoS) function is only for the VoIP feature. When this function is enabled, the Vigor 3300 will set rate limitation for incoming and outgoing transmissions to ensure the best quality of service in VoIP.*

9.9 NAT Traversal Setup

NAT traversal is a challenge that all Service Providers looking to deliver public IP-based voice and multimedia services must solve. The goal 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.

The Vigor3300 series supports this feature to keep voice application behind any NAT routers as it is in Figure 9-15.


Vigor3300 series
MultiService Security
VIGOROUS BROADBAND ACCESS
Quick Setup
System
Network
Advanced
Firewall
QoS
VPN
VoIP
6:25:09 P.M.
Apply
Cancel
DrayTek Corp. © 1997 - 2005 All rights reserved. DrayTek provides enterprise network solution.

VoIP - NAT Traversal

NAT Traversal

● Disable

○ Manually Input NAT IP Address

NAT IP Address : 127.0.0.1

○ Auto Discover NAT IP Address

○ Semi-auto, need to config NAT ● Full-auto, no need to config NAT

STUN Local Port : 3478

STUN Server Address : stun.fwdnet.net

STUN Server Port : 3478

Symmetric Media

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

NAT Status

NAT Type: N/A, Local IP Address: 172.16.2.225, WAN IP Address: 172.16.2.225

Figure 9-15. NAT traversal configuration

There are three parts supported as below.

Disable	Disable this function. The feature is used if 3300V has a public WAN IP address and not behind a NAT router.
Manually Input NAT IP Address	
NAT IP Address	The IP address to be used as the NAT IP address. The feature is used if 3300V is behind a NAT router, and the NAT router uses static WAN IP address. This value is the same as the WAN IP of the front NAT router.
Auto Discovery NAT IP Address	
Semi-auto	Click this function; User needs to configure NAT information.
Full-auto	Click this function; User does not configure NAT information.
STUN Local Port	The port number of the STUN server.
STUN Server Address	The IP address of the STUN server.
STUN Server Port	The server port number of the STUN server.
Symmetric Media	
Disable	RTP and T.38 are not symmetrical.
Enable	RTP and T.38 are symmetrical.

Note

"Auto Discovery NAT IP Address" option is used when the 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.

Note

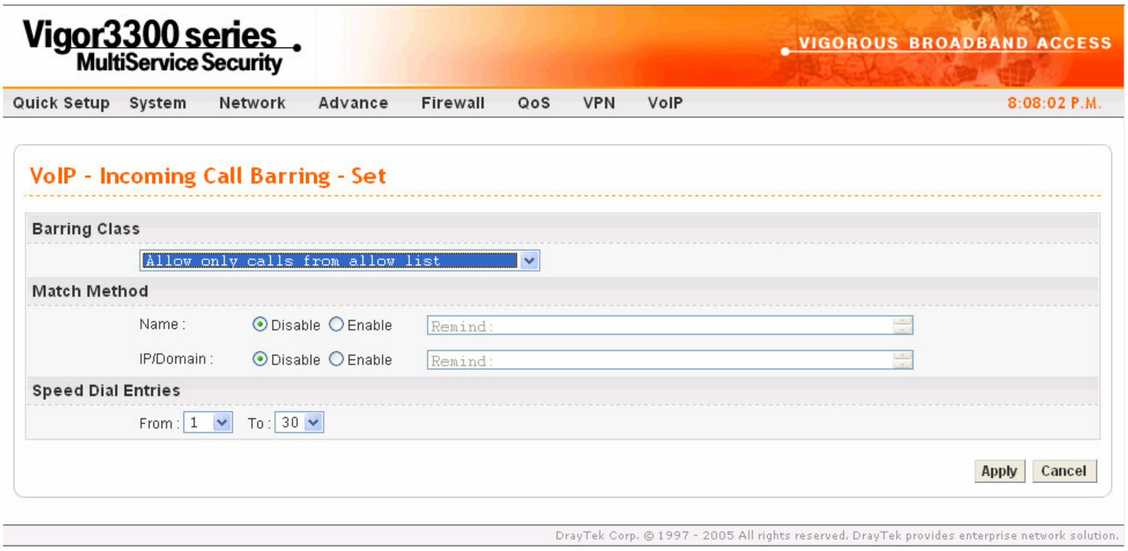
The "STUN" (Simple Traversal of UDP through NATs) server is an implementation of the STUN protocol that enables STUN functionality in SIP-based systems. STUN is an application-layer protocol that can determine the public IP and nature of a NAT device that sits between the STUN client and STUN server.

9.10 Incoming Call Barring Setup

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.”

9.10.1 Set

Click the **Set** option to bring up the following web page as Figure 9-16.


Vigor3300 series
MultiService Security
VIGOROUS BROADBAND ACCESS
Quick Setup
System
Network
Advance
Firewall
QoS
VPN
VoIP
8:08:02 P.M.
Apply
Cancel
DrayTek Corp. © 1997 - 2005 All rights reserved. DrayTek provides enterprise network solution.

VoIP - Incoming Call Barring - Set

Barring Class

Allow only calls from allow list

Match Method

Name : ● Disable ○ Enable Remind :

IP/Domain : ● Disable ○ Enable Remind :

Speed Dial Entries

From : 1 To : 30

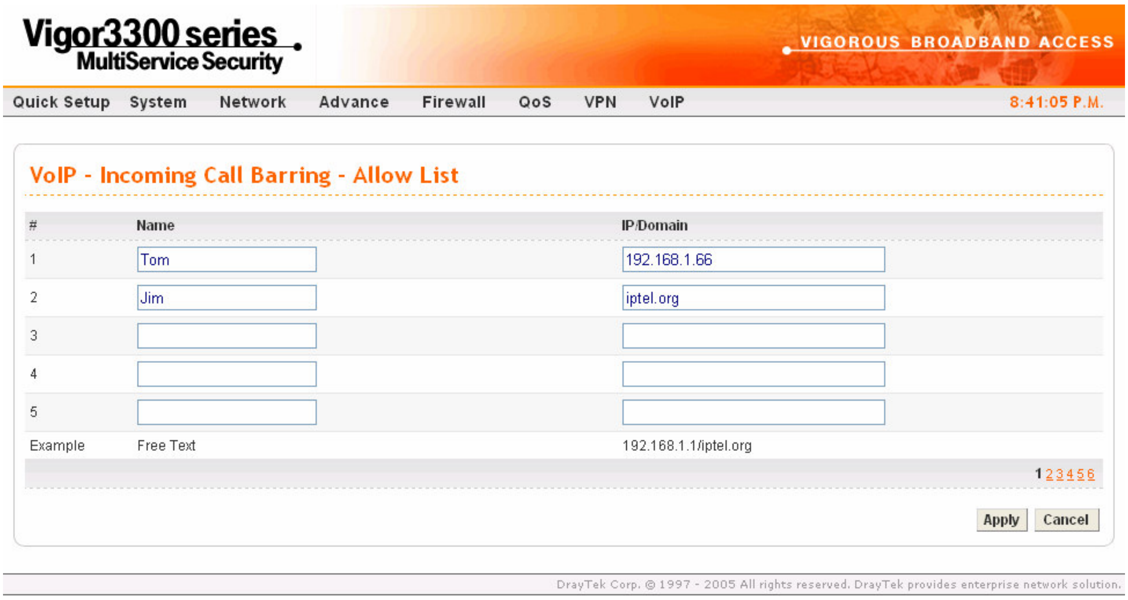
Figure 9-16. Set incoming call barring configuration

Barring Class	There are five options as below. ● **Allow all incoming calls.** ● **Allow only calls from allow list.** ● **Allow only calls from speed dial entries** ● **Deny only calls from deny list.** ● **Deny all incoming calls.**

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	The range to be checked. The default value is from 1 to 150.

9.10.2 Allow List[4]

Click the **Allow List** option to bring up the following web page as Figure 9-17.



VoIP - Incoming Call Barring - Allow List

#	Name	IP/Domain
1	Tom	192.168.1.66
2	Jim	iptel.org
3		
4		
5		
Example	Free Text	192.168.1.1/iptel.org

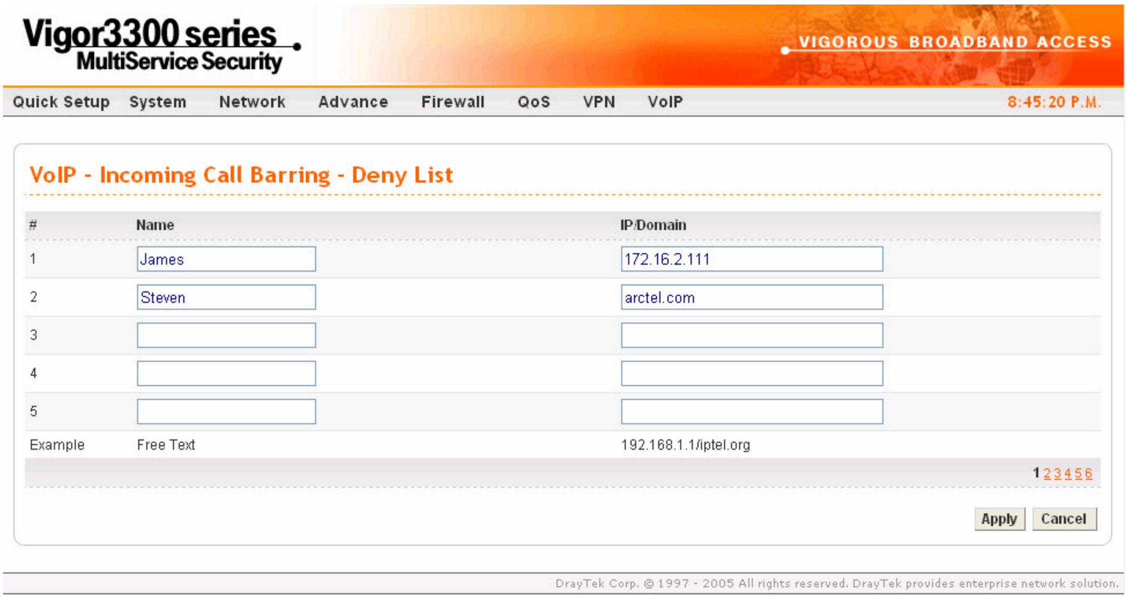
Figure 9-17. Allow list configuration

[4] ***The Vigor3300 series supports up to 30 entries in the AllowLlist table.***

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.

9.10.3 Deny List[5]

Click **Deny List** to bring up the following web page as Figure 9-18.



VoIP - Incoming Call Barring - Deny List

#	Name	IP/Domain
1	James	172.16.2.111
2	Steven	arctel.com
3		
4		
5		
Example	Free Text	192.168.1.1/iptel.org

Figure 9-18. Deny list configuration

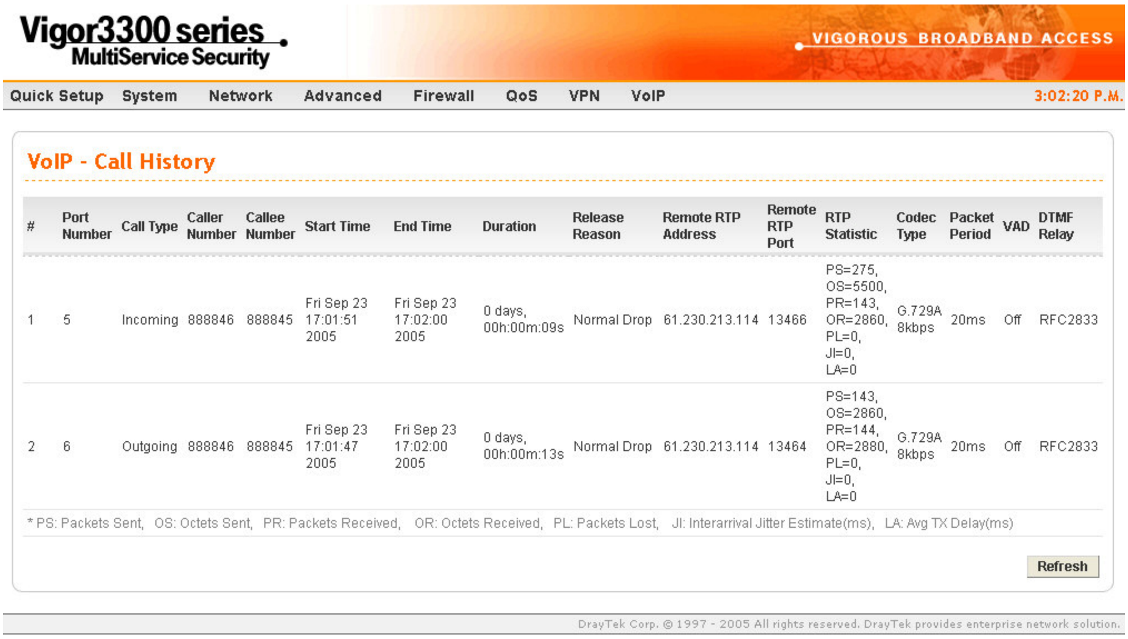
[5] *Note*

Vigor3300 series of router support up to 30 entries in deny list table.

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.

9.11 Call History

Click **VoIP->Call History** to bring up the connection history status page in Figure 9-19**.** Click "**Refresh**" to get the latest status information for these VoIP phones. The 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)

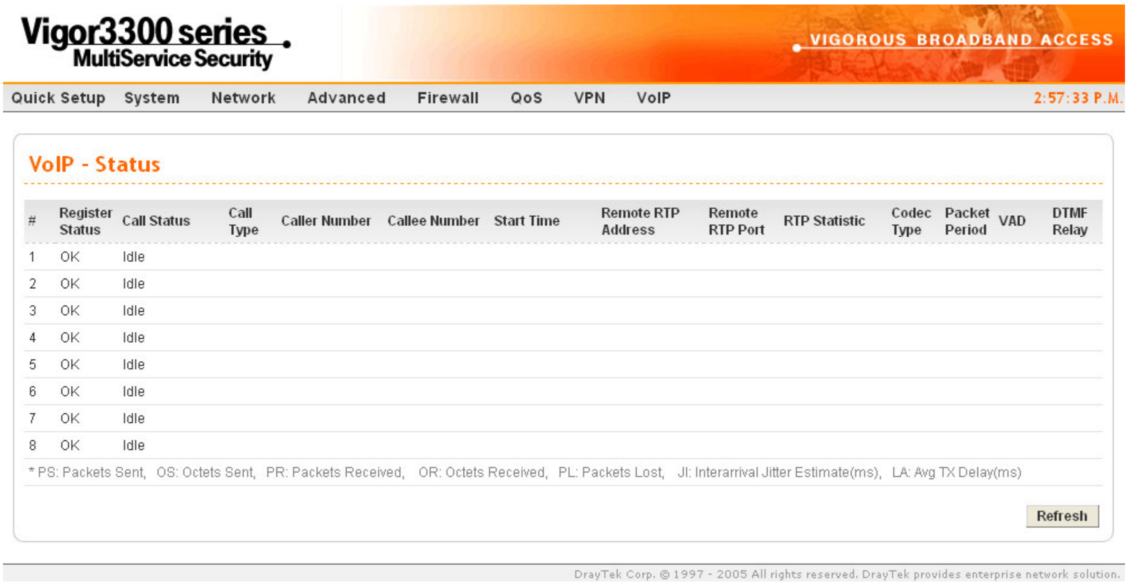
Refresh
DrayTek Corp. © 1997 - 2005 All rights reserved. DrayTek provides enterprise network solution.

Figure 9-19. VoIP call history log

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.
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.

9.12 Status

Click **Status** to bring up the connection status page as Figure 9-20**.**



VoIP - Status

#	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	OK	Idle											
2	OK	Idle											
3	OK	Idle											
4	OK	Idle											
5	OK	Idle											
6	OK	Idle											
7	OK	Idle											
8	OK	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)

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

Figure 9-20. VoIP status

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.

Click “**Refresh**” to get new status information for these VoIP phones. The page refreshes automatically every 10 seconds.

CHAPTER 10

Quality of Service Setup

This chapter shows how to configure the capabilities of the QoS facility and uses the following setup link on the Main Menu to configure the QoS control function.

This chapter is divided into the following sections.

- Section 10.1: Introduction
- Section 10.2: Incoming/outgoing Class Setup
- Section 10.3: Incoming/outgoing Class Filter Setup

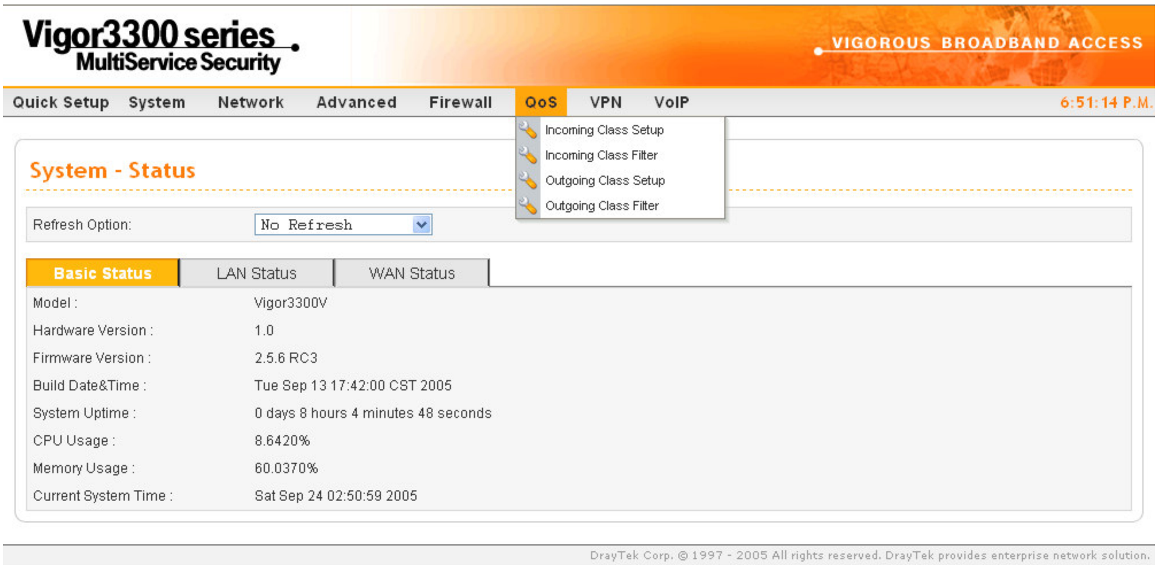
10.1 Introduction

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 theQoS-guaranteed control module.

In the **QoS** group, Figure 10-1 illustrates the functions of **QoS** option.

The QoS function handles incoming and outgoing classes independently. Users can configure incoming or outgoing separately without any impact on the other.

Click the **QoS** option to bring up the QoS Setup menu as Figure 10-1.



System - Status

Refresh Option: No Refresh

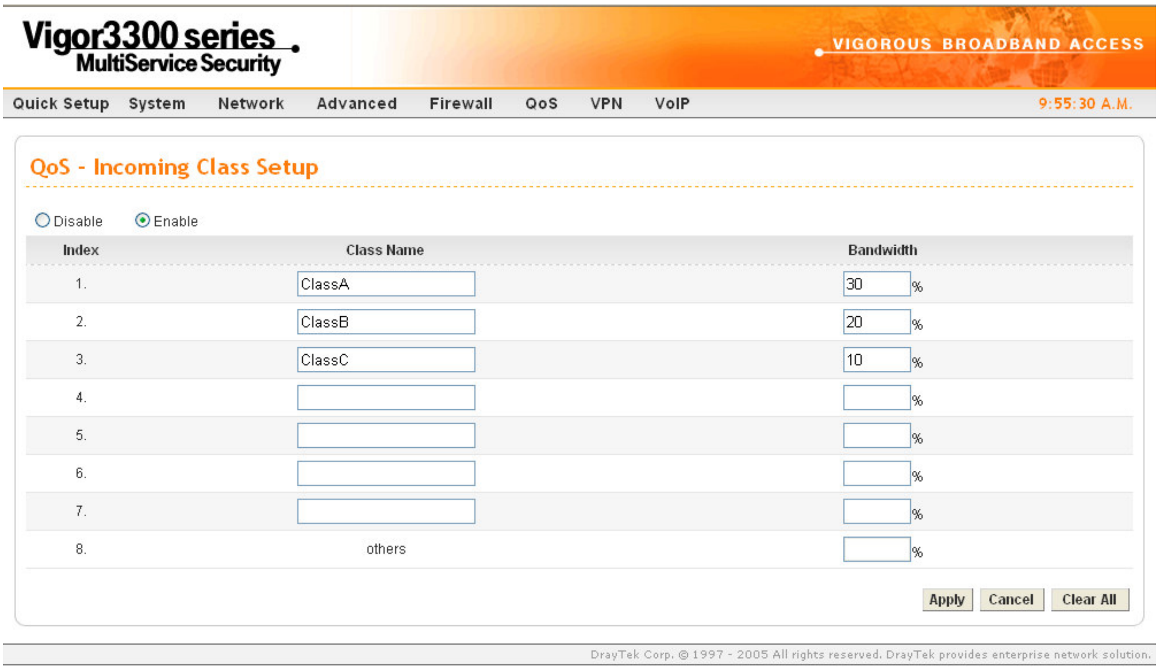
Model :	Vigor3300V
Hardware Version :	1.0
Firmware Version :	2.5.6 RC3
Build Date&Time :	Tue Sep 13 17:42:00 CST 2005
System Uptime :	0 days 8 hours 4 minutes 48 seconds
CPU Usage :	8.6420%
Memory Usage :	60.0370%
Current System Time :	Sat Sep 24 02:50:59 2005

Figure 10-1. The QoS menu

10.2 Incoming/Outgoing Class Setup

This section describes how to configure incoming/outgoing classes.

Click **Incoming Class Setup** to see the following setup page as Figure 10-2.


Vigor3300 series
MultiService Security
VIGOROUS BROADBAND ACCESS
Quick Setup
System
Network
Advanced
Firewall
QoS
VPN
VoIP
9:55:30 A.M.
Apply
Cancel
Clear All
DrayTek Corp. © 1997 - 2005 All rights reserved. DrayTek provides enterprise network solution.

QoS - Incoming Class Setup

○ Disable ● Enable

Index	Class Name	Bandwidth
1.	ClassA	30 %
2.	ClassB	20 %
3.	ClassC	10 %
4.		%
5.		%
6.		%
7.		%
8.	others	%

Figure 10-2. The QoS class configuration

Status	**Enable** or **Disable** this function.
Index	The number for each queue.
Class Name	The name for each queue.
Bandwidth	The usage percentage for each queue.

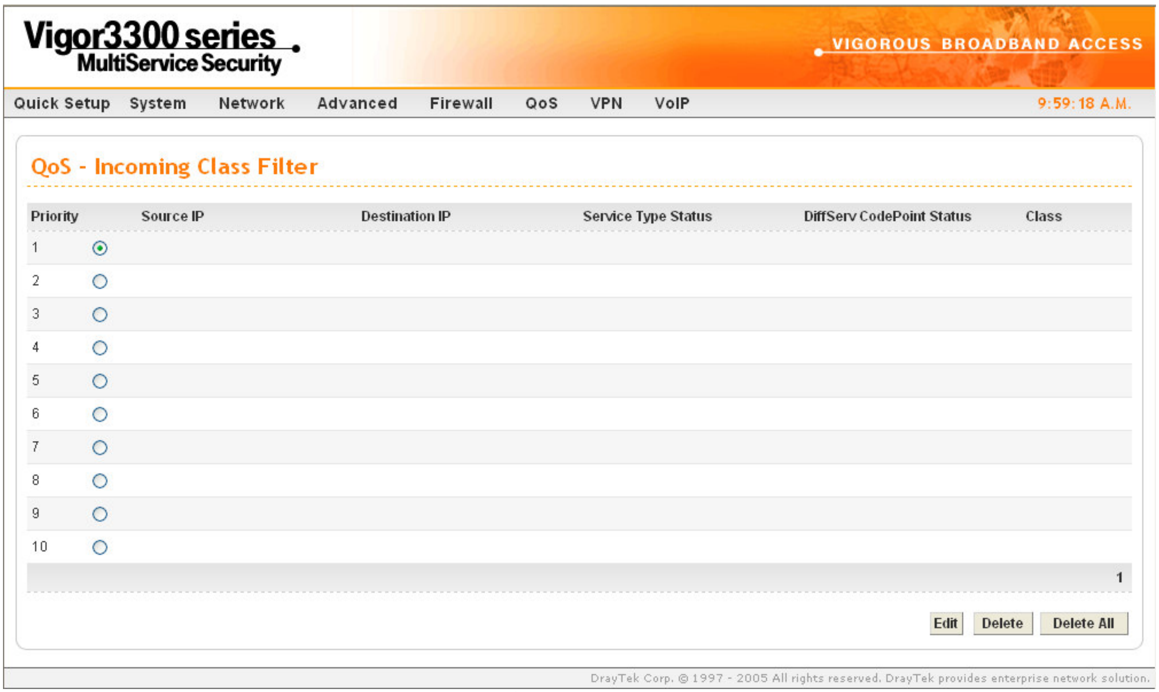
There are eight queues that can be configured. The total sum of bandwidth has to be 100 percent for all configured queues. Any leftover bandwidth is assigned to eight queues to meet 100 percent totally.

Click **Apply** to apply these settings.

10.3 Incoming/Outgoing Class Filter Setup

This section describes how to configure each queue as below.

Click **Incoming Class Filter** to see the following setup page as Figure10-3.


Vigor3300 series
MultiService Security
VIGOROUS BROADBAND ACCESS
Quick Setup
System
Network
Advanced
Firewall
QoS
VPN
VoIP
9:59:18 A.M.

QoS - Incoming Class Filter

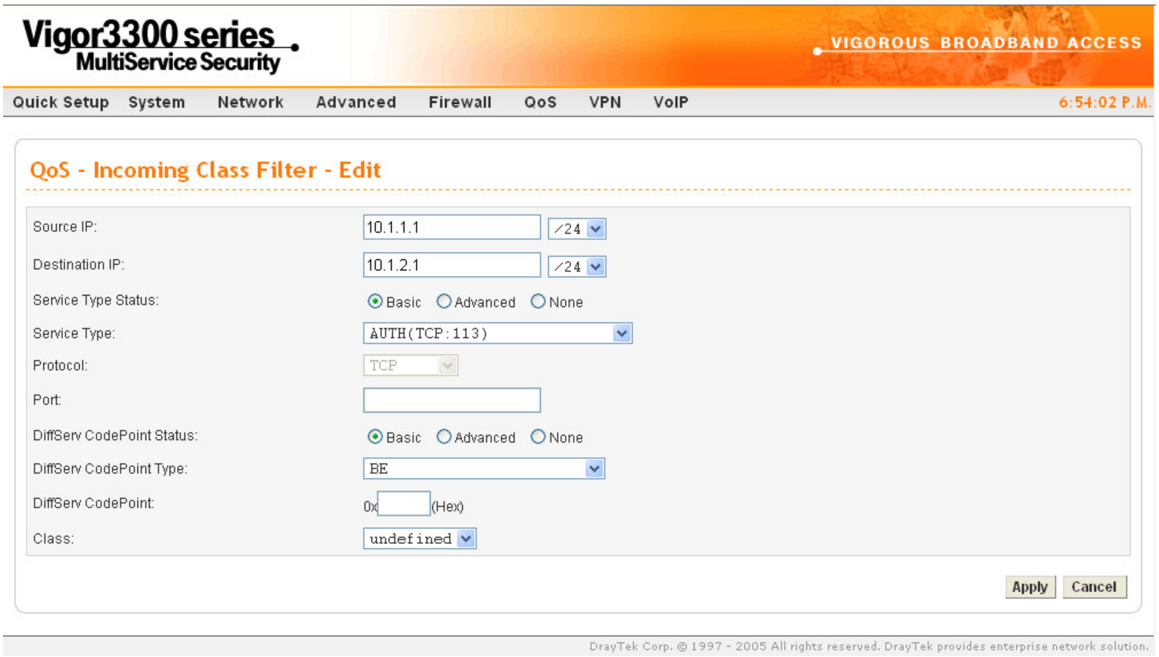
Priority		Source IP	Destination IP	Service Type Status	DiffServ CodePoint Status	Class
1	●					
2	○					
3	○					
4	○					
5	○					
6	○					
7	○					
8	○					
9	○					
10	○					

1

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

Figure 10-3. Class filter configuration

Click **Edit** to bring up the following page and edit filter conditions to be applied on the specific queue in Figure 10-4.


Vigor3300 series
MultiService Security
VIGOROUS BROADBAND ACCESS
Quick Setup
System
Network
Advanced
Firewall
QoS
VPN
VoIP
6:54:02 P.M.
Apply
Cancel
DrayTek Corp. © 1997 - 2005 All rights reserved. DrayTek provides enterprise network solution.

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: AUTH(TCP:113)
Protocol: TCP
Port:
DiffServ CodePoint Status: ● Basic ○ Advanced ○ None
DiffServ CodePoint Type: BE
DiffServ CodePoint: 0x (Hex)
Class: undefined

Figure 10-4. Edit incoming class filter

Source IP	The source IP address with subnet mask value to be applied.
Destination IP	The destination IP address with subnet mask value to be applied.
Service Type Status	There are three options: ***Basic –*** The **Service Type** field can be configured. ***Advanced –*** The **Protocol** and **Port** fields can be configured. ***None –*** No fields need to be configured.
Service Type	The service type to be used. There are thirty-five service types supported.
Protocol	There are three options: **TCP**, **UDP**, and **TCP/UDP**.

APPENDIX A

PC Web Browser Setup

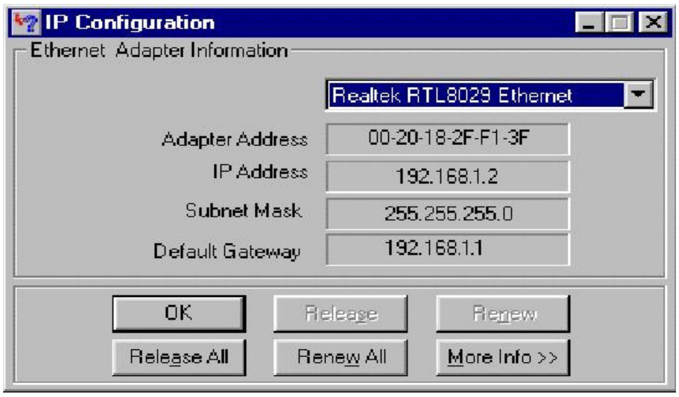
The chapter describes the setup of PC to configure Vigor 3300. The setup items are including PC IP setting to communicate with Vigor 3300, Microsoft Web Browser version.

Part1-PCs/LAN communicating with Vigor 3300

1. Your PC should be connected to the router via an Ethernet (RJ45) cable. Then, the appropriate Ethernet switch LED (1/2/3/4) will light up (green = 100Mbps, off = 10Mbps). The Vigor3300's Ethernet ports are auto-sensing to speed and cable configuration. It can automatically adjust crossover/straight or uplink/normal connections.

2. Every device on your network must have a unique IP address. The router's DHCP server facility will automatically allocate these to your client PCs, assuming that they are set to obtain their details automatically. The default IP address of Vigor 3300 is 192.168.1.1 and all local PCs must have an IP address within the same 'subnet', e.g. IP address should be 192.168.1.10 or 192.168.1.254 for local PCs.

3. Check that the PC is actually getting the IP details from Vigor 3300. You can check this from the winipcfg utility. To run this, press the Windows Start button, select 'Run', type **winipcfg** and press OK.



IP Configuration

Ethernet Adapter Information

Realtek RTL8029 Ethernet

Adapter Address: 00-20-18-2F-F1-3F

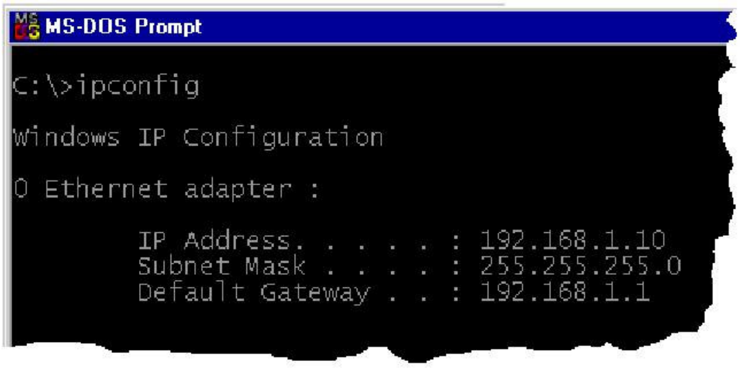
IP Address: 192.168.1.2

Subnet Mask: 255.255.255.0

Default Gateway: 192.168.1.1

In the above example, the PC has been given an IP address of 192.168.1.2 and has been told that the default gateway (router) is at 192.168.1.1. Ensure that your network card is selected in the top pulldown box (not 'PPP Adaptor'). If you click 'Release', the details should be cleared 'Renew' should get them back.

If you do not have the winipcfg utility, you can try **ipconfig.exe** from the MS-DOS command prompt.

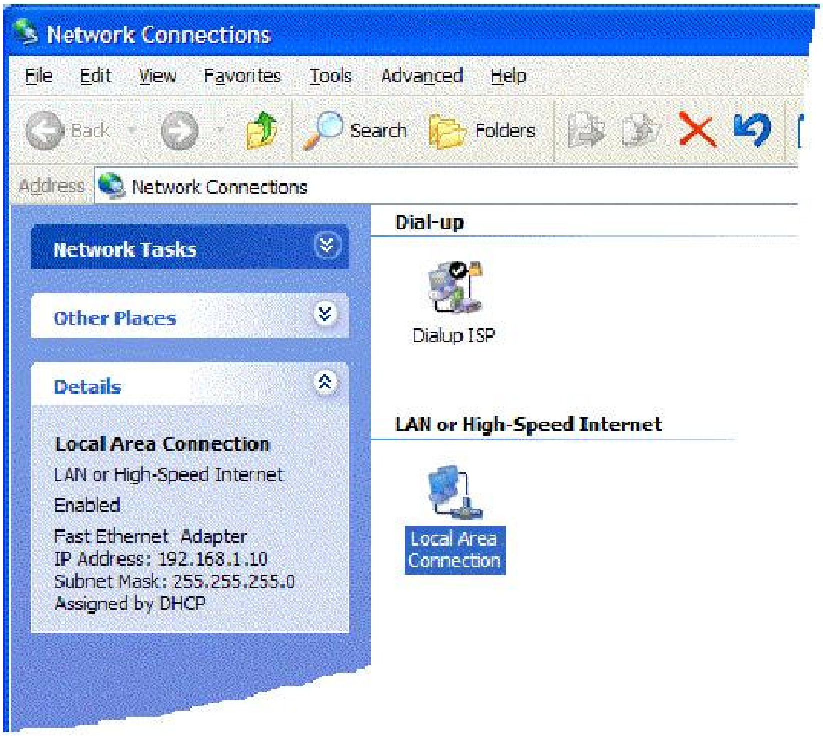


```
C:\>ipconfig

Windows IP Configuration

0 Ethernet adapter :

        IP Address. . . . . : 192.168.1.10
        Subnet Mask . . . . : 255.255.255.0
        Default Gateway . . : 192.168.1.1
```

Winipcfg is not supplied as standard with Windows 2000.

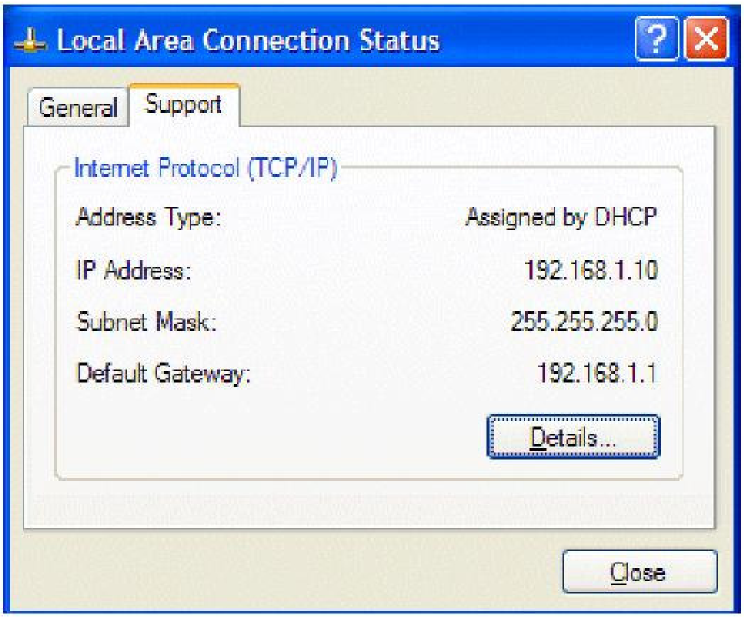
4. In **Windows XP**, you can check your PC's current IP address by opening Network Connections; if you select the LAN connection, the settings will appear on the left of the screen–like the example below. Here we can see that the Network connection is

enabled and that the PC has obtained an IP address of 192.168.1.10.



Local Area Connection
LAN or High-Speed Internet
Enabled
Fast Ethernet Adapter
IP Address: 192.168.1.10
Subnet Mask: 255.255.255.0
Assigned by DHCP

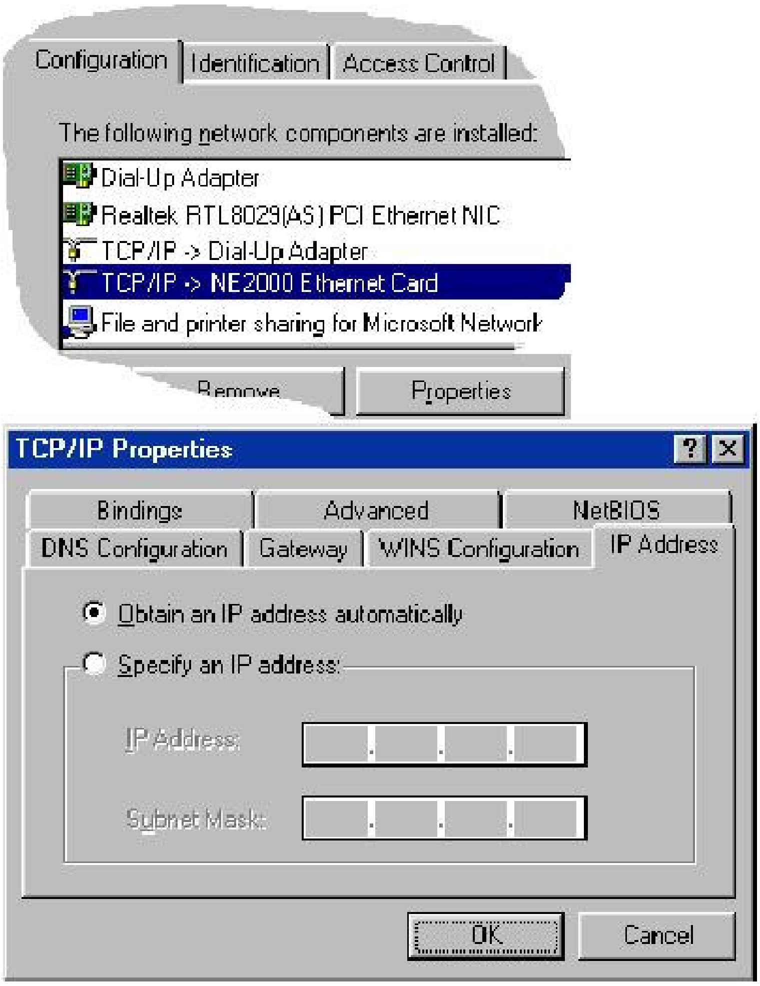
You can obtain the same information by right clicking on the Network Connection's icon in the system tray and selecting 'Status'.



Internet Protocol (TCP/IP)

Address Type: Assigned by DHCP
IP Address: 192.168.1.10
Subnet Mask: 255.255.255.0
Default Gateway: 192.168.1.1

5. If your PC is not getting an IP address (as described in previous sections), you need to check that your PC's TCP/IP settings are correct. As mentioned earlier, we recommend that you make use of the router's DHCP facility, which is enabled by default. From Windows98/Me Control Panel/Network, check your TCP/IP Properties are like this:



The following network components are installed:

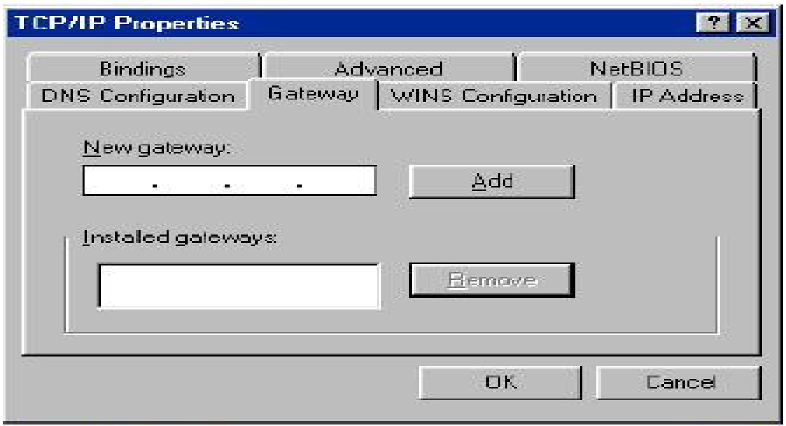
- Dial-Up Adapter
- Realtek RTL8029(AS) PCI Ethernet NIC
- TCP/IP -> Dial-Up Adapter
- TCP/IP -> NE2000 Ethernet Card
- File and printer sharing for Microsoft Network

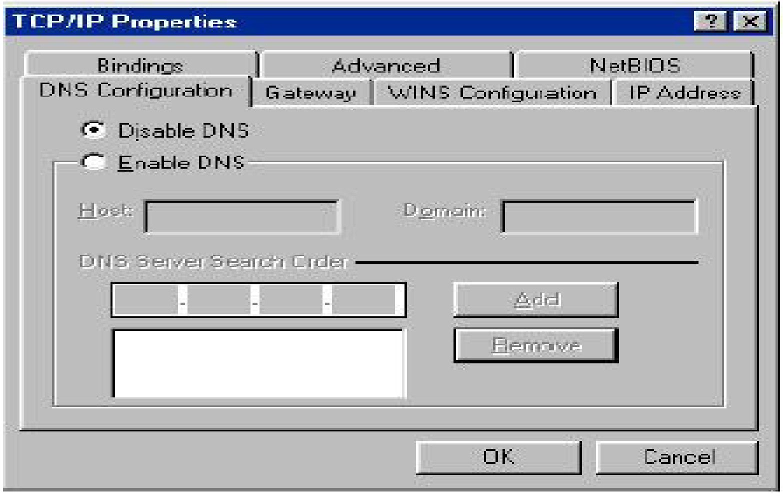
● Obtain an IP address automatically

○ Specify an IP address:

IP Address: . . .

Subnet Mask: . . .

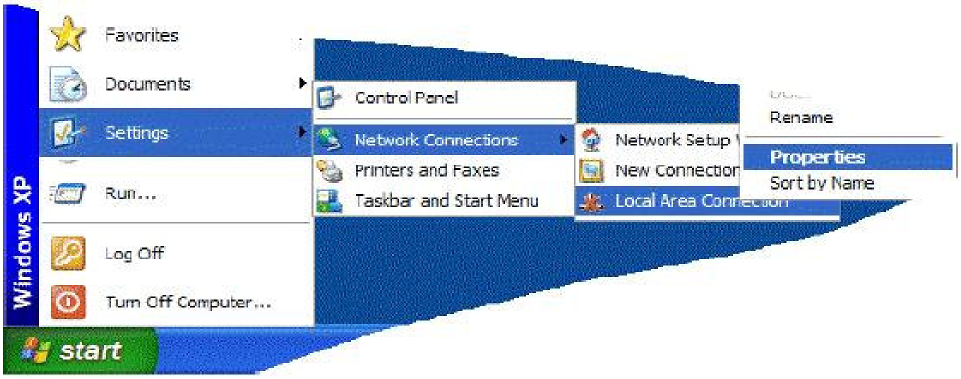




● Disable DNS

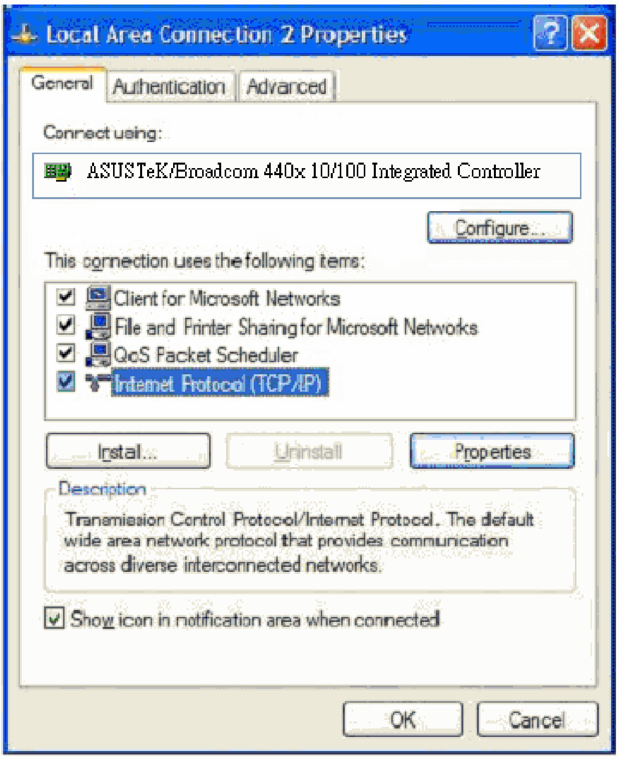
○ Enable DNS

6. For **Windows XP**, the LAN/Network card setup is very similar to Windows98/Me, but the screens look a little different. Once your network card (Ethernet 10/100BaseT) is installed, it may be automatically set up correctly be default. You can check the settings from your PC's 'Network Connections' menu.



Select the TCP/IP protocol as shown below and click on 'properties' and then check that.

Obtain IP address & DNS Automatically are both selected:


Local Area Connection 2 Properties

General | Authentication | Advanced

Connect using:

ASUSTeK/Broadcom 440x 10/100 Integrated Controller

Configure...

This connection uses the following items:

☑ Client for Microsoft Networks
☑ File and Printer Sharing for Microsoft Networks
☑ QoS Packet Scheduler
☑ Internet Protocol (TCP/IP)

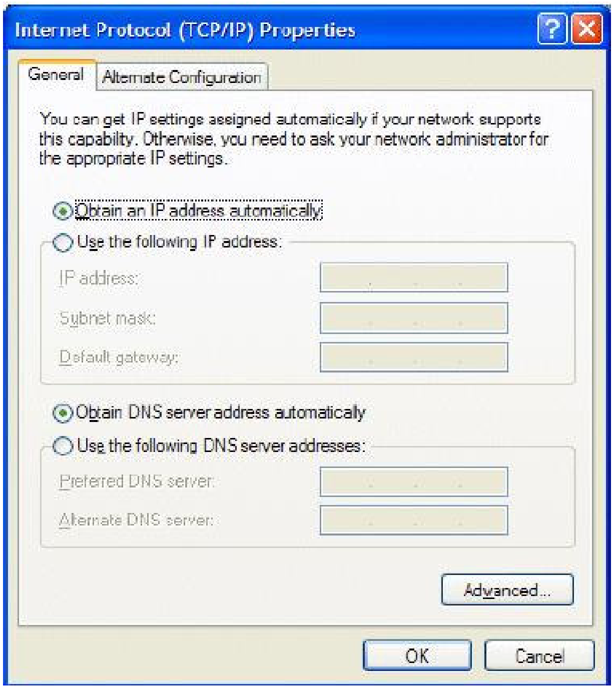
Install... | Uninstall | Properties

Description

Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

☑ Show icon in notification area when connected

OK | Cancel



Internet Protocol (TCP/IP) Properties

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

● Obtain an IP address automatically

○ Use the following IP address:

IP address:

Subnet mask:

Default gateway:

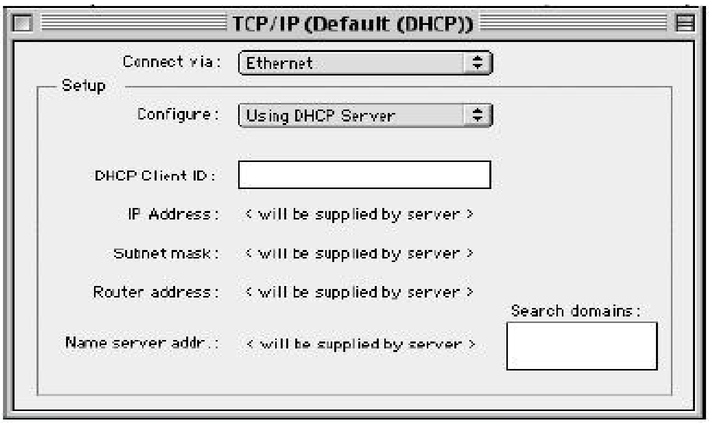
● Obtain DNS server address automatically

○ Use the following DNS server addresses:

Preferred DNS server:

Alternate DNS server:

7. For **Apple MacOS**, to select and enable the DHCP client facility on your computer, the TCP/IP control panel should be set like this for MacOS 8/9 and X respectively.



TCP/IP (Default (DHCP))

Connect via: Ethernet

Setup

Configure: Using DHCP Server

DHCP Client ID:

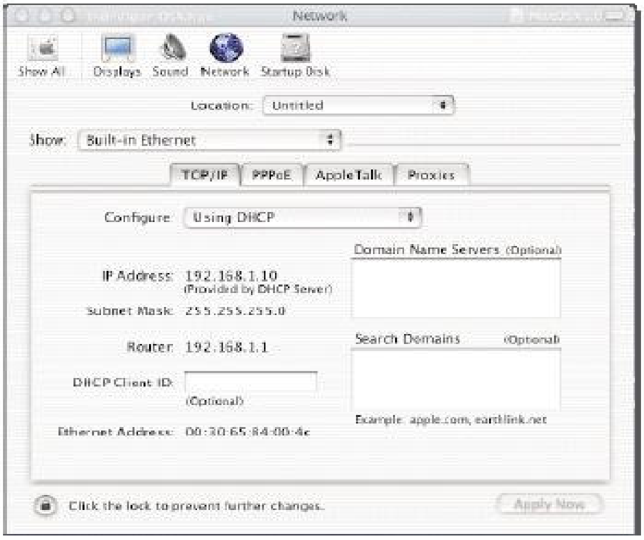
IP Address: < will be supplied by server >

Subnet mask: < will be supplied by server >

Router address: < will be supplied by server >

Name server addr.: < will be supplied by server >

Search domains:



Location: Untitled

Show: Built-in Ethernet

TCP/IP | PPPoE | AppleTalk | Proxies

Configure: Using DHCP

IP Address: 192.168.1.10 (Provided by DHCP Server)

Subnet Mask: 255.255.255.0

Router: 192.168.1.1

DHCP Client ID: (Optional)

Ethernet Address: 00:30:65:84:00:4c

Domain Name Servers (Optional)

Search Domains (Optional)

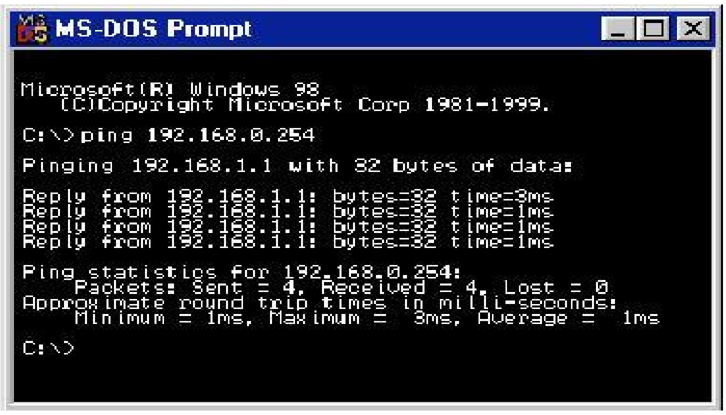
Example: apple.com, earthlink.net

Click the lock to prevent further changes.

Once IP addresses are assigned by Vigor 3300, then they will appear on the above screen.

8. If you are **not** using DHCP (i.e. 'Obtain IP Address Automatically' as shown above) then you must manually give your PCs an IP address, This address must be within the same subnet as the router's own LAN IP address. This means that if the router is 192.168.1.1, then the other PCs must be numbered 192.168.1.nnn where 'nnn' is a number from 2 to 254. Additionally, each PC must have the 'Default Gateway' and "DNS Server Address" set to the router's IP address (192.168.1.1 unless you changed it.) None of this is necessary if you are using DHCP, hence it's recommended to rely on DHCP whenever possible.

9. To confirm the connectivity between your PC and the router, you can use the Windows ‘ping’ utility. This sends a small packet to the router, which the router sends back, to confirm the connectivity. From an MS-DOS prompt, enter ‘ping 19.168.1.1’ and you should get replies with a time in milliseconds (e.g. 12ms).

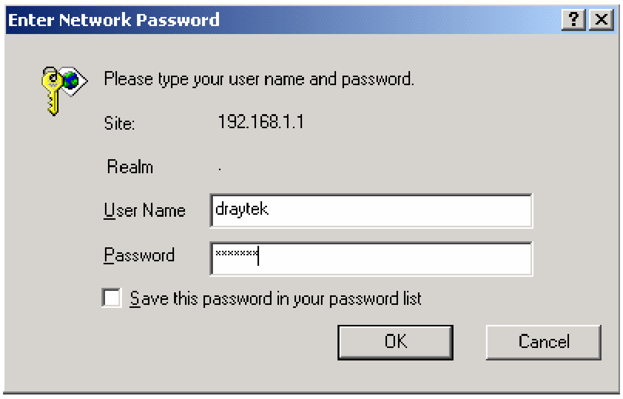


```
Microsoft(R) Windows 98
   (C)Copyright Microsoft Corp 1981-1999.

C:\>ping 192.168.0.254

Pinging 192.168.1.1 with 32 bytes of data:

Reply from 192.168.1.1: bytes=32 time=3ms
Reply from 192.168.1.1: bytes=32 time=1ms
Reply from 192.168.1.1: bytes=32 time=1ms
Reply from 192.168.1.1: bytes=32 time=1ms

Ping statistics for 192.168.0.254:
    Packets: Sent = 4, Received = 4, Lost = 0
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum =  3ms, Average =  1ms

C:\>
```

Part2-Setup and Check your Web Browser Version

10. The above checks will confirm that your PC and network are connected to the Vigor 3300 correctly, so you should be able to access the Vigor 3300’s Web Configuration interface. This is the main method for setting up, controlling and monitoring the router. Load your updated standard web browser (e.g. IE 6.0 or Netscape 7.1 is preferred.). You can go to www.microsoft.com ands then on **resources** field to choose **downloads** item. **Search for a Download** on **Product/ Technology** field to find **Internet Explore** software. You can choose newest update Internet Explore version e.g. Internet Explore 6.

11. Press bar and simply enter http://192.168.1.1 (that is the default IP of Vigor 3300). Enter login by user name and password. The factory default for username is “Draytek”, and password is “1234”, then click **OK**. The login message is shown as below.



Please type your user name and password.

Site: 192.168.1.1

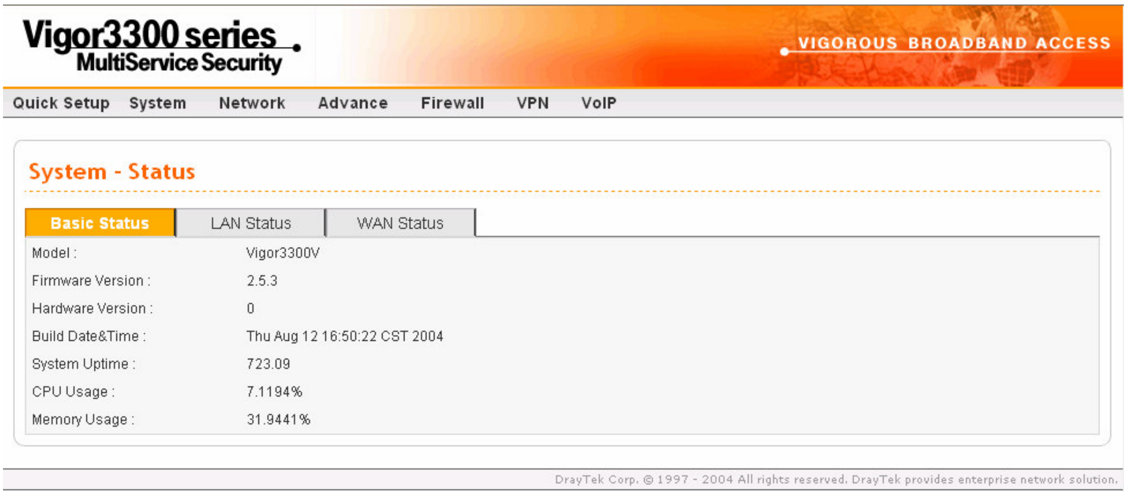
Realm .

User Name draytek

Password *******

☐ Save this password in your password list

Then, the main menu should appear as shown below.

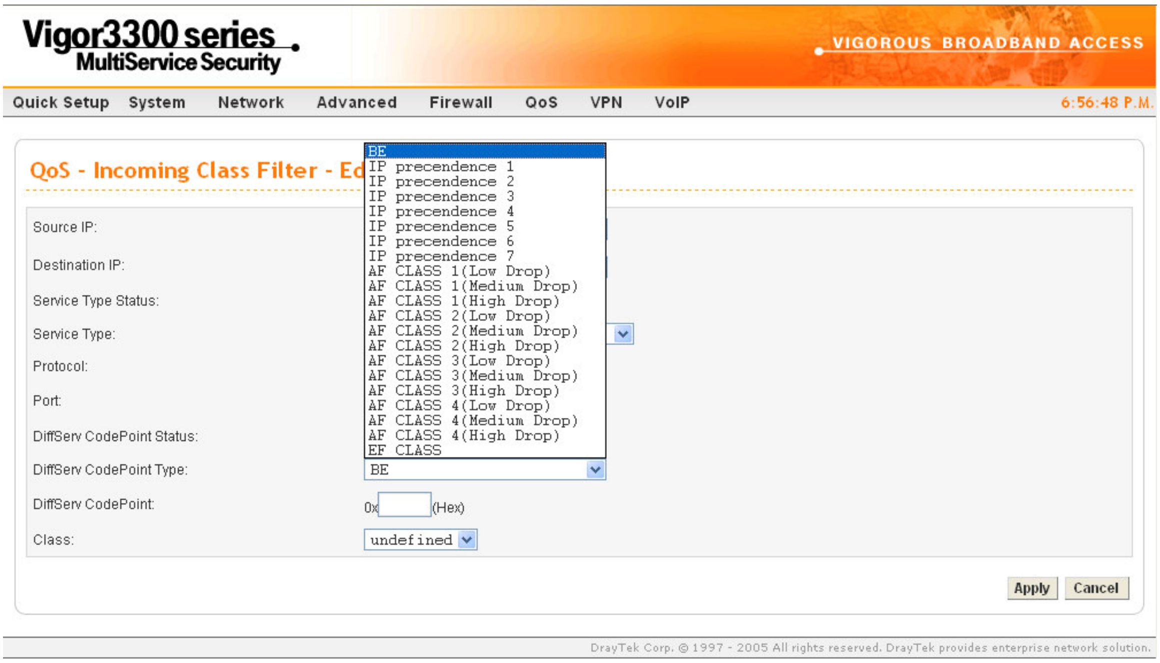


System - Status

Model :	Vigor3300V
Firmware Version :	2.5.3
Hardware Version :	0
Build Date&Time :	Thu Aug 12 16:50:22 CST 2004
System Uptime :	723.09
CPU Usage :	7.1194%
Memory Usage :	31.9441%

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

Port	The port number to be applied.
DiffServ CodePoint Status	There are three options: ***Basic*** **–** The **DiffServ CodePoint Type** field can be configured. ***Advanced*** **–** The **DiffServ CodePoint** field can be configured. ***None*** **–** No fields need to be configured.
DiffServ CodePoint Type	There are twenty-one types supported (Figure 10-5**).**
DiffServ CodePoint	The number (by hex mode) to be applied.
Class	The filtering conditions to be applied.



QoS - Incoming Class Filter - Ed

Source IP:

Destination IP:

Service Type Status:

Service Type:

Protocol:

Port:

DiffServ CodePoint Status:

DiffServ CodePoint Type: BE

```
BE
IP precendence 1
IP precendence 2
IP precendence 3
IP precendence 4
IP precendence 5
IP precendence 6
IP precendence 7
AF CLASS 1(Low Drop)
AF CLASS 1(Medium Drop)
AF CLASS 1(High Drop)
AF CLASS 2(Low Drop)
AF CLASS 2(Medium Drop)
AF CLASS 2(High Drop)
AF CLASS 3(Low Drop)
AF CLASS 3(Medium Drop)
AF CLASS 3(High Drop)
AF CLASS 4(Low Drop)
AF CLASS 4(Medium Drop)
AF CLASS 4(High Drop)
EF CLASS
```

DiffServ CodePoint: 0x (Hex)

Class: undefined

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

Figure 10-5. DiffServ CodePoint type list

Click **Apply** to apply these settings.