LevelOne

FBR-1415TX

Broadband Router

w/1USB+1 Parallel Printer Server

User`s Manual

Copyright

The contents of this publication may not be reproduced in any part or as a whole, stored, transcribed in an information retrieval system, translated into any language, or transmitted in any form or by any means, mechanical, magnetic, electronic, optical, photocopying, manual, or otherwise, without the prior written permission.

Trademarks

All product, company, brand names are trademarks or registered trademarks of their respective companies. They are used for identification purpose only. Specifications are subject to be changed without prior notice.

FCC Interference Statement

This equipment has been tested and found to comply with the limits for a Class B digital device pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against radio interference in a commercial environment. This equipment can generate, use and radiate radio frequency energy and, if not installed and used in accordance with the instructions in this manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause interference, in which case the user, at his own expense, will be required to take whatever measures are necessary to correct the interference.

CE Declaration of Conformity

This equipment complies with the requirements relating to electromagnetic compatibility, EN 55022/A1 Class B

.

The specification is subject to change without notice.

Table of Contents

CHAPTER 1 INTRODUCTION 5

FUNCTIONS AND FEATURES 5
PACKING LIST 7

CHAPTER 2 HARDWARE INSTALLATION 8

2.1 PANEL LAYOUT 8
2.2 PROCEDURE FOR HARDWARE INSTALLATION 10

CHAPTER 3 NETWORK SETTINGS AND SOFTWARE INSTALLATION 11

3.1 MAKE CORRECT NETWORK SETTINGS OF YOUR COMPUTER 11
3.2 INSTALL THE SOFTWARE INTO YOUR COMPUTERS 12

CHAPTER 4 CONFIGURING BROADBAND ROUTER 14

4.1 START-UP AND LOG IN 15
4.2 STATUS 16
4.3 WIZARD 17
4.4 BASIC SETTING 19
4.4.1 Primary Setup – WAN Type, Virtual Computers 19
4.5 FORWARDING RULES 25
4.5.1 Virtual Server 26
4.5.2 Special AP 27
4.5.3 Miscellaneous Items 28
4.6 SECURITY SETTINGS 29
4.6.1 Packet Filter 30
4.6.2 Domain Filter 35
4.6.3 URL Blocking 37
4.6.4 MAC Address Control 39
4.6.6 Miscellaneous Items 41
4.7 ADVANCED SETTINGS 43
4.7.1 System Time 44
4.7.2 System Log 45
4.7.3 Dynamic DNS 47
4.7.4 SNMP Setting 49
4.7.5 Routing Table 51
4.7.6 Schedule Rule 53
4.8 TOOLBOX 57

CHAPTER 5 PRINTER SERVER.....61

5.1 CONFIGURING ON WINDOWS 95/98 PLATFORMS 61
5.2 CONFIGURING ON WINDOWS NT PLATFORMS 64
5.3 CONFIGURING ON WINDOWS 2000 AND XP PLATFORMS.....65
5.4 CONFIGURING ON UNIX-LIKE BASED PLATFORMS 70
5.5 CONFIGURING ON APPLE PC 75

APPENDIX A TCP/IP CONFIGURATION FOR WINDOWS 95/98.....77

APPENDIX B RESET TO FACTORY DEFAULT.....83

RESET TO FACTORY DEFAULT.....83

Chapter 1 Introduction

Congratulations on your purchase of this outstanding LevelOne FBR-1415TX Broadband Router. This product is specifically designed for Small Office and Home Office needs. It provides a complete SOHO solution for Internet surfing, and is easy to configure and operate even for non-technical users. Instructions for installing and configuring this product can be found in this manual. Before you install and use this product, please read this manual carefully for fully exploiting the functions of this product.

Functions and Features

Router Basic functions

- **Broadband modem and NAT Router**
  Connects multiple computers to a broadband (cable or DSL) modem or an Ethernet router to surf the Internet.
- **Auto-sensing Ethernet Switch**
  Equipped with a 4-port auto-sensing Ethernet switch.
- **Printer sharing**
  Embedded a print server to allow all of the networked computers to share one printer.
  Built-in USB and parallel host to connect to USB or parallel printer for printer sharing
- **WAN type supported**
  The router supports some WAN types, Static ,Dynamic, PPPoE ,PPTP, and L2TP etc.
- **Firewall**
  All unwanted packets from outside intruders are blocked to protect your Intranet.
- **DHCP server supported**
  All of the networked computers can retrieve TCP/IP settings automatically from this product.
- **Web-based configuring**
  Configurable through any networked computer's web browser using Netscape or Internet Explorer.
- **Virtual Server supported**
  Enables you to expose WWW, FTP and other services on your LAN to be accessible to Internet users.
- **User-Definable Application Sensing Tunnel**
  User can define the attributes to support the special applications requiring multiple connections, like Internet gaming, video conferencing, Internet telephony and so on, then

this product can sense the application type and open multi-port tunnel for it.

- **DMZ Host supported**

  Lets a networked computer be fully exposed to the Internet; this function is used when special application sensing tunnel feature is insufficient to allow an application to function correctly.

- **Statistics of WAN Supported**

  Enables you to monitor inbound and outbound packets

Security functions

- **Packet filter supported**

  Packet Filter allows you to control access to a network by analyzing the incoming and outgoing packets and letting them pass or halting them based on the IP address of the source and destination.

- **Domain Filter Supported**

  Let you prevent users under this device from accessing specific URLs.

- **URL Blocking Supported**

  URL Blocking can block hundreds of websites connection by simply a **keyword**.

- **VPN Pass-through**

  The router supports vpn pass-through.

- **SPI Mode Supported**

  When SPI Mode is enabled, the router will check every incoming packet to detect if this packet is valid.

- **DoS Attack Detection Supported**

  When this feature is enabled, the router will detect and log the DoS attack comes from the Internet.

Advanced functions

- **System time Supported**

  Allow you to synchronize system time with network time server.

- **E-mail Alert Supported**

  The router can send its info by mail.

- **Dynamic dns Supported**

  At present,FBR-1415TX supports 3 DDNS servers.dyndns,TZO.com and dhs.org.

- **SNMP Supported**

  Because SNMP this function has many versions, anyway, the router supports V1 and V2c.

- **Routing Table Supported**

Now, the router supports static routing and two kinds of dynamic routing RIP1 and RIP2.

- **Schedule Rule supported**

  Customers can control some functions, like virtual server and packet filters when to access or block.

Other functions

- **UPNP (Universal Plug and Play)Supported**

  FBR-1415TX also supports this function. The applications: X-box, Msn Messenger.

Packing List

- FBR-1415TX
- Installation CD-ROM with user`s manual
- Power adapter
- CAT-5 cable
- QIG

Chapter 2 Hardware Installation

2.1 Panel Layout

2.1.1. Front Panel

Figure 2-1 Front Panel

LED:

LED	Function	Color	Status	Description
POWER	Power indication	Green	On	Power is being applied to this product.
STATUS	System status	Green	Blinking	This product is functioning properly.
WAN	WAN port activity	Green	On	The WAN port is linked.
			Blinking	The WAN port is sending or receiving data.
Reset	reset	--------	--------	To reset system settings to factory defaults
Link/Act. 1~4	Link status	Green	On	An active station is connected to the corresponding LAN port.
			Blinking	The corresponding LAN port is sending or receiving data.
10/100	Data Rate	Green	On	Data is transmitting in 100Mbps on the corresponding LAN port.
USB	USB port activity	Green	On	The USB printing port is linked.
			Blinking	The USB port is sending or receiving data.

※For details, please refer to Appendix B, Reset to factory default .

2.1.2. Rear Panel

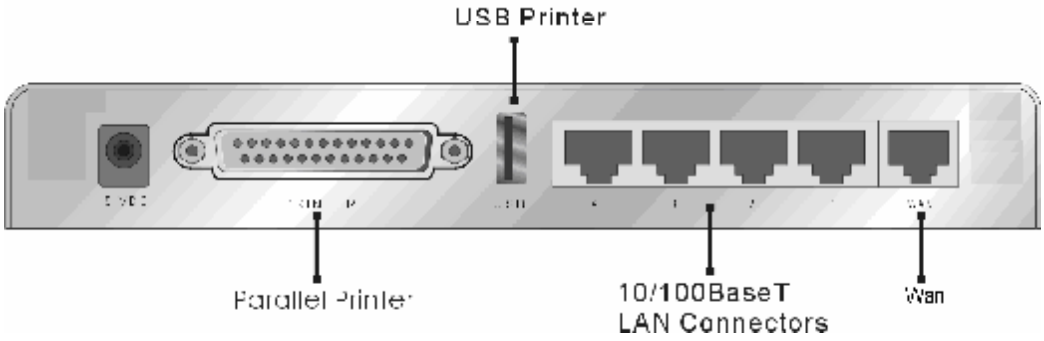


Figure 2-2 Rear Panel

Ports:

Port	Description
5VDC	Power inlet: DC 5V, 2A
WAN	The port where you will connect your cable (or DSL) modem or Ethernet router.
Port 1-4	The ports where you will connect networked computers and other devices.
USB	USB Ports for USB printer.
PRINTER	Printer Port

2.2 Procedure for Hardware Installation

1. Decide where to place your Broadband Router

You can place your FBR-1415TX on a desk or other flat surface, or you can mount it on a wall. For optimal performance, place your Broadband Router in the center of your office (or your home) in a location that is away from any potential source of interference, such as a metal wall or microwave oven. This location must be close to power and network connection.

2. Setup LAN connection

a. Wired LAN connection: connects an Ethernet cable from your computer's Ethernet port to one of the LAN ports of this product.

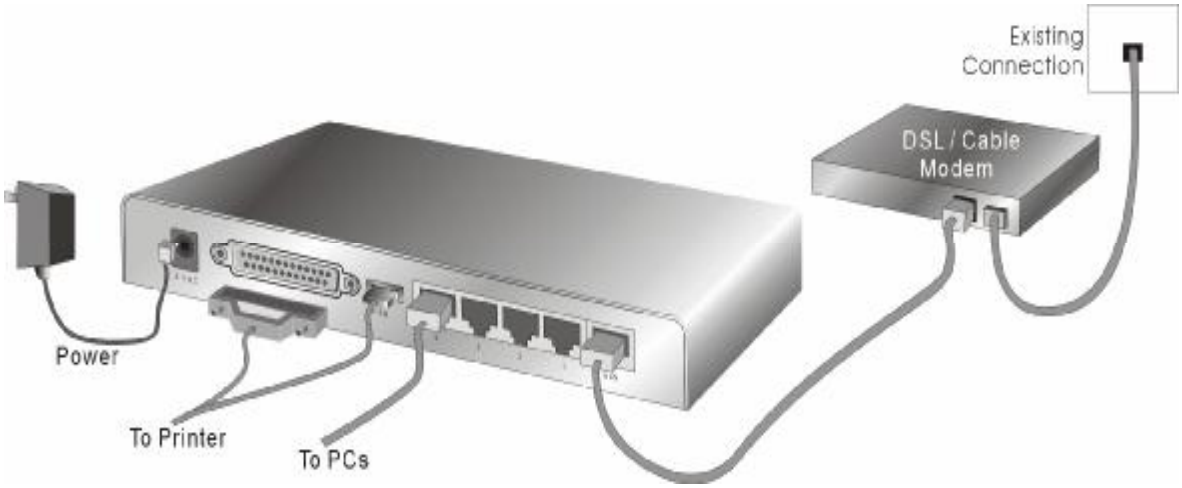


Figure 2-3 Setup of LAN and WAN connections for this product.

3. Setup WAN connection

Prepare an Ethernet cable for connecting this product to your cable/xDSL modem or Ethernet backbone. Figure 2-3 illustrates the WAN connection.

4. Connecting this product with your printer

Use the printer cable to connect your printer to the printer port of this product.

5. Power on

Connecting the power cord to power inlet and turning the power switch on, this product will automatically enter the self-test phase. When it is in the self-test phase, the STATUS Led will be lighted ON for about 10 seconds, and then STATUS will be flashed 3 times to indicate that the self-test operation has finished. Finally, the STATUS will be continuously flashed once per second to indicate that this product is in normal operation.

Chapter 3 Network Settings and Software Installation

To use this product correctly, you have to properly configure the network settings of your computers and install the attached setup program into your MS Windows platform (Windows 95/98/NT/2000).

3.1 Make Correct Network Settings of Your Computer

The default IP address of this product is 192.168.123.254, and the default subnet mask is 255.255.255.0. These addresses can be changed on your need, but the default values are used in this manual. If the TCP/IP environment of your computer has not yet been configured, you can refer to **Appendix A** to configure it. For example,

1. configure IP as 192.168.123.1, subnet mask as 255.255.255.0 and gateway as 192.168.123.254, or more easier,
2. configure your computers to load TCP/IP setting automatically, that is, via DHCP server of this product.

After installing the TCP/IP communication protocol, you can use the **ping** command to check if your computer has successfully connected to this product. The following example shows the ping procedure for Windows 95 platforms. First, execute the **ping** command

ping 192.168.123.254

If the following messages appear:

Pinging 192.168.123.254 with 32 bytes of data:

Reply from 192.168.123.254: bytes=32 time=2ms TTL=64

a communication link between your computer and this product has been successfully established. Otherwise, if you get the following messages,

Pinging 192.168.123.254 with 32 bytes of data:

Request timed out.

There must be something wrong in your installation procedure. You have to check the following items in sequence:

1. Is the Ethernet cable correctly connected between this product and your computer?

   Tip: The LAN LED of this product and the link LED of network card on your computer must be lighted.

2. Is the TCP/IP environment of your computers properly configured?

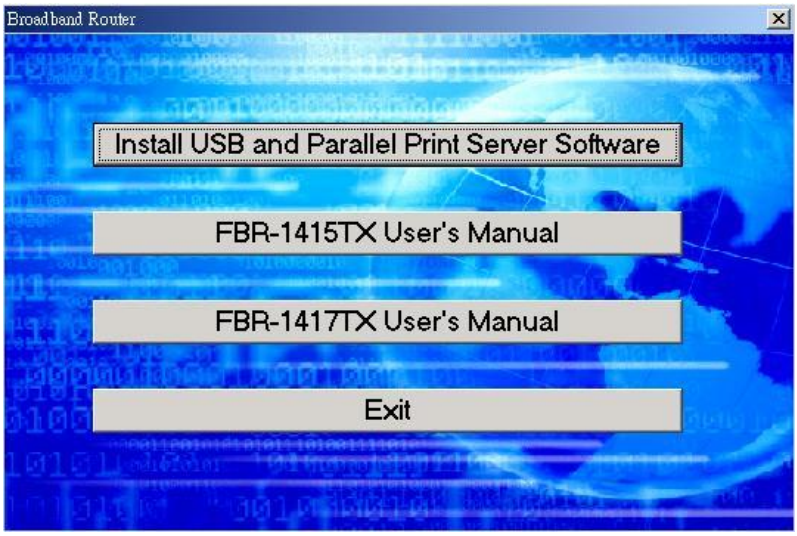
   Tip: If the IP address of this product is 192.168.123.254, the IP address of your computer must be 192.168.123.X and default gateway must be 192.168.123.254.

3.2 Install the Software into Your Computers

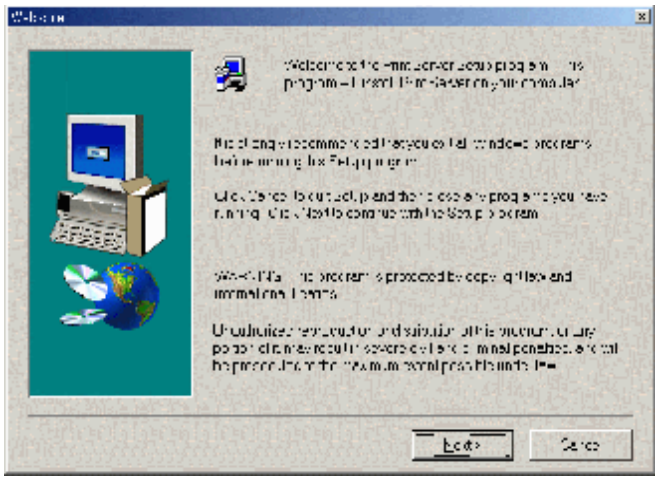
Skip this section if you do not want to use the print server function of this product.

Notice: If you are using Windows 2000/XP, please refer to **Chapter 5 Printer** - 5.3 Configuring on Windows 2000 and XP Platforms. It is not necessary to setup any program and the print-server can work.

Step 1: Insert the installation CD-ROM into the CD-ROM drive. The following window will be shown automatically. If it isn't, please run "install.exe" on the CD-ROM.

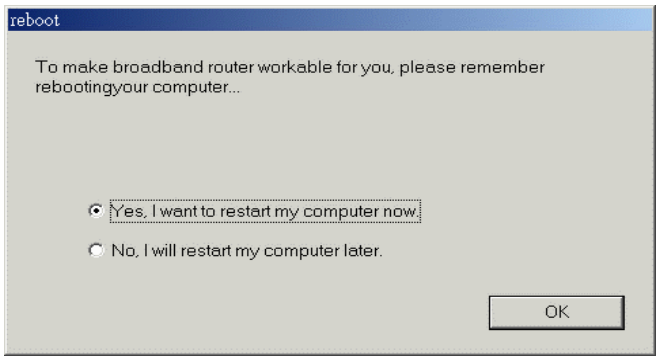


Step 2: Click on the **INSTALL USB and Parallel Print Server Software** button. Wait until the following **Welcome** dialog to appear, and click on the **Next** button.



Step 3: Select the destination folder and click on the **Next** button. Then, the setup program will begin to install the programs into the destination folder .Step 4: When the following window is displayed, click on the **Finish** button.

Select the item to restart the computer and then click the **OK** button to reboot your computer.

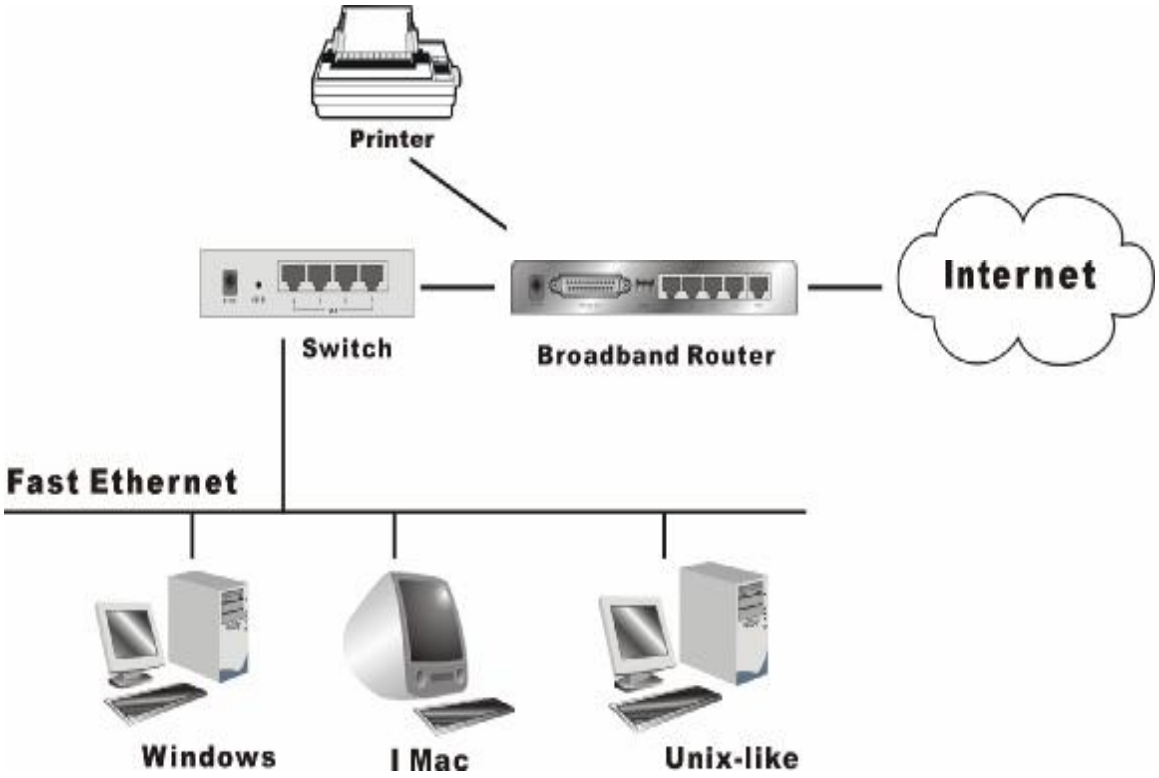


Step 4: After rebooting your computer, the software installation procedure is finished.

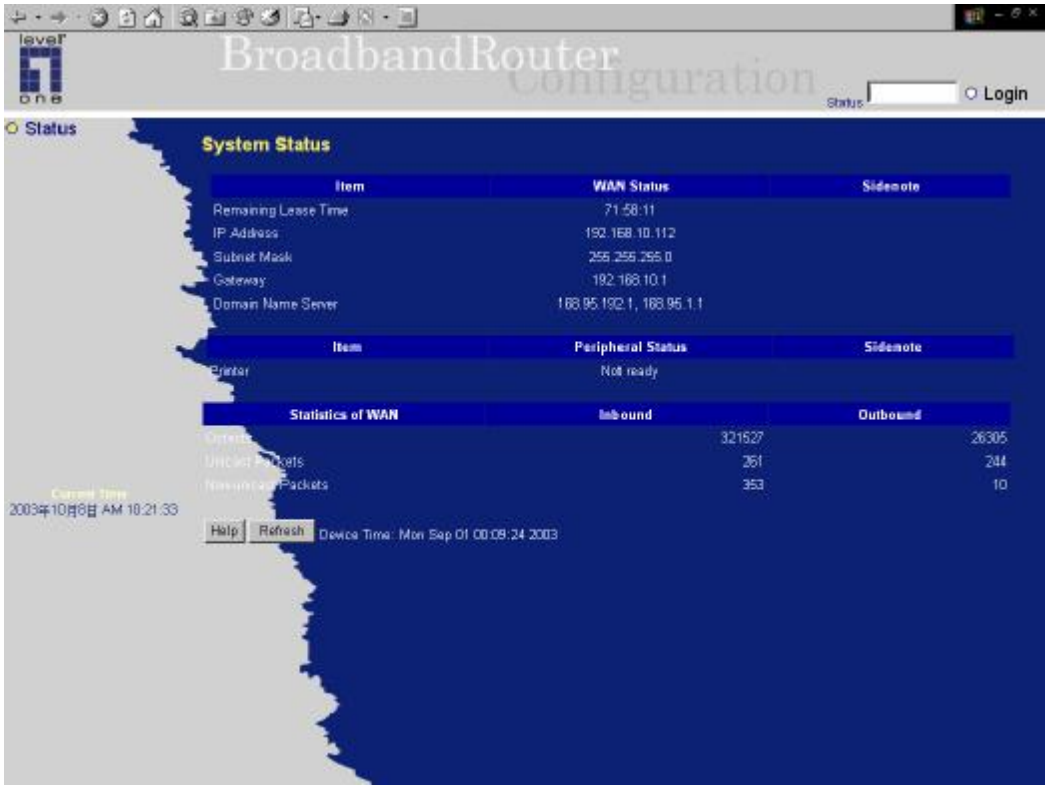
Now, you can configure the FBR-1415TX (refer to Chapter 4) and setup the Print Server (refer to Chapter 5).

Chapter 4 Configuring Broadband Router

This product provides Web based configuration scheme, that is, configuring by your Web browser, such as Netscape Communicator or Internet Explorer. This approach can be adopted in any MS Windows, Macintosh or UNIX based platforms.



4.1 Start-up and Log in

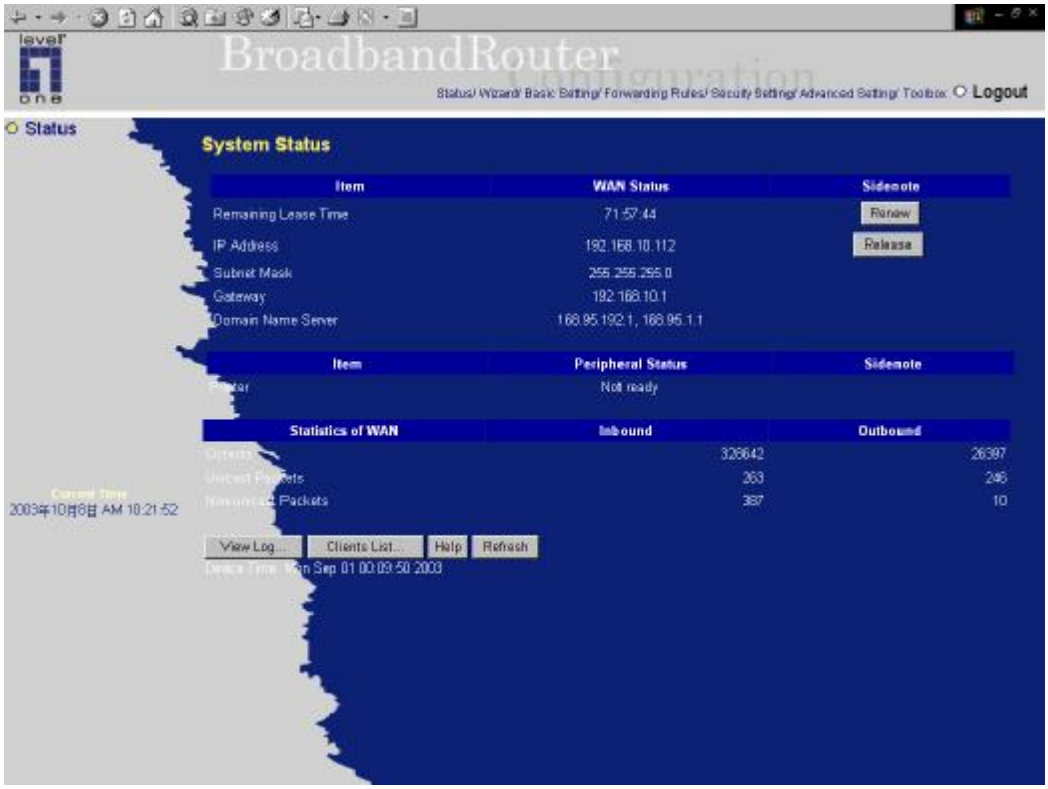


Activate your browser, and **disable the proxy** or **add the IP address of this product into the exceptions**. Then, type this product's IP address in the Location (for Netscape) or Address (for IE) field and press ENTER. For example: **http://192.168.123.254**.

After the connection is established, you will see the web user interface of this product. There are two appearances of web user interface: for general users and for system administrator.

To log in as an administrator, enter the system password (the factory setting is "**admin**") in the **System Password** field and click on the **Log in** button. If the password is correct, the web appearance will be changed into administrator configure mode. As listed in its main menu, there are several options for system administration.

4.2 Status



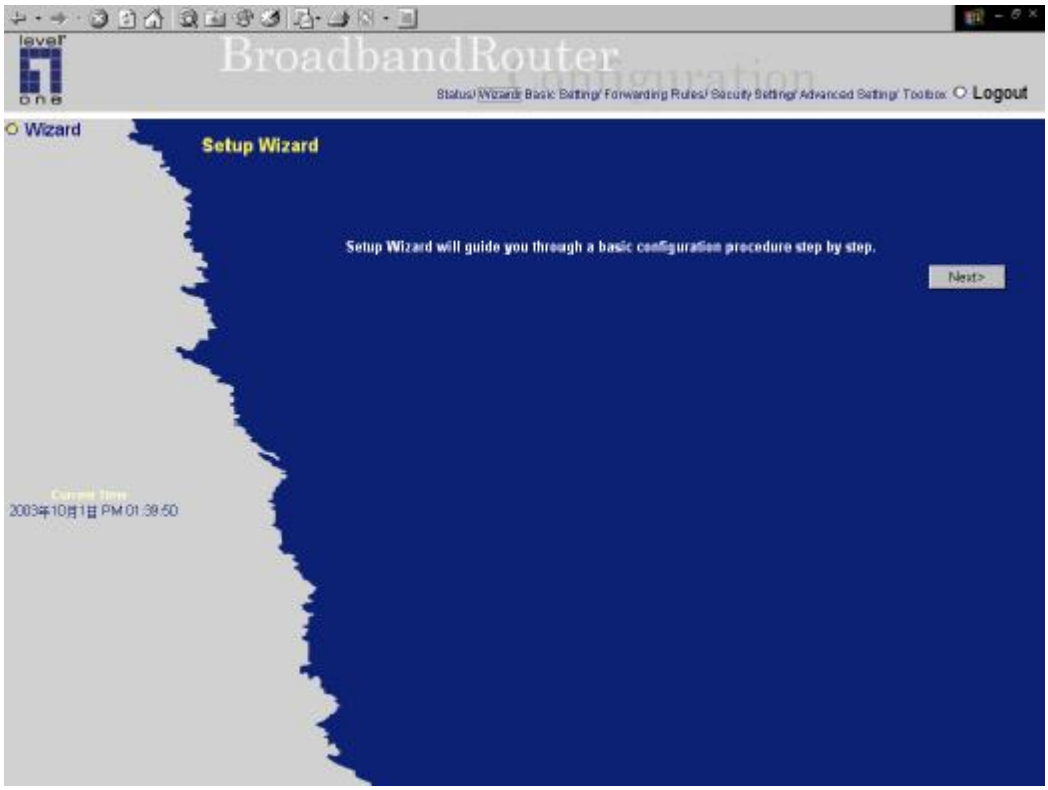
This option provides the function for observing this product's working status:

A. WAN Port Status.

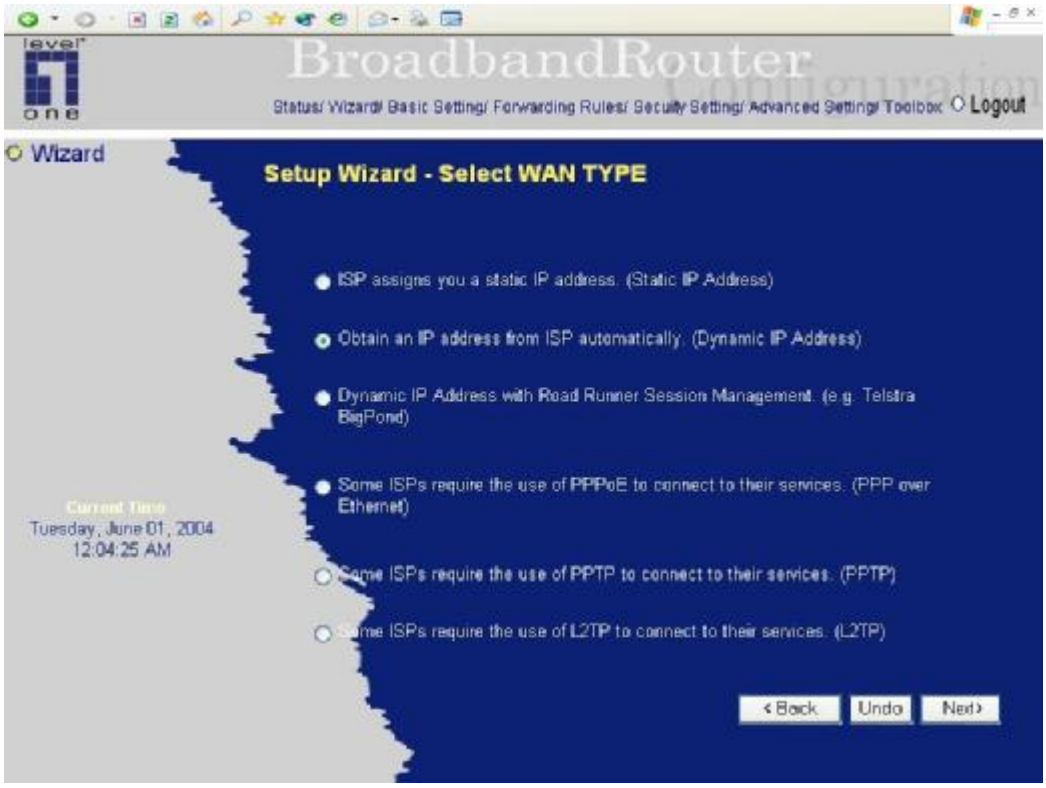
If the WAN port is assigned a dynamic IP, there may appear a "**Renew**" or "**Release**" button on the Sidenote column. You can click this button to renew or release IP manually.

B. Statistics of WAN: enables you to monitor inbound and outbound packets

4.3 Wizard

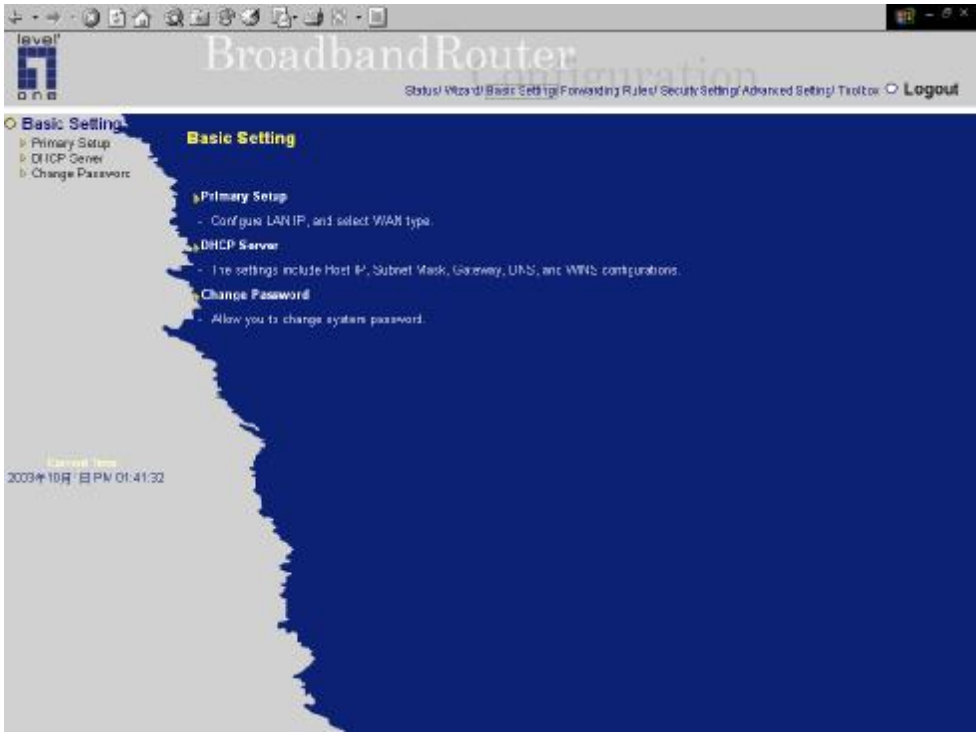


Setup Wizard will guide you through a basic configuration procedure step by step.Press **"Next >"**

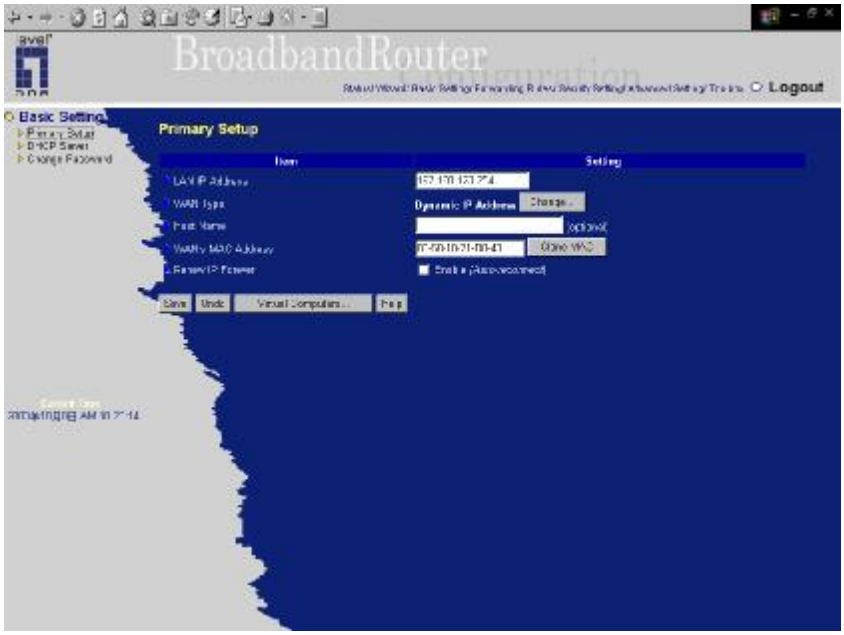


Setup Wizard - Select WAN Type: For detail settings, please refer to **4.4.1 primary setup.**

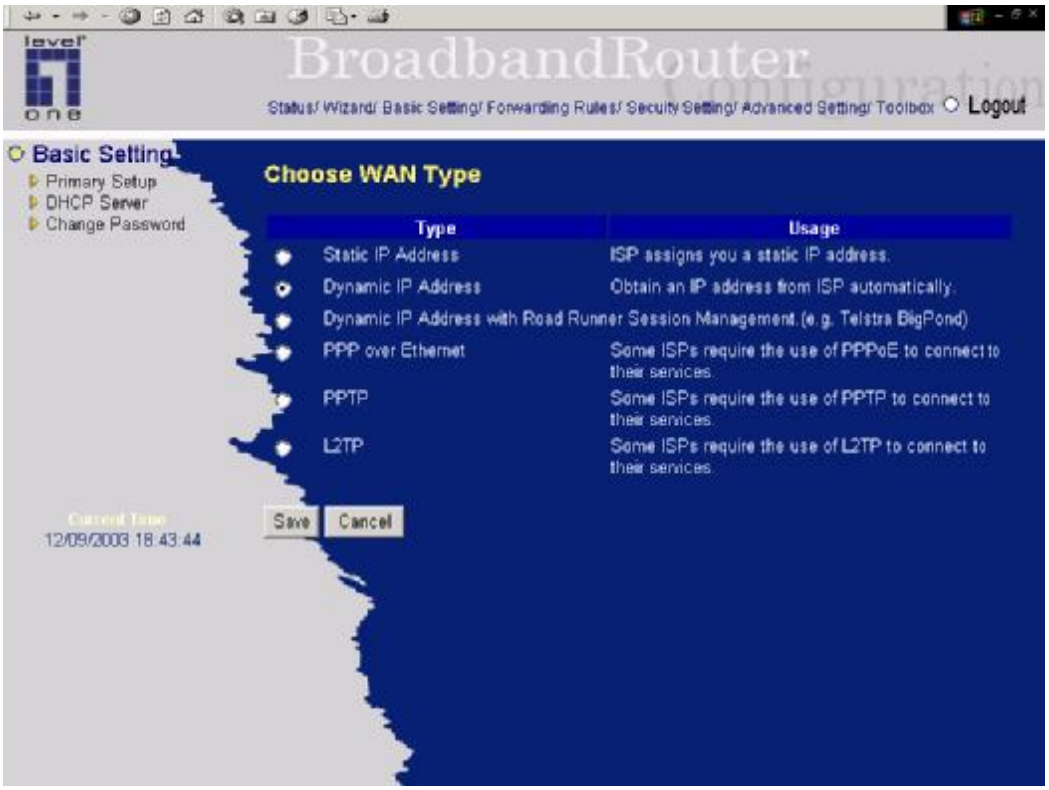
4.4 Basic Setting



4.4.1 Primary Setup – WAN Type, Virtual Computers



Press **"Change"**



This option is primary to enable this product to work properly. The setting items and the web appearance depend on the WAN type. Choose correct WAN type before you start.

1. **LAN IP Address**: the local IP address of this device. The computers on your network must use the LAN IP address of your product as their Default Gateway. You can change it if necessary.
2. **WAN Type**: WAN connection type of your ISP. You can click **Change** button to choose a correct one from the following four options:
   A. Static IP Address: ISP assigns you a static IP address.
   B. Dynamic IP Address: Obtain an IP address from ISP automatically.
   C. Dynamic IP Address with Road Runner Session Management.(e.g. Telstra BigPond)
   D. PPP over Ethernet: Some ISPs require the use of PPPoE to connect to their services.
   E. PPTP: Some ISPs require the use of PPTP to connect to their services.

4.4.1.1 Static IP Address

WAN IP Address, Subnet Mask, Gateway, Primary and Secondary DNS: enter the proper setting provided by your ISP.

4.4.1.2 Dynamic IP Address

1. Host Name: optional. Required by some ISPs, for example, @Home.
2. Renew IP Forever: this feature enables this product to renew your IP address automatically when

the lease time is expiring-- even when the system is idle.

4.4.1.3 Dynamic IP Address with Road Runner Session Management.(e.g. Telstra BigPond)

1. LAN IP Address is the IP address of this product. It must be the default gateway of your computers.
2. WAN Type is Dynamic IP Address. If the WAN type is not correct, change it!
3. Host Name: optional. Required by some ISPs, e.g. @Home.
4. Renew IP Forever: this feature enable this product renew IP address automatically when the lease time is being expired even the system is in idle state.

4.4.1.4 PPP over Ethernet

1. PPPoE Account and Password: the account and password your ISP assigned to you. For security, this field appears blank. If you don't want to change the password, leave it empty.
2. PPPoE Service Name: optional. Input the service name if your ISP requires it. Otherwise, leave it blank.
3. Maximum Idle Time: the amount of time of inactivity before disconnecting your PPPoE session. Set it to zero or enable Auto-reconnect to disable this feature.

4.4.1.5 PPTP

1. My IP Address and My Subnet Mask: the private IP address and subnet mask your ISP assigned to you.
2. Server IP Address: the IP address of the PPTP server.
3. PPTP Account and Password: the account and password your ISP assigned to you. If you don't want to change the password, keep it empty.
3. Connection ID: optional. Input the connection ID if your ISP requires it.
4. Maximum Idle Time: the time of no activity to disconnect your PPTP session. Set it to zero or enable Auto-reconnect to disable this feature. If Auto-reconnect is enabled, this product will automatically connect to ISP after system is restarted or connection is dropped.

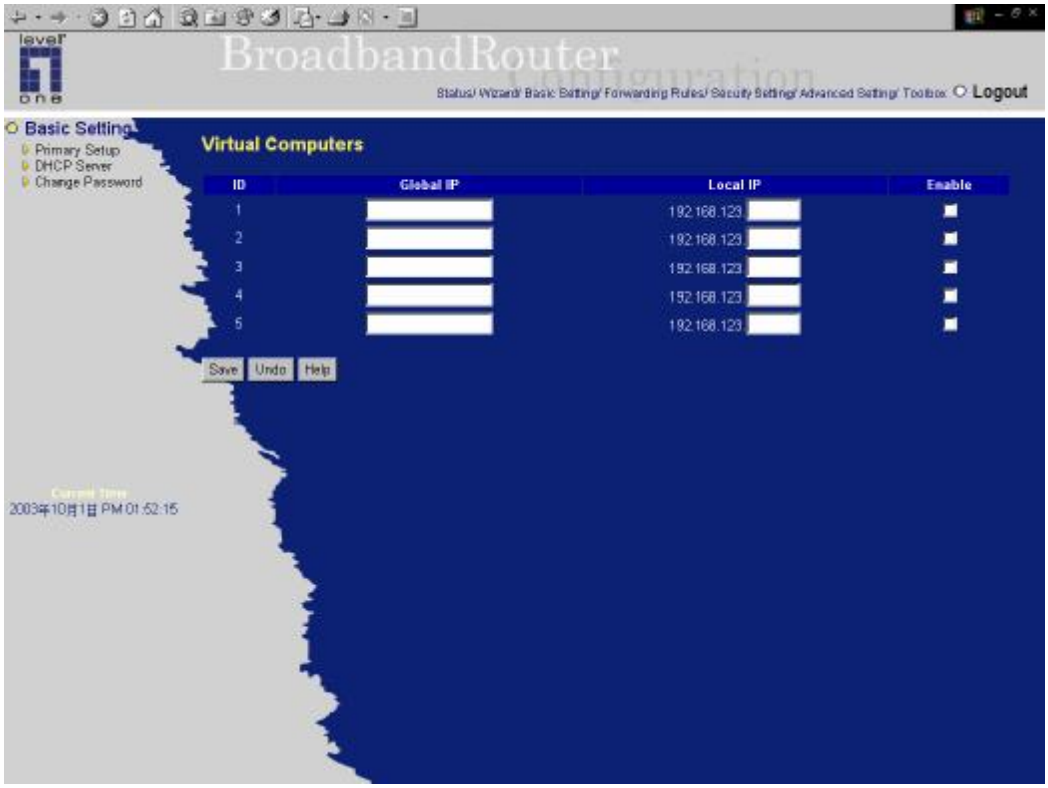
4.4.1.6 L2TP

1. IP Mode: The IP Mode assigned by your ISP. You can select either Static IP Address or Dynamic IP address.
2. My IP Address and My Subnet Mask: the private IP address and subnet mask your ISP assigned to you when your IP Mode is Static IP Address.

3. Server IP Address: the IP address of the L2TP server.
4. L2TP Account and Password: the account and password your ISP assigned to you. If you don't want to change the password, keep it empty.

Maximum Idle Time: the time of no activity to disconnect your L2TP session. Set it to zero or enable Auto-reconnect to disable this feature. If Auto-reconnect is enabled, this product will automatically connect to ISP after system is restarted or connection is dropped.

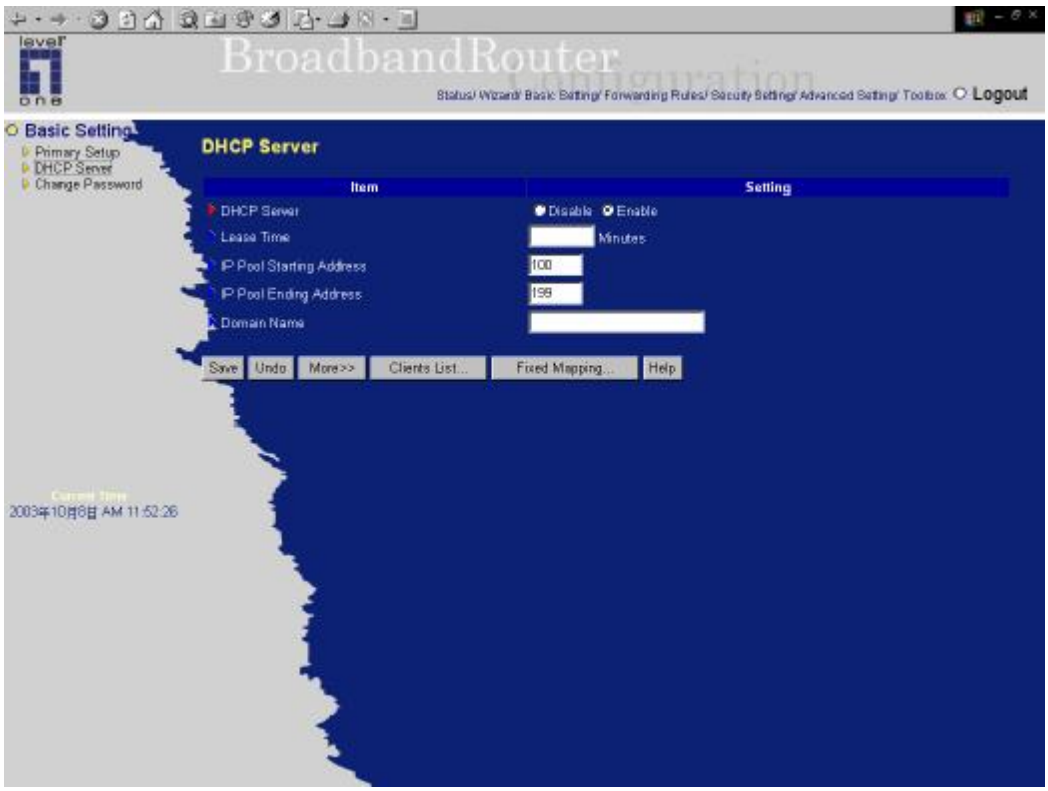
4.4.1.7 Virtual Computers



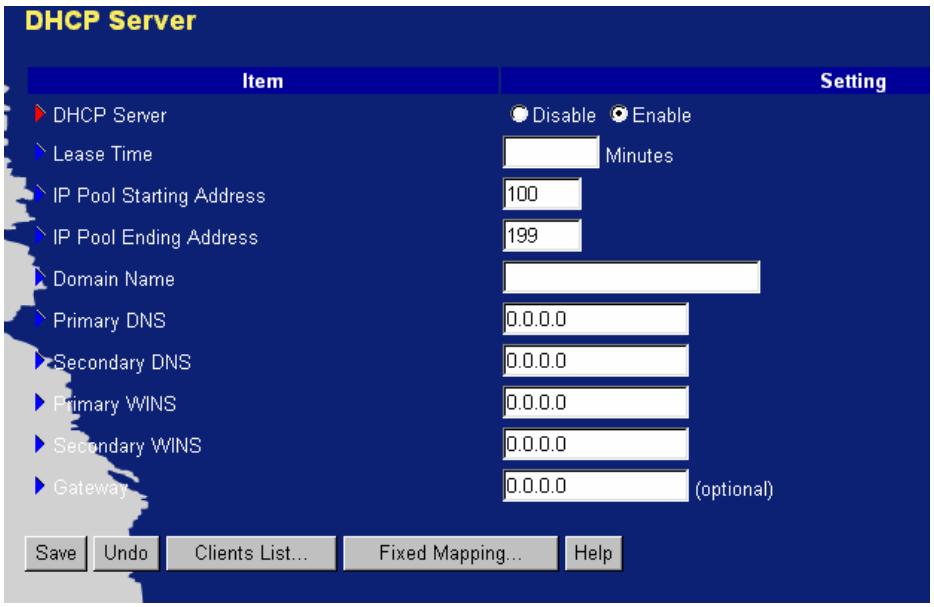
Virtual Computer enables you to use the original NAT feature, and allows you to setup the one-to-one mapping of multiple global IP address and local IP address.

- Global IP: Enter the global IP address assigned by your ISP.
- Local IP: Enter the local IP address of your LAN PC corresponding to the global IP address.
- Enable: Check this item to enable the Virtual Computer feature.

4.4.2 DHCP Server



Press **"More>>"**

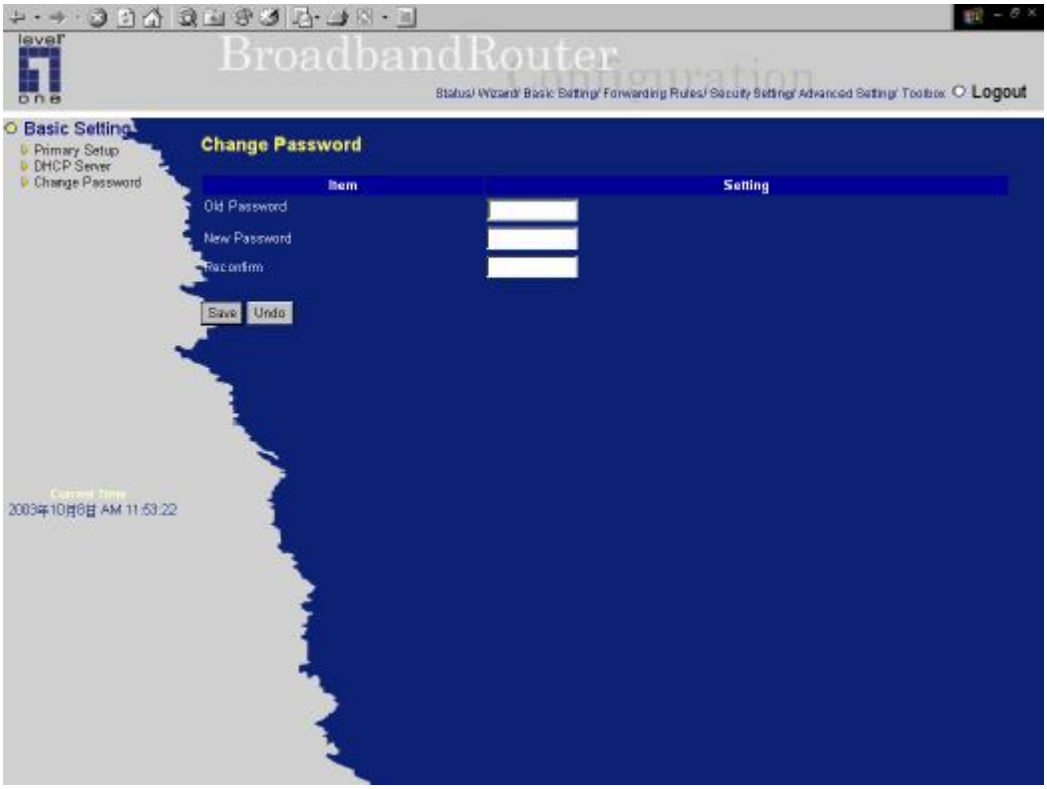


The settings of a TCP/IP environment include host IP, Subnet Mask, Gateway, and DNS configurations. It is not easy to manually configure all the computers and devices in your network. Fortunately, DHCP Server provides a rather simple approach to handle all these settings. This product supports the

function of DHCP server. If you enable this product's DHCP server and configure your computers as "automatic IP allocation" mode, then when your computer is powered on, it will automatically load the proper TCP/IP settings from this product. The settings of DHCP server include the following items:

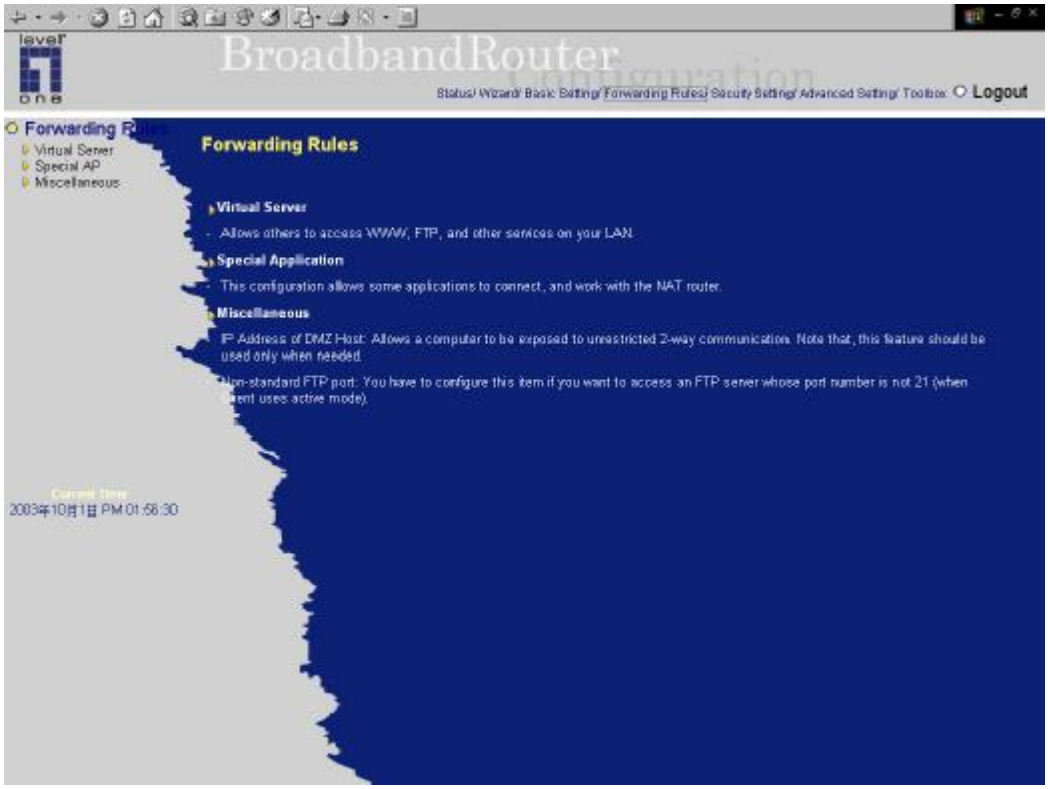
1. **DHCP Server**: Choose "Disable" or "Enable."
2. **Lease Time:** this feature allows you to configure IP's lease time (DHCP client).
3. **IP pool starting Address/ IP pool starting Address**: Whenever there is a request, the DHCP server will automatically allocate an unused IP address from the IP address pool to the requesting computer. You must specify the starting and ending address of the IP address pool.
4. **Domain Name**: Optional, this information will be passed to the client.
5. **Primary DNS/Secondary DNS**: This feature allows you to assign DNS Servers
6. **Primary WINS/Secondary WINS**: This feature allows you to assign WINS Servers
7. **Gateway**: The Gateway Address would be the IP address of an alternate Gateway. This function enables you to assign another gateway to your PC, when DHCP server offers an IP to your PC.

4.4.4 Change Password

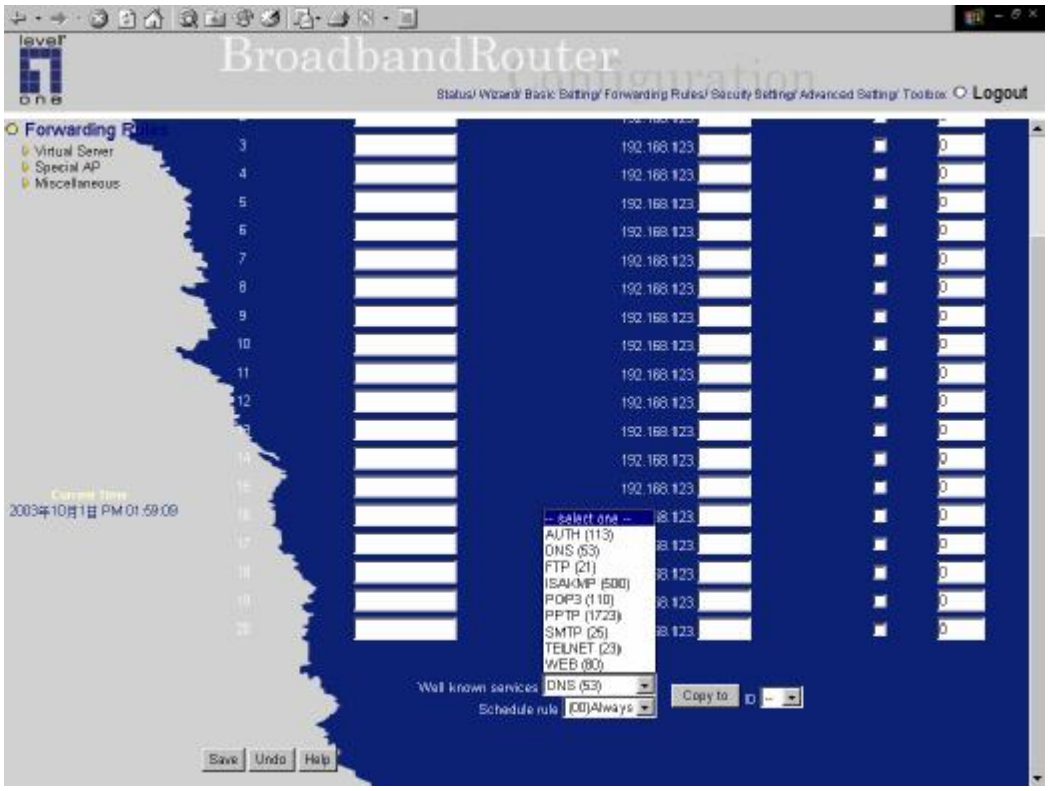


You can change Password here. We **strongly** recommend you to change the system password for security reason.

4.5 Forwarding Rules



4.5.1 Virtual Server



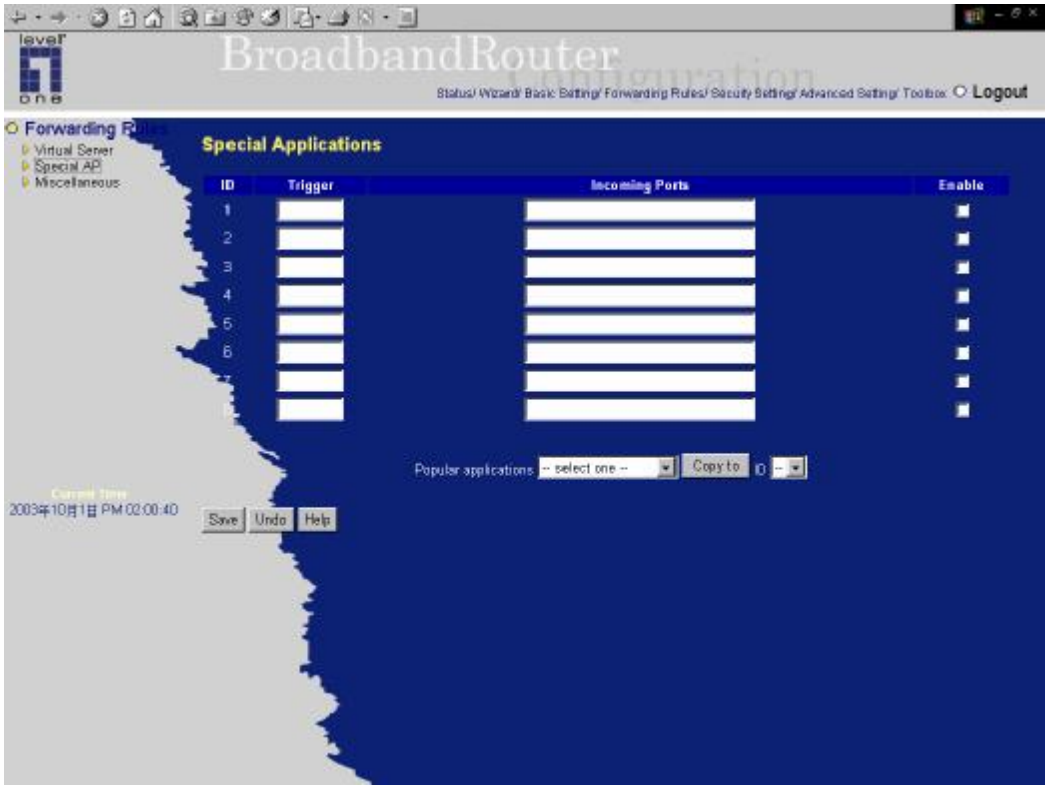
This product's NAT firewall filters out unrecognized packets to protect your Intranet, so all hosts behind this product are invisible to the outside world. If you wish, you can make some of them accessible by enabling the Virtual Server Mapping.

A virtual server is defined as a **Service Port**, and all requests to this port will be redirected to the computer specified by the **Server IP**. **Virtual Server** can work with **Scheduling Rules**, and give user more flexibility on Access control. For Detail, please refer to **Scheduling Rule**.

For example, if you have an FTP server (port 21) at 192.168.123.1, a Web server (port 80) at 192.168.123.2, and a VPN server at 192.168.123.6, then you need to specify the following virtual server mapping table:

Service Port	Server IP	Enable
21	192.168.123.1	V
80	192.168.123.2	V
1723	192.168.123.6	V

4.5.2 Special AP



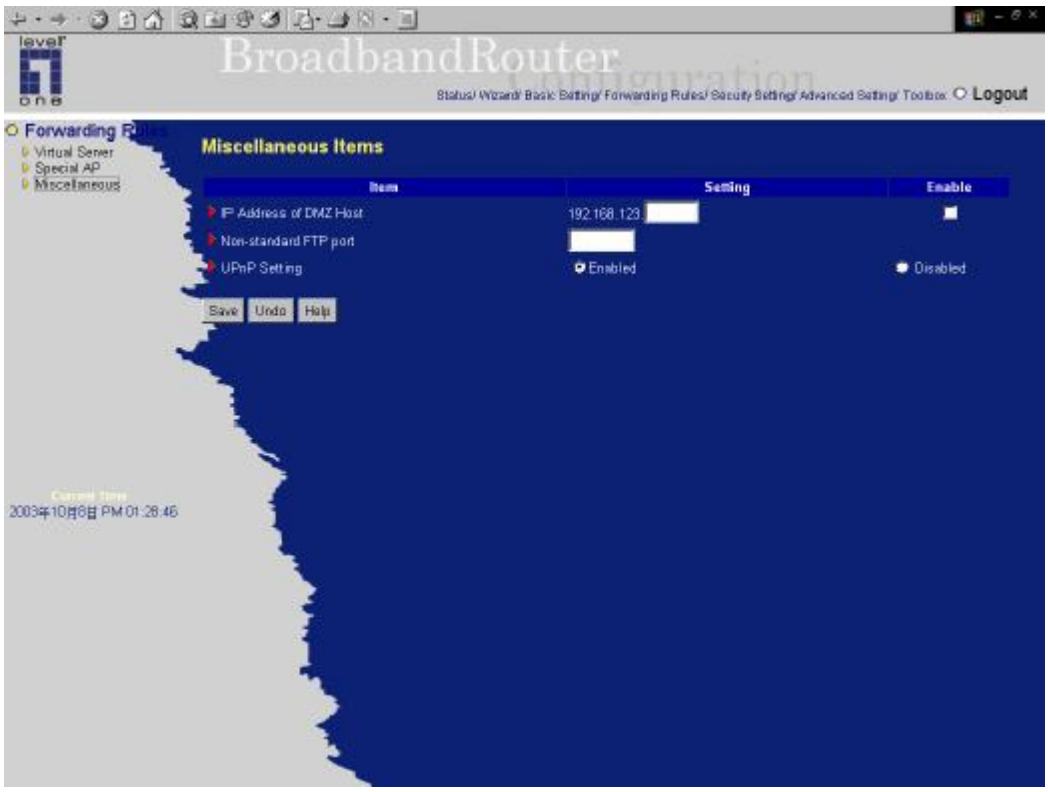
Some applications require multiple connections, like Internet games, Video conferencing, Internet telephony, etc. Because of the firewall function, these applications cannot work with a pure NAT router. The **Special Applications** feature allows some of these applications to work with this product. If the mechanism of Special Applications fails to make an application work, try setting your computer as the **DMZ** host instead.

1. **Trigger**: the outbound port number issued by the application..
2. **Incoming Ports**: when the trigger packet is detected, the inbound packets sent to the specified port numbers are allowed to pass through the firewall.

This product provides some predefined settings Select your application and click **Copy to** to add the predefined setting to your list.

Note! At any given time, only one PC can use each Special Application tunnel.

4.5.3 Miscellaneous Items



IP Address of DMZ Host

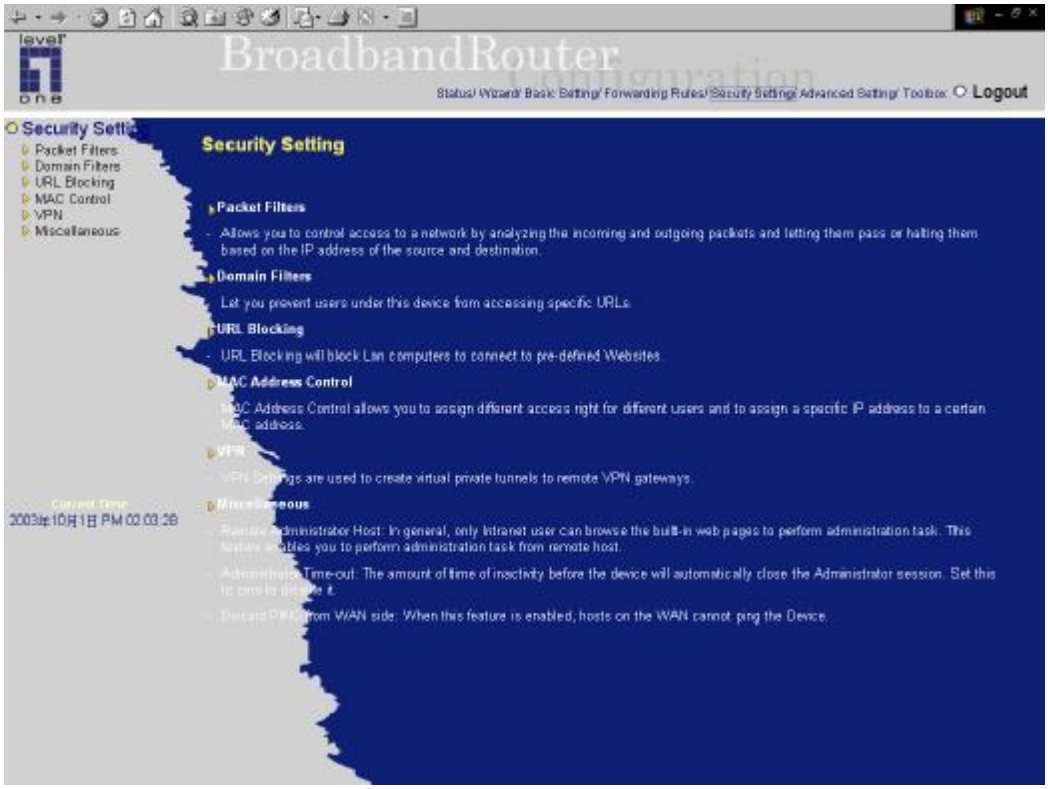
DMZ (DeMilitarized Zone) Host is a host without the protection of firewall. It allows a computer to be exposed to unrestricted 2-way communication for Internet games, Video conferencing, Internet telephony and other special applications.

NOTE: This feature should be used only when needed.

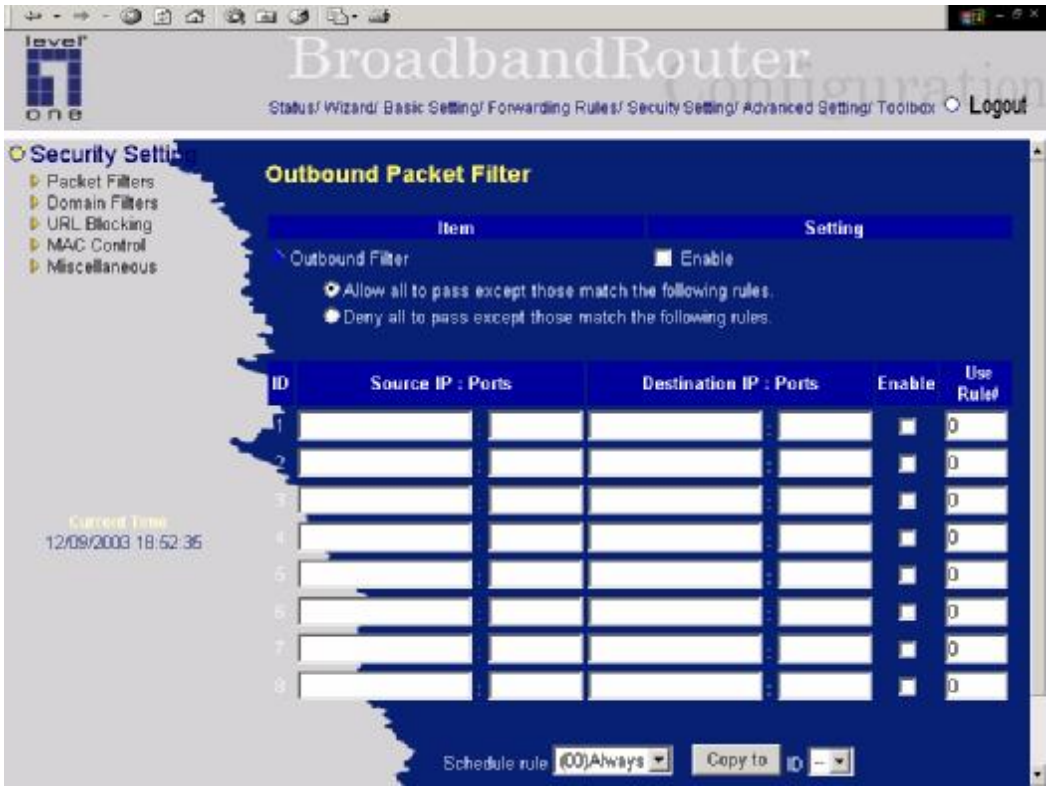
Non-standard FTP port

You have to configure this item if you want to access an FTP server whose port number is not 21. This setting will be lost after rebooting.

4.6 Security Settings



4.6.1 Packet Filter



Packet Filter enables you to control what packets are allowed to pass the router. Outbound filter applies on all outbound packets. However, Inbound filter applies on packets that destined to Virtual Servers or DMZ host only. You can select one of the two filtering policies:

1. Allow all to pass except those match the specified rules
2. Deny all to pass except those match the specified rules

You can specify 8 rules for each direction: inbound or outbound. For each rule, you can define the following:

- Source IP address
- Source port address
- Destination IP address
- Destination port address
- Protocol: TCP or UDP or both.
- Use Rule#

For source or destination IP address, you can define a single IP address (4.3.2.1) or a range of IP addresses (4.3.2.1-4.3.2.254). An empty implies all IP addresses.
For source or destination port, you can define a single port (80) or a range of ports (1000-1999). Add prefix "T" or "U" to specify TCP or UDP protocol. For example, T80, U53, U2000-2999. No prefix indicates both TCP and UDP are defined. An empty implies all port addresses. **Packet Filter** can work with **Scheduling Rules**, and give user more flexibility on Access control. For Detail, please refer to **Scheduling Rule**.

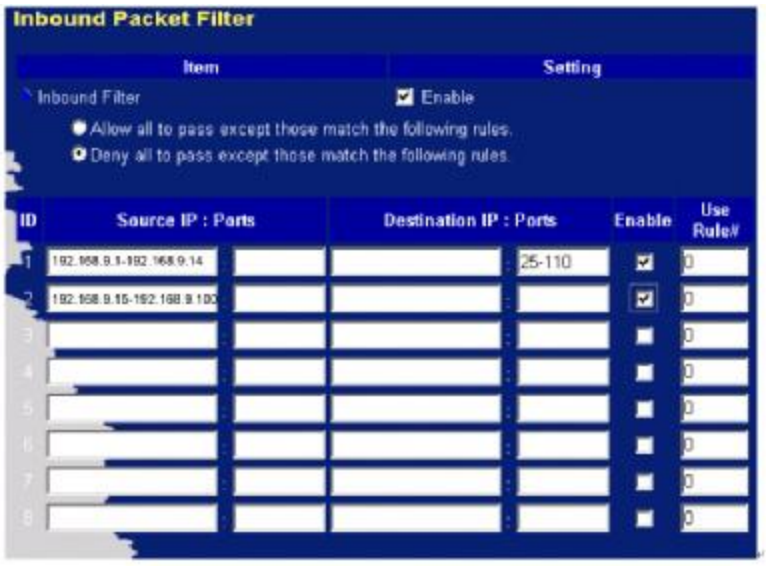
Each rule can be enabled or disabled individually.

Inbound Filter:

To enable Inbound Packet Filter click the check box next to Enable in the Inbound Packet Filter field.

Suppose you have SMTP Server (25), POP Server (110), Web Server (80), FTP Server (21), and News Server (119) defined in Virtual Server or DMZ Host.

Example 1:

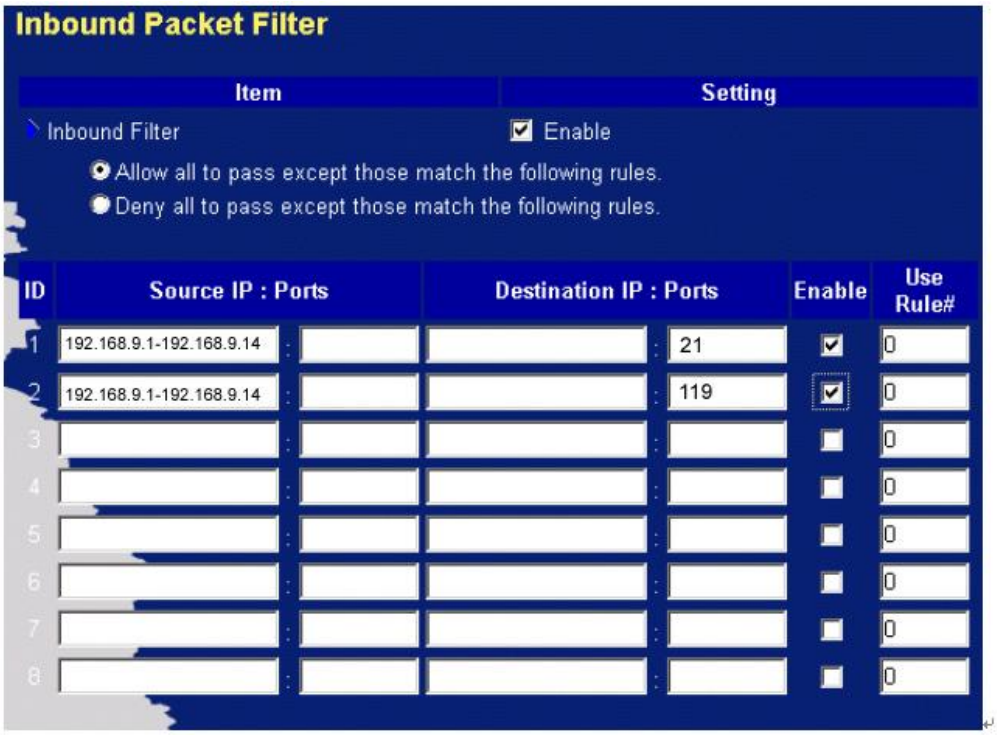


(192.168.9.1-192.168.9.14) They are allow to send mail (port 25), receive mail (port 110), and browse your web server as above. (port 80)

(192.168.9.15-192.168.9.100) They can do everything (block nothing)

Others are all blocked.

Example 2:



(192.168.9.1-192.168.9.14) They can do everything except read net news (port 119) and transfer files via FTP (port 21)

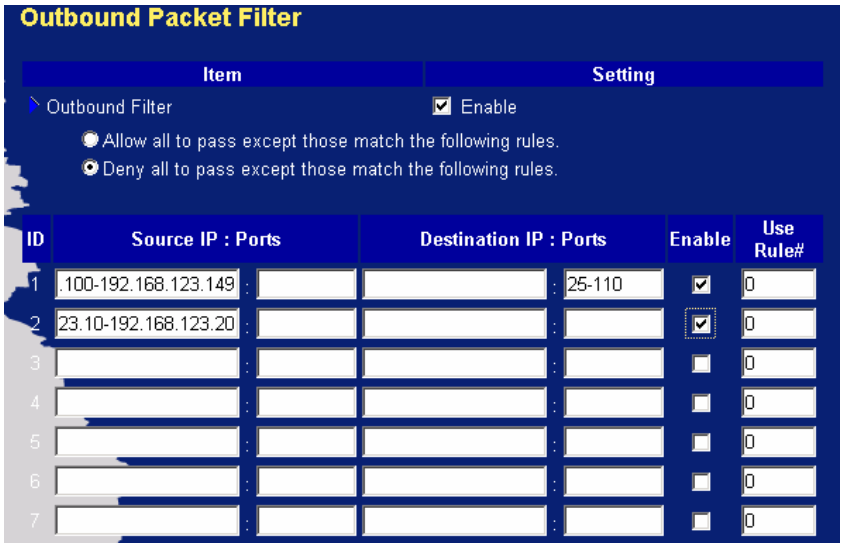
Others are all allowed.

After **Inbound Packet Filter** setting is configured, click the **save** button.

Outbound Filter:

To enable **Outbound Packet Filter** click the check box next to **Enable** in the **Outbound Packet Filter** field.

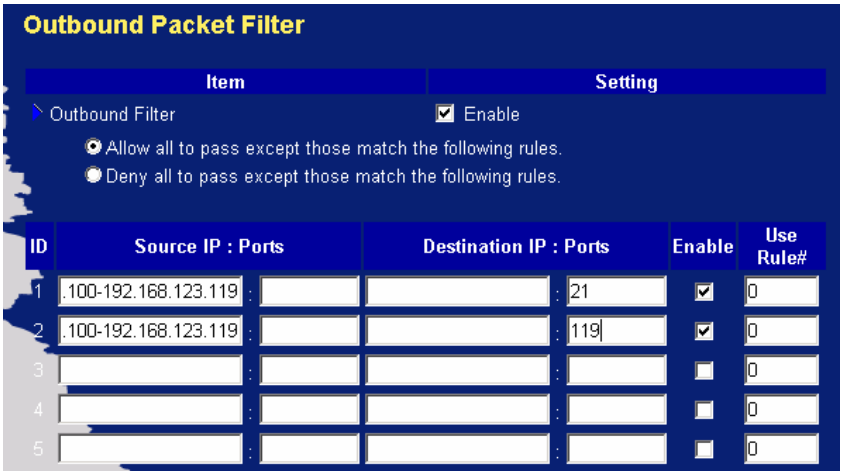
Example 1:



(192.168.123.100-192.168.123.149) They are allowed to send mail (port 25), receive mail (port 110), and browse Internet (port 80); port 53 (DNS) is necessary to resolve the domain name.

(192.168.123.10-192.168.123.20) They can do everything (block nothing)
Others are all blocked.

Example 2:

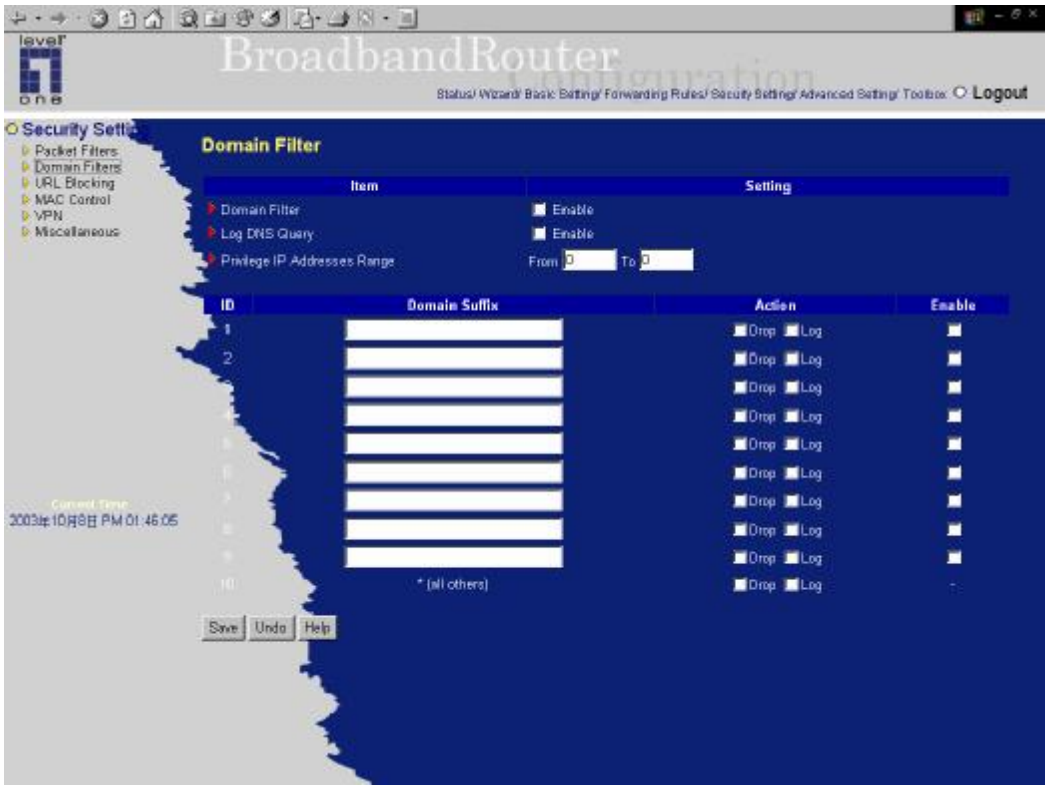


(192.168.123.100-192.168.123.119) They can do everything except read net news (port 119) and transfer files via FTP (port 21)

Others are allowed

After **Outbound Packet Filter** setting is configured, click the **save** button.

4.6.2 Domain Filter



Domain Filter

let you prevent users under this device from accessing specific URLs.

Domain Filter Enable

Check if you want to enable Domain Filter.

Log DNS Query

Check if you want to log the action when someone accesses the specific URLs.

Privilege IP Addresses Range

Setting a group of hosts and privilege these hosts to access network without restriction.

Domain Suffix

A suffix of URL to be restricted. For example, ".com", "xxx.com".

Action

When someone is accessing the URL met the domain-suffix, what kind of action you want.

Check drop to block the access. Check log to log these access.

Enable

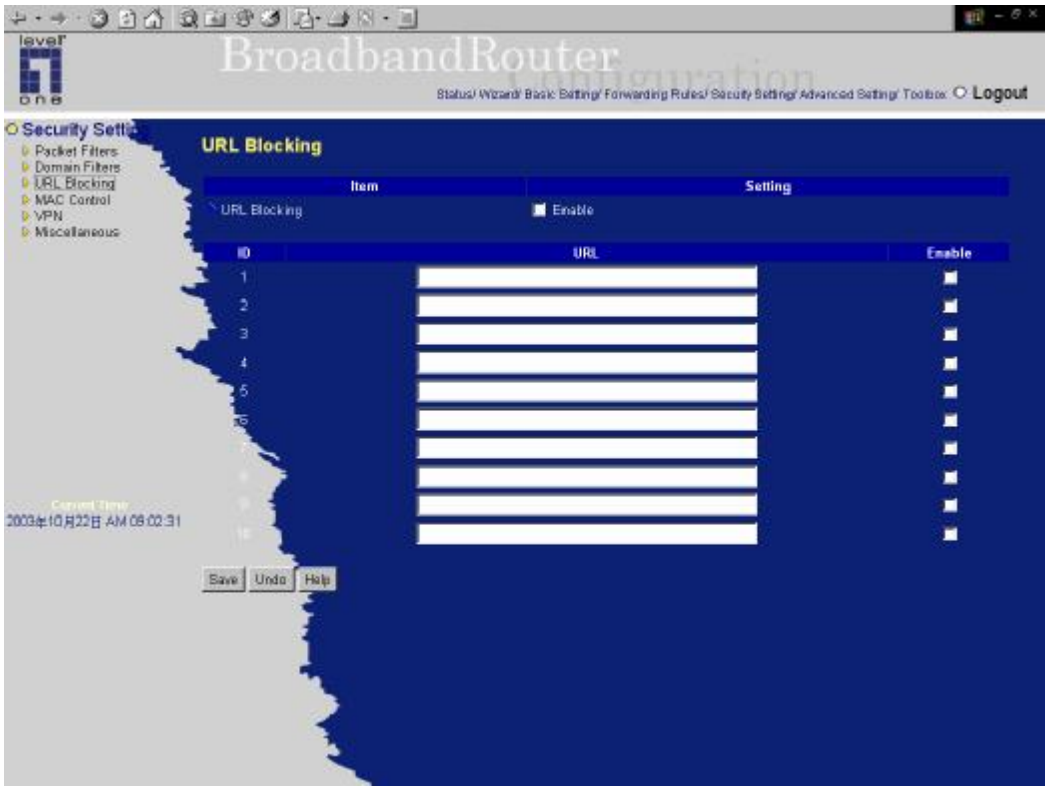
Check to enable each rule.

Example:

In this example:

1. URL include “sex.com” will be blocked, and the action will be record in log-file.
2. URL include “girl.com” will not be blocked, but the action will be record in log-file.
3. URL include “erotica.com” will be blocked, but the action will not be record in log-file.
4. IP address X.X.X.1~ X.X.X.10 can access network without restriction.

4.6.3 URL Blocking



URL Blocking will block LAN computers to connect to pre-defined Websites.

The major difference between “Domain filter” and “URL Blocking” is Domain filter require user to input suffix (like .com or .org, etc), while URL Blocking require user to input a keyword only. In other words, Domain filter can block specific website, while URL Blocking can block hundreds of websites by simply a **keyword**.

URL Blocking Enable

Checked if you want to enable URL Blocking.

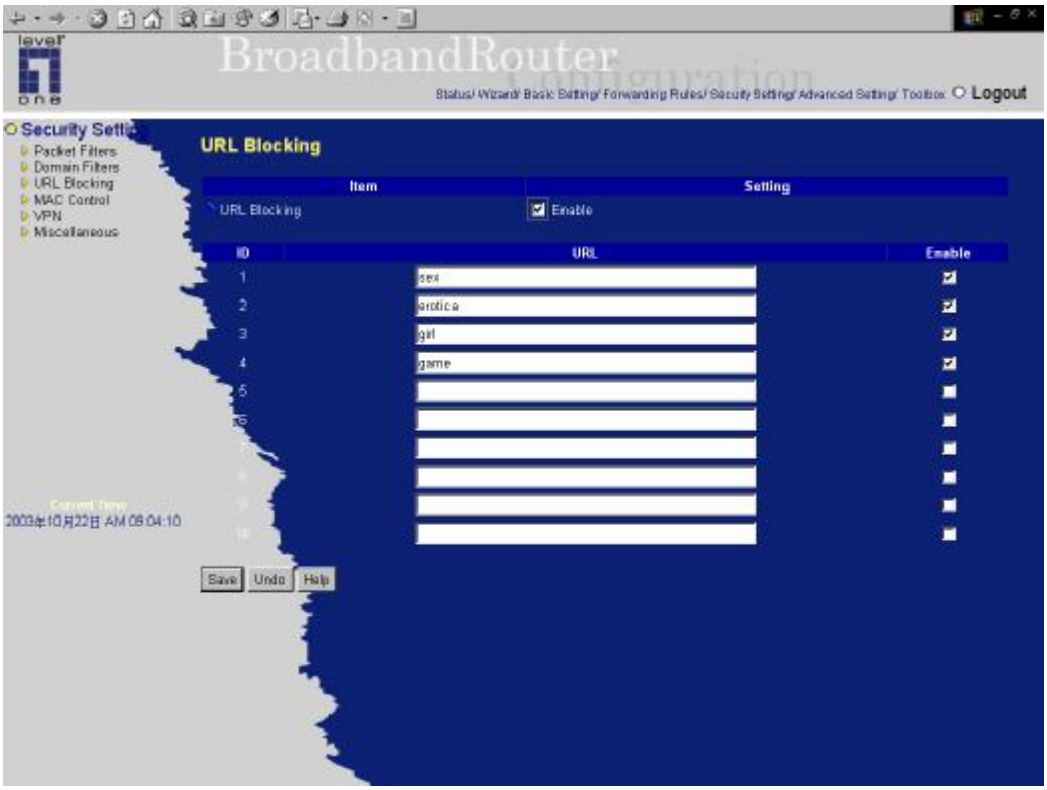
URL

If any part of the Website's URL matches the pre-defined word, the connection will be blocked.

For example, you can use pre-defined word "sex" to block all websites if their URLs contain pre-defined word "sex".

Enable

Checked to enable each rule.



In this example:

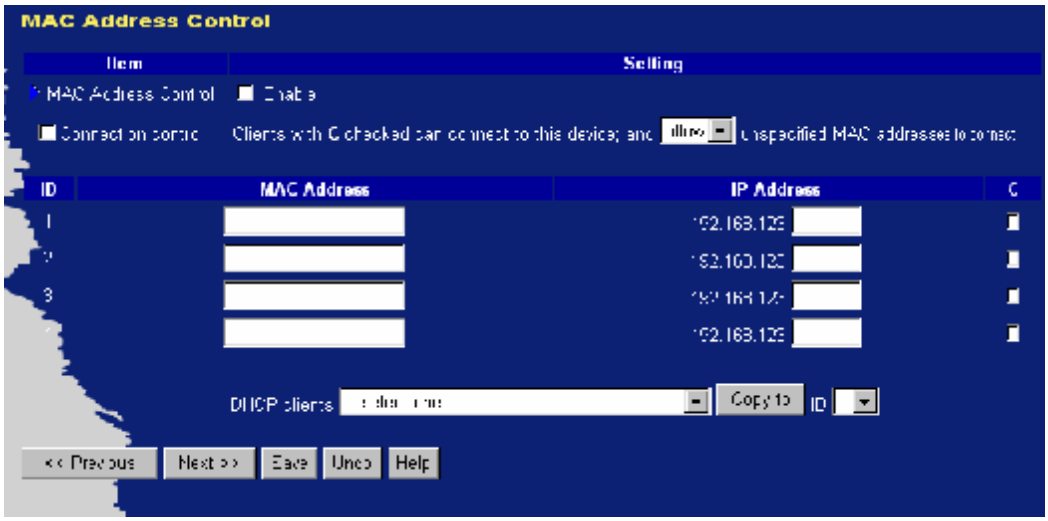
1.URL include “sex” will be blocked, and the action will be record in log-file.

2.URL include “erotica” will be blocked, but the action will be record in log-file

3.URL include “girl” will not be blocked, but the action will be record in log-file.

4. URL include “game” will be blocked, but the action will be record in log-file

4.6.4 MAC Address Control

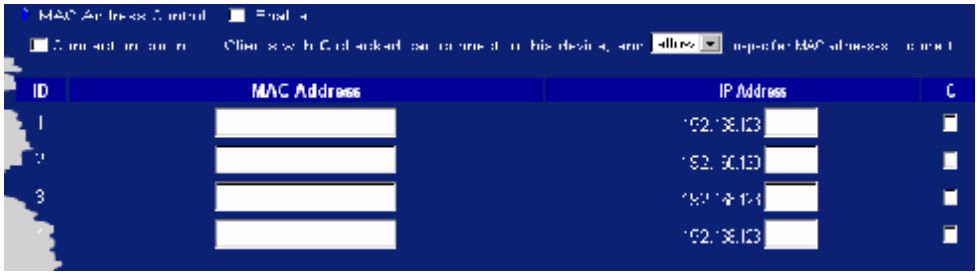


MAC Address Control allows you to assign different access right for different users and to assign a specific IP address to a certain MAC address.

MAC Address Control Check “Enable” to enable the “MAC Address Control”. All of the settings in this page will take effect only when “Enable” is checked.

Connection control Check "Connection control" to enable the controlling of which wired can connect to this device. If a client is denied to connect to this device, it means the client can't access to the Internet either. Choose "allow" or "deny" to allow or deny the clients, whose MAC addresses are not in the "Control table" (please see below), to connect to this device.

Control table



"Control table" is the table at the bottom of the "MAC Address Control" page. Each row of this table indicates the MAC address and the expected IP address mapping of a client. There are four columns in this table:

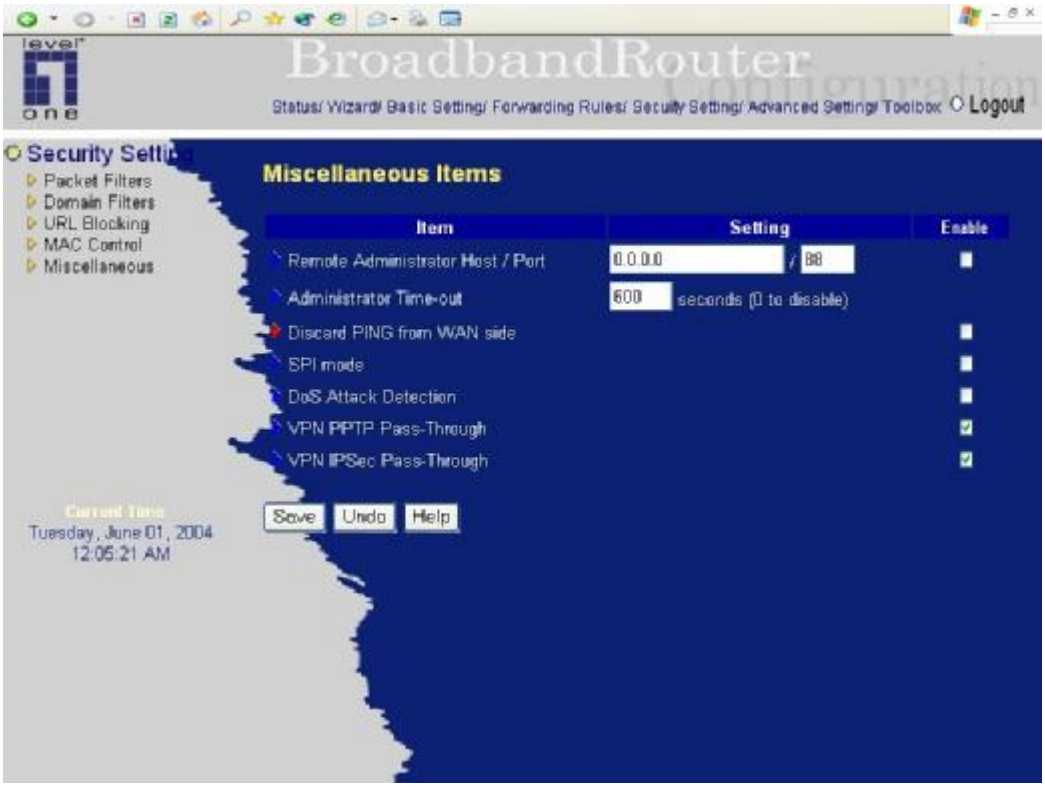
MAC Address	MAC address indicates a specific client.
IP Address	Expected IP address of the corresponding client. Keep it empty if you don't care its IP address.
C	When "**Connection control**" is checked, check "**C**" will allow the corresponding client to connect to this device.

In this page, we provide the following Combobox and button to help you to input the MAC address.

You can select a specific client in the “DHCP clients” Combobox, and then click on the “Copy to” button to copy the MAC address of the client you select to the ID selected in the “ID” Combobox.

Previous page and Next Page To make this setup page simple and clear, we have divided the “Control table” into several pages. You can use these buttons to navigate to different pages.

4.6.6 Miscellaneous Items



Remote Administrator Host/Port

In general, only Intranet user can browse the built-in web pages to perform administration task. This feature enables you to perform administration task from remote host. If this feature is enabled, only the specified IP address can perform remote administration. If the specified IP address is 0.0.0.0, any host can connect to this product to perform administration task. You can use subnet mask bits "/nn" notation to specified a group of trusted IP addresses. For example, "10.1.2.0/24".

NOTE: When Remote Administration is enabled, the web server port will be shifted to 88. You can change web server port to other port, too.

Administrator Time-out

The time of no activity to logout automatically. Set it to zero to disable this feature.

Discard PING from WAN side

When this feature is enabled, any host on the WAN cannot ping this product.

SPI Mode

When this feature is enabled, the router will record the packet information pass through the router like IP address, port address, ACK, SEQ number and so on. And the router will check every incoming packet to detect if this packet is valid.

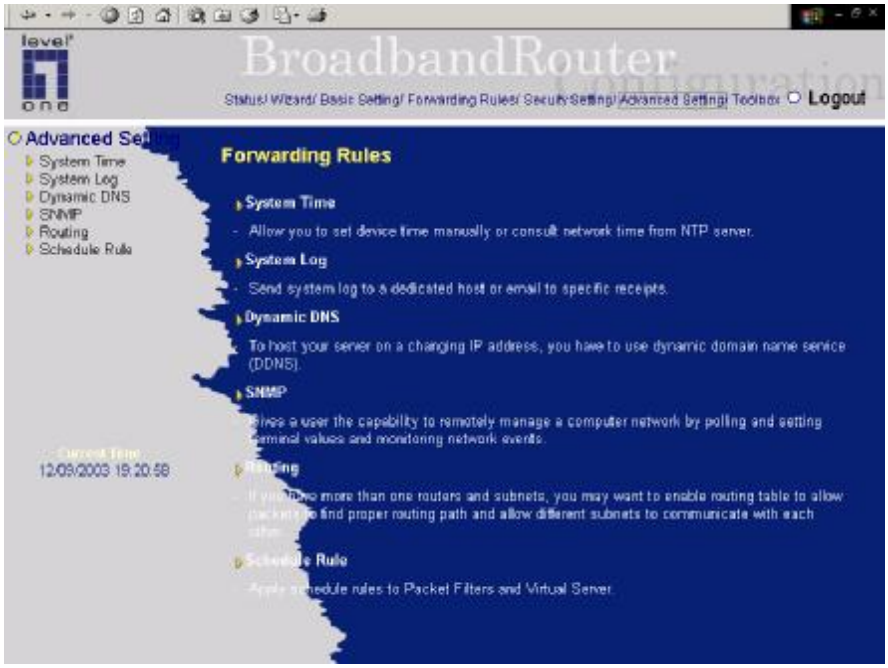
DoS Attack Detection

When this feature is enabled, the router will detect and log the DoS attack comes from the Internet. Currently, the router can detect the following DoS attack: SYN Attack, WinNuke, Port Scan, Ping of Death, Land Attack etc.

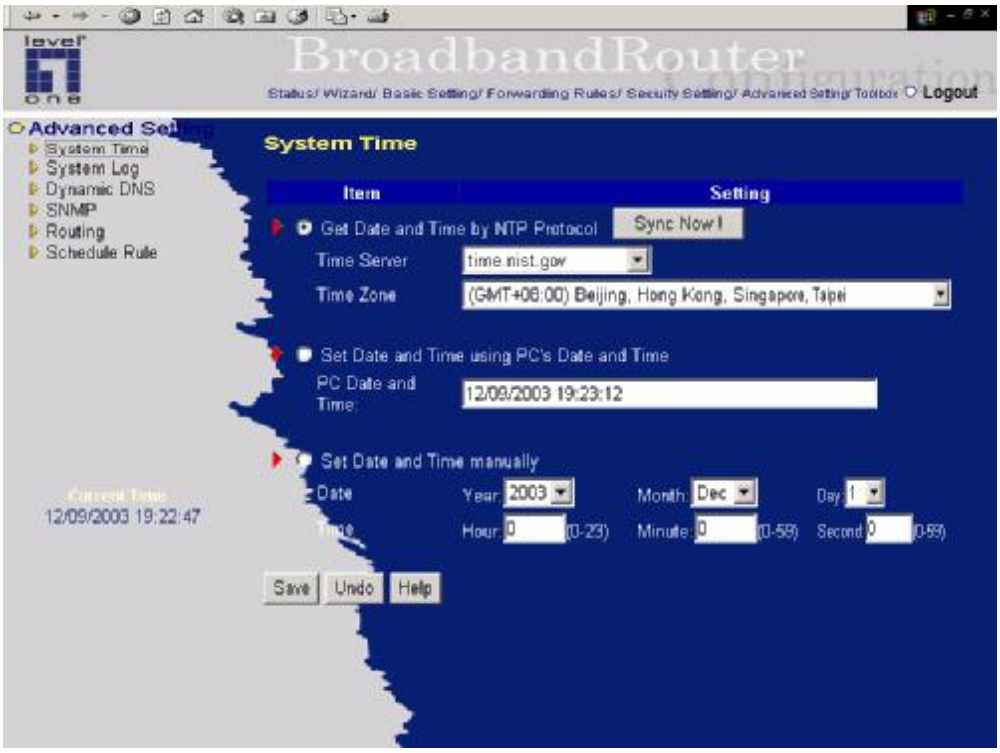
VPN PPTP/IPSec Pass-Through

Please enable this feature, if you need to establish a PPTP or IPSEC connection that will pass through this device.

4.7 Advanced Settings



4.7.1 System Time



Get Date and Time by NTP Protocol

Selected if you want to Get Date and Time by NTP Protocol.

Time Server

Select a NTP time server to consult UTC time

Time Zone

Select a time zone where this device locates.

Set Date and Time manually

Selected if you want to Set Date and Time manually.

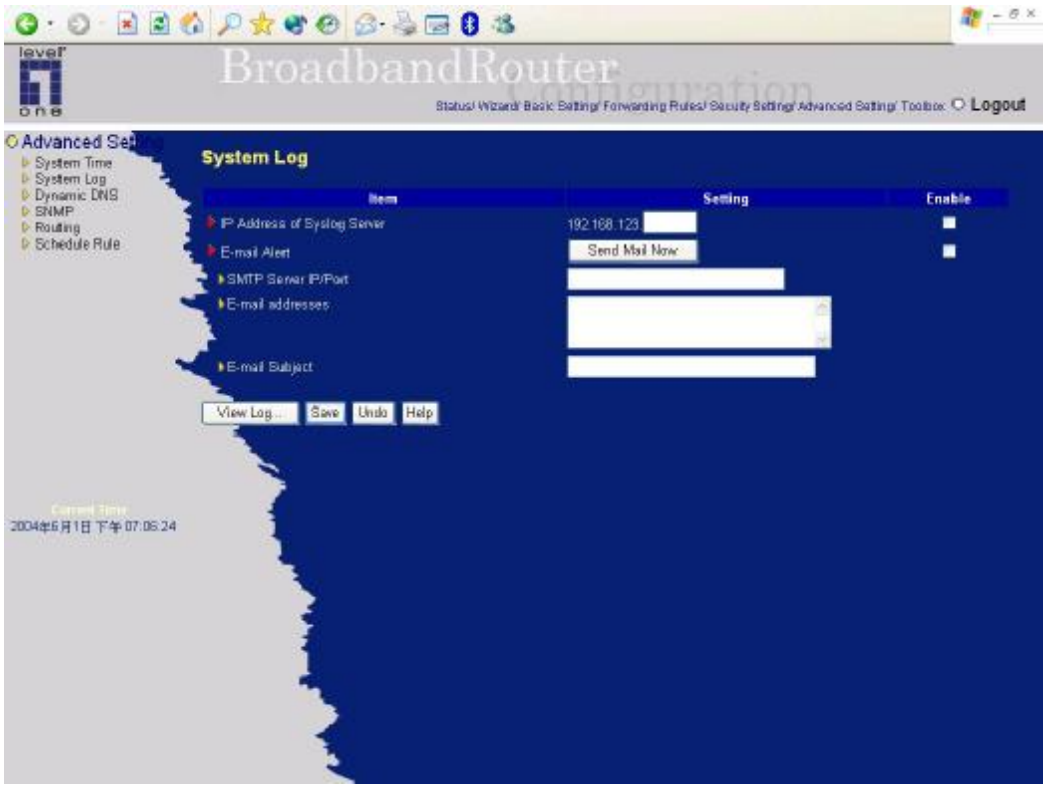
Daylight Saving

Select and configure the daylight saving period to fit the local environment.

Function of Buttons

Sync Now: Synchronize system time with network time server

4.7.2 System Log



This page support two methods to export system logs to specific destination by means of syslog(UDP) and SMTP(TCP). The items you have to setup including:

IP Address for Syslog Server

Host IP of destination where syslogs will be sent to.

Check **Enable** to enable this function.

E-mail Alert Enable

Check if you want to enable Email alert(send syslog via email).

SMTP Server IP/Port

Input the SMTP server IP and port, which are concated with ':'. If you do not specify port number, the default value is 25.

For example, "mail.your_url.com" or "192.168.1.100:26".

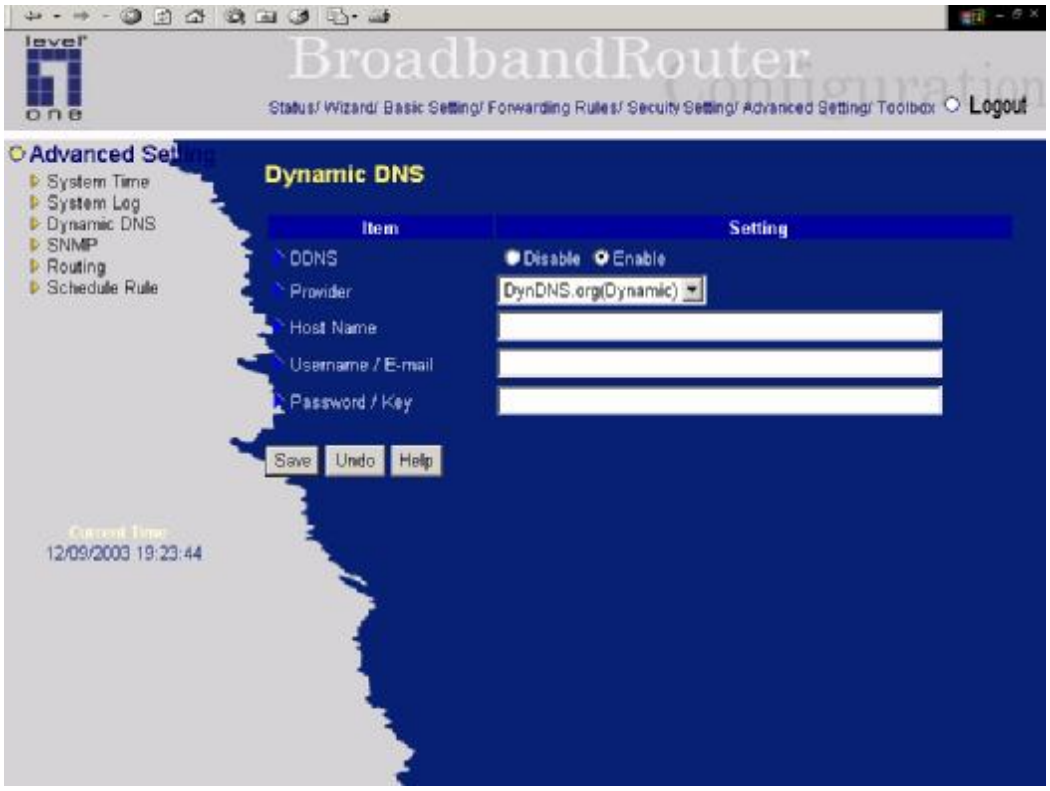
E-mail addresses

The recipients who will receive these logs. You can assign more than 1 recipient, using ';' or ',' to separate these email addresses.

E-mail Subject

The subject of email alert. This setting is optional.

4.7.3 Dynamic DNS



To host your server on a changing IP address, you have to use dynamic domain name service (DDNS).

So that anyone wishing to reach your host only needs to know the name of it. Dynamic DNS will map the name of your host to your current IP address, which changes each time you connect your Internet service provider.

Before you enable **Dynamic DNS**, you need to register an account on one of these Dynamic DNS servers that we list in **provider** field.

To enable **Dynamic DNS** click the check box next to **Enable** in the **DDNS** field.

Next you can enter the appropriate information about your Dynamic DNS Server.

You have to define:

Provider

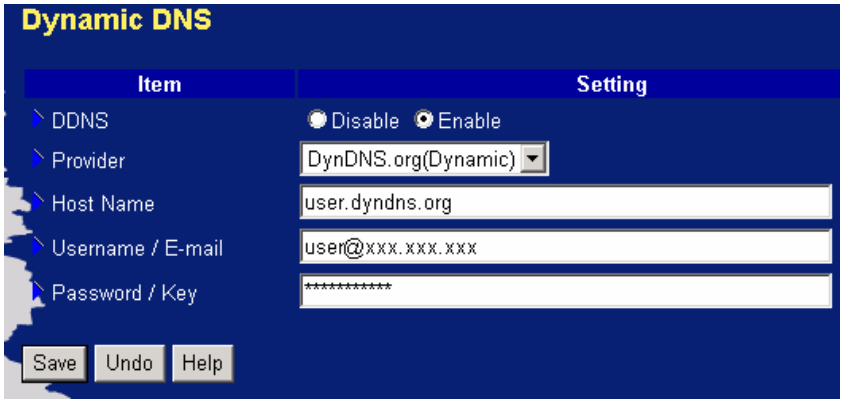
Host Name

Username/E-mail

Password/Key

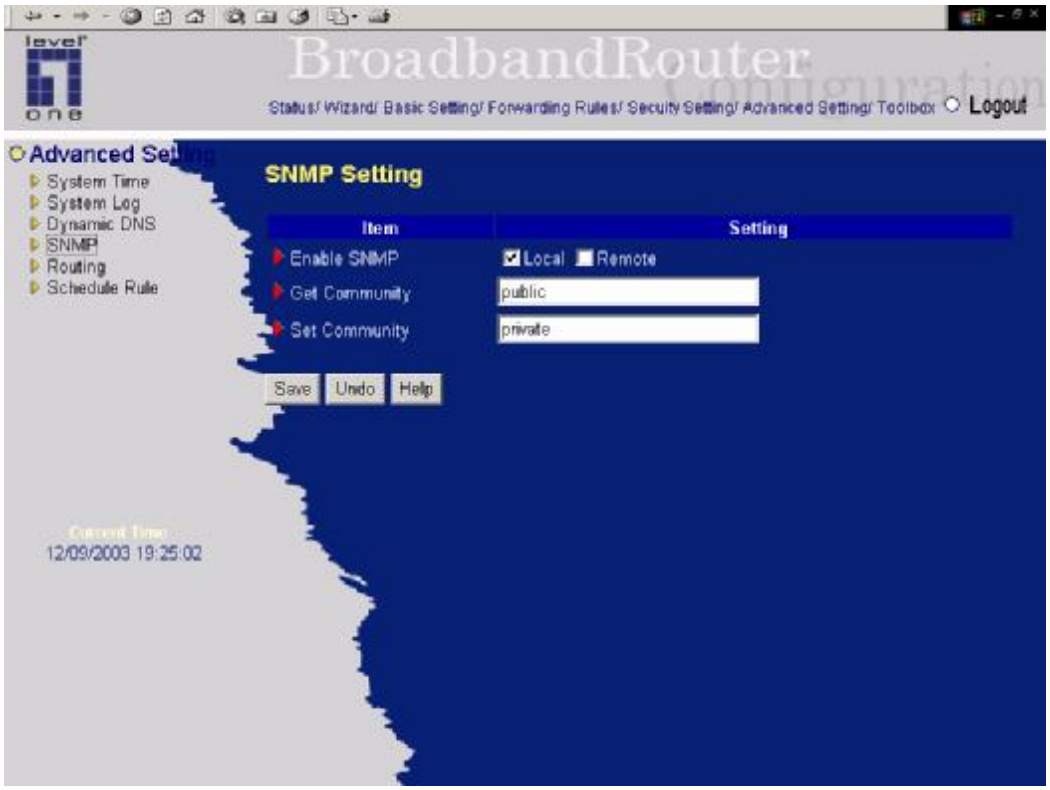
You will get this information when you register an account on a Dynamic DNS server.

Example:



After Dynamic DNS setting is configured, click the save button.

4.7.4 SNMP Setting



In brief, SNMP, the Simple Network Management Protocol, is a protocol designed to give a user the capability to remotely manage a computer network by polling and setting terminal values and monitoring network events.

Enable SNMP

You must check either Local or Remote or both to enable SNMP function. If Local is checked, this device will response request from LAN. If Remote is checked, this device will response request from WAN.

Get Community

Setting the community of GetRequest your device will response.

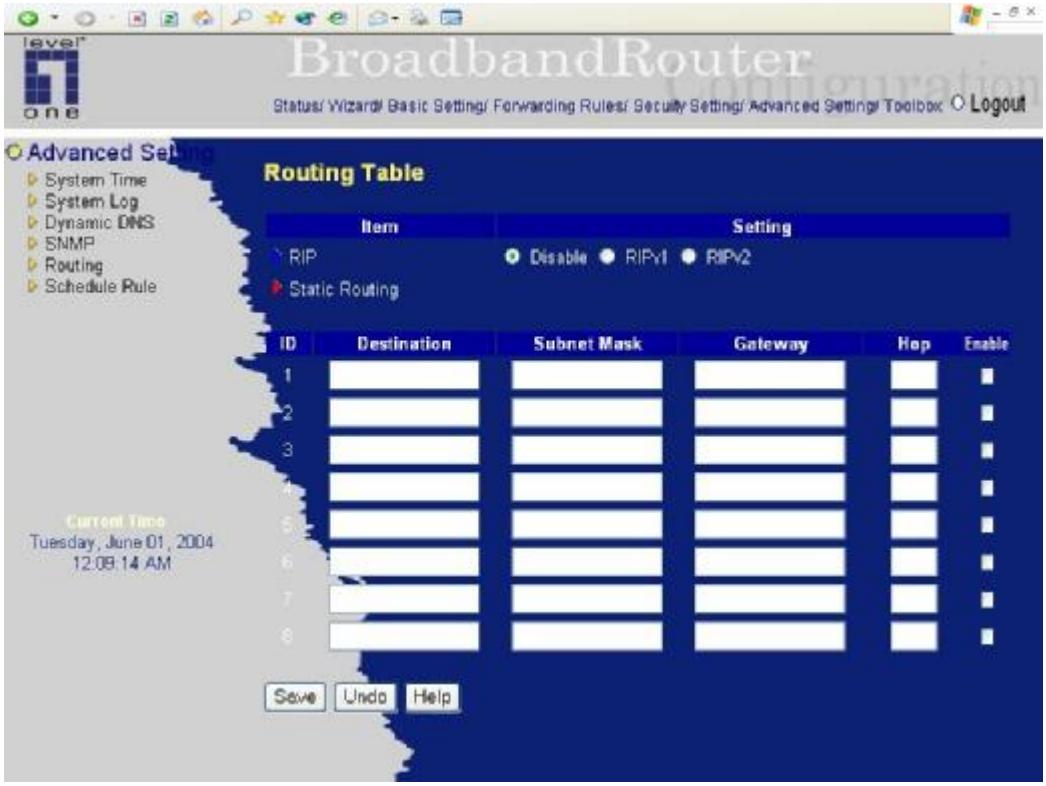
Set Community

Setting the community of SetRequest your device will accept.

Example:

1. This device will response to SNMP client which's **get community** is set as "public"
2. This device will response to SNMP client which's **set community** is set as "private"
3. This device will response request from both LAN and WAN
4. This device will send SNMP Trap message to 192.168.123.33 (Use SNMP Version V2c)

4.7.5 Routing Table



Routing Tables allow you to determine which physical interface address to use for outgoing IP data grams. If you have more than one routers and subnets, you will need to enable routing table to allow packets to find proper routing path and allow different subnets to communicate with each other.

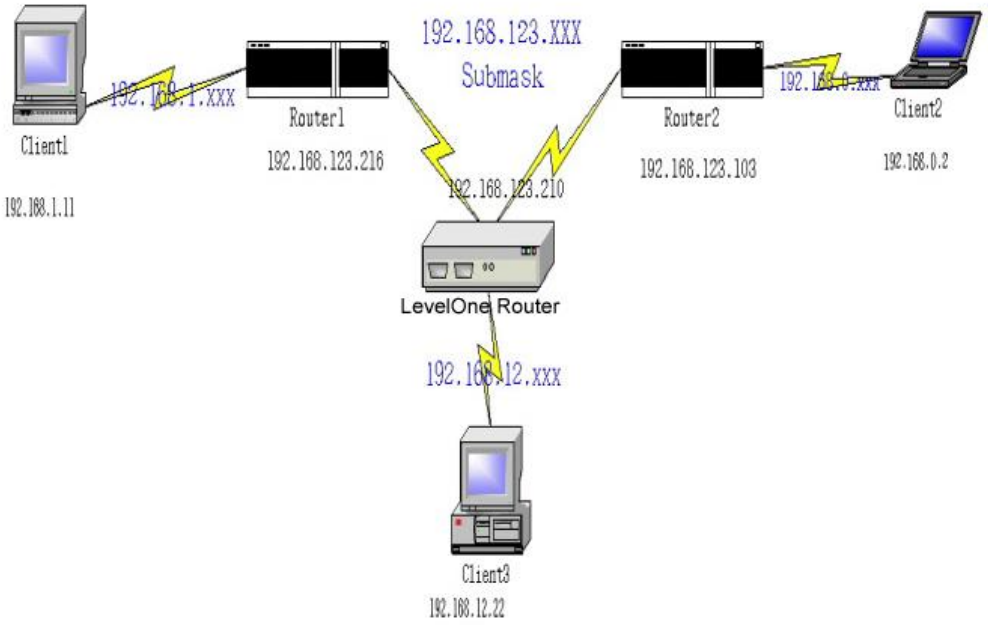
Routing Table settings are settings used to setup the functions of static and dynamic routing.

RIP

Routing Information Protocol (RIP) will exchange information about destinations for computing routes throughout the network. Please select RIPv2 only if you have different subnet in your network. Otherwise, please select RIPv1 if you need this protocol.

Static Routing: For static routing, you can specify up to 8 routing rules. You can enter the destination IP address, subnet mask, gateway, hop for each routing rule, and then enable or disable the rule by checking or unchecking the Enable checkbox.

Example:



Configuration on NAT Router

Destination	SubnetMask	Gateway	Hop	Enabled
192.168.1.0	255.255.255.0	192.168.123.216	1	V
192.168.0.0	255.255.255.0	192.168.123.103	1	V

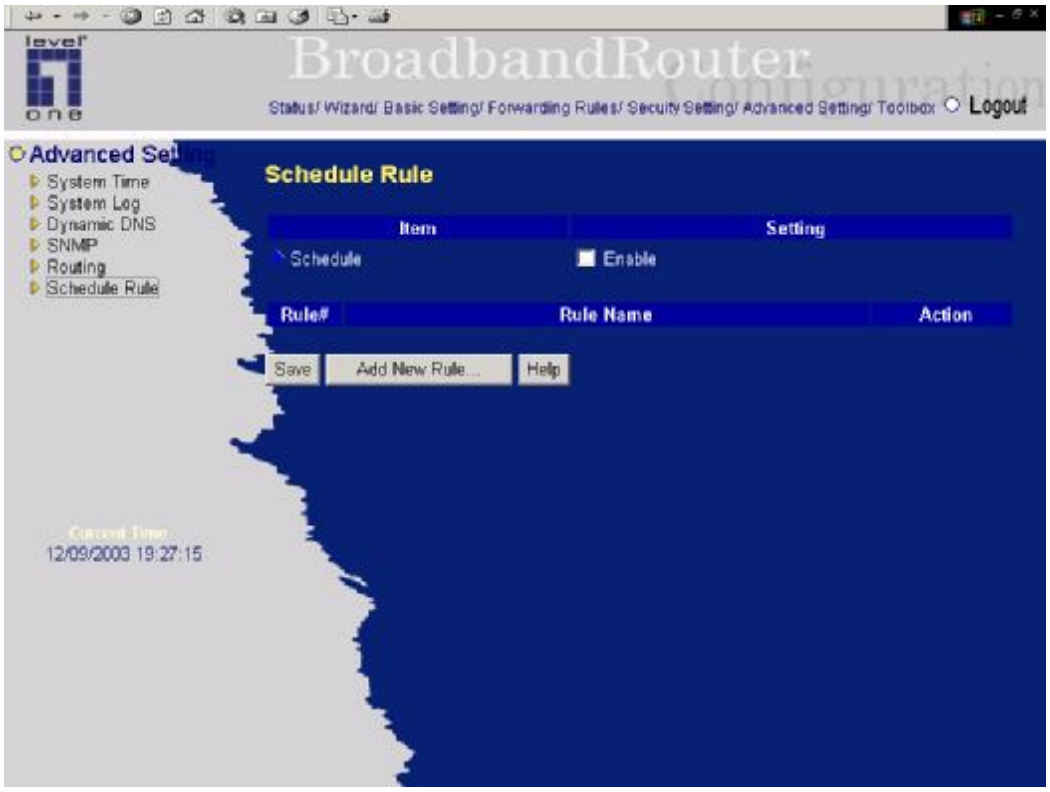
So if, for example, the client3 wanted to send an IP data gram to 192.168.0.2, it would use the above table to determine that it had to go via 192.168.123.103 (a gateway),

And if it sends Packets to 192.168.1.11 will go via 192.168.123.216

Each rule can be enabled or disabled individually.

After **routing table** setting is configured, click the **save** button.

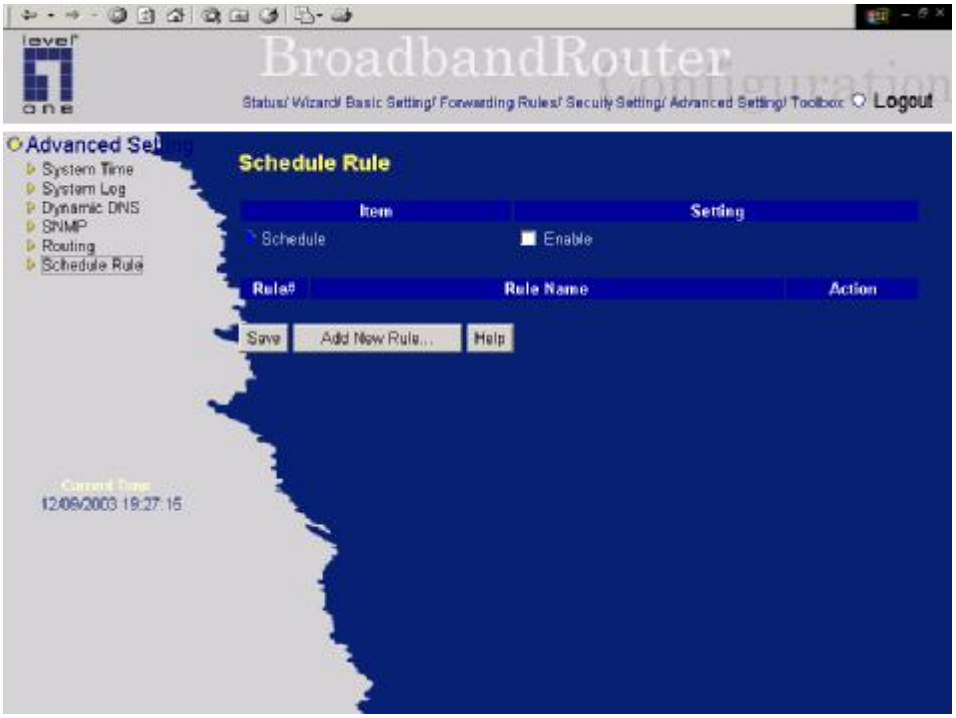
4.7.6 Schedule Rule



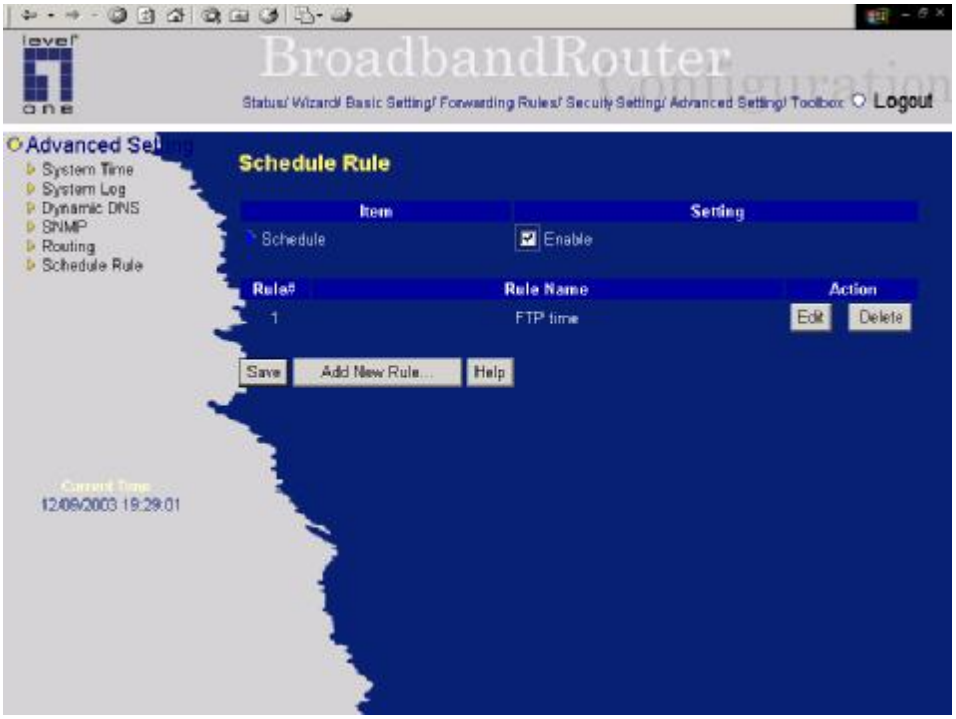
You can set the schedule time to decide which service will be turned on or off. Select the "enable" item.

Press **"Add New Rule"**

You can write a rule name and set which day and what time to schedule from “Start Time” to “End Time”. The following example configure “ftp time” as everyday 14:10 to 16:20



After configure Rule 1 à



Schedule Enable

Selected if you want to Enable the Scheduler.

Edit

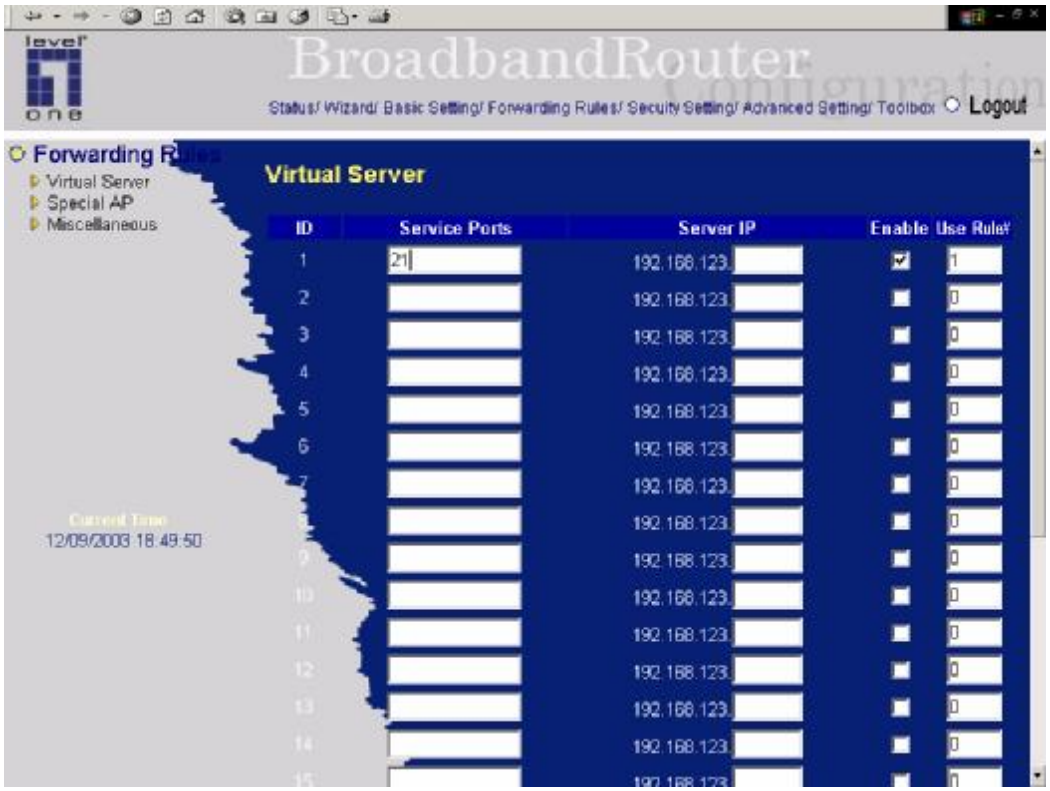
To edit the schedule rule.

Delete

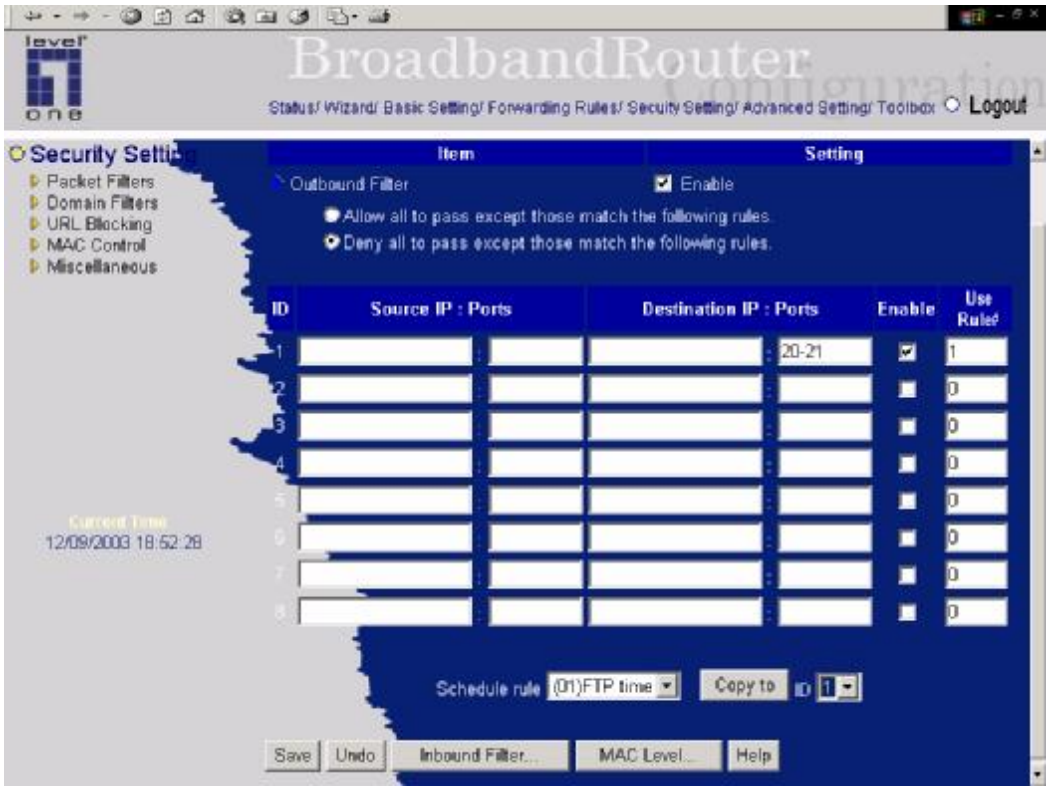
To delete the schedule rule, and the rule# of the rules behind the deleted one will decrease one automatically.

Schedule Rule can be apply to Virtual server and Packet Filter, for example:

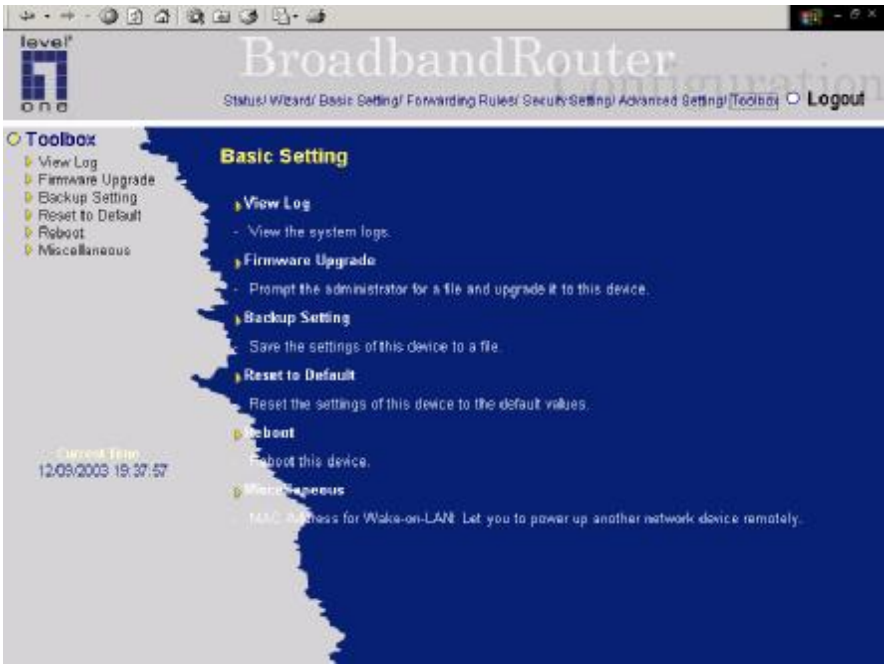
Exanple1: **Virtual Server** – Apply Rule#1 (ftp time: everyday 14:10 to 16:20)



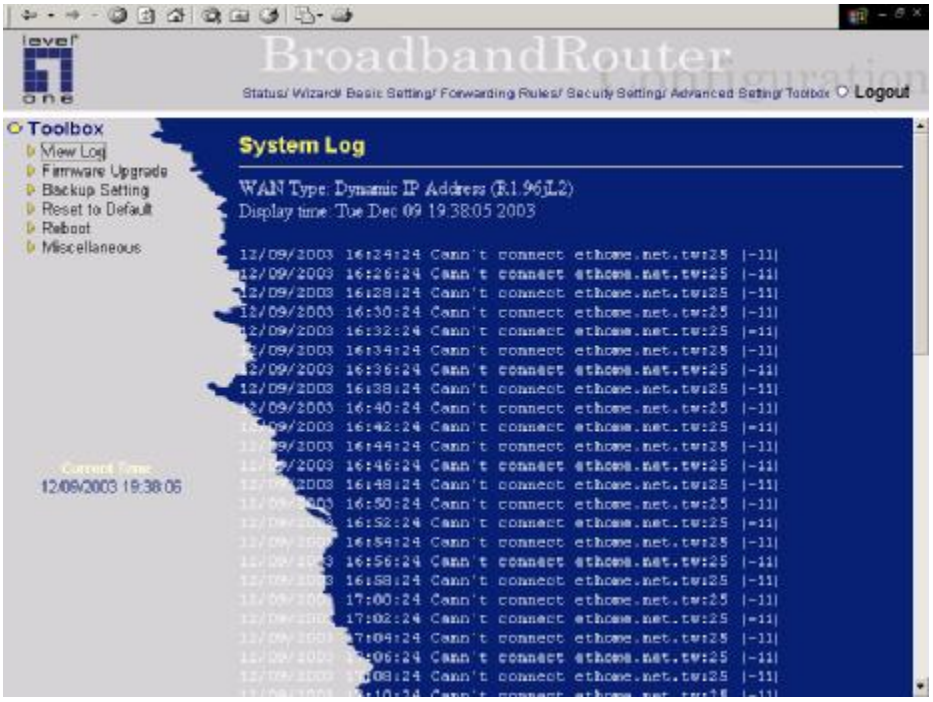
Exanple2: **Packet Filter** – Apply Rule#1 (ftp time: everyday 14:10 to 16:20).


BroadbandRouter
Status/ Wizard/ Basic Setting/ Forwarding Rules/ Security Setting/ Advanced Setting/ Toolbox
Logout
Security Setting
Packet Filters
Domain Filters
URL Blocking
MAC Control
Miscellaneous
Item
Setting
Outbound Filter
Enable
Allow all to pass except those match the following rules.
Deny all to pass except those match the following rules.
ID
Source IP : Ports
Destination IP : Ports
Enable
Use Rule#
20-21
Current Time
12/09/2003 18:52:28
Schedule rule
(01)FTP time
Copy to
ID
Save
Undo
Inbound Filter...
MAC Level...
Help

4.8 Toolbox

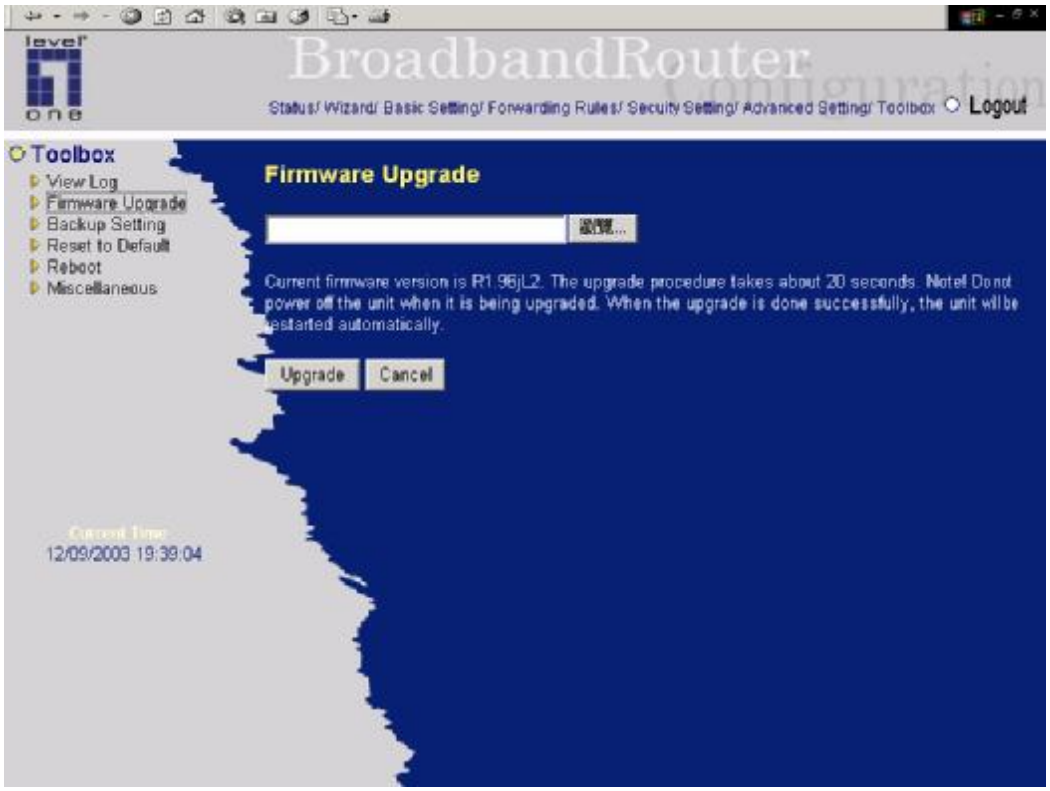


4.8.1 System Log



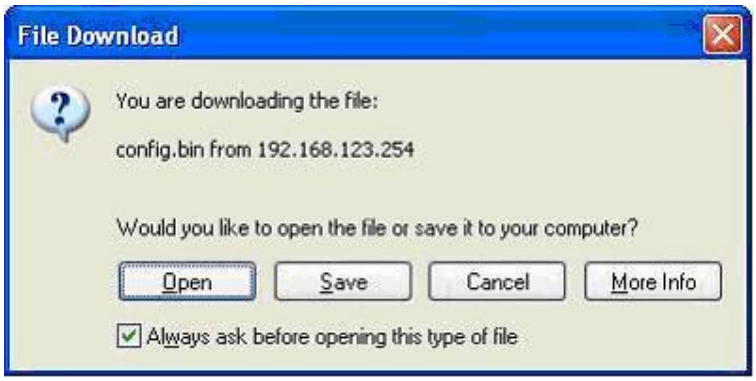
You can View system log by clicking the **View Log** button

4.8.2 Firmware Upgrade



You can upgrade firmware by clicking **Firmware Upgrade** button.

4.8.3 Backup Setting



You can backup your settings by clicking the **Backup Setting** button and save it as a bin file. Once you want to restore these settings, please click **Firmware Upgrade** button and use the bin file you saved.

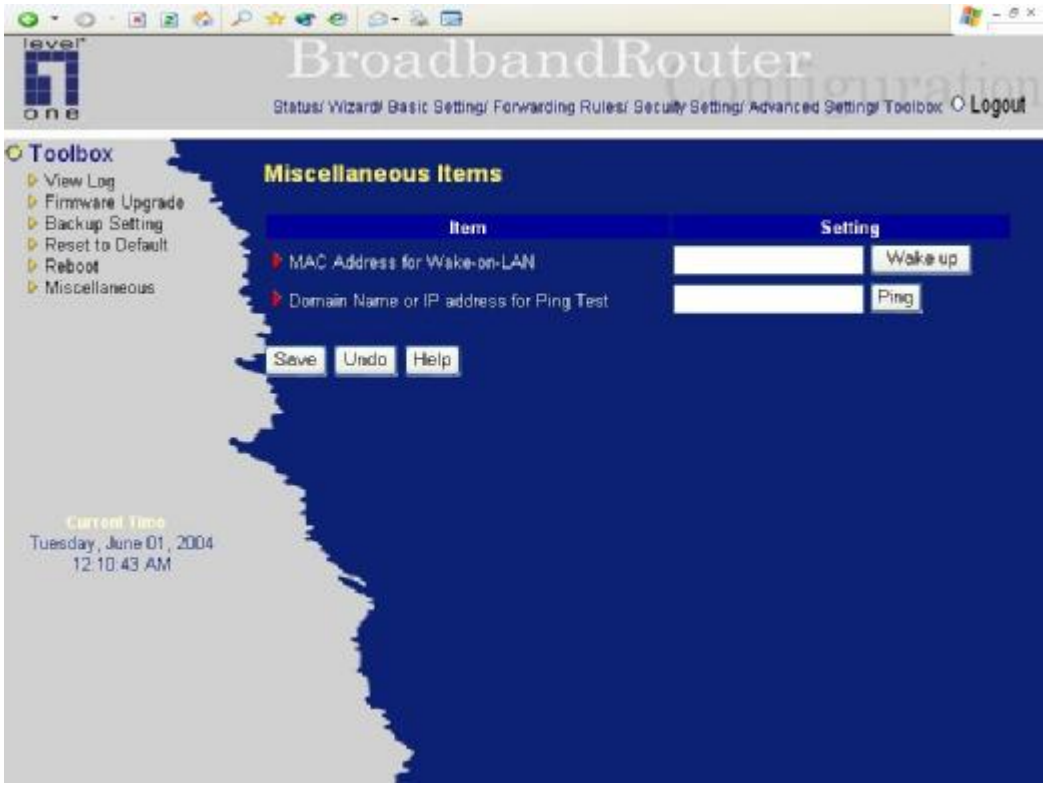
4.8.4 Reset to default

You can also reset this product to factory default by clicking the **Reset to default** button.

4.8.5 Reboot

You can also reboot this product by clicking the **Reboot** button.

4.8.6 Miscellaneous Items



MAC Address for Wake-on-LAN

Wake-on-LAN is a technology that enables you to power up a networked device remotely. In order to enjoy this feature, the target device must be Wake-on-LAN enabled and you have to know the MAC address of this device, say 00-11-22-33-44-55. Clicking "Wake up" button will make the router to send the wake-up frame to the target device immediately.

Domain Name or IP address for Ping Test

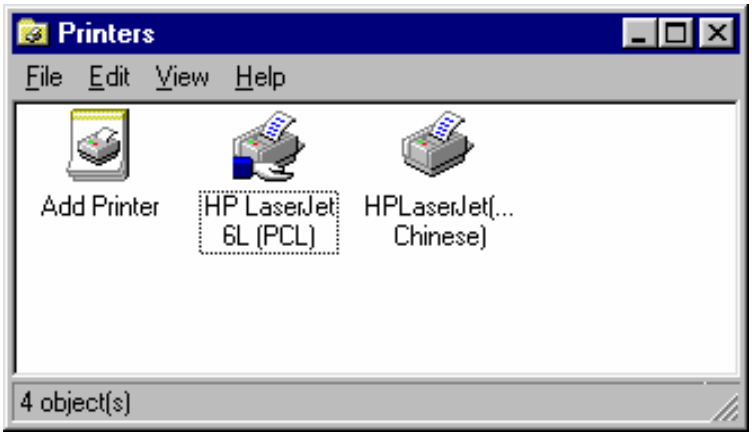
Allow you to configure an IP, and ping the device. You can ping a specific IP to test whether it is alive.

Chapter 5 Printer Server

This product provides the function of network print server for MS Windows 95/98/NT/2000 and Unix based platforms. (If the product you purchased doesn't have printer port, please skip this chapter.)

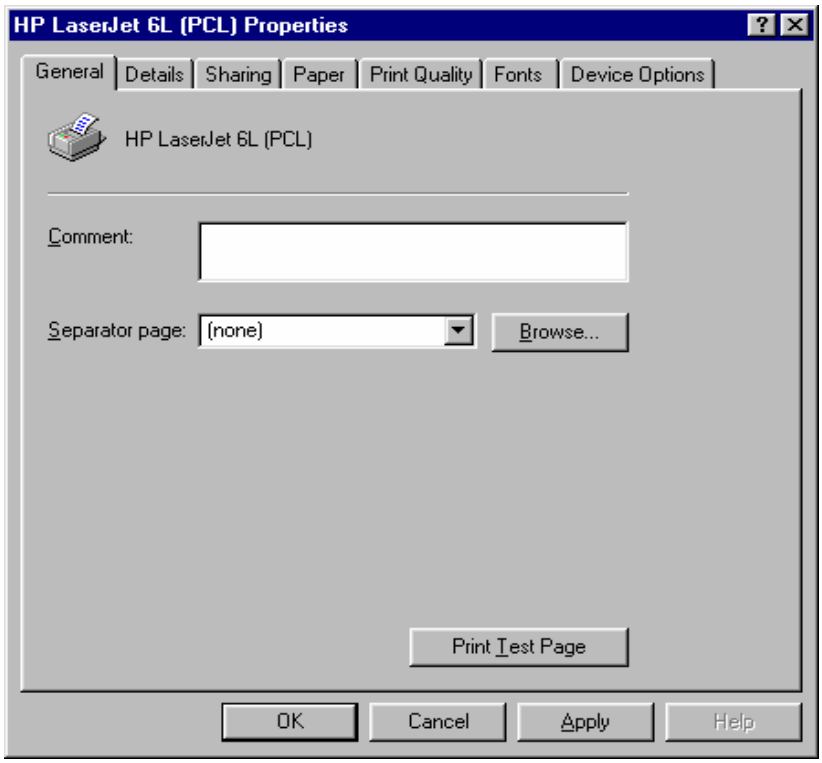
5.1 Configuring on Windows 95/98 Platforms

After you finished the software installation procedure described in Chapter 3, your computer has possessed the network printing facility provided by this product. For convenience, we call the printer connected to the printer port of this product as server printer. On a Windows 95/98 platform, open the **Printers** window in the **My Computer** menu:

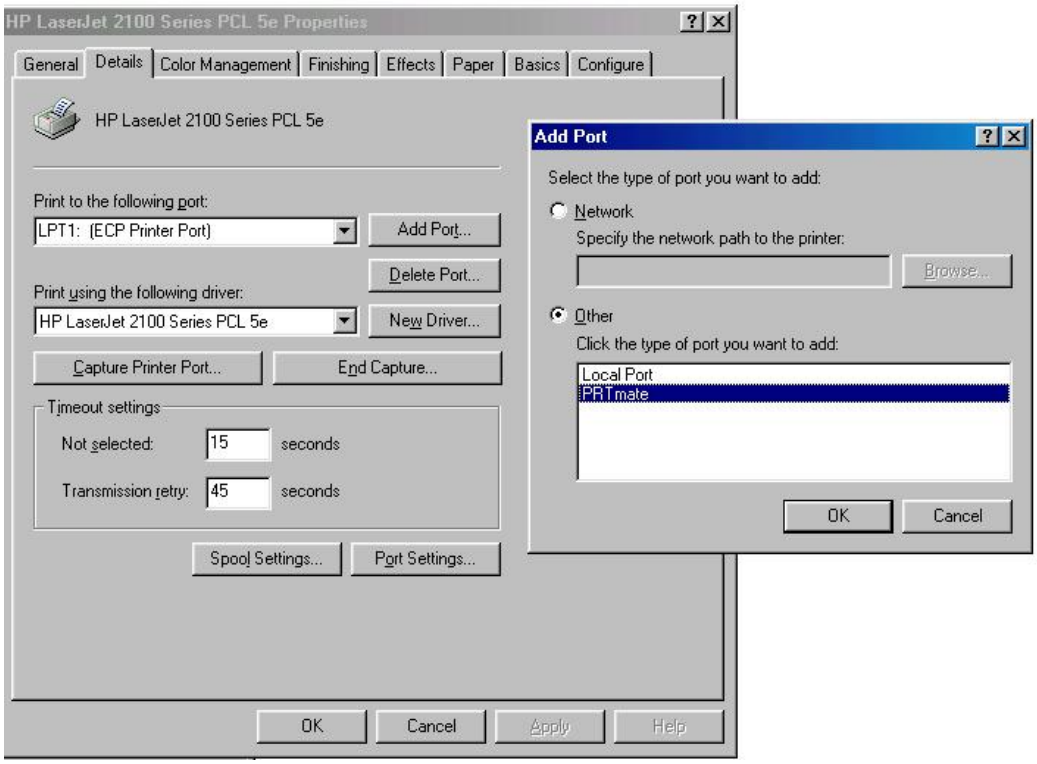


Now, yon can configure the print server of this product:

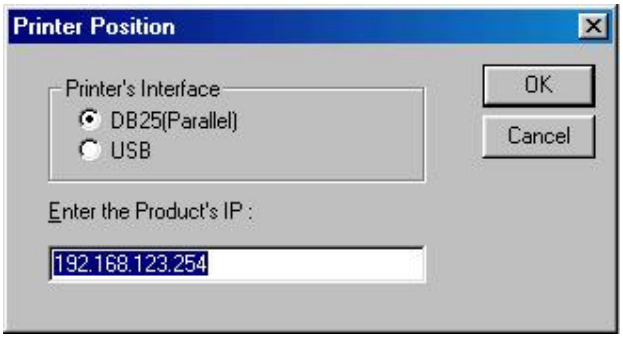
1. Find out the corresponding icon of your server printer, for example, the **HP LaserJet 6L**. Click the mouse's right button on that icon, and then select the **Properties** item:



2. Click the **Details** item:



3. Choose the "PRTmate: (All-in-1)" from the list attached at the **Add Port** item. Be sure that the **Printer Driver** item is configured to the correct driver of your server printer.
4. Click on the button of **OK**:

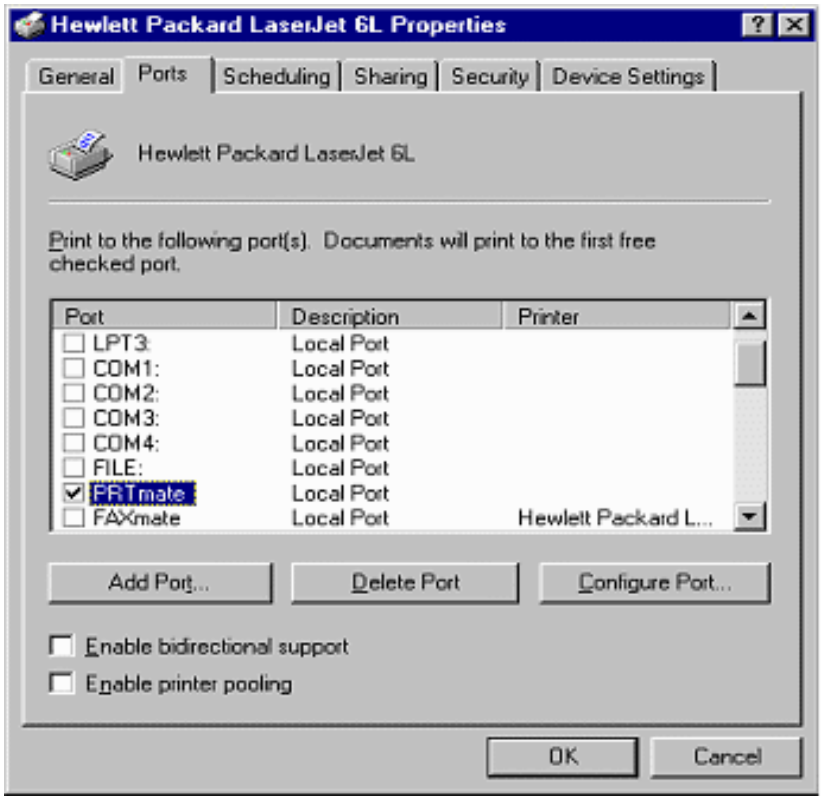


Type in the IP address of this product and then click the **OK** button.

1. Make sure that all settings mentioned above are correct and then click the **OK** button.

5.2 Configuring on Windows NT Platforms

The configuration procedure for a Windows NT platform is similar to that of Windows 95/98 except the screen of printer **Properties**:



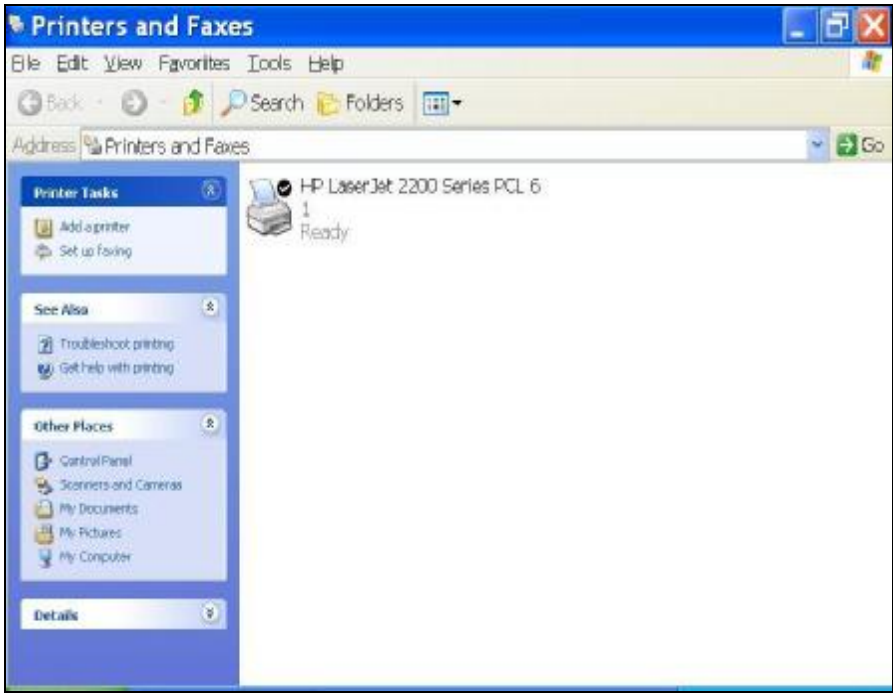
Compared to the procedure in last section, the selection of **Details** is equivalent to the selection of **Ports**, and **Port Settings** is equivalent to **Configure Port**.

5.3 Configuring on Windows 2000 and XP Platforms

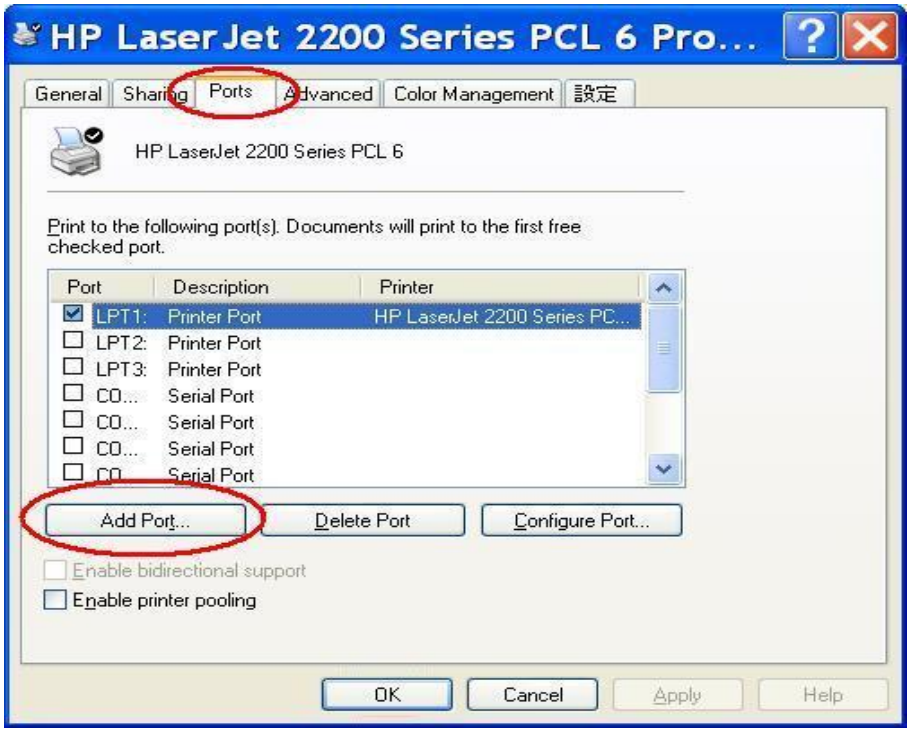
Windows 2000 and XP have built-in LPR client, users could utilize this feature to Print.

You have to install your Printer Driver on LPT1 or other ports before you preceed the following sequence.

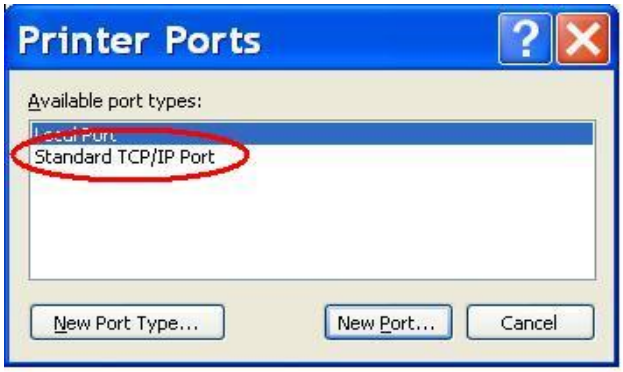
1.Open Printers and Faxs.



2.Select “Ports” page, Click “Add Port…”

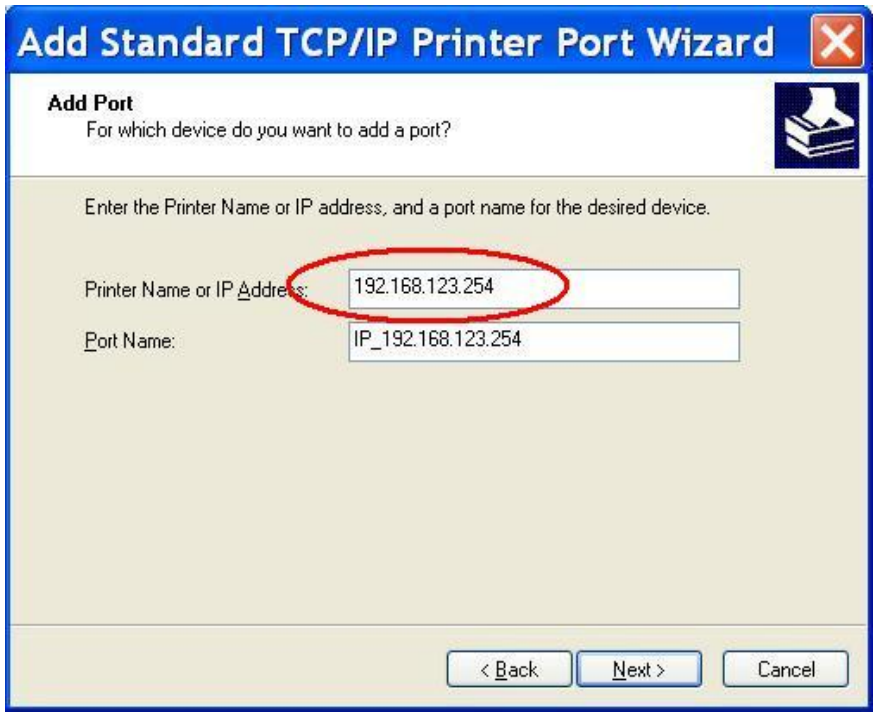


3. Select “Standard TCP/IP Port”, and then click “New Port…”

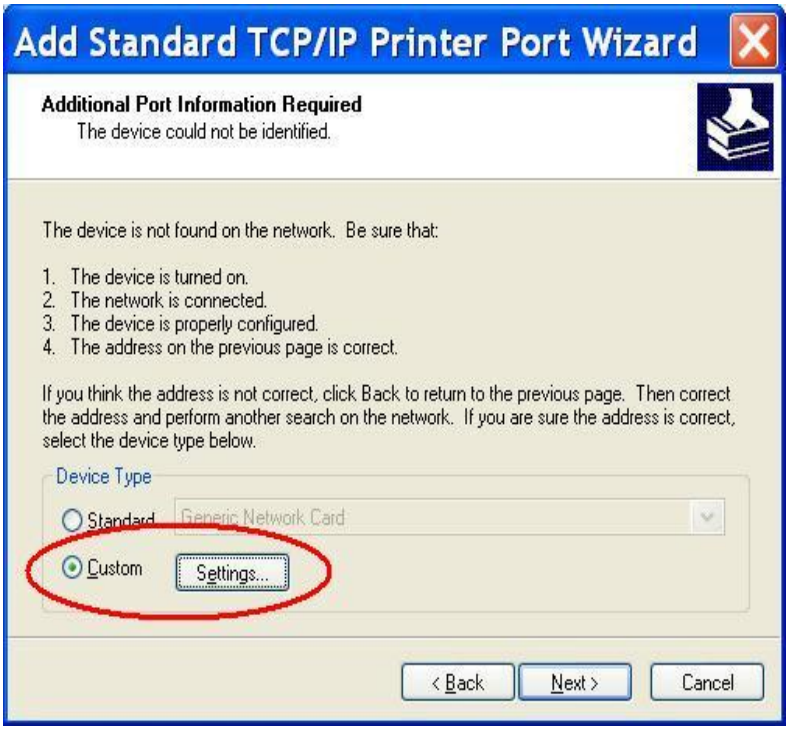


4.Click Next and then provide the following information:

Type address of server providing LPD that is our NAT device:192.168.123.254

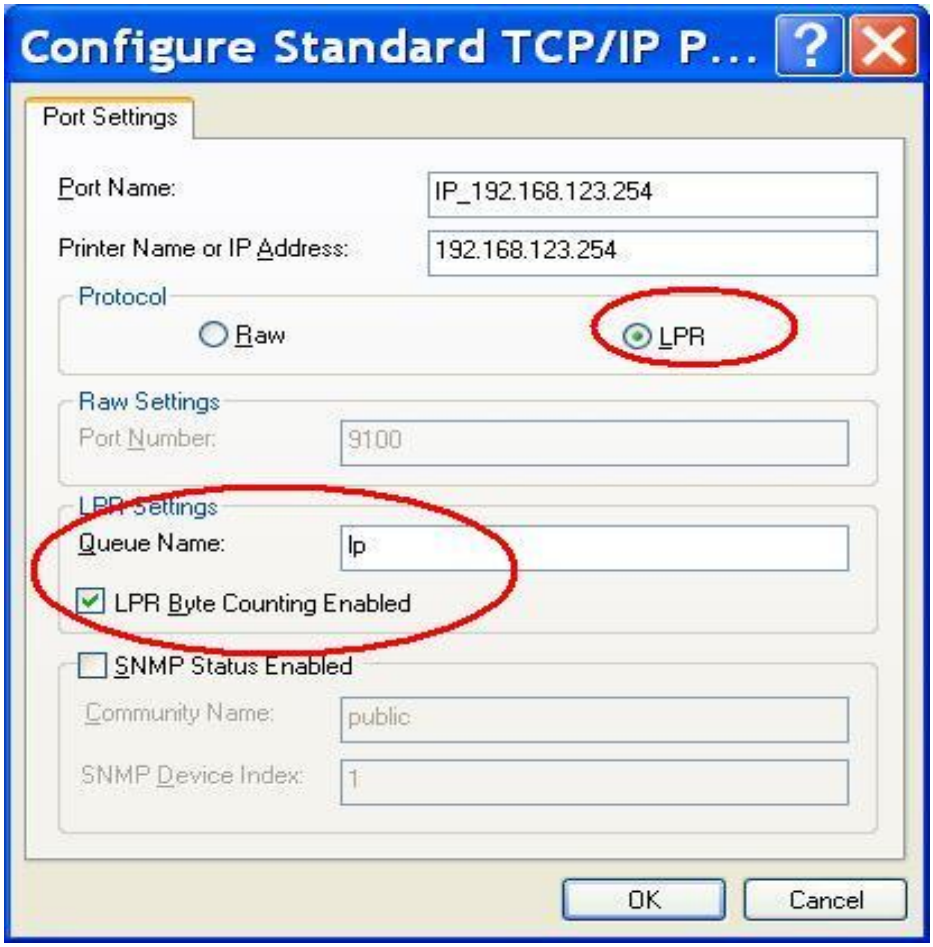


5. Select Custom, then click “Settings…”

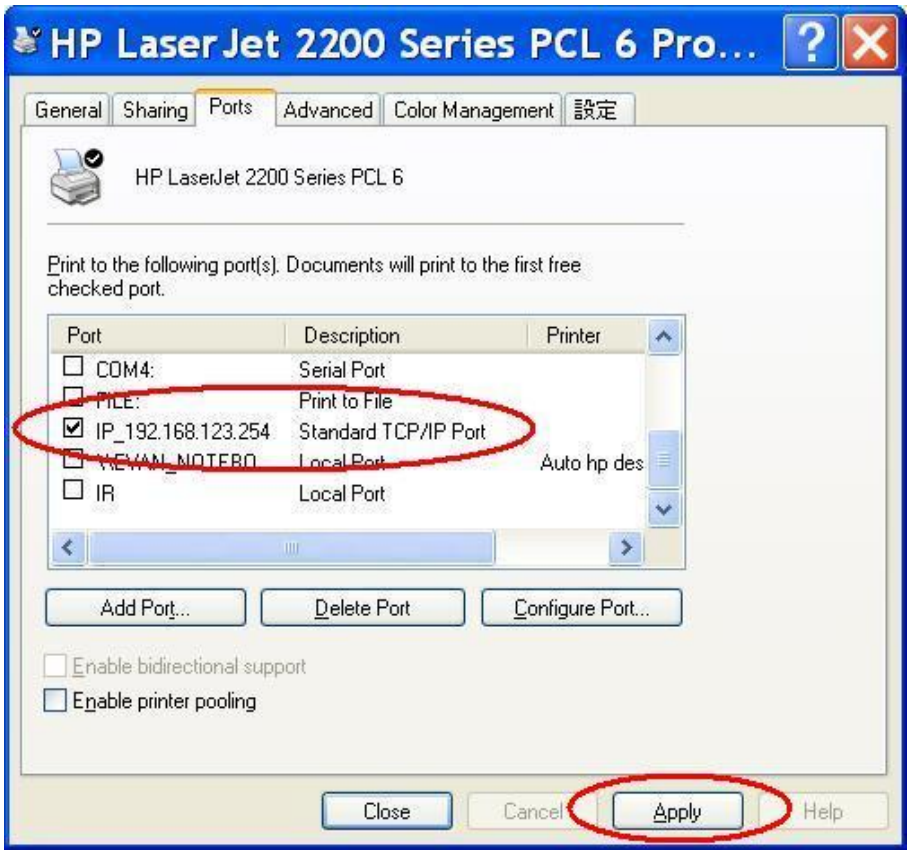


6.Select “LPR”, type ” **lp**“ lowercase letter in “Queue Name:”

And enable “LPR Byte Counting Enabled”.



7.Apply your settings



5.4 Configuring on Unix-like based Platforms

Please follow the traditional configuration procedure on Unix platforms to setup the print server of this product. The printer name is “lp.”

※Noticed: If the router has USB and Parallel port at the same time, Please be careful to setup.

1.Use Parallel to print

Queue Name: lp

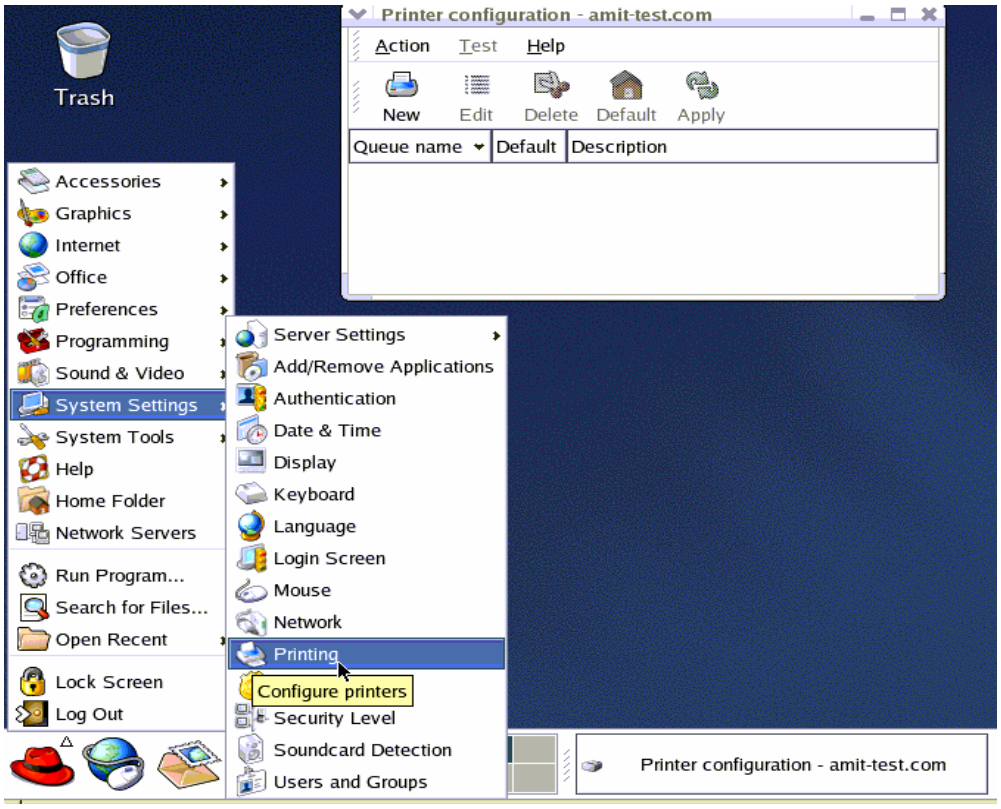
2.Use USB to print

Queue Name: lpUSB0

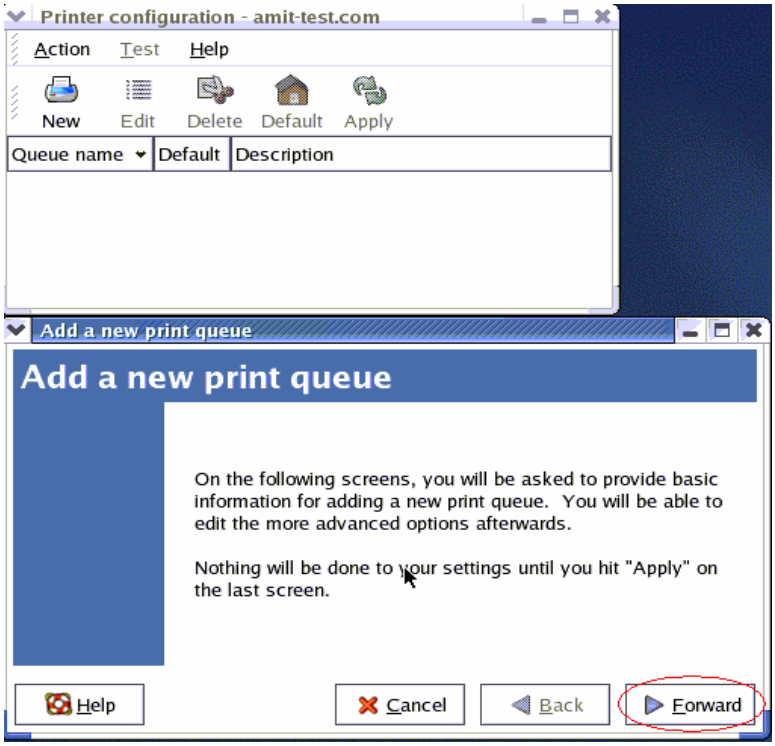
In X-Windows, for example, In Redhat Platforms,

Please follow the below steps to configure your printer on Red Hat 9.0.1. Start from the Red Hat--->

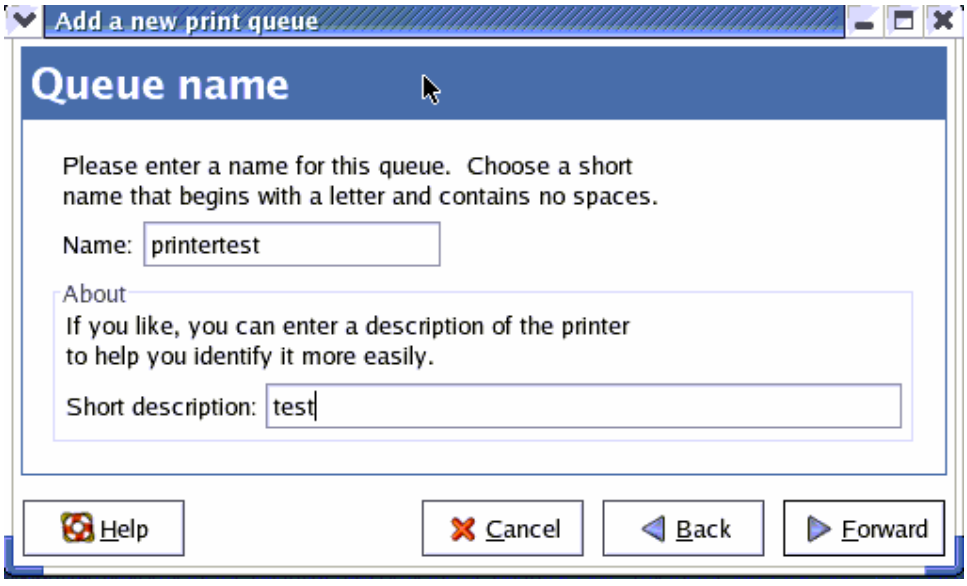
System Setting---> Printing.



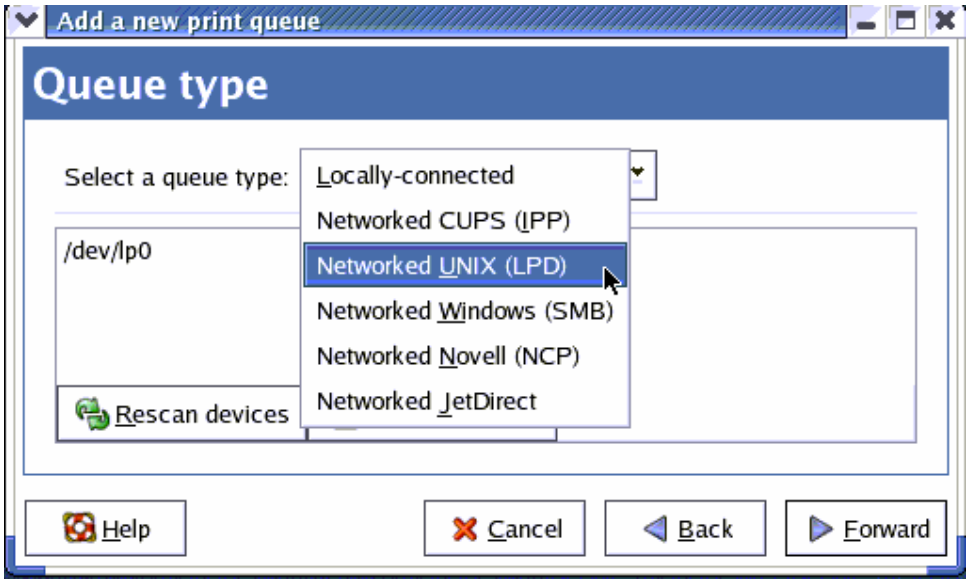
2. Click New---> Forward.



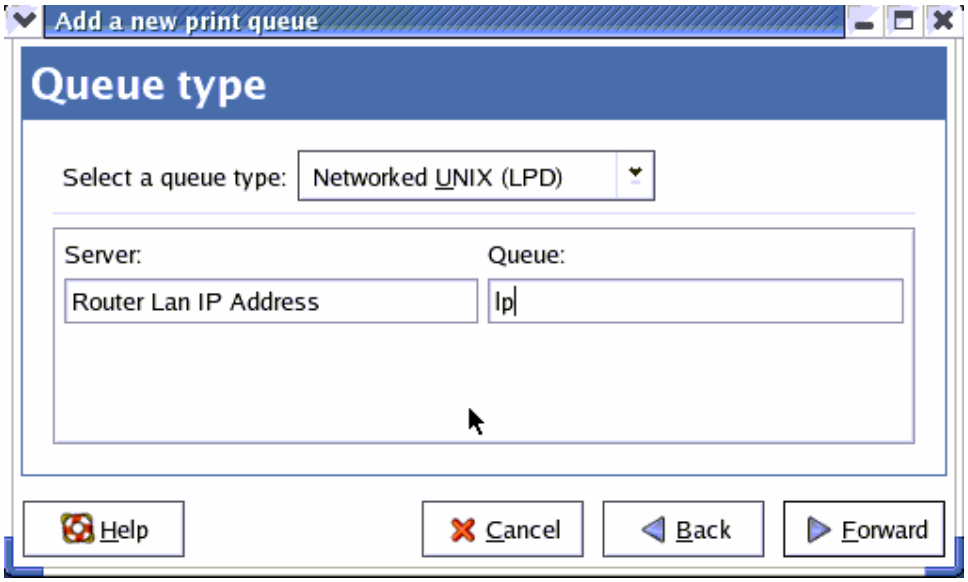
1. Enter the Pinter Name, Comments then forward.



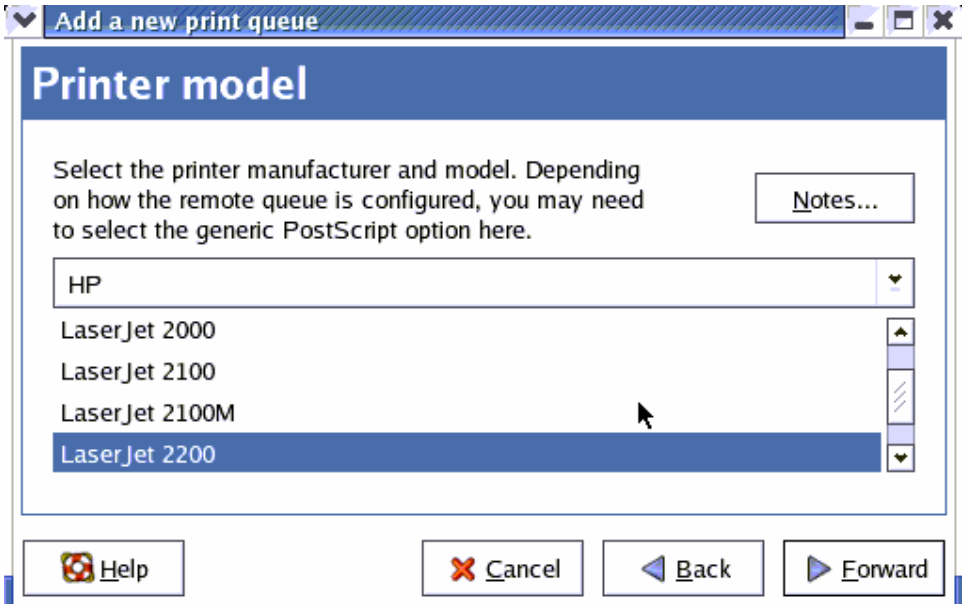
4. Select LPD protocol and then forward.



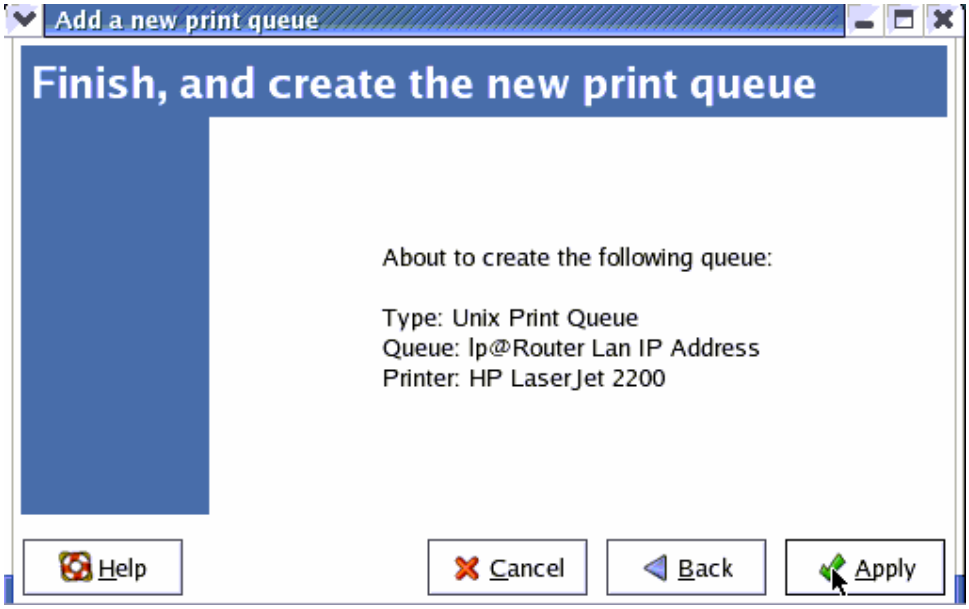
5. Enter Router LAN IP Address and the queue name "lp". Then forward.



6. Select the Printer Brand and Model Name. Then Forward.



7. Click Apply to finish setup.



8. At last you must click Apply on the toolbox to make the change take effective.

In Command Mode:

Linux has built-in LPR client ,You can utilize it for printing.

You can manual set it or via the tool "printtool" in X-windows.

PS: The spool name is "lp"------all lowercase letter.

Below is my setting.

/etc/printcap

```
lp:\
:sd=/var/spool/lpd/lp:\
:mx#0:\
:sh:\
:rm=192.168.123.254:\
:rp=lp:\ ---------->key point
:if=/var/spool/lpd/lp/filter:
```

Then add the corresponding directory

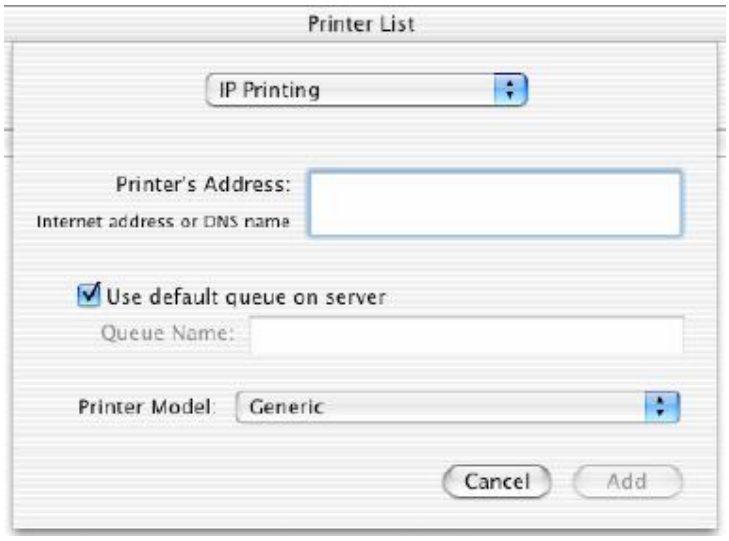
```
#mkdir /var/spool/lpd/lp
```

Too see the detail ,please refer to the online manual in linux.

```
#man printcap
```

5.5 Configuring on Apple PC

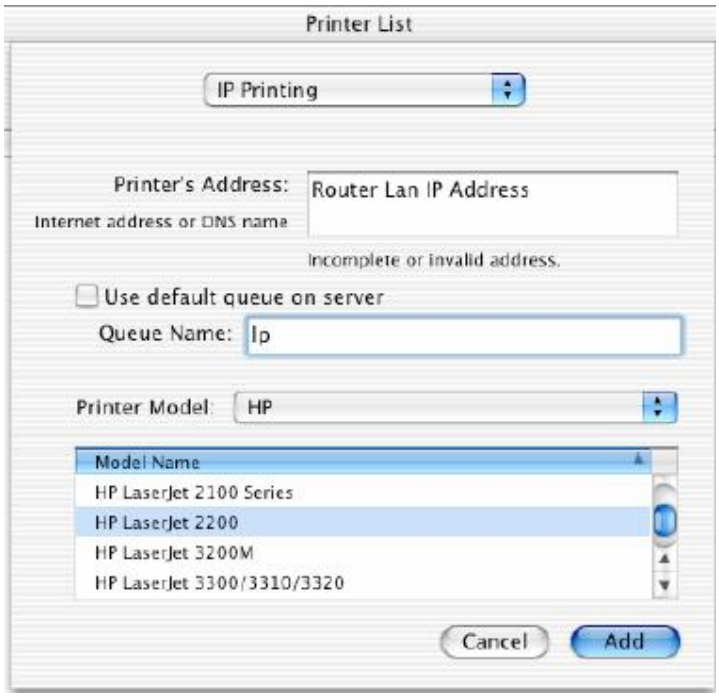
1.First, go to Printer center (Printer list) and add printer



2.Choose IP print and setup printer ip address (router Lan ip address).

3.Disable "Default Queue of Server." And fill in ' **lp** ' in Queue name item.

4.Printer Model: Choose "General" or Printer as below.



※Noticed: If the router has USB and Parallel port at the same time, Please be careful to setup.

1.Use Parallel to print

Queue Name: lp

2.Use USB to print

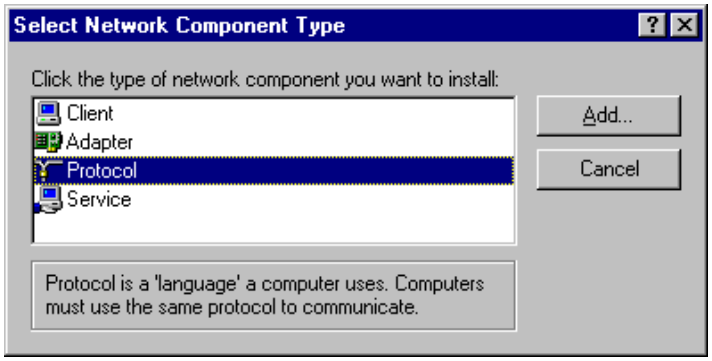
Queue Name: lpUSB0

Appendix A TCP/IP Configuration for Windows 95/98

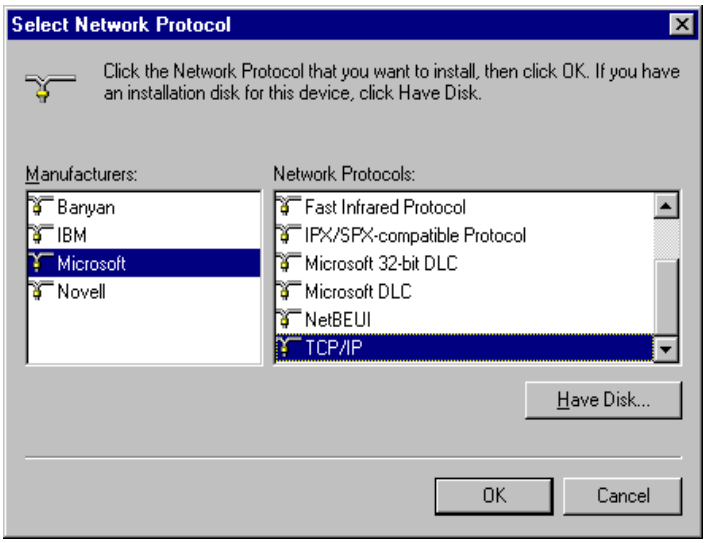
This section introduces you how to install TCP/IP protocol into your personal computer. And suppose you have been successfully installed one network card on your personal computer. If not, please refer to your network card manual. Moreover, the Section B.2 tells you how to set TCP/IP values for working with this NAT Router correctly.

A.1 Install TCP/IP Protocol into Your PC

1. Click **Start** button and choose **Settings**, then click **Control Panel**.
2. Double click **Network** icon and select **Configuration** tab in the Network window.
3. Click **Add** button to add network component into your PC.
4. Double click **Protocol** to add TCP/IP protocol.



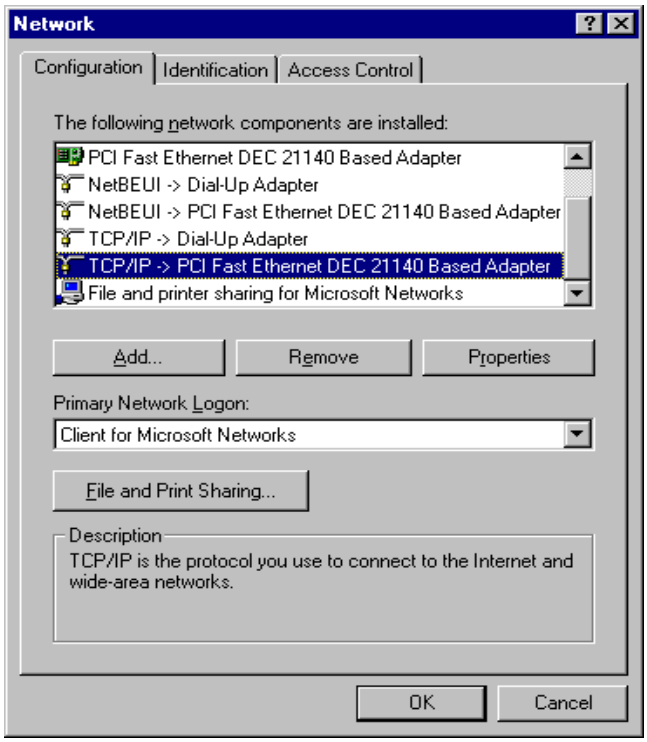
5. Select **Microsoft** item in the manufactures list. And choose **TCP/IP** in the Network Protocols. Click **OK** button to return to Network window.



6. The TCP/IP protocol shall be listed in the Network window. Click **OK** to complete the install procedure and restart your PC to enable the TCP/IP protocol.

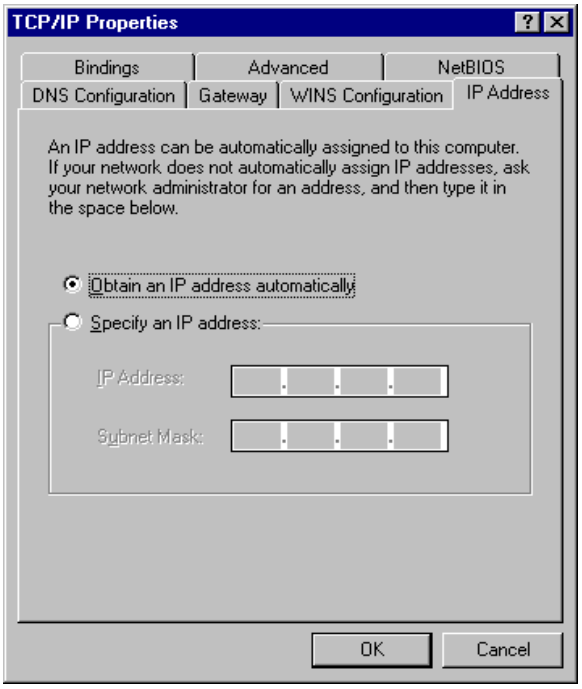
A.2 Set TCP/IP Protocol for Working with NAT Router

1. Click **Start** button and choose **Settings**, then click **Control Panel**.
2. Double click **Network** icon. Select the TCP/IP line that has been associated to your network card in the **Configuration** tab of the Network window.

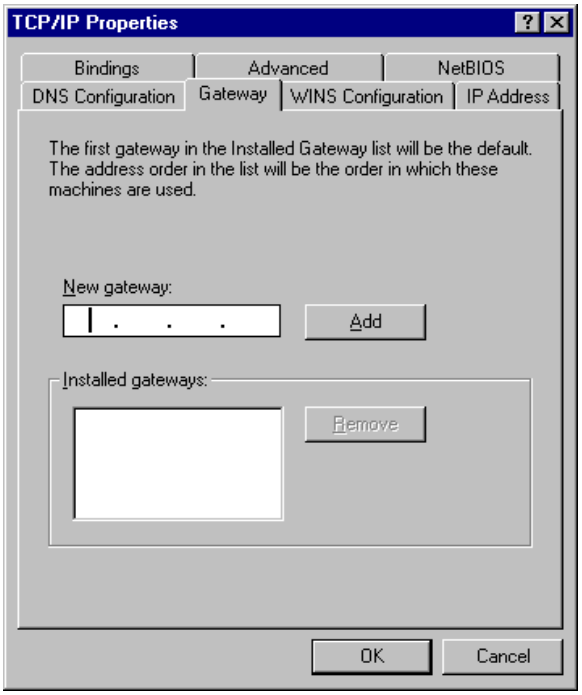


3. Click **Properties** button to set the TCP/IP protocol for this NAT Router.
4. Now, you have two setting methods:

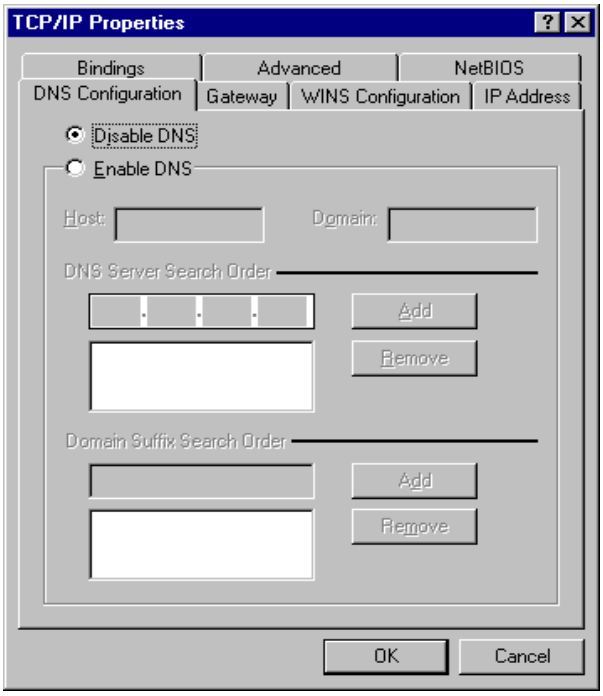
a. Select **Obtain an IP address automatically** in the IP Address tab.



b. Don't input any value in the Gateway tab.

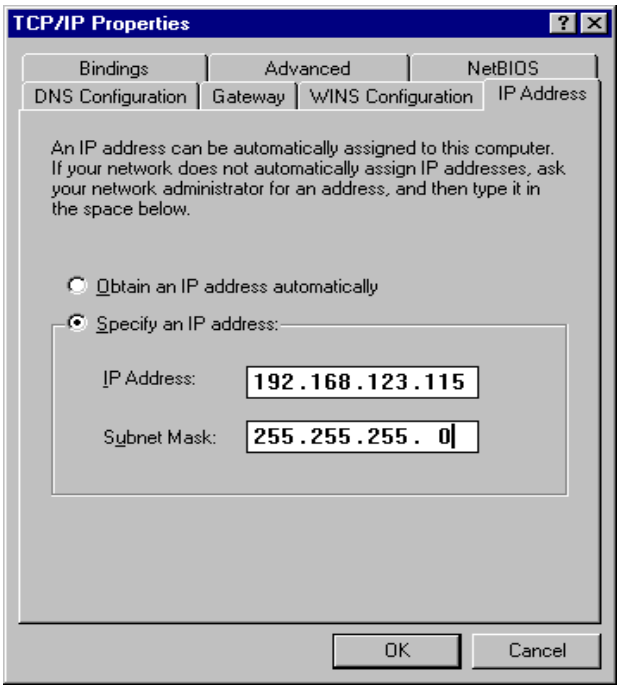


c. Choose **Disable DNS** in the DNS Configuration tab.

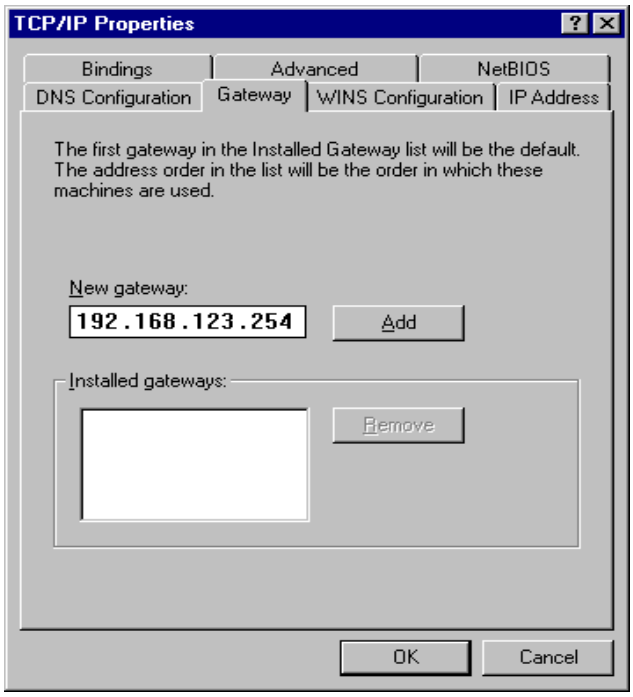


B. Configure IP manually

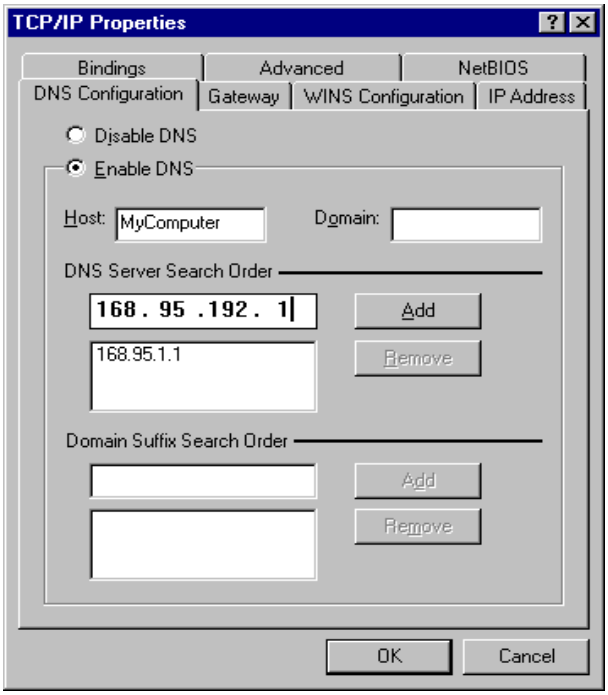
a. Select **Specify an IP address** in the IP Address tab. The default IP address of this product is 192.168.123.254. So please use 192.168.123.xxx (xxx is between 1 and 253) for IP Address field and 255.255.255.0 for Subnet Mask field.



b. In the Gateway tab, add the IP address of this product (default IP is 192.168.123.254) in the New gateway field and click **Add** button.



c. In the DNS Configuration tab, add the DNS values which are provided by the ISP into DNS Server Search Order field and click **Add** button.



Appendix B Reset to Factory Default

Reset to factory Default

There are 2 methods to reset to default.

1. **Restore with RESET button**

First, turn off the router and press the RESET button in. And then, power on the router and hold the RESET button down until the STATUS and or M2 LED (or Status LED) start flashing, then move away the hand. If LED flashes about 8 times, the RESTORE process is completed. However, if LED flashes 2 times, repeat.

2. **Restore directly when the router power on**

First, hold the RESET button about 5 seconds(STATUS will start flashing about 5 times),move away the hand. The RESTORE process is completed.