

LevelOne

FBR-1409TX

Broadband Router

w/VPN/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, and EN 50082-1. This meets the essential protection requirements of the European Council Directive 89/336/EEC on the approximation of the laws of the member states relation to electromagnetic compatibility.

Table of Contents

Chapter 1	Introduction	1
	Functions and Features	1
	Packing List	3
Chapter 2	Hardware Installation	4
	2.1 Panel Layout	4
	2.2 Installation Requirements	6
	2.3 Procedure for Hardware Installation.....	6
Chapter 3	Network Settings and Software Installation.....	7
	3.1 Make Correct Network Settings of Your Computer.....	7
	3.2 Install the Software into Your Computers.....	8
Chapter 4	Configuring NAT Router.....	11
	4.1 Start-up and Log in	11
	4.2 Status.....	12
	4.3 Wizard.....	13
	4.4 Basic Setting	15
	4.4.1 Primary Setup – WAN Type, Virtual Computers	16
	4.4.2 DHCP Server.....	21
	4.4.3 Change Password.....	23
	4.5 Forwarding Rules.....	24
	4.5.1 Virtual Server	25
	4.5.2 Special AP.....	26
	4.5.3 Miscellaneous Items.....	27
	4.6 Security Settings	28
	4.6.1 Packet Filter	29
	4.6.2 Domain Filter.....	34
	4.6.3 URL Blocking	36
	4.6.4 MAC Address Control	38
	4.6.5 VPN setting	40
	4.6.6 Miscellaneous Items.....	46
	4.7 Advanced Setting	47
	4.7.1 System Time.....	48
	4.7.2 System Log	49
	4.7.3 Dynamic DNS	50
	4.7.4 SNMP Setting	52
	4.7.5 Routing Table.....	54

4.7.6 Schedule Rule	56
4.8 Toolbox	60
4.8.1 System Log	61
4.8.2 Firmware Upgrade	62
4.8.3 Backup Setting	63
4.8.4 Reset to default	63
4.8.5 Reboot	63
4.8.6 Miscellaneous Items.....	64
Chapter 5 Print Server.....	65
5.1 Configuring on Windows 95/98 Platforms	65
5.2 Configuring on Windows NT Platforms	68
5.3 Configuring on Windows 2000 and XP Platforms.....	69
5.4 Configuring on Unix based Platforms	75
Appendix A TCP/IP Configuration for Windows 95/98	76
A.1 Install TCP/IP Protocol into Your PC.....	76
A.2 Set TCP/IP Protocol for Working with NAT Router	78

Chapter 1 Introduction

Congratulations on your purchase of this outstanding LevelOne FBR-1409TX Broadband Router. This product is specifically designed for Small Office and Home Office needs. It provides a complete SOHO solution for Internet surfing and office resources sharing, and it is easy to configure and operate for even 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

- **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.
- **VPN supported**
Supports multiple PPTP sessions and allows you to setup VPN server and VPN clients.
- **Printer sharing**
Embeds a print server to allow all of the networked computers to share one printer.
Built-in USB host to connect to USB printer for printer sharing.
- **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.
- **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.
- **Universal Plug and Play (UPnP) supported**
Universal Plug and Play (UPnP) enable devices such as PCs, routers or other devices to be plugged into a network and automatically know about each other.
- **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.

- **Domain Filter Supported**

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

- **SNMP Supported**

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.

- **Routing Table Supported**

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.

- **System Time Supported**

Allow you to synchronize system time with network time server.

- **Statistics of WAN Supported**

Enables you to monitor inbound and outbound packets

- **VPN Supported**

Enables you to create virtual private tunnels to remote VPN gateways.

- **Virtual Computers supported:** 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.

Packing List

- Broadband router unit
- Installation CD-ROM
- Power adapter

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 indicators	Orange	Blinking	STATUS is flashed once per second to indicate system is alive.
WAN	WAN port activity	Green	On	The WAN port is linked.
			Blinking	The WAN port is sending or receiving data.
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.
Speed 10/100	Data Rate	Green	On	Data is transmitting in 100Mbps on the corresponding LAN port.
USB	USB port activity	Green	On	The USB port is linked.
			Blinking	The USB port is sending or receiving data.

Port:

RESET

To reset system settings to factory defaults, please follow the steps:

1. Power off the device,
2. Press the reset button and hold,
3. Power on the device,
4. Keep the button pressed about 5 seconds,
5. Release the button,
6. Watch the STATUS LED, it will flash 2 times and then flash once per second.

2.1.2. Rear Panel

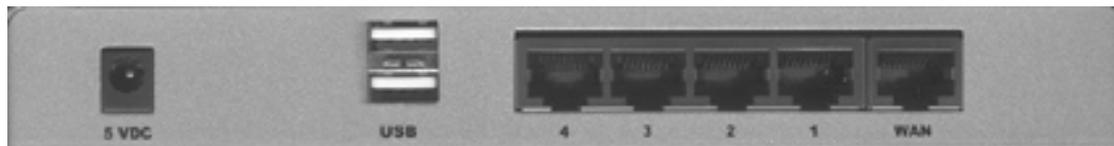


Figure 2-2 Rear Panel

Ports:

Port	Description
5VDC	Power inlet: DC 5V, 1.5A (minimum)
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 port for USB printer.

2.2 Installation Requirements

FBR-1409TX can be positioned at any convenient place in your office or house. No special wiring or cooling requirements is needed. However, you should comply with the following guidelines to install:

- Place this product on a flat horizontal plane.
- Keep this product away from any heating devices.
- Do not place this product in dusty or wet environment.

In addition, remember to turn off the power, remove the power cord from the outlet, and keep your hands dry when you try to install the hardware of this product.

2.3 Procedure for Hardware Installation

- 1. Setup LAN connection:** connect an Ethernet cable from your computer's Ethernet port to one of the LAN ports of this product.
- 2. Setup WAN connection:** prepare an Ethernet cable for connecting this product to your cable/xDSL modem or Ethernet backbone.

3. Power on:

Connecting the power cord to power inlet, this product will automatically enter the self-test phase. When it is in the self-test phase, the indicators STATUS will be lighted ON for about 5 seconds, and then STATUS will be flashed 2 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 LevelOne FBR-1409TX 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 LevelOne FBR-1409TX 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.

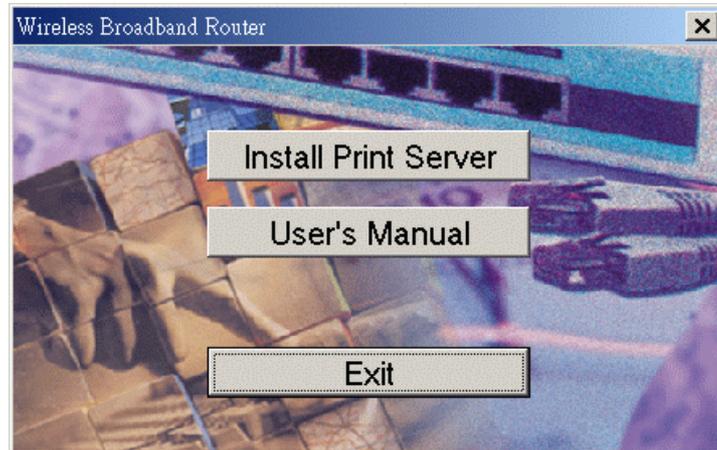
2. *Is the TCP/IP environment of your computers properly configured?*

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.

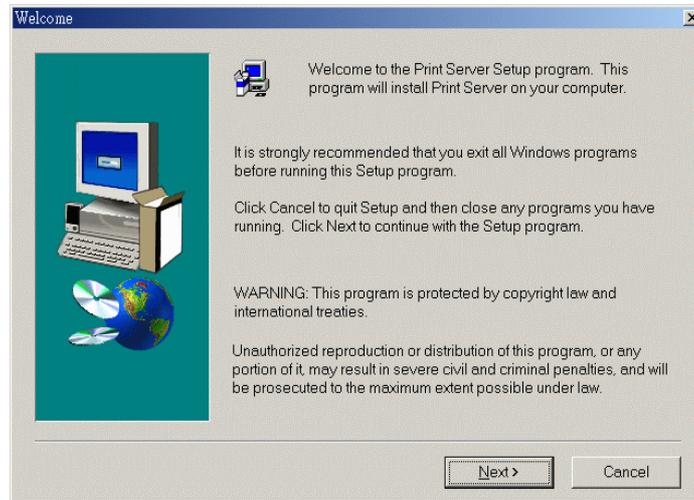
3.2 Install the Software into Your Computers

Skip this section if you do not want to use the print server function of FBR-1409TX.

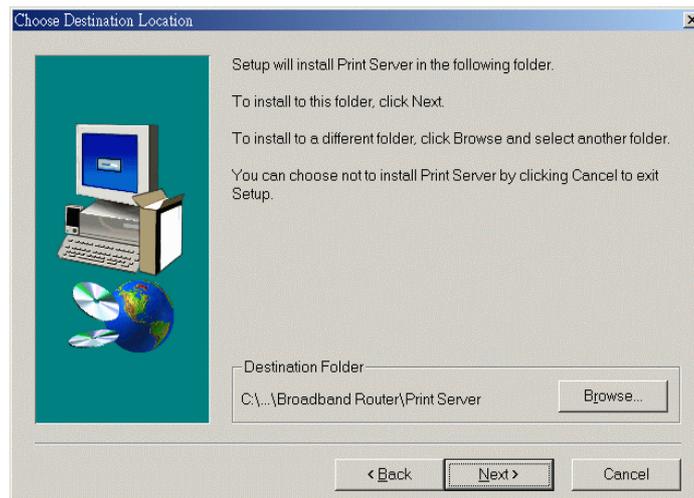
Step 1: Insert the installation CD-ROM into the CD-ROM drive. The following window will be shown automatically. If it isn't, please run "install.exe" on the CD-ROM.



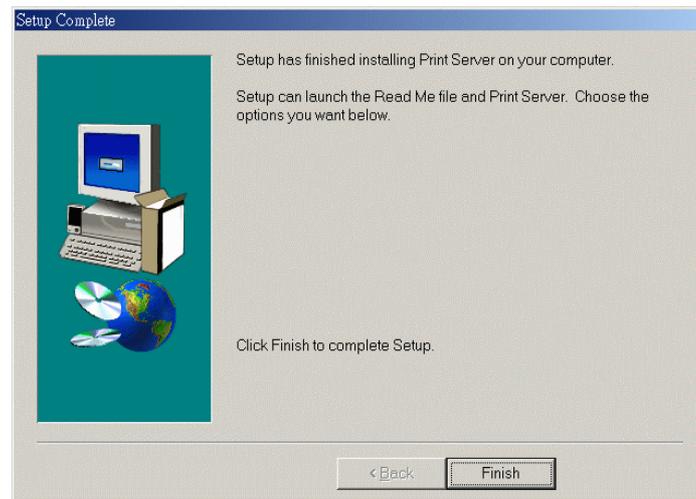
Step 2: Click on the **INSTALL** button. Wait until the following **Welcome** dialog to appear, and click on the **Next** button.



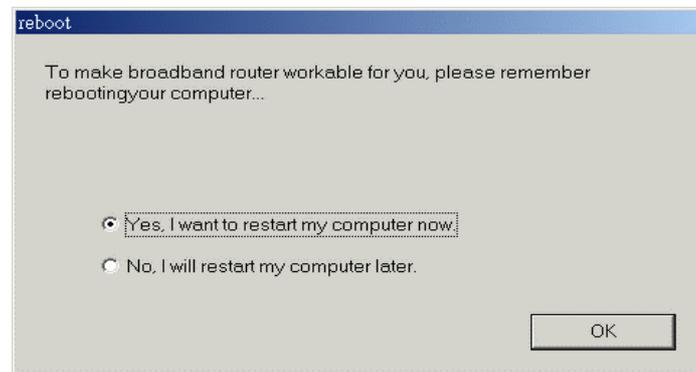
Step 3: Select the destination folder and click on the **Next** button. Then, the setup program will begin to install the programs into the destination folder.



Step 4: When the following window is displayed, click on the **Finish** button.



Step 5: Select the item to restart the computer and then click the **OK** button to reboot your computer.



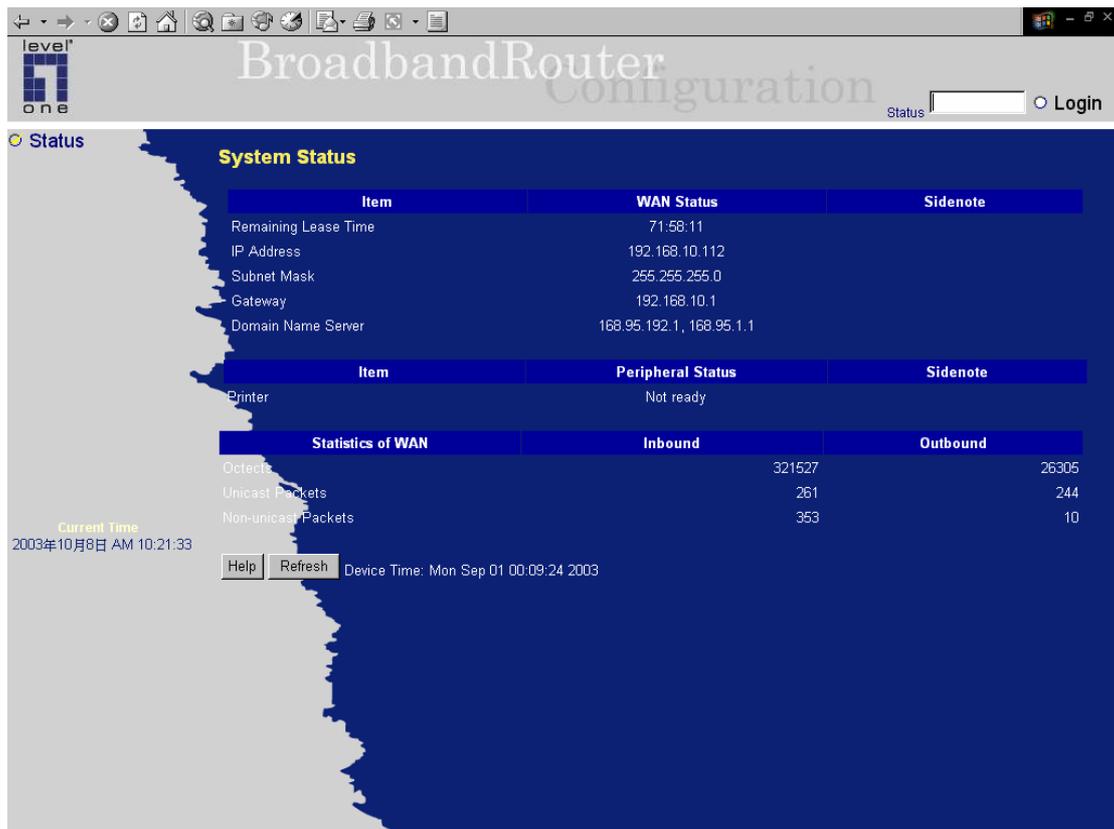
Step 6: After rebooting your computer, the software installation procedure is finished.

Now, you can configure the NAT Router (refer to Chapter 4) and setup the Print Server (refer to Chapter 5).

Chapter 4 Configuring NAT Router

LevelOne FBR-1409TX 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

The screenshot shows the 'level one' BroadbandRouter configuration interface. The main content area is titled 'System Status' and contains three tables. The first table, 'WAN Status', lists items like 'Remaining Lease Time', 'IP Address', 'Subnet Mask', 'Gateway', and 'Domain Name Server'. The second table, 'Peripheral Status', shows a 'Printer' with a status of 'Not ready'. The third table, 'Statistics of WAN', shows inbound and outbound packet counts for 'Octets', 'Unicast Packets', and 'Non-unicast Packets'. There are also buttons for 'View Log...', 'Clients List...', 'Help', and 'Refresh', and a 'Device Time' display.

Item	WAN Status	Sidenote
Remaining Lease Time	71:57:44	<input type="button" value="Renew"/>
IP Address	192.168.10.112	<input type="button" value="Release"/>
Subnet Mask	255.255.255.0	
Gateway	192.168.10.1	
Domain Name Server	168.95.192.1, 168.95.1.1	

Item	Peripheral Status	Sidenote
Printer	Not ready	

Statistics of WAN	Inbound	Outbound
Octets	328642	26397
Unicast Packets	263	246
Non-unicast Packets	387	10

Current Time: 2003年10月8日 AM 10:21:52
Device Time: Mon Sep 01 00:09:50 2003

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

A. WAN Port Status.

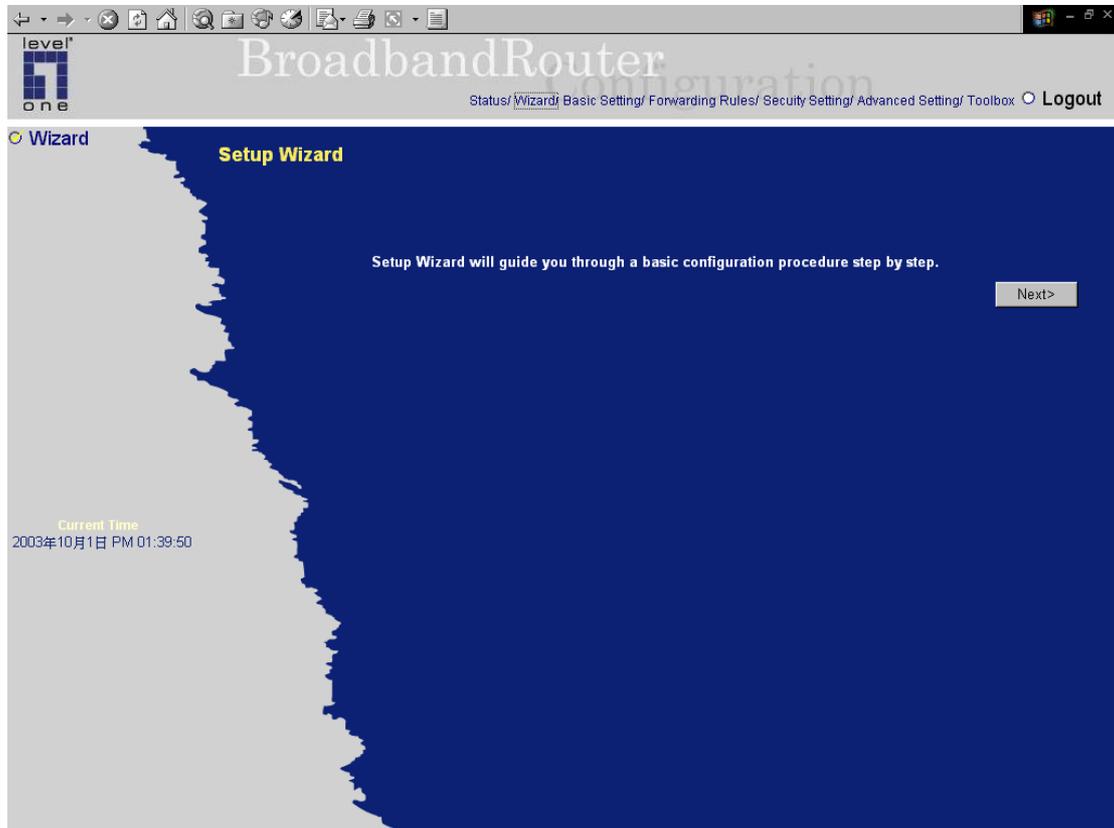
If the WAN port is assigned a dynamic IP, there may appear a **“Renew”** or **“Release”** button on the *Sidenote* column. You can click this button to renew or release IP manually.

B. Printer Status. The possible kinds of printer status include *“Ready”*, *“Not ready”*, *“Printing...”*, and *“Device error”*.

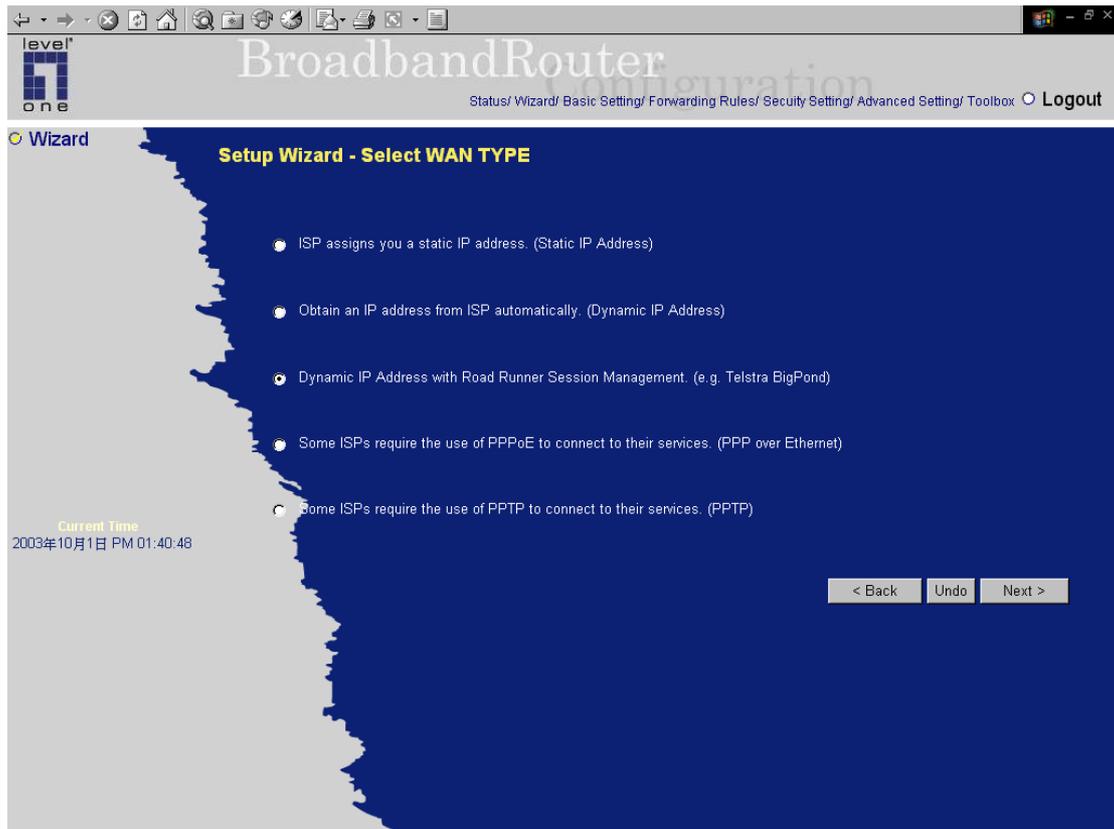
When a job is printing, there may appear a “Kill Job” button on the Sidenote column. You can click this button to kill current printing job manually.

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

4.3 Wizard

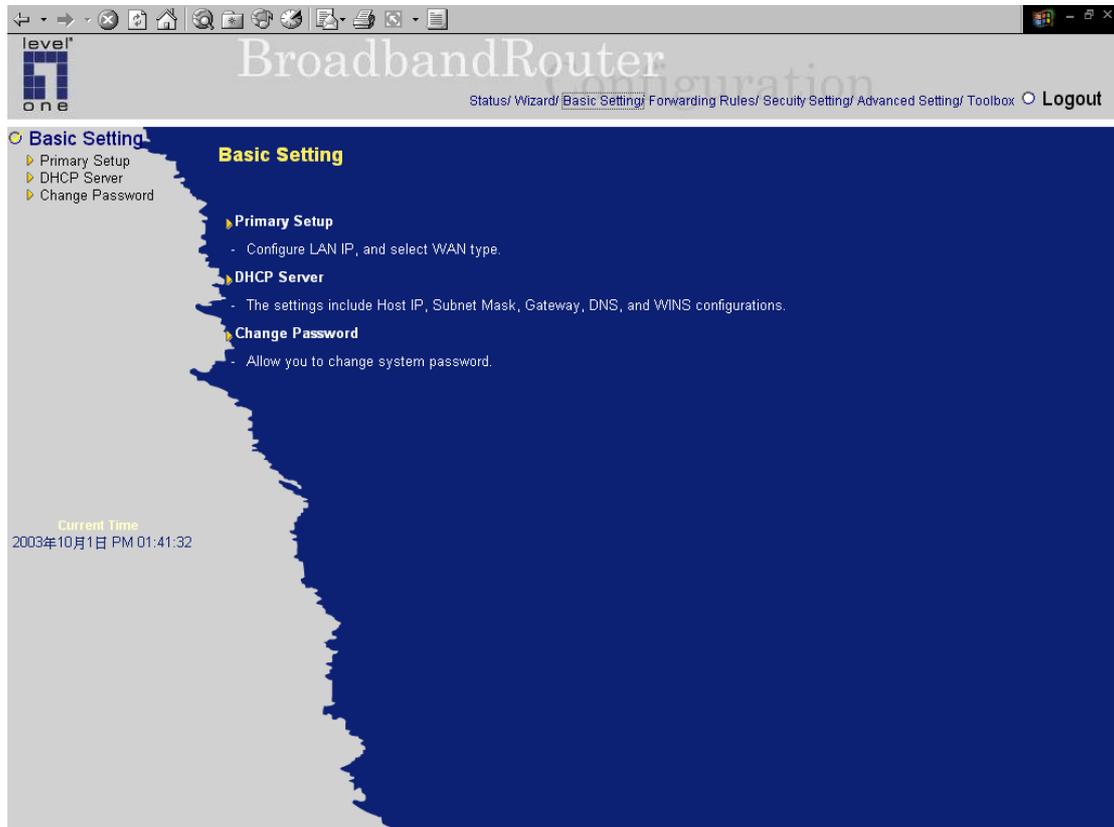


Setup Wizard will guide you through a basic configuration procedure step by step.
Press "Next >"



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

4.4 Basic Setting



The screenshot displays the web interface of a level one BroadbandRouter. The browser's address bar shows the URL [http://192.168.1.1/levelone/Configuration](#). The page title is "BroadbandRouter Configuration". The navigation menu includes: Status / Wizard / **Basic Setting** / Forwarding Rules / Security Setting / Advanced Setting / Toolbox / Logout.

The "Basic Setting" section is expanded, showing a sidebar with the following options:

- ▶ Primary Setup
- ▶ DHCP Server
- ▶ Change Password

The main content area lists the following sub-sections:

- Primary Setup**
 - Configure LAN IP, and select WAN type.
- DHCP Server**
 - The settings include Host IP, Subnet Mask, Gateway, DNS, and WINS configurations.
- Change Password**
 - Allow you to change system password.

At the bottom left, the "Current Time" is displayed as 2003年10月1日 PM 01:41:32.

4.4.1 Primary Setup – WAN Type, Virtual Computers

The screenshot shows the LevelOne BroadbandRouter configuration interface. The main title is "BroadbandRouter Configuration". The navigation menu includes: Status / Wizard / Basic Setting / Forwarding Rules / Security Setting / Advanced Setting / Toolbox / Logout.

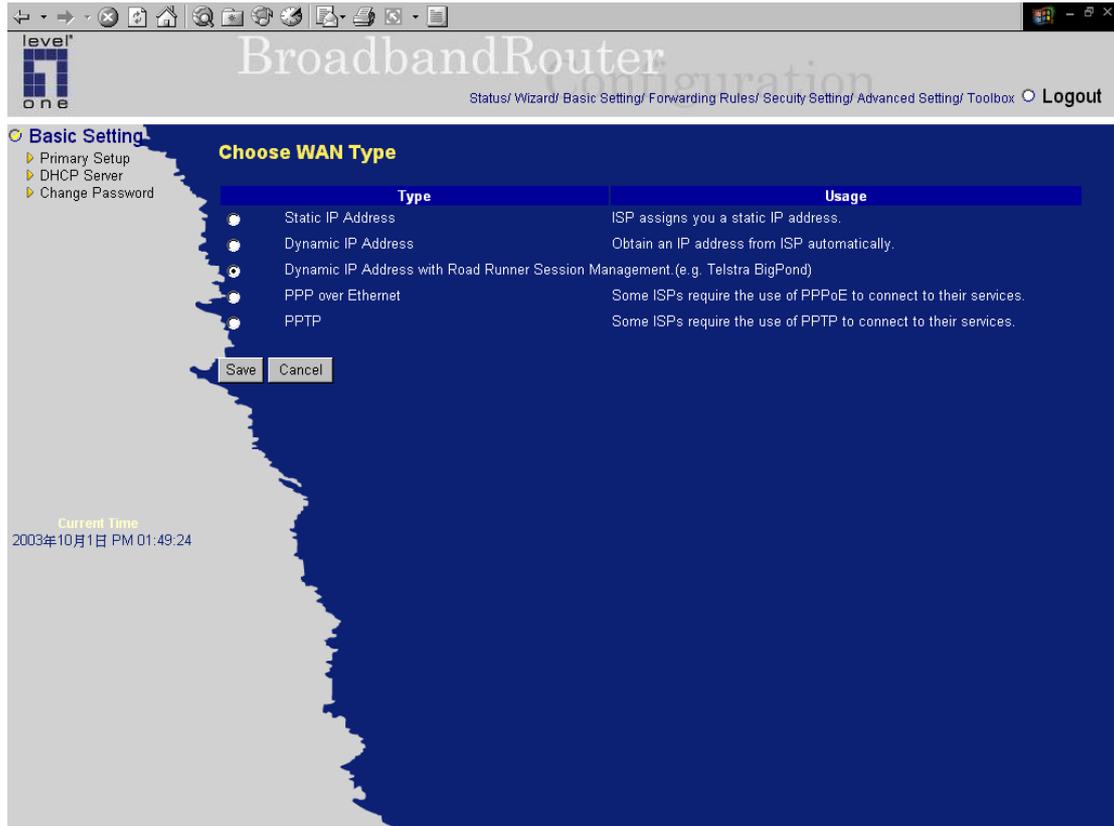
The "Basic Setting" menu is expanded, showing: Primary Setup, DHCP Server, and Change Password. The "Primary Setup" section is active, displaying a table of settings:

Item	Setting
LAN IP Address	192.168.123.254
WAN Type	Dynamic IP Address <input type="button" value="Change..."/>
Host Name	<input type="text"/> (optional)
WAN's MAC Address	00-50-18-21-60-43 <input type="button" value="Clone MAC"/>
Renew IP Forever	<input type="checkbox"/> Enable (Auto-reconnect)

At the bottom of the Primary Setup section, there are buttons for: Save, Undo, Virtual Computers..., and Help.

The current time is displayed as: 2003年10月8日 AM 10:23:14.

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)

LAN IP Address is the IP address of this product. It must be the default gateway of your computers.

WAN Type is *Dynamic IP Address*. If the WAN type is not correct, change it!

Host Name: optional. Required by some ISPs, e.g. @Home.

- *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.

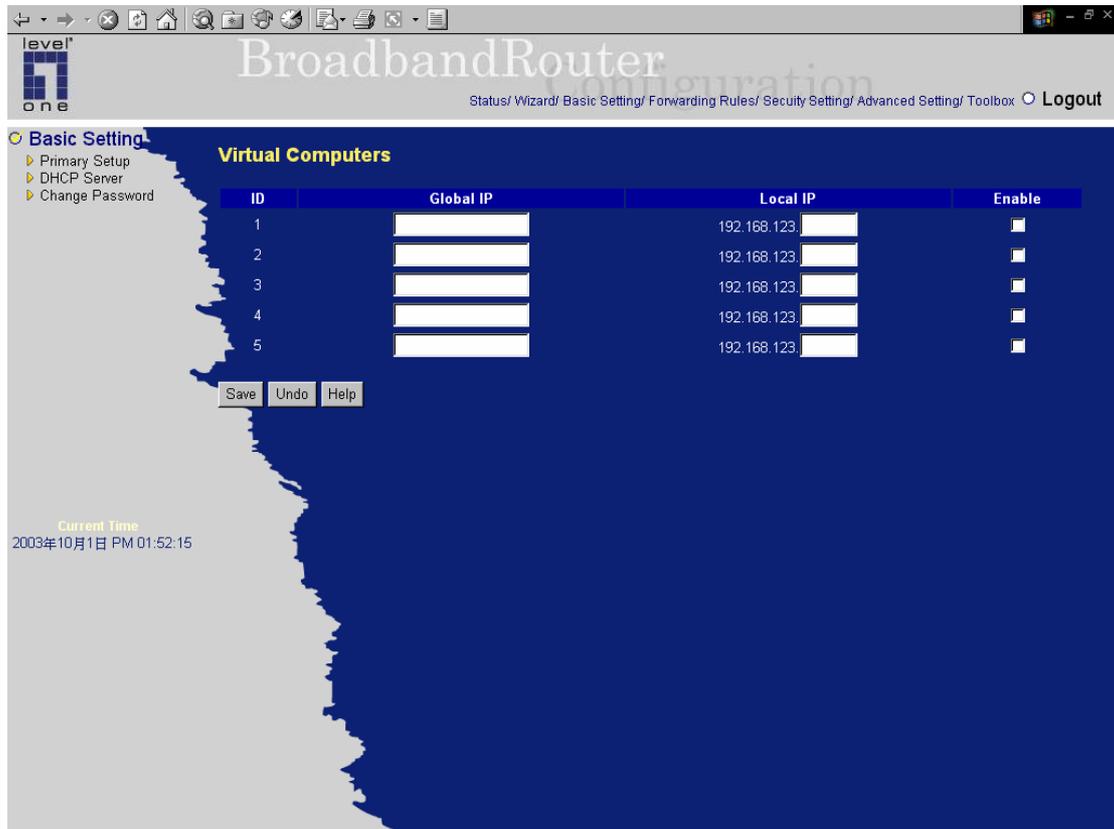
4.4.1.5 PPTP

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.
4. *Connection ID*: optional. Input the connection ID if your ISP requires it.
5. *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.

Primary Setup

Item	Setting
▶ LAN IP Address	<input type="text" value="192.168.123.254"/>
▶ WAN Type	Static IP Address <input type="button" value="Change..."/>
▶ WAN IP Address	<input type="text" value="0.0.0.0"/>
▶ WAN Subnet Mask	<input type="text" value="255.255.255.0"/>
▶ WAN Gateway	<input type="text" value="0.0.0.0"/>
▶ Primary DNS	<input type="text" value="0.0.0.0"/>
▶ Secondary DNS	<input type="text" value="0.0.0.0"/>

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

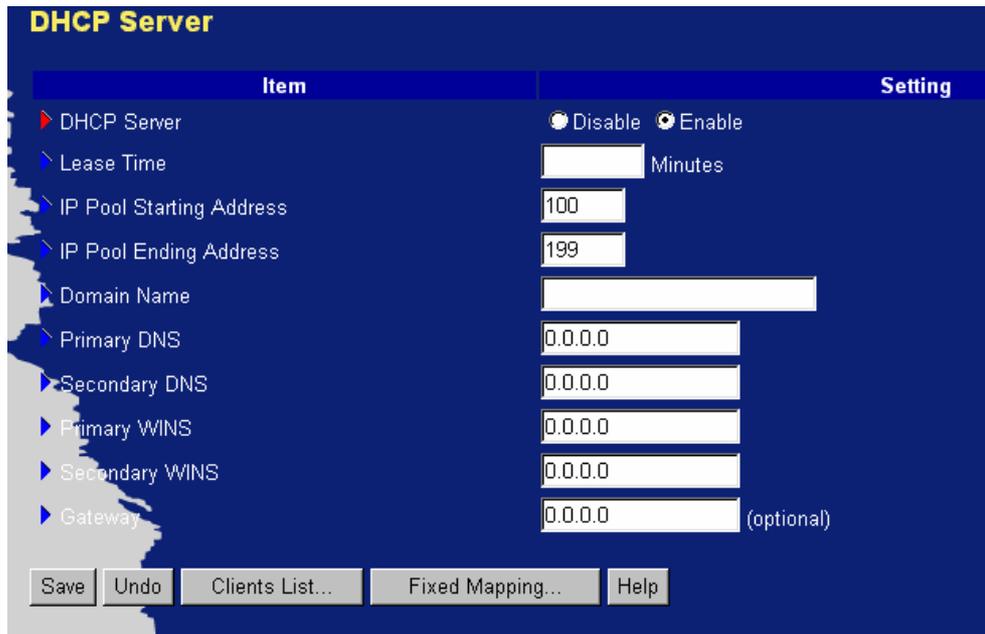
The screenshot shows the configuration interface for a BroadbandRouter. The browser window title is "BroadbandRouter Configuration". The navigation menu includes: Status / Wizard / Basic Setting / Forwarding Rules / Security Setting / Advanced Setting / Toolbox / Logout. The "Basic Setting" menu is expanded, showing: Primary Setup, DHCP Server, and Change Password. The "DHCP Server" configuration page is displayed with the following settings:

Item	Setting
DHCP Server	<input checked="" type="radio"/> Disable <input checked="" type="radio"/> Enable
Lease Time	<input type="text"/> Minutes
IP Pool Starting Address	<input type="text" value="100"/>
IP Pool Ending Address	<input type="text" value="199"/>
Domain Name	<input type="text"/>

Buttons at the bottom of the configuration area: Save, Undo, More>>, Clients List..., Fixed Mapping..., Help.

Current Time: 2003年10月8日 AM 11:52:26

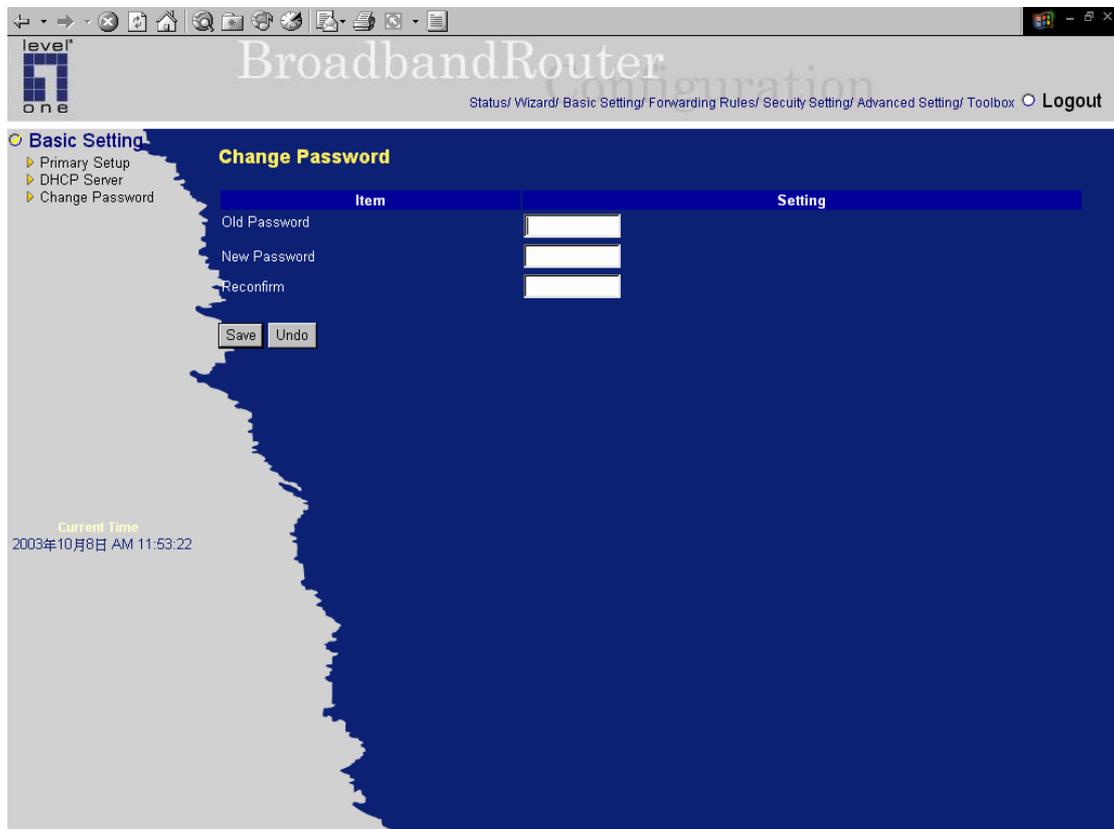
Press “More>>”



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 ending 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.

4.4.3 Change Password



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

4.5 Forwarding Rules

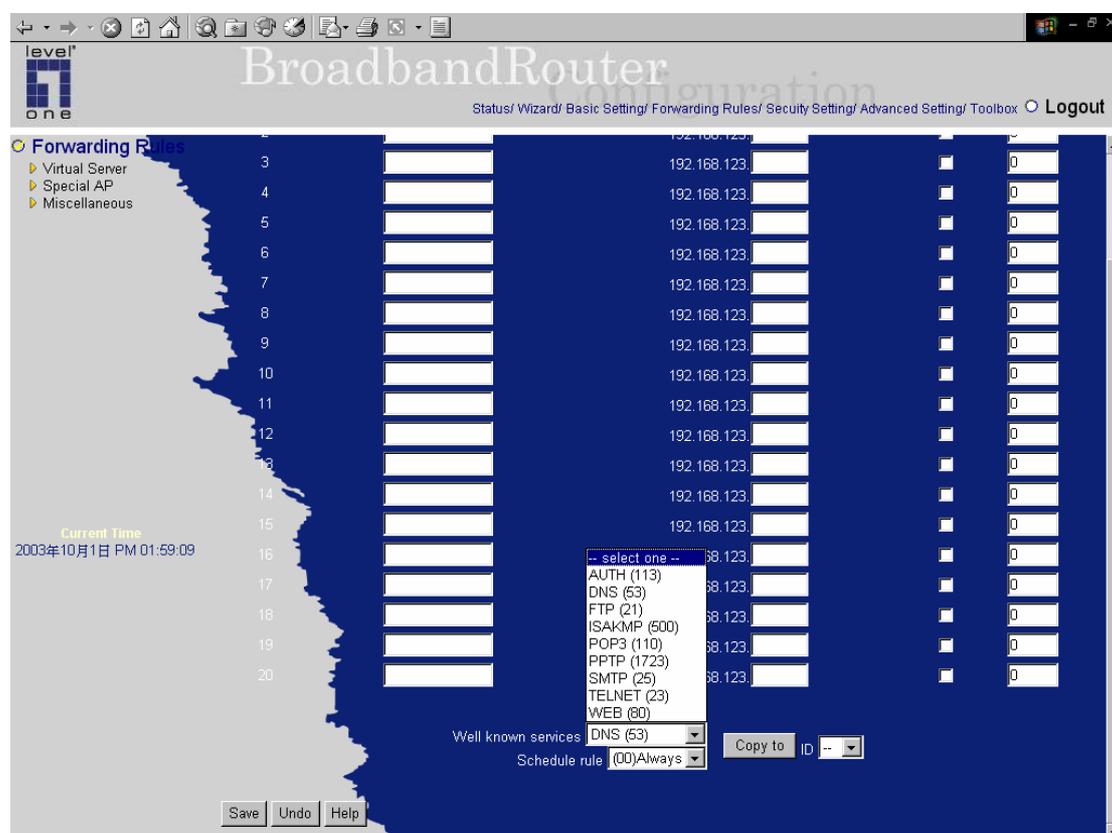
The screenshot shows a web browser window displaying the configuration page for a level one BroadbandRouter. The browser's address bar is empty, and the page title is "BroadbandRouter Configuration". The navigation menu includes "Status", "Wizard", "Basic Setting", "Forwarding Rules", "Security Setting", "Advanced Setting", "Toolbox", and "Logout".

The main content area is titled "Forwarding Rules" and contains the following sections:

- Virtual Server**
 - Allows others to access WWW, FTP, and other services on your LAN.
- Special Application**
 - This configuration allows some applications to connect, and work with the NAT router.
- Miscellaneous**
 - IP Address of DMZ Host: Allows a computer to be exposed to unrestricted 2-way communication. Note that, 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 (when Client uses active mode).

At the bottom left of the page, the current time is displayed as "Current Time 2003年10月1日 PM 01:56:30".

4.5.1 Virtual Server



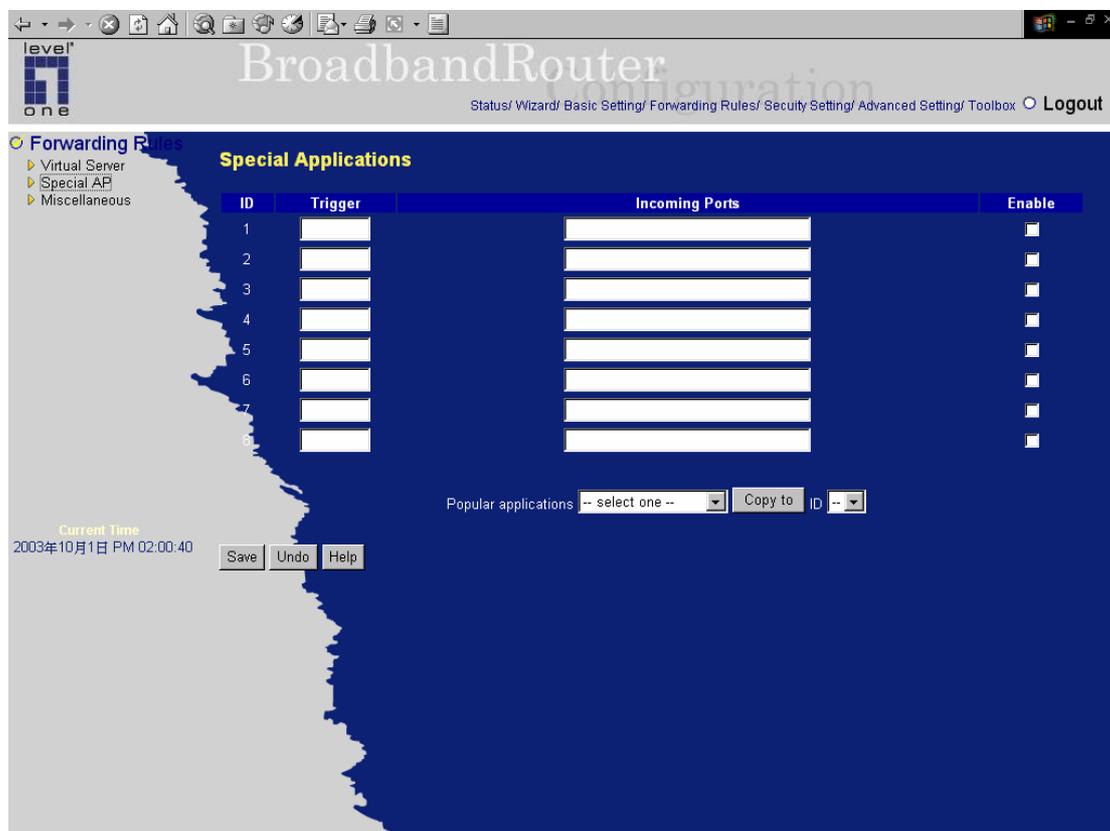
This product's NAT firewall filters out unrecognized packets to protect your Intranet, so all hosts behind this product are invisible to the outside world. If you wish, you can make some of them accessible by enabling the *Virtual Server Mapping*.

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**.

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



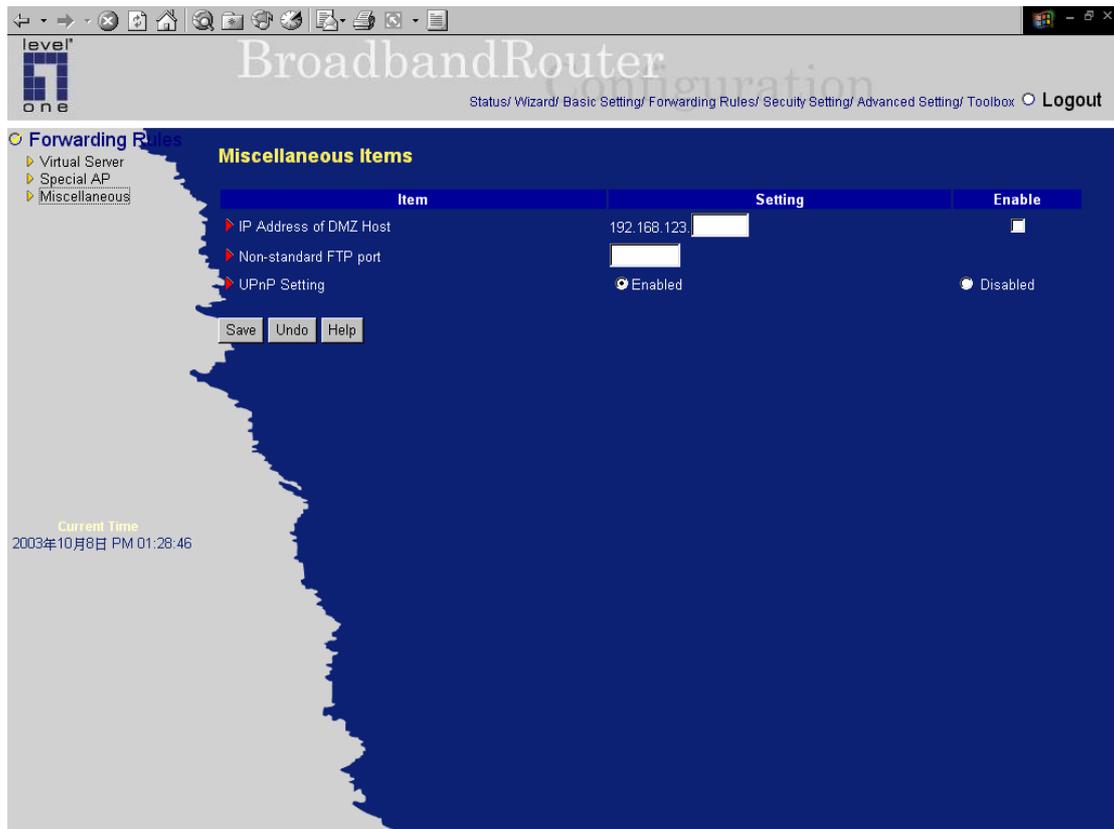
Some applications require multiple connections, like Internet games, Video conferencing, Internet telephony, etc. Because of the firewall function, these applications cannot work with a pure NAT router. The **Special Applications** feature allows some of these applications to work with this product. 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

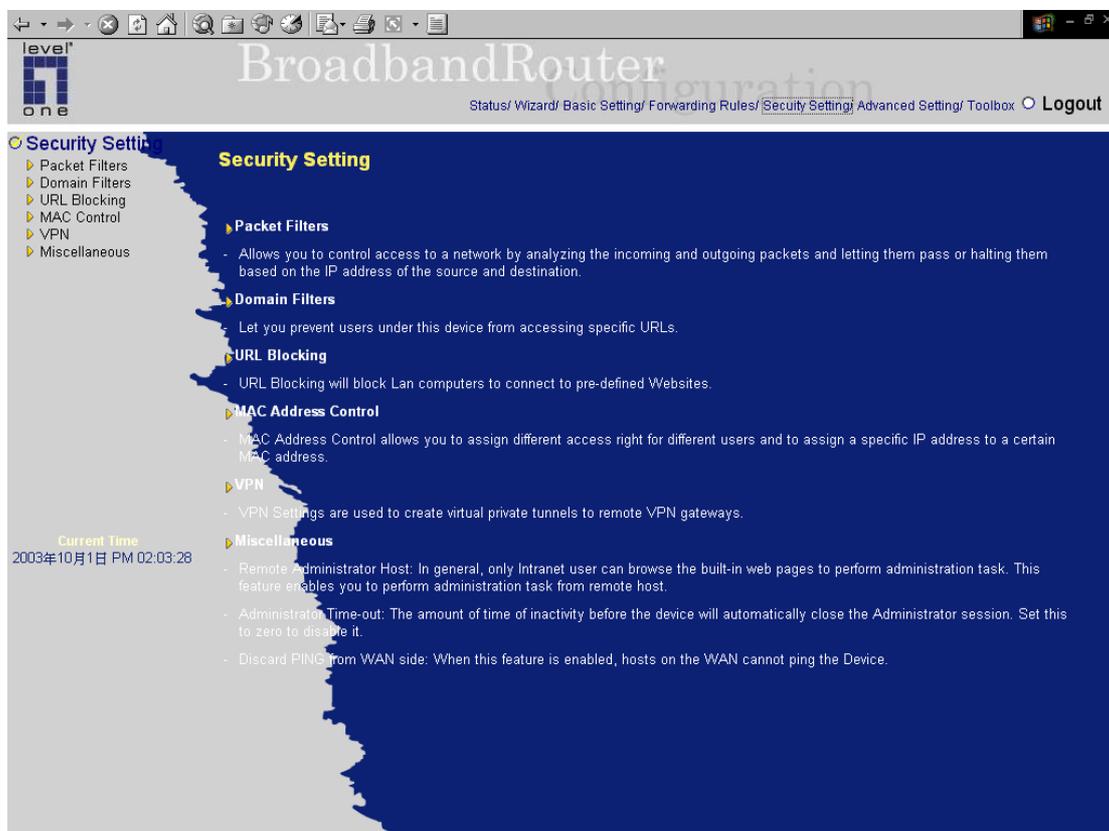
DMZ (DeMilitarized Zone) Host is a host without the protection of firewall. It allows a computer to be exposed to unrestricted 2-way communication for Internet games, Video conferencing, Internet telephony and other special applications.

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

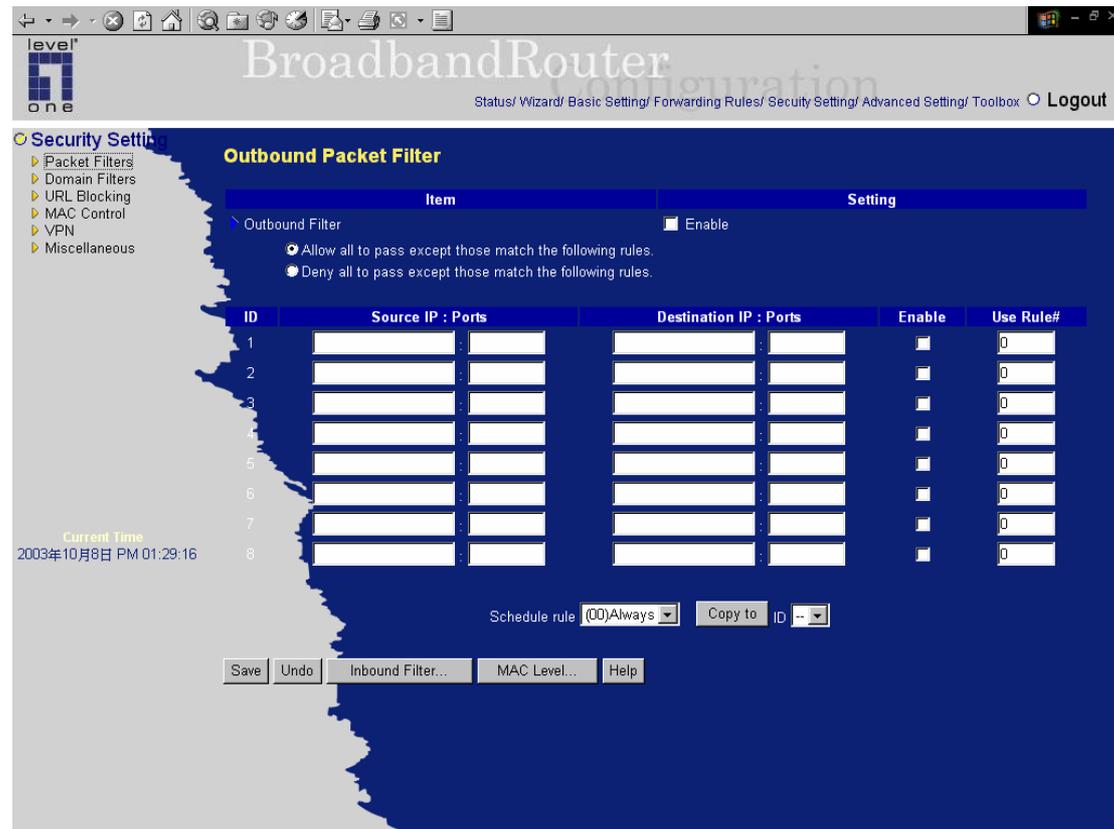


The screenshot displays the configuration interface for a level one BroadbandRouter. The browser window title is "level one BroadbandRouter Configuration". The navigation menu includes: Status/ Wizard/ Basic Setting/ Forwarding Rules/ Security Setting/ Advanced Setting/ Toolbox Logout. The "Security Setting" page is active, showing a sidebar with a tree view of settings: Security Setting (selected), Packet Filters, Domain Filters, URL Blocking, MAC Control, VPN, and Miscellaneous. The main content area, titled "Security Setting", provides descriptions for each category:

- Packet Filters**
 - 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 Filters**
 - Let you prevent users under this device from accessing specific URLs.
- URL Blocking**
 - URL Blocking will block Lan computers to connect to pre-defined Websites.
- 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.
- VPN**
 - VPN Settings are used to create virtual private tunnels to remote VPN gateways.
- Miscellaneous**
 - Remote Administrator Host: 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.
 - Administrator Time-out: The amount of time of inactivity before the device will automatically close the Administrator session. Set this to zero to disable it.
 - Discard PING from WAN side: When this feature is enabled, hosts on the WAN cannot ping the Device.

Current Time: 2003年10月1日 PM 02:03:28

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.

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.

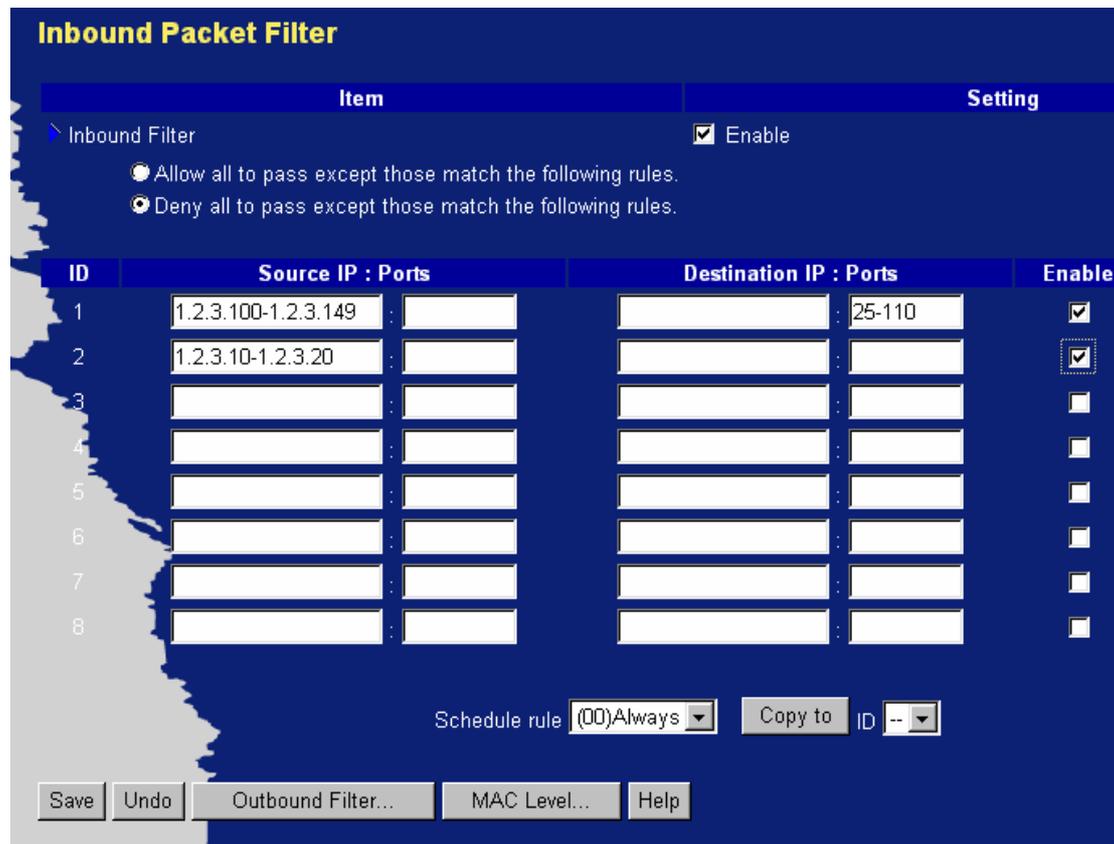
Each rule can be enabled or disabled individually.

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:



(1.2.3.100-1.2.3.149) They are allow to send mail (port 25), receive mail (port 110), and browse the Internet (port 80)

(1.2.3.10-1.2.3.20) They can do everything (block nothing)

Others are all blocked.

Example 2:

ID	Source IP : Ports	Destination IP : Ports	Enable
1	1.2.3.100-1.2.3.119	: 21	<input checked="" type="checkbox"/>
2	1.2.3.100-1.2.3.119	: 119	<input checked="" type="checkbox"/>
3			<input type="checkbox"/>
4			<input type="checkbox"/>
5			<input type="checkbox"/>
6			<input type="checkbox"/>
7			<input type="checkbox"/>
8			<input type="checkbox"/>

(1.2.3.100-1.2.3.119) They can do everything except read net news (port 119) and transfer files via FTP (port 21)

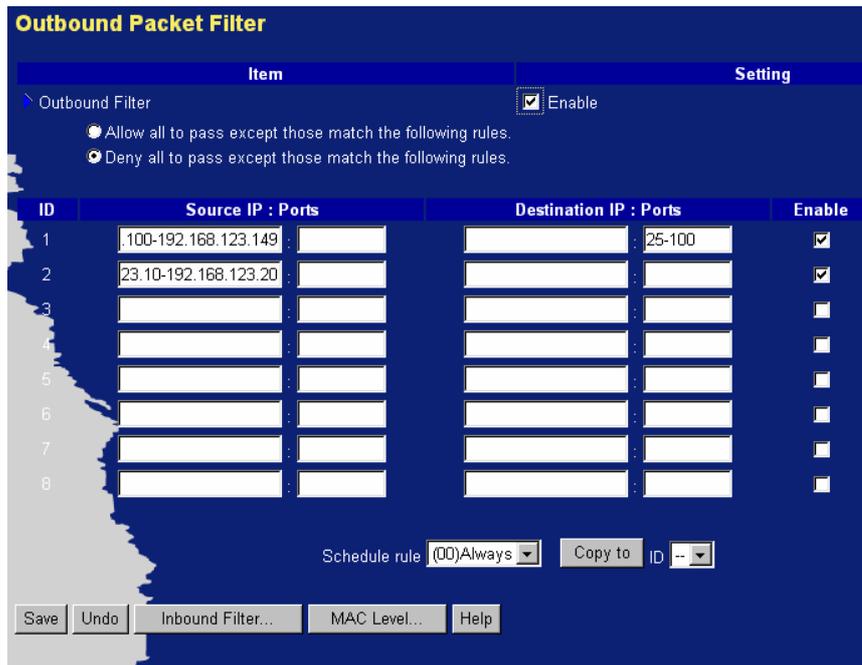
Others are all allowed.

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.

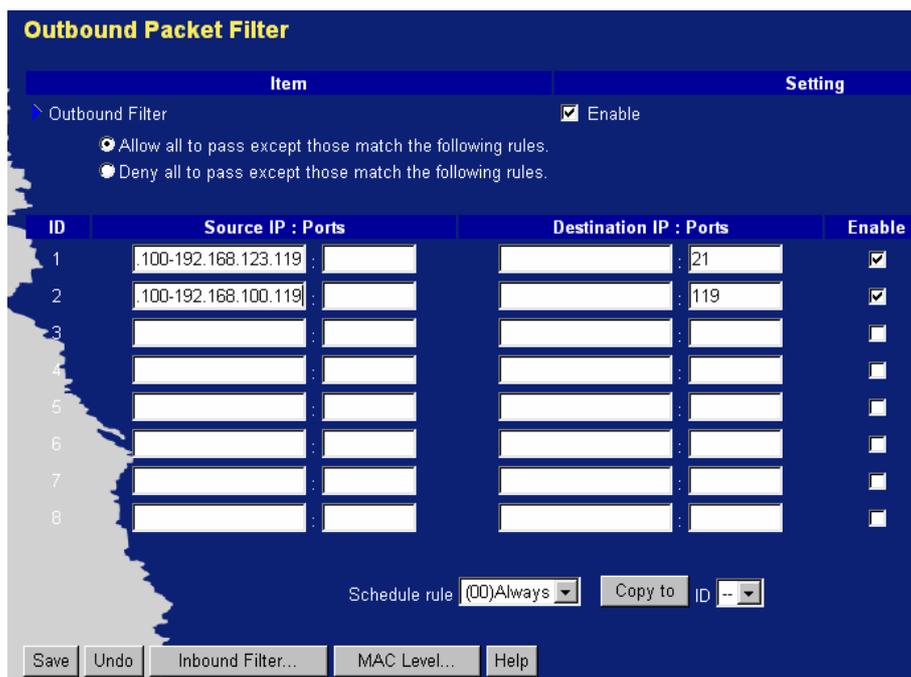
Example 1:



(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:

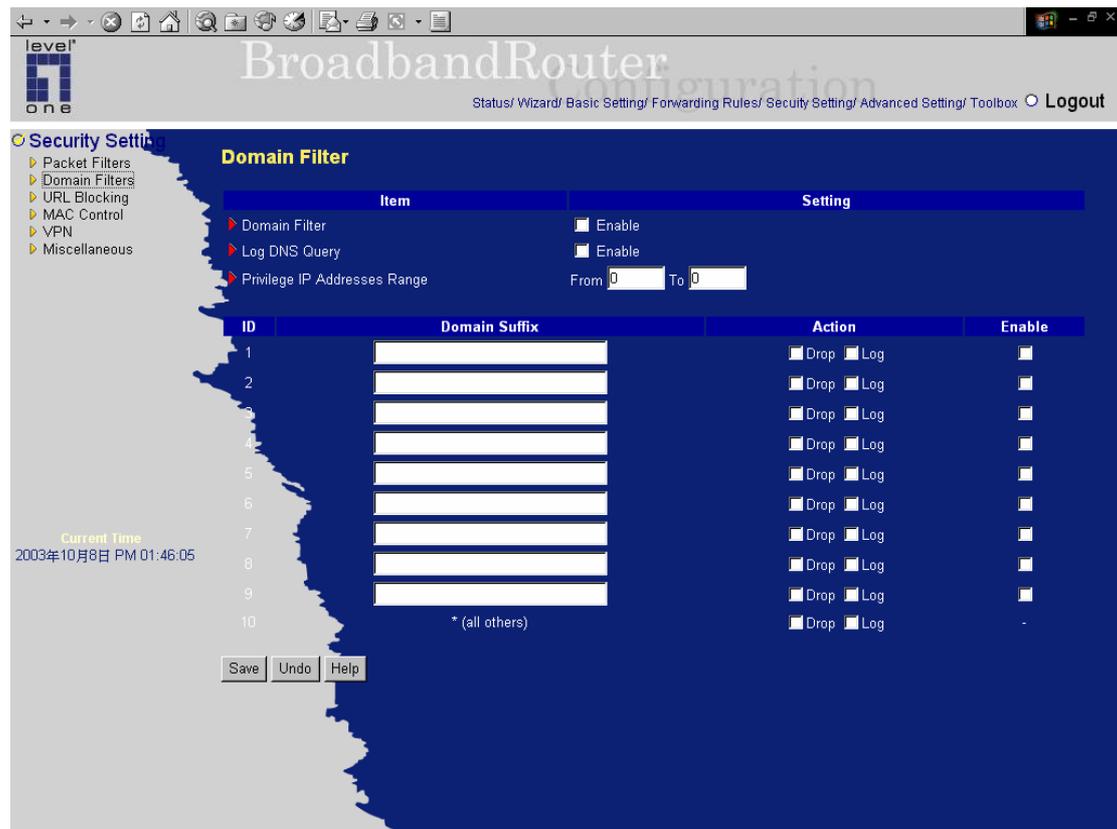


(192.168.123.100-192.168.123.119) They can do everything except read net news (port 119) and transfer files via FTP (port 21)

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

Checke if you want to enable Domain Filter.

Log DNS Query

Checke 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

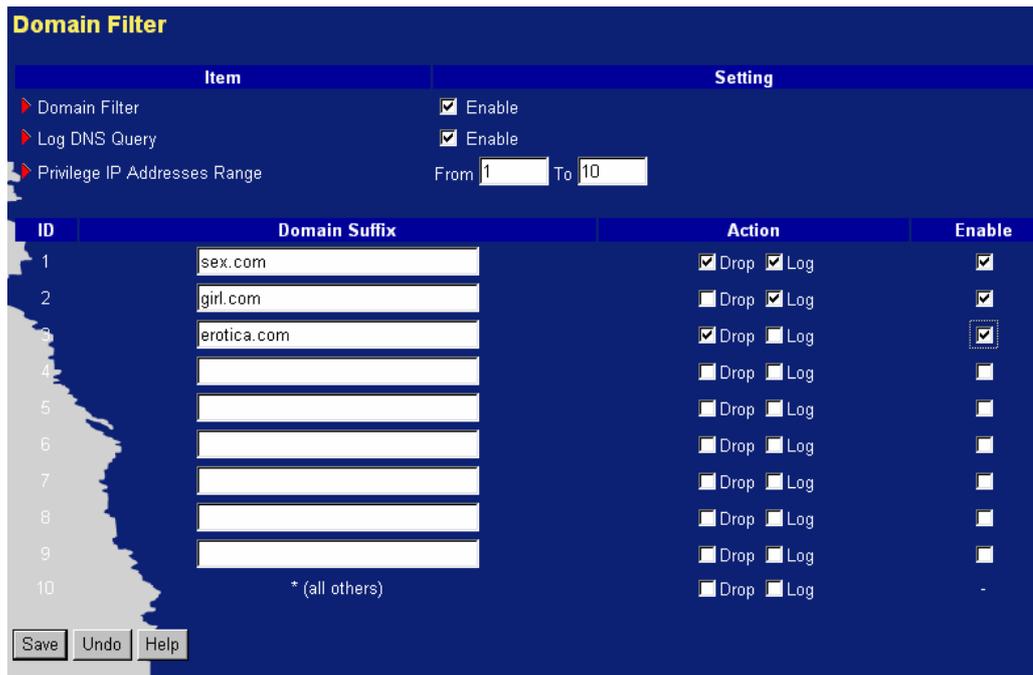
When someone is accessing the URL met the domain-suffix, what kind of action you want.

Checke **drop** to block the access. *Checke* **log** to log these access.

Enable

Checke to enable each rule.

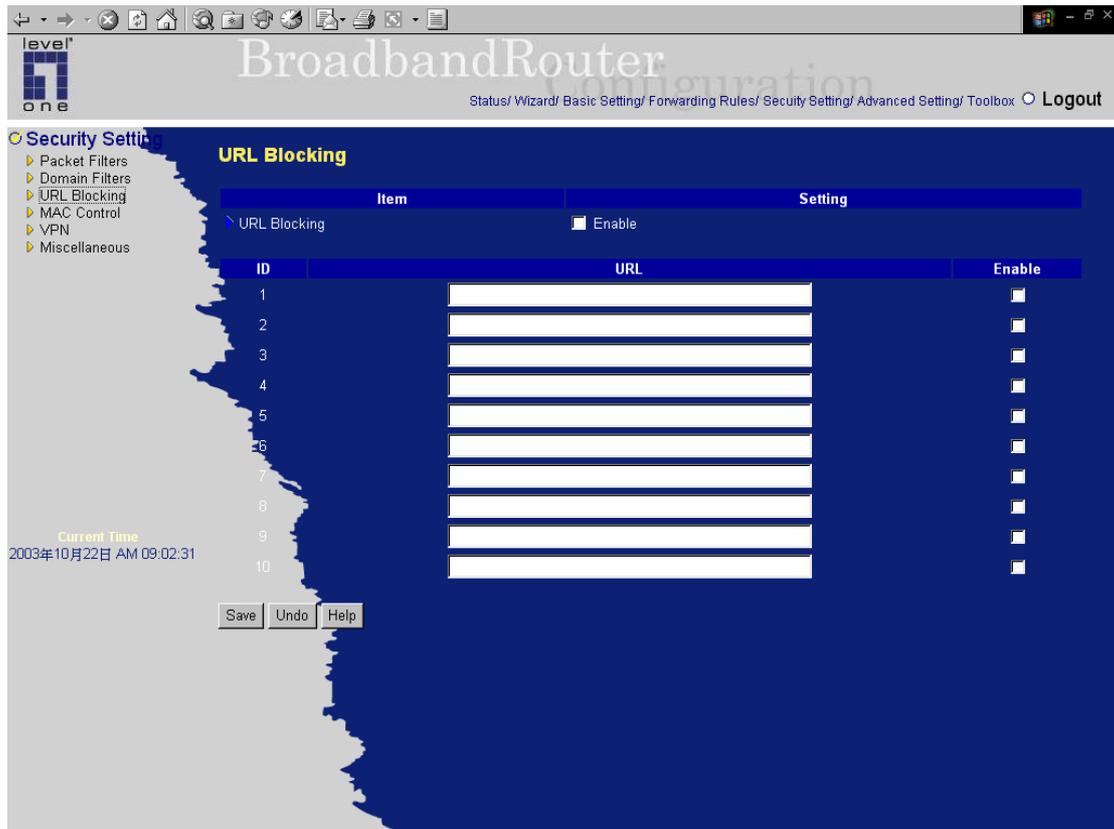
Example:



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.

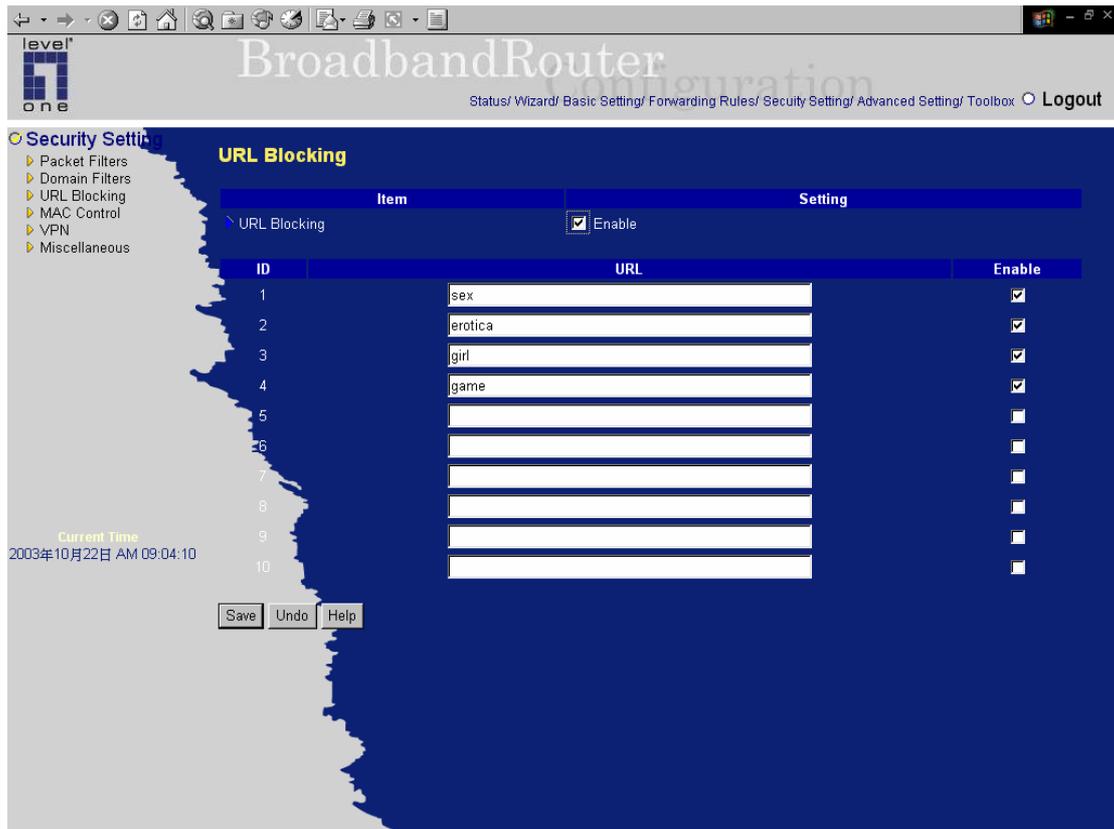
URL

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

Item	Setting
MAC Address Control	<input checked="" type="checkbox"/> Enable
Connection control	Clients with C checked can connect to this device; and <input type="text" value="allow"/> unspecified MAC addresses to connect.

ID	MAC Address	IP Address	C
1	<input type="text"/>	192.168.123. <input type="text"/>	<input type="checkbox"/>
2	<input type="text"/>	192.168.123. <input type="text"/>	<input type="checkbox"/>
3	<input type="text"/>	192.168.123. <input type="text"/>	<input type="checkbox"/>
4	<input type="text"/>	192.168.123. <input type="text"/>	<input type="checkbox"/>

DHCP clients:

<< Previous Next >> Save Undo Help

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 and wireless clients 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

MAC Address Control Enable

Connection control Clients with **C** checked can connect to this device; and **allow** unspecified MAC addresses to connect.

ID	MAC Address	IP Address	C
1	<input type="text"/>	192.168.123. <input type="text"/>	<input type="checkbox"/>
2	<input type="text"/>	192.168.123. <input type="text"/>	<input type="checkbox"/>
3	<input type="text"/>	192.168.123. <input type="text"/>	<input type="checkbox"/>
4	<input type="text"/>	192.168.123. <input type="text"/>	<input type="checkbox"/>

"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.

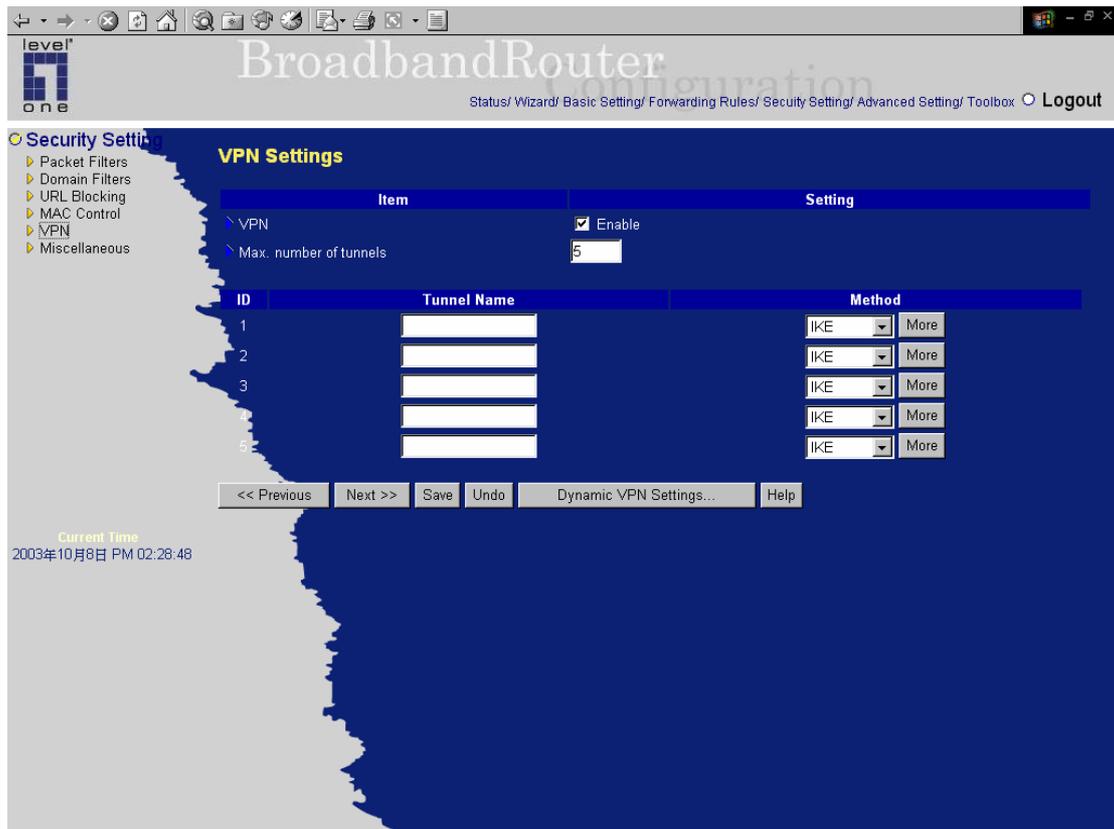
In this page, we provide the following Combobox and button to help you to input the MAC address.

DHCP clients -- select one -- ID --

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.

4.6.5 VPN setting



VPN Settings are settings that are used to create virtual private tunnels to remote VPN gateways. The tunnel technology supports data confidentiality, data origin authentication and data integrity of network information by utilizing encapsulation protocols, encryption algorithms, and hashing algorithms.

- **VPN enable item**

VPN protects network information from ill network inspectors. But it greatly degrades network throughput. Enable it when you really need a security tunnel. It is disabled for default.

- **Max. number of tunnels item**

Since VPN greatly degrades network throughput, the allowable maximum number of tunnels is limited. Be careful to set the value for allowing the number of tunnels can be created simultaneously. Its value ranges from 1 to 5.

- **Tunnel name**

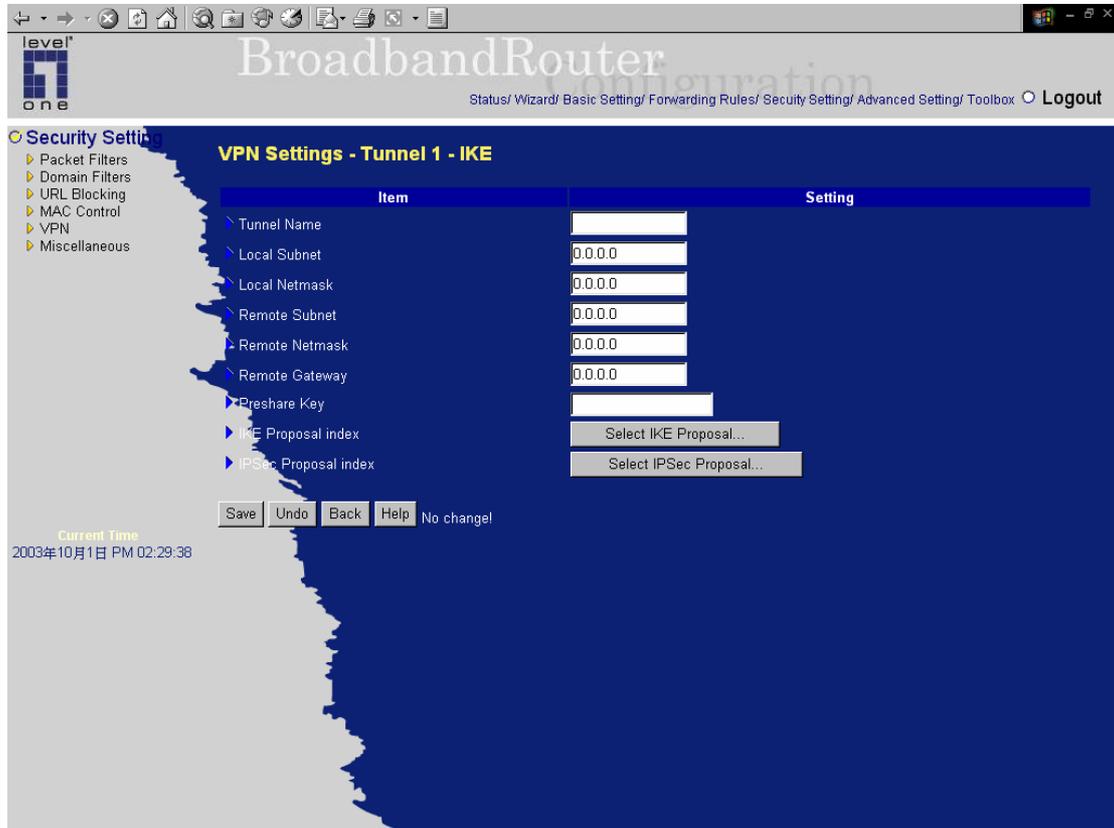
Indicate which tunnel that is focused now.

- **Method**

IPSec VPN supports two kinds of key-obtained methods: manual key and automatic key exchange. Manual key approach indicates that two end VPN gateways setup authenticator and encryption key by system managers manually. However, IKE approach will perform automatic Internet key exchange. System managers of both end gateways only need set the same pre-shared key.

Function of Buttons

More: To setup detailer configuration for manual key or IKE approaches by clicking the "More" button.



•VPN Settings - IKE

There are three parts that are necessary to setup the configuration of IKE for the dedicated tunnel: basic setup, IKE proposal setup, and IPSec proposal setup.

Basic setup includes the setting of following items: local subnet, local netmask, remote subnet, remote netmask, remote gateway, and pre-shared key. The tunnel name is derived from previous page of VPN setting. IKE proposal setup includes the setting of a set of frequent-used IKE proposals and the selecting from the set of IKE proposals. Similarly, IPSec proposal setup includes the setting of a set of frequent-used IPSec proposals and the selecting from the set of IPSec proposals.

- Basic setup:

Local subnet

The subnet of LAN site of local VPN gateway. It can be a host, a partial subnet, and the whole subnet of LAN site of local gateway.

Local netmask

Local netmask combined with local subnet to form a subnet domain.

Remote subnet

The subnet of LAN site of remote VPN gateway, it can be a host, a partial subnet, and the whole subnet of LAN site of remote gateway.

Remote netmask

Remote netmask combined with remote subnet to form a subnet domain of remote end.

Remote gateway

The IP address of remote VPN gateway.

Pre-shared key

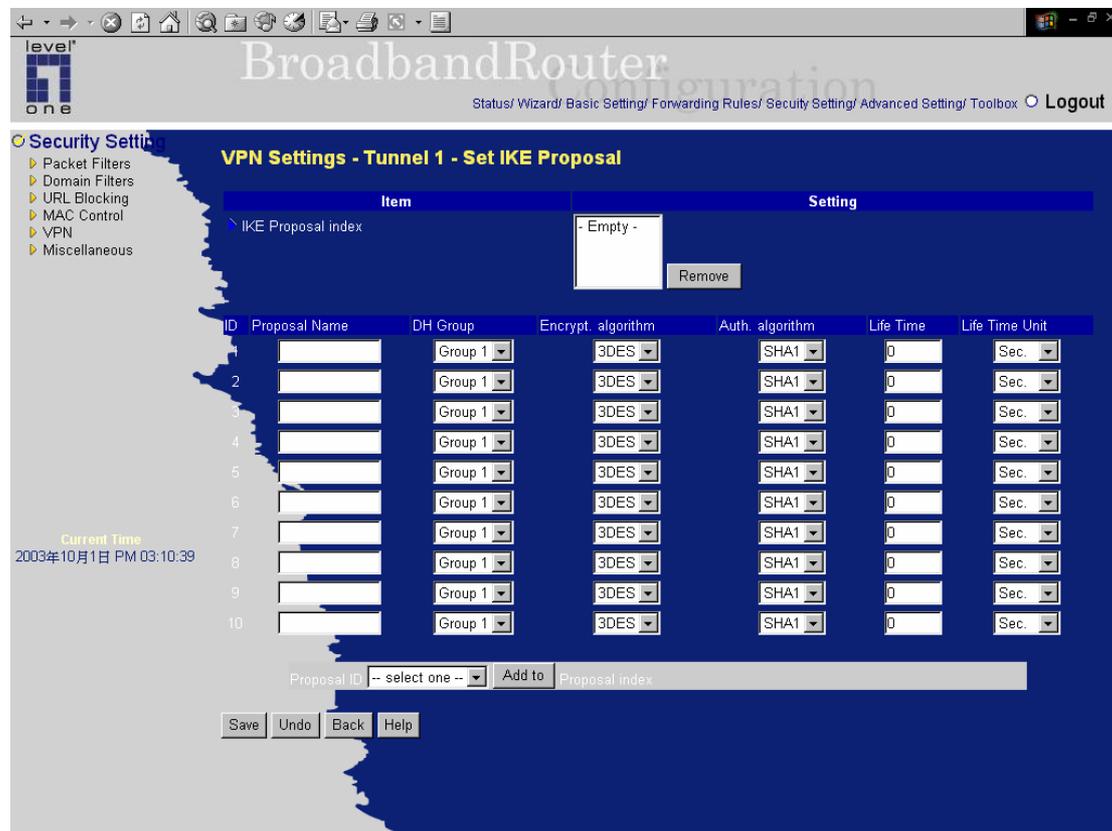
The first key that supports IKE mechanism of both VPN gateways for negotiating further security keys.

The pre-shared key must be same for both end gateways.

Function of Buttons

Select IKE proposal: Click the button to setup a set of frequent-used IKE proposals and select from the set of IKE proposals for the dedicated tunnel. proposals for the dedicated tunnel.

Select IPSec proposal: Click the button to setup a set of frequent-used IPSec proposals and select from the set of IKE proposals for the dedicated tunnel.



•VPN Settings - Set IKE Proposal

IKE Proposal index

A list of selected proposal indexes from the IKE proposal pool listed below. The selecting activity is performed by selecting a proposal ID and clicking "add to" button in the bottom of the page. There are only four indexes can be chosen from the proposal pool for the dedicated tunnel. Remove button beside the index list can remove selected proposal index before.

Proposal name

It indicates which IKE proposal to be focused. First char of the name with 0x00 value stands for the IKE proposal is not available.

• **DH group**

There are three groups can be selected: group 1 (MODP768), group 2 (MODP1024), group 5 (MODP1536).

Encryption algorithm

There are two algorithms can be selected: 3DES and DES.

Authentication algorithm

There are two algorithms can be selected: SHA1 and MD5.

Life time

The unit of life time is based on the value of Life Time Unit. If the value of unit is second, the value of life time represents the life time of dedicated VPN tunnel between both end gateways. Its value ranges from 300 seconds to 172,800 seconds. If the value of unit is KB, the value of life time represents the maximum allowable amount of transmitted packets through the dedicated VPN tunnel between both end gateways. Its value ranges from 20,480 KBs to 2,147,483,647 KBs.

Life time unit

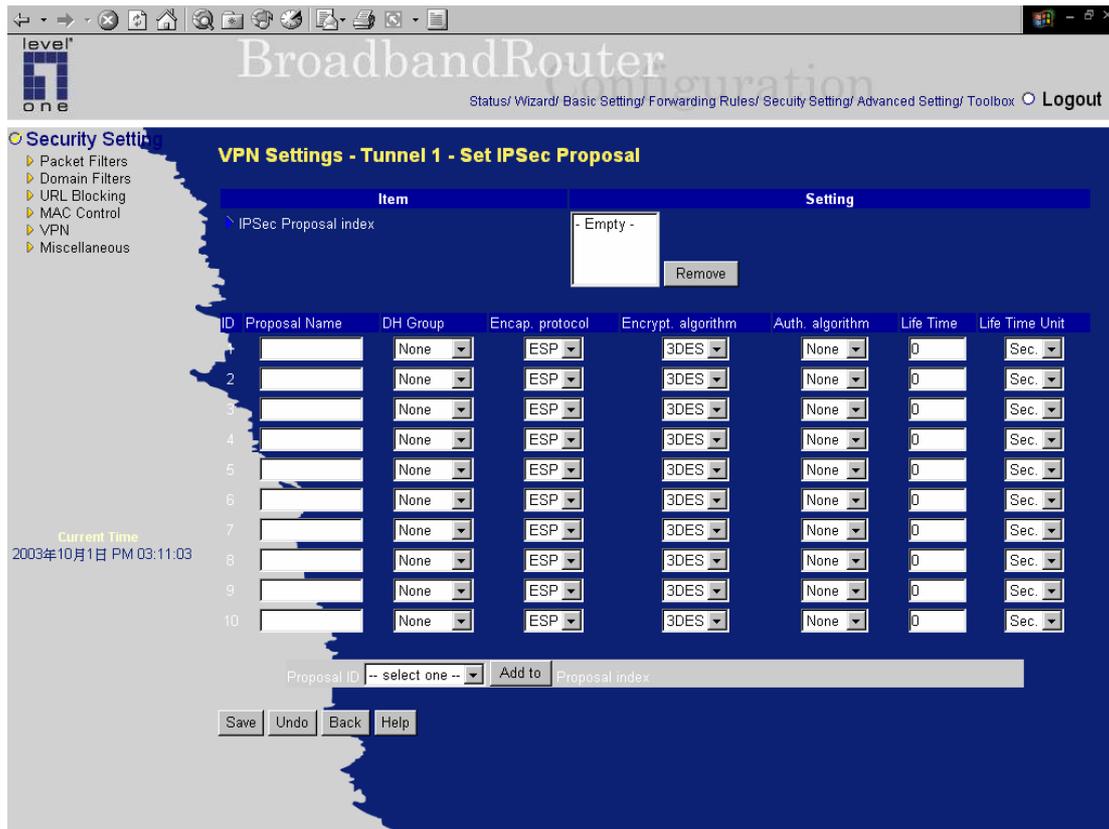
There are two units can be selected: second and KB.

Proposal ID

The identifier of IKE proposal can be chosen for adding corresponding proposal to the dedicated tunnel. There are total ten proposals can be set in the proposal pool. At most only four proposals from the pool can be applied to the dedicated tunnel as shown in the proposal index list.

Function of Buttons

Add to button: Click it to add the chosen proposal indicated by proposal ID to IKE Proposal index list. The proposals in the index list will be used in phase 1 of IKE negotiation for getting the IKSAMP SA of dedicated tunnel.



•VPN Settings -Set IPSec Proposal

IPSec Proposal index

A list of selected proposal indexes from the IPSec proposal pool listed below. The selecting activity is performed by selecting a proposal ID and clicking "add to" button in the bottom of the page. There are only four indexes can be chosen for the dedicated tunnel. Remove button beside the index list can remove selected proposal index before.

Proposal name

It indicates which IPSec proposal to be focused. First char of the name with 0x00 value stands for the proposal is not available.

• DH group

There are three groups can be selected: group 1 (MODP768), group 2 (MODP1024), group 5 (MODP1536). But none also can be selected here for IPSec proposal.

Encapsulation protocol

There are two protocols can be selected: ESP and AH.

Encryption algorithm

There are two algorithms can be selected: 3DES and DES. But when the encapsulation protocol is AH, encryption algorithm is unnecessarily set.

Authentication algorithm

There are two algorithms can be selected: SHA1 and MD5. But none also can be selected here for

IPSec proposal.

Life time

The unit of life time is based on the value of Life Time Unit. If the value of unit is second, the value of life time represents the life time of dedicated VPN tunnel between both end gateways. Its value ranges from 300 seconds to 172,800 seconds. If the value of unit is KB, the value of life time represents the maximum allowable amount of transmitted packets through the dedicated VPN tunnel between both end gateways for. Its value ranges from 20,480 KBs to 2,147,483,647 KBs.

Life time unit

There are two units can be selected: second and KB.

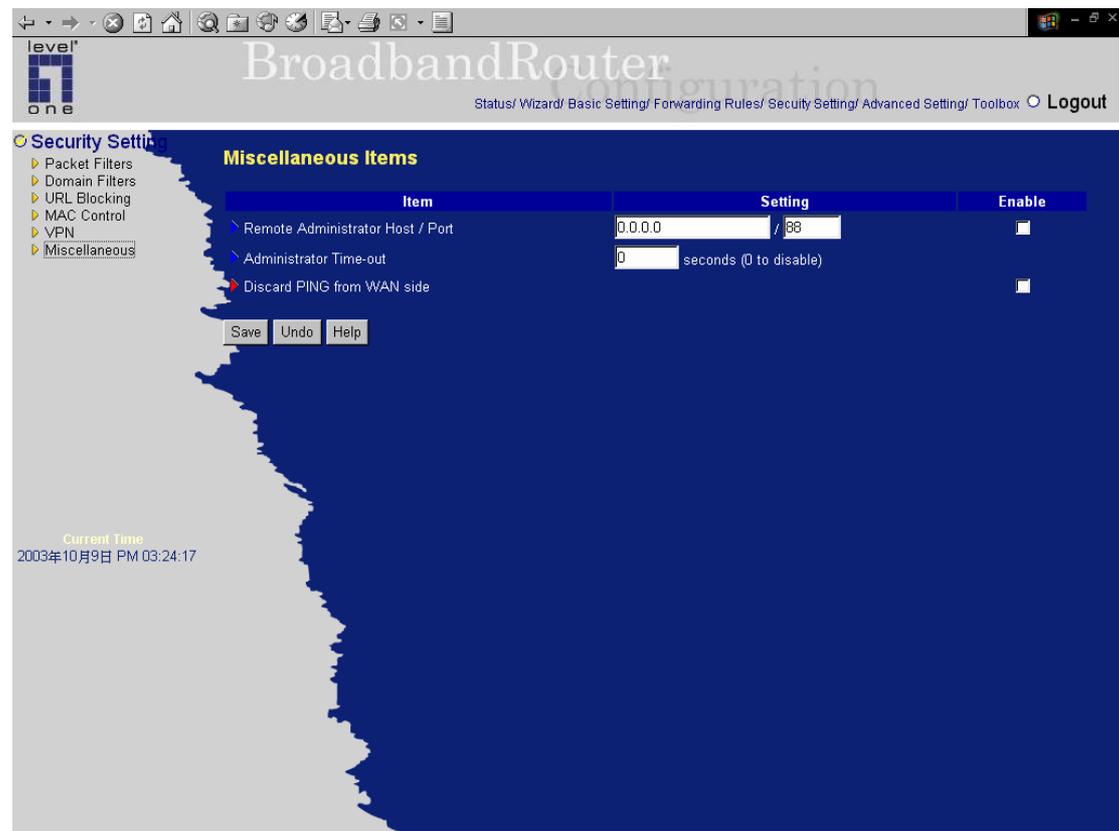
Proposal ID

The identifier of IPSec proposal can be chosen for adding the proposal to the dedicated tunnel. There are total ten proposals can be set in the proposal pool. At most only four proposals from the pool can be applied to the dedicated tunnel as shown in the proposal index list.

Function of Buttons

Add to button: Click it to add the chosen proposal indicated by proposal ID to IPSec Proposal index list. The proposals in the index list will be used in phase 2 of IKE negotiation for getting the IPSec SA of dedicated tunnel.

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.

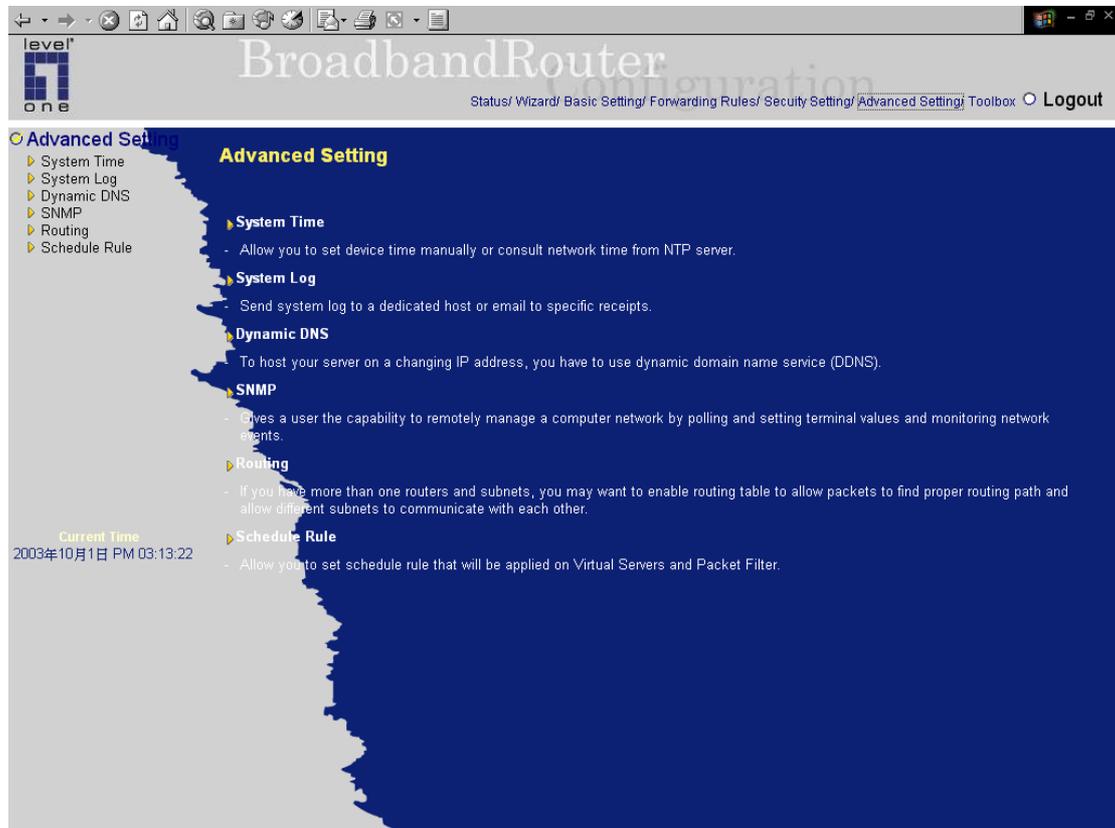
Administrator Time-out

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.

4.7 Advanced Setting



The screenshot displays the configuration interface for a LevelOne BroadbandRouter. The browser window title is "BroadbandRouter Configuration". The navigation menu includes: Status / Wizard / Basic Setting / Forwarding Rules / Security Setting / **Advanced Setting** / Toolbox / Logout.

The "Advanced Setting" page is active, showing a sidebar menu with the following items:

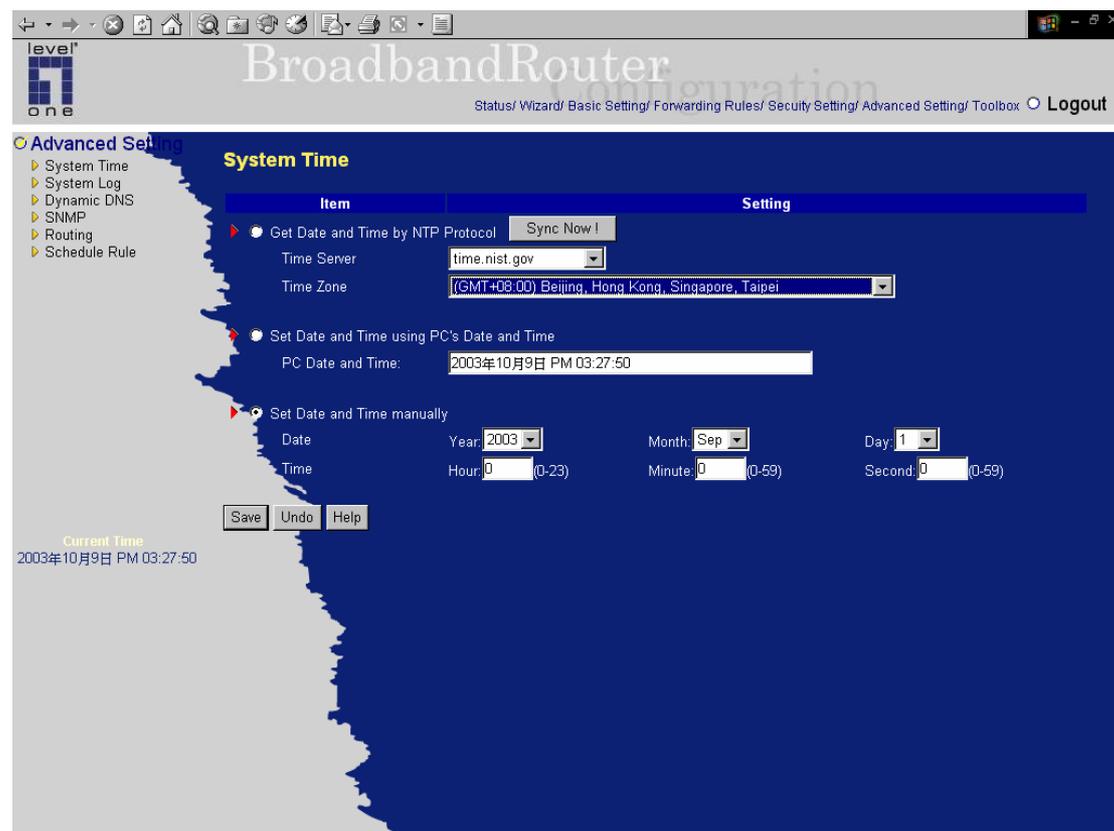
- ▶ System Time
- ▶ System Log
- ▶ Dynamic DNS
- ▶ SNMP
- ▶ Routing
- ▶ Schedule Rule

The main content area, titled "Advanced Setting", provides descriptions for each menu item:

- System Time**: Allow you to set device time manually or consult network time from NTP server.
- System Log**: Send system log to a dedicated host or email to specific receipts.
- Dynamic DNS**: To host your server on a changing IP address, you have to use dynamic domain name service (DDNS).
- SNMP**: Gives a user the capability to remotely manage a computer network by polling and setting terminal values and monitoring network events.
- Routing**: If you have more than one routers and subnets, you may want to enable routing table to allow packets to find proper routing path and allow different subnets to communicate with each other.
- Schedule Rule**: Allow you to set schedule rule that will be applied on Virtual Servers and Packet Filter.

At the bottom left, the "Current Time" is displayed as 2003年10月1日 PM 03:13:22.

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.

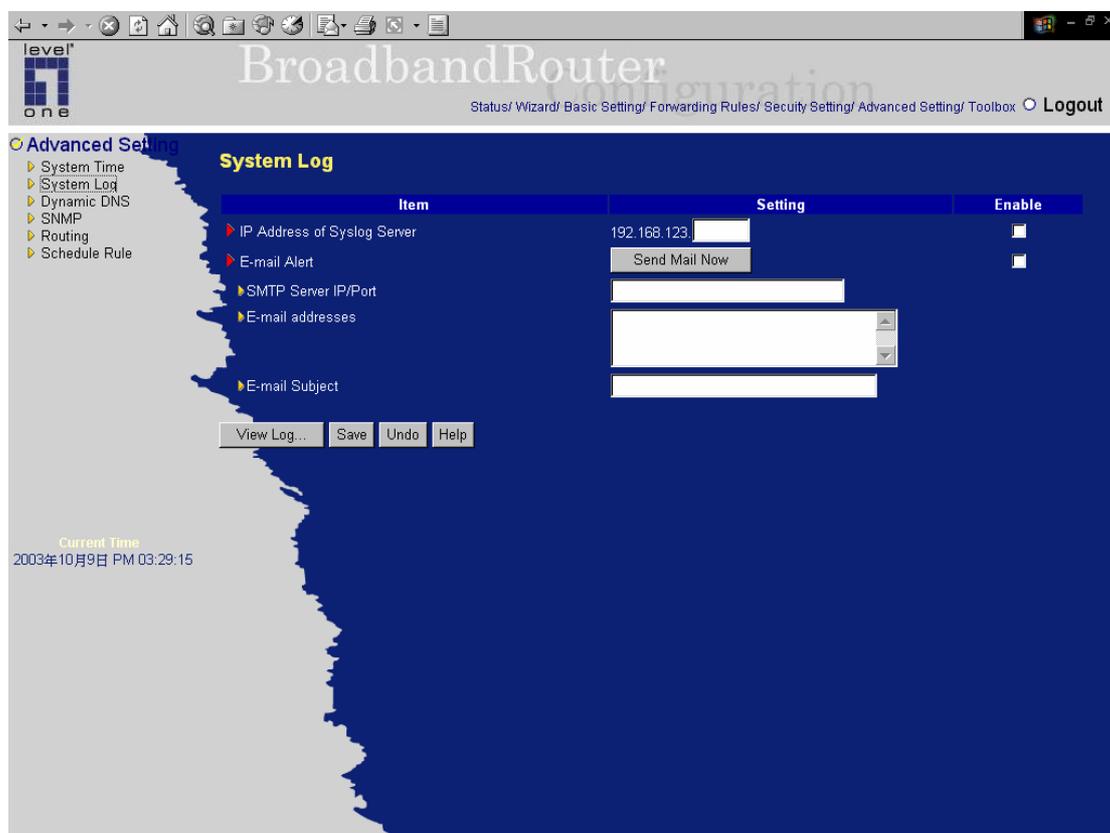
Set Date and Time manually

Selected if you want to Set Date and Time manually.

Function of Buttons

Sync Now: Synchronize system time with network time server

4.7.2 System Log



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

IP Address for Syslog

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 and Port

Input the SMTP server IP and port, which are concatenated 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".

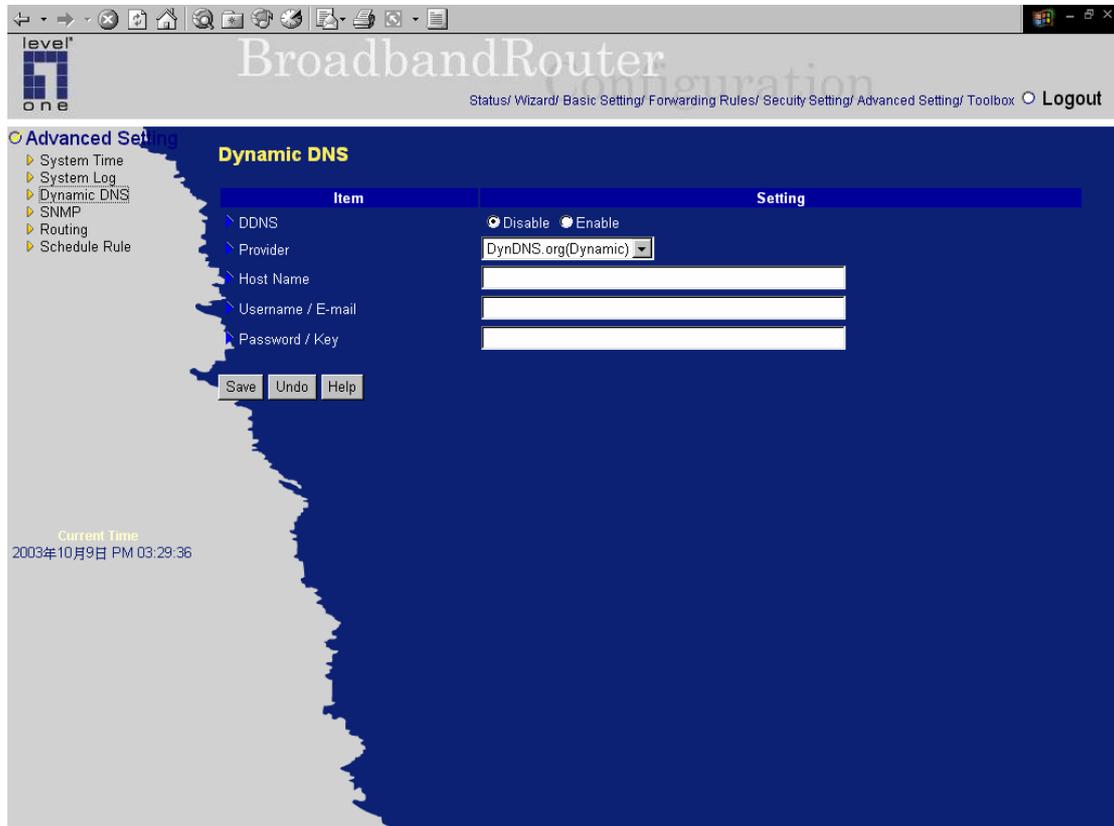
Send E-mail alert to

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.

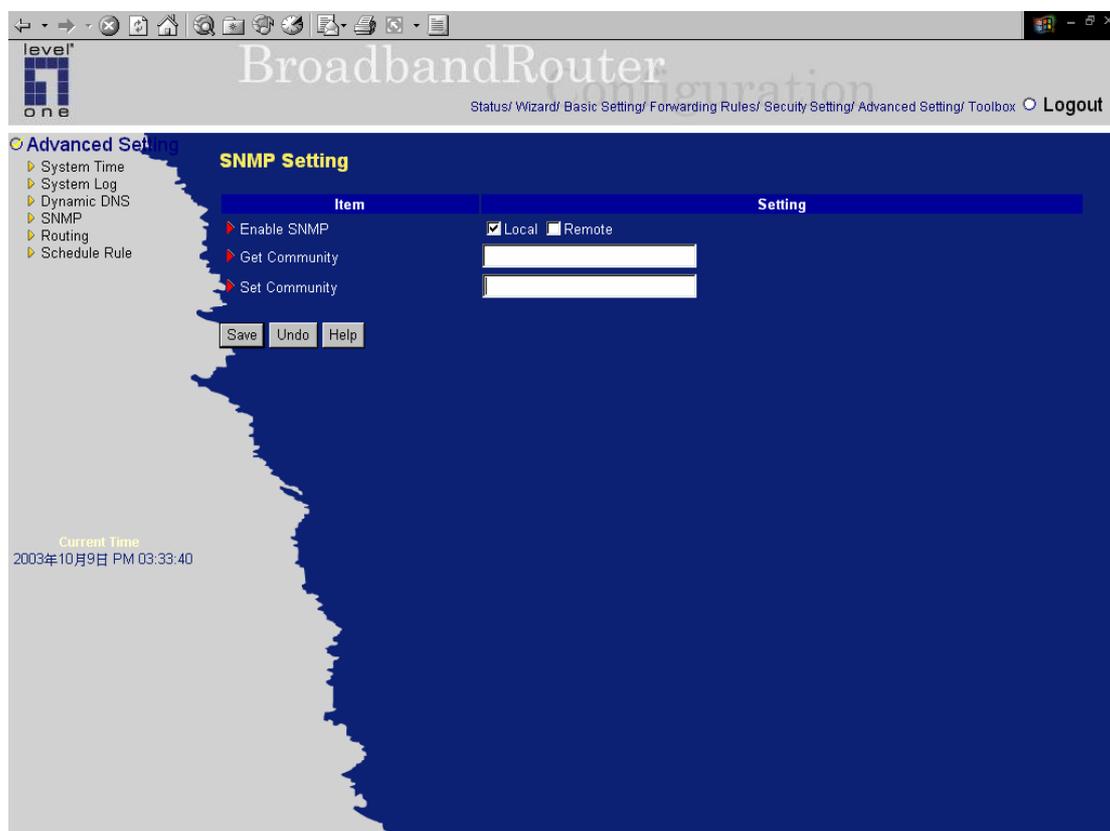
Example:

Item	Setting
DDNS	<input checked="" type="radio"/> Disable <input type="radio"/> Enable
Provider	DynDNS.org(Dynamic)
Host Name	user.dyndns.org
Username / E-mail	user
Password / Key	*****

Save Undo Help

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

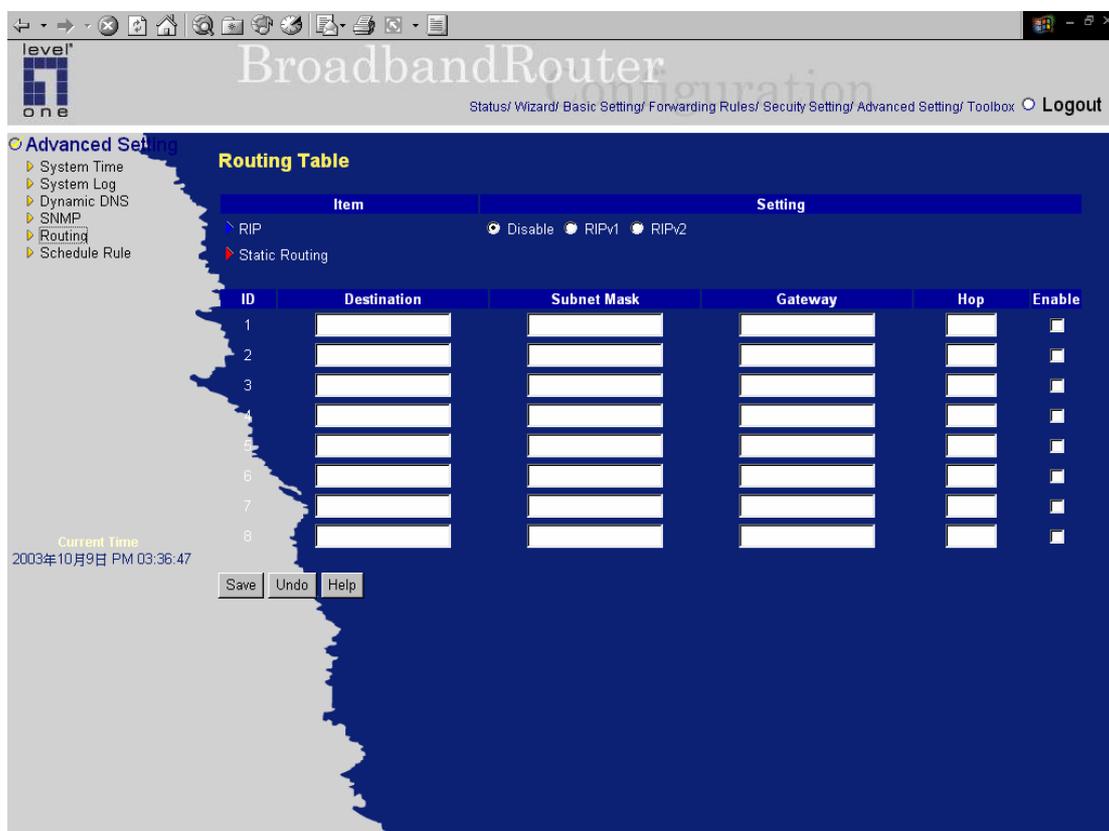
Setting the community of SetRequest your device will accept.

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

4.7.5 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.

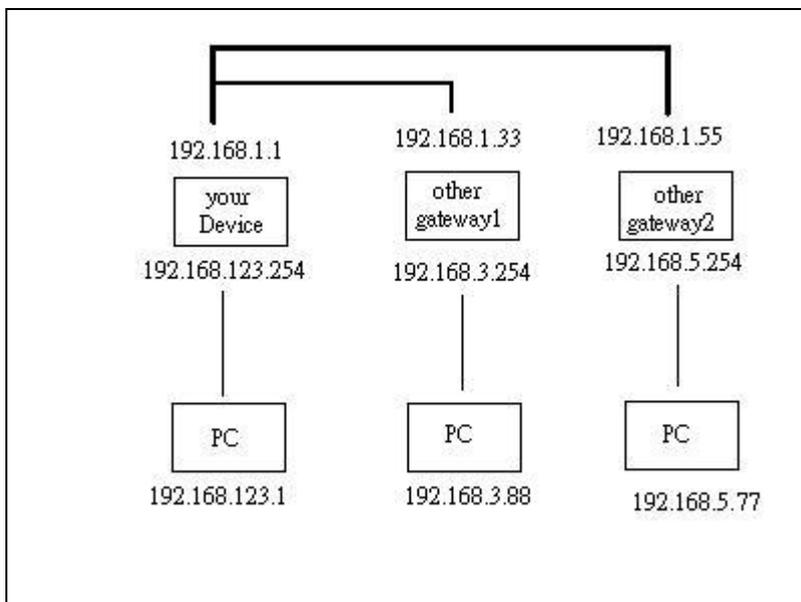
Routing Table settings are settings used to setup the functions of static and dynamic routing.

RIP Enable: Check to enable RIP function.

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:

ID	Destination	Subnet Mask	Gateway	Hop
1	192.168.3.0	255.255.255.0	192.168.1.33	1
2	192.168.5.0	255.255.255.0	192.168.1.55	1
3				
4				
5				
6				
7				
8				



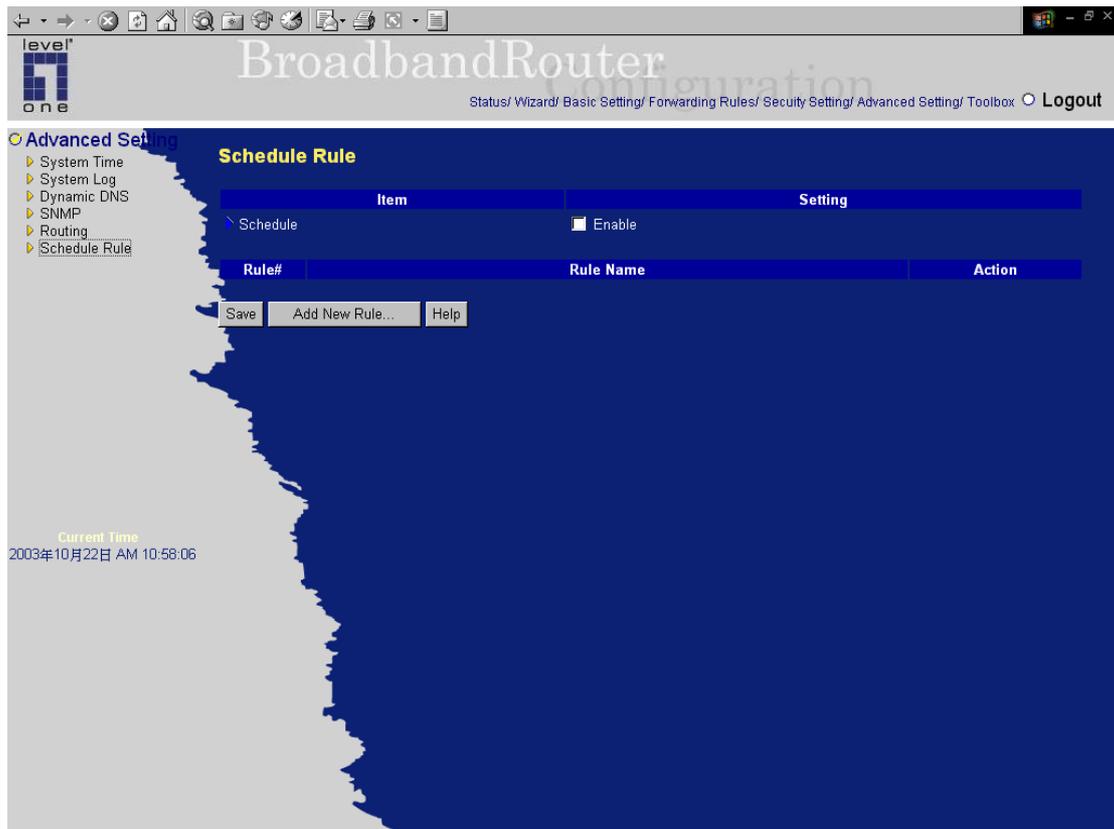
So if, for example, the host wanted to send an IP data gram to 192.168.3.88, it would use the above table to determine that it had to go via 192.168.1.33 (a gateway),

And if it sends Packets to 192.168.5.77 will go via 192.168.1.55

Each rule can be enabled or disabled individually.

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

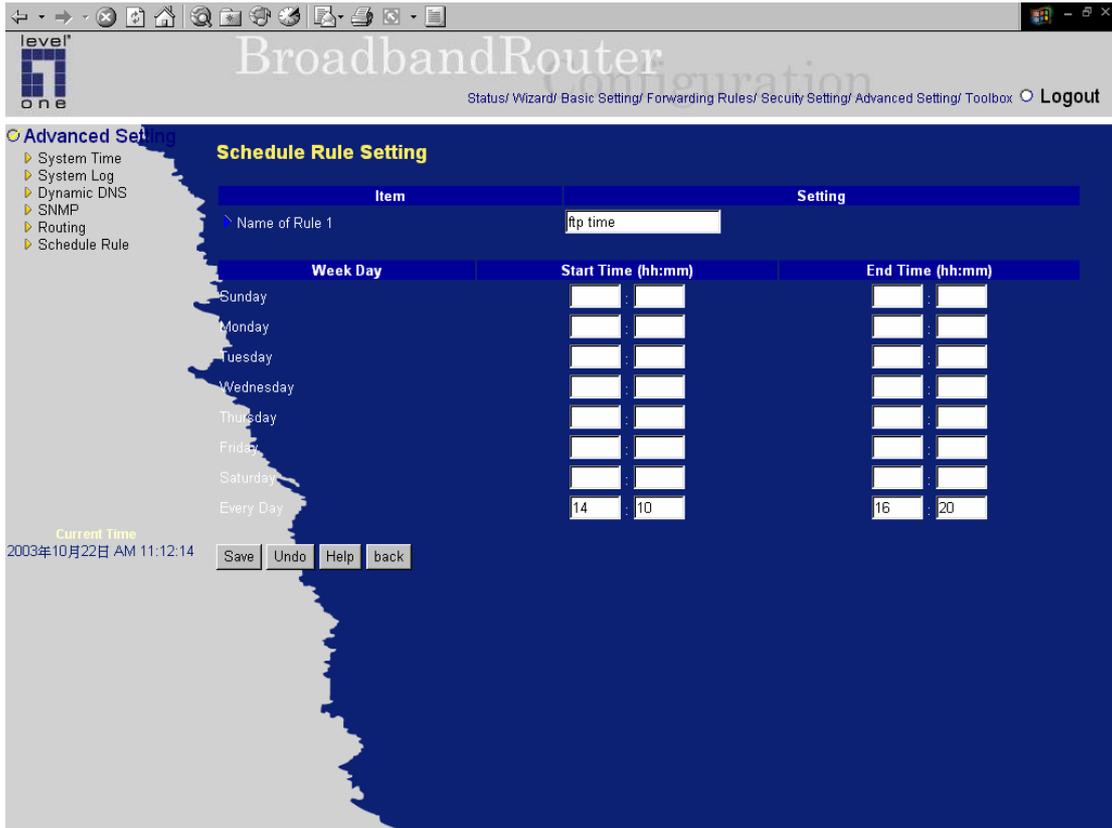
4.7.6 Schedule Rule



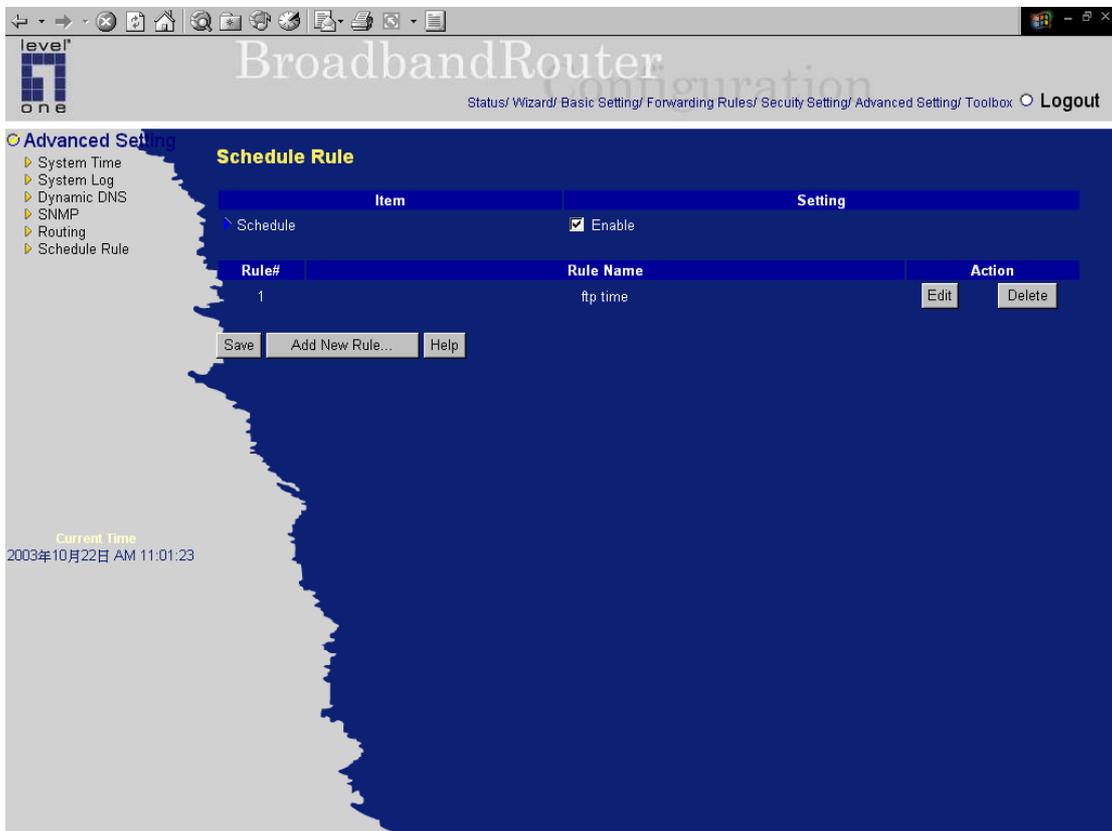
You can set the schedule time to decide which service will be turned on or off. Select the “enable” item.

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 →



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)

level one BroadbandRouter Configuration

Status/ Wizard/ Basic Setting/ Forwarding Rules/ Security Setting/ Advanced Setting/ Toolbox Logout

Forwarding Rules

- Virtual Server
- Special AP
- Miscellaneous

Virtual Server

ID	Service Ports	Server IP	Enable	Use Rule#
1	21	192.168.10.	<input checked="" type="checkbox"/>	1
2		192.168.10.	<input type="checkbox"/>	0
3		192.168.10.	<input type="checkbox"/>	0
4		192.168.10.	<input type="checkbox"/>	0
5		192.168.10.	<input type="checkbox"/>	0
6		192.168.10.	<input type="checkbox"/>	0
7		192.168.10.	<input type="checkbox"/>	0
8		192.168.10.	<input type="checkbox"/>	0
9		192.168.10.	<input type="checkbox"/>	0
10		192.168.10.	<input type="checkbox"/>	0
11		192.168.10.	<input type="checkbox"/>	0
12		192.168.10.	<input type="checkbox"/>	0
13		192.168.10.	<input type="checkbox"/>	0
14		192.168.10.	<input type="checkbox"/>	0
15		192.168.10.	<input type="checkbox"/>	0
16		192.168.10.	<input type="checkbox"/>	0
17		192.168.10.	<input type="checkbox"/>	0
18		192.168.10.	<input type="checkbox"/>	0
19		192.168.10.	<input type="checkbox"/>	0
20		192.168.10.	<input type="checkbox"/>	0

Current Time
2003年10月22日 AM 11:03:16

Well known services FTP (21)

Schedule rule (01)ftp time

Copy to ID 1

Example2: **Packet Filter** – Apply Rule#1 (ftp time: everyday 14:10 to 16:20).

The screenshot shows the configuration page for the Inbound Packet Filter. The interface includes a navigation menu on the left, a breadcrumb trail at the top, and a main configuration area. The 'Inbound Filter' section is active, showing a table of rules. Rule #1 is selected and enabled, with a schedule of '(01)ftp time'. The 'Use Rule#' column for rule #1 is set to 1.

Security Setting

- Packet Filters
- Domain Filters
- URL Blocking
- MAC Control
- VPN
- Miscellaneous

BroadbandRouter Configuration

Status/ Wizard/ Basic Setting/ Forwarding Rules/ Security Setting/ Advanced Setting/ Toolbox Logout

Inbound Packet Filter

Inbound 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#
1			<input checked="" type="checkbox"/>	1
2			<input type="checkbox"/>	0
3			<input type="checkbox"/>	0
4			<input type="checkbox"/>	0
5			<input type="checkbox"/>	0
6			<input type="checkbox"/>	0
7			<input type="checkbox"/>	0
8			<input type="checkbox"/>	0

Current Time
2003年10月22日 AM 11:07:06

Schedule rule: (01)ftp time

4.8 Toolbox

The screenshot shows a web browser window displaying the configuration interface for a LevelOne BroadbandRouter. The browser's address bar shows the URL `http://192.168.1.1:8080/`. The page title is "BroadbandRouter Configuration". The navigation menu includes "Status", "Wizard", "Basic Setting", "Forwarding Rules", "Security Setting", "Advanced Setting", "Toolbox", and "Logout".

The "Toolbox" section is expanded, showing a list of tools:

- View Log
- Firmware Upgrade
- Backup Setting
- Reset to Default
- Reboot
- Miscellaneous

The "Forwarding Rules" section is also expanded, showing a list of tools:

- View Log
 - View the system logs.
- Firmware Upgrade
 - Prompt the administrator for a file and upgrade it to this device.
- Backup Setting
 - Save the settings of this device to a file.
- Reset to Default
 - Reset the settings of this device to the default values.
- Reboot
 - Reboot this device.
- Miscellaneous
 - MAC Address for Wake-on-LAN: Let you to power up another network device remotely.
 - 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 this alive.

The "Current Time" is displayed as 2003年10月9日 PM 03:45:41.

4.8.1 System Log

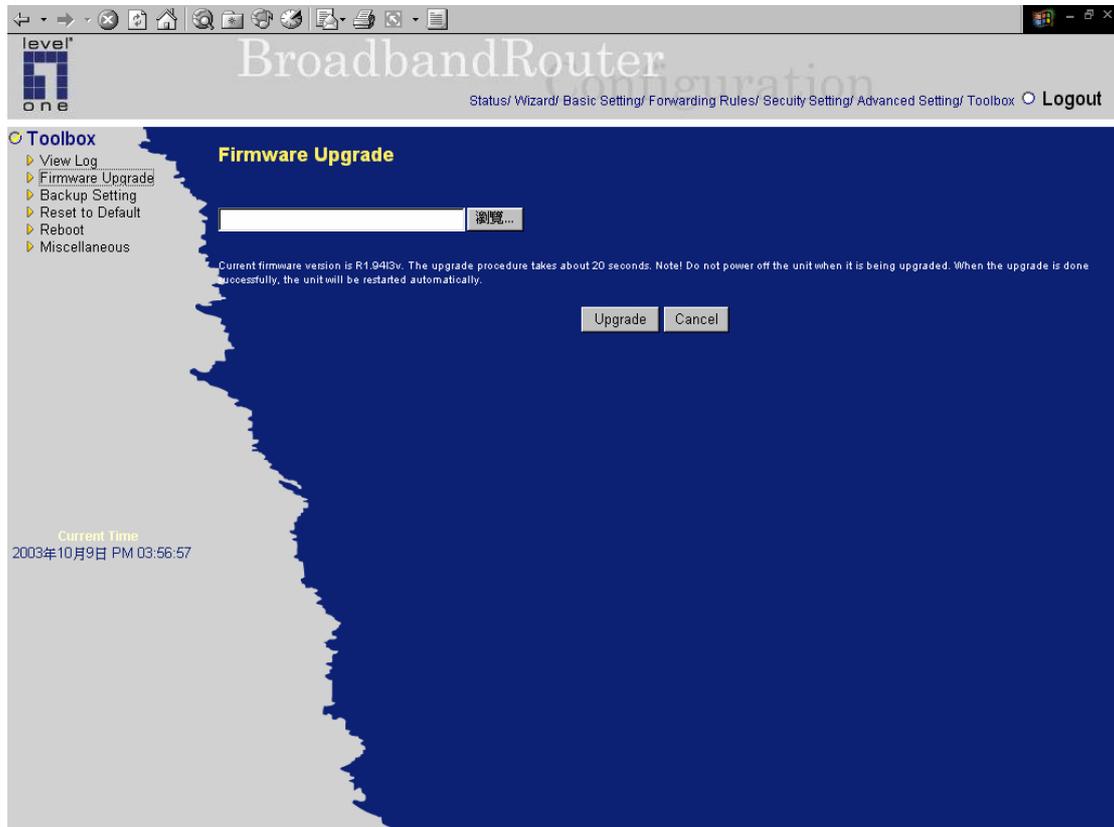
The screenshot displays the 'level one BroadbandRouter' configuration page. The top navigation bar includes 'Status/ Wizard/ Basic Setting/ Forwarding Rules/ Security Setting/ Advanced Setting/ Toolbox' and a 'Logout' button. On the left, a 'Toolbox' menu is visible with options: 'View Log', 'Firmware Upgrade', 'Backup Setting', 'Reset to Default', 'Reboot', and 'Miscellaneous'. The main content area shows a system log with the following entries:

```
2003年9月1日 PM 11:06:28 Receive IKE H3(KEYINIT) : 192.168.10.130 --> 192.168.10.114
2003年9月1日 PM 11:06:28 Send IKE H4(RESPEP) : 192.168.10.114 --> 192.168.10.130
2003年9月1日 PM 11:06:29 Receive IKE H5(IDINIT) : 192.168.10.130 --> 192.168.10.114
2003年9月1日 PM 11:06:29 Send IKE H6(IDRESP) : 192.168.10.114 --> 192.168.10.130
2003年9月1日 PM 11:06:29 IKE Phase1 (ISAKMP SA) established : 192.168.10.114 <-> 192.168.10.130
2003年9月1日 PM 11:06:29 Receive IKE Q1(QINIT) : [192.168.10.130]>=>[192.168.10.114]
2003年9月1日 PM 11:06:29 Requested routing is [192.168.10.130|192.168.10.130]<->[192.168.10.114|192.168.123.0]
2003年9月1日 PM 11:06:29 Try to match with MODE:Tunnel PROTOCOL:ESP-3DES AUTH:MD5 HASH:Others PFS(Group):Group2
2003年9月1日 PM 11:06:29 Send IKE Q2(QRESP) : 192.168.123.0 --> 192.168.10.130
2003年9月1日 PM 11:06:29 Receive IKE Q3(QHASH) : [192.168.10.130|192.168.10.130]>=>[192.168.10.114|192.168.123.0]
2003年9月1日 PM 11:06:29 IKE Phase2 (IPSEC SA) established : [192.168.10.130|192.168.10.130]<->[192.168.10.114|192.168.123.0]
2003年9月1日 PM 11:06:29 inbound SPI = 0x3000010, outbound SPI = 0xb4a24767
2003年9月1日 PM 11:11:39 Connection is broken
2003年9月1日 PM 11:11:39 DHCP:release
2003年9月1日 PM 11:20:14 DHCP:discover()
2003年9月1日 PM 11:20:14 DHCP:offer(192.168.10.1)
2003年9月1日 PM 11:20:14 DHCP:request(192.168.10.114)
2003年9月1日 PM 11:20:15 DHCP:ack(DOL=259200,T1=129600,T2=226800)
2003年9月1日 PM 11:20:23 Receive IKE Q1(QINIT) : [192.168.10.130]>=>[192.168.10.114]
2003年9月1日 PM 11:20:23 Requested routing is [192.168.10.130|192.168.10.130]<->[192.168.10.114|192.168.123.0]
2003年9月1日 PM 11:20:23 Try to match with MODE:Tunnel PROTOCOL:ESP-3DES AUTH:MD5 HASH:Others PFS(Group):Group2
2003年9月1日 PM 11:20:23 Send IKE Q2(QRESP) : 192.168.123.0 --> 192.168.10.130
2003年9月1日 PM 11:20:23 Receive IKE Q3(QHASH) : [192.168.10.130|192.168.10.130]>=>[192.168.10.114|192.168.123.0]
2003年9月1日 PM 11:20:23 IKE Phase2 (IPSEC SA) established : [192.168.10.130|192.168.10.130]<->[192.168.10.114|192.168.123.0]
2003年9月1日 PM 11:20:23 inbound SPI = 0x4000010, outbound SPI = 0x143f7c1f
2003年9月1日 PM 11:20:26 IKE phase2 (IPSec SA) remove : 192.168.123.0 <-> 192.168.10.130
2003年9月1日 PM 11:20:26 inbound SPI = 0x3000010, outbound SPI = 0xb4a24767
2003年9月1日 PM 11:20:49 Restarted by 192.168.123.100
2003年9月1日 PM 11:20:54 DHCP:discover()
2003年9月1日 PM 11:20:54 DHCP:offer(192.168.10.1)
2003年9月1日 PM 11:20:54 DHCP:request(192.168.10.114)
2003年9月1日 PM 11:20:55 DHCP:ack(DOL=259200,T1=129600,T2=226800)
2003年9月1日 PM 11:25:52 Connection is broken
2003年9月1日 PM 11:25:52 DHCP:release
2003年9月1日 PM 11:31:15 BOB:192.168.123.100 query DNS for tw.yahoo.com
2003年9月1日 PM 11:31:15 DHCP:discover()
2003年9月1日 PM 11:31:19 DHCP:discover()
2003年9月1日 PM 11:31:27 DHCP:discover()
2003年9月1日 PM 11:31:53 DHCP:discover()
2003年9月1日 PM 11:31:53 DHCP:offer(192.168.10.1)
2003年9月1日 PM 11:31:53 DHCP:request(192.168.10.114)
2003年9月1日 PM 11:31:54 DHCP:ack(DOL=259200,T1=129600,T2=226800)
```

At the bottom of the log area, there are buttons for 'Back', 'Refresh', 'Download', and 'Clear'. The 'Current Time' is displayed as '2003年10月9日 PM 03:56:40'.

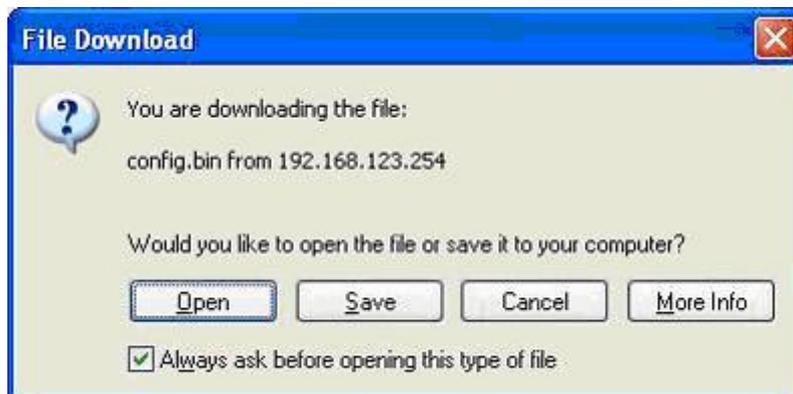
You can View system log by clicking the **View Log** button

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



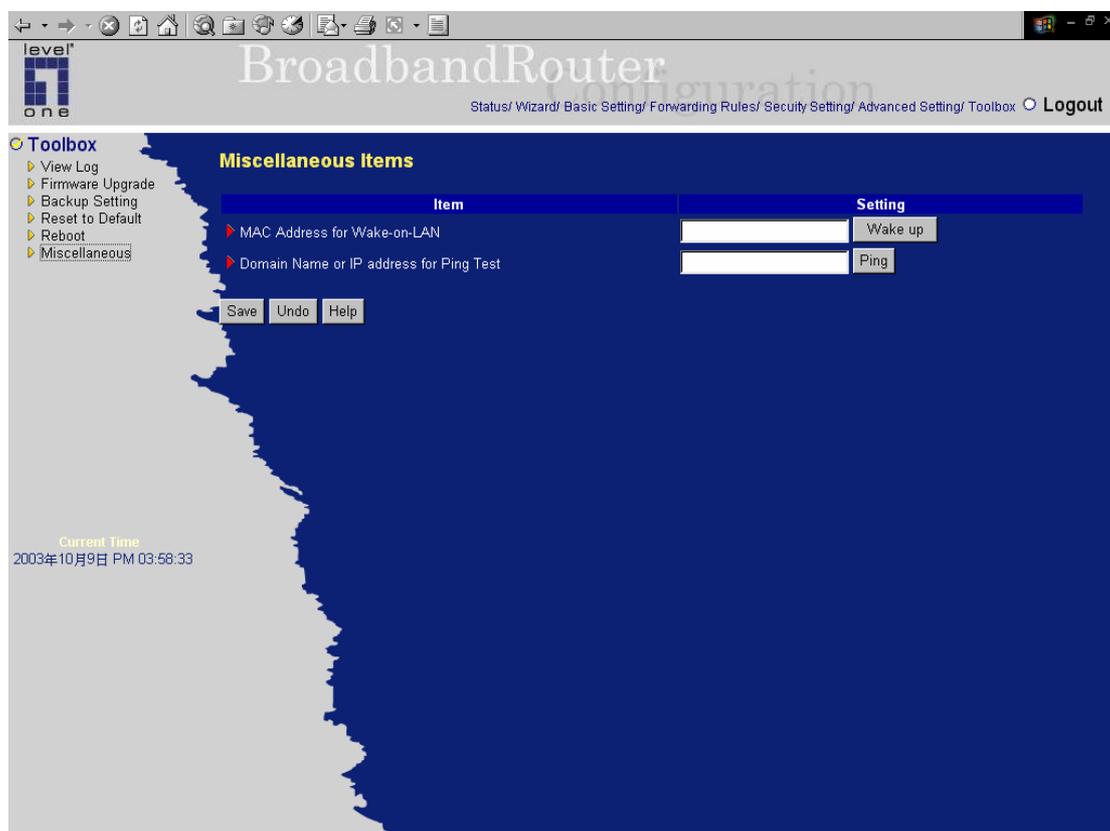
You can also reset this product to factory default by clicking the **Reset to default** button.

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

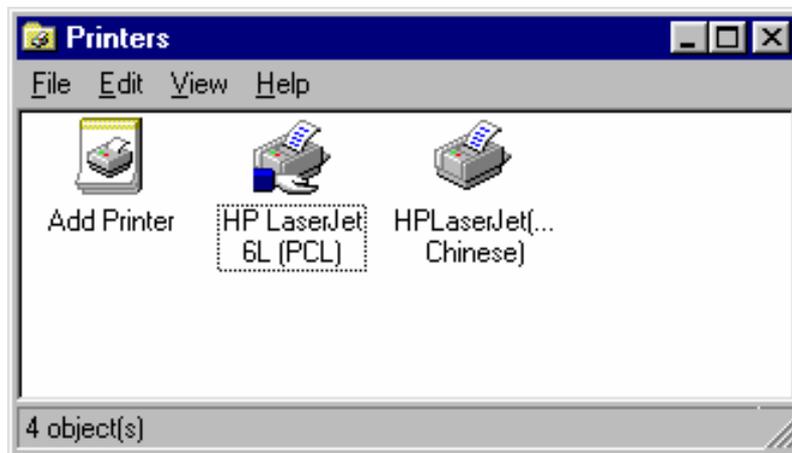
Allow you to configure an IP, and ping the device. You can ping a specific IP to test whether it is alive.

Chapter 5 Print Server

LevelOne FBR-1409TX 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.)

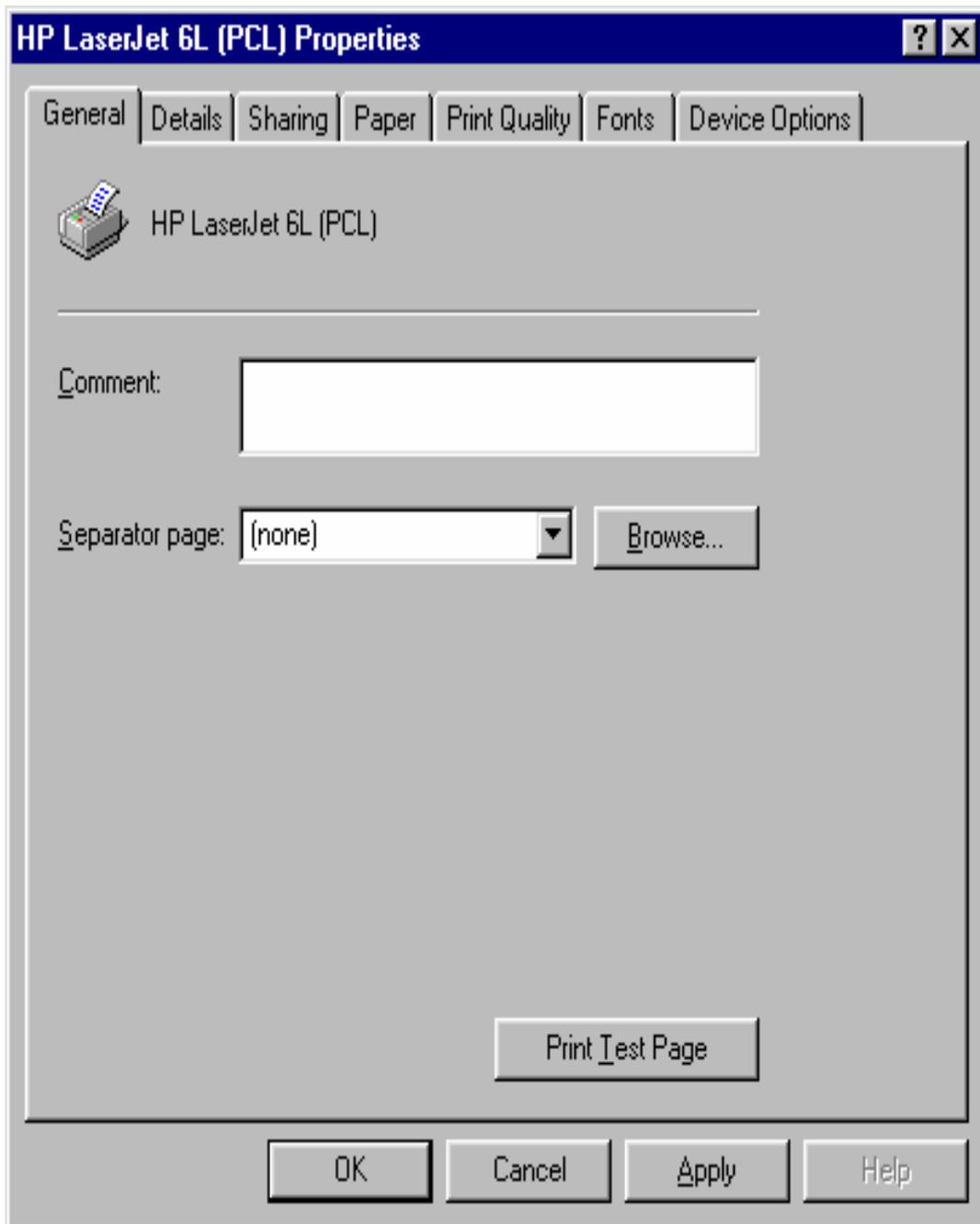
5.1 Configuring on Windows 95/98 Platforms

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 LevelOne FBR-1409TX as *server printer*. On a Windows 95/98 platform, open the *Printers* window in the *My Computer* menu:

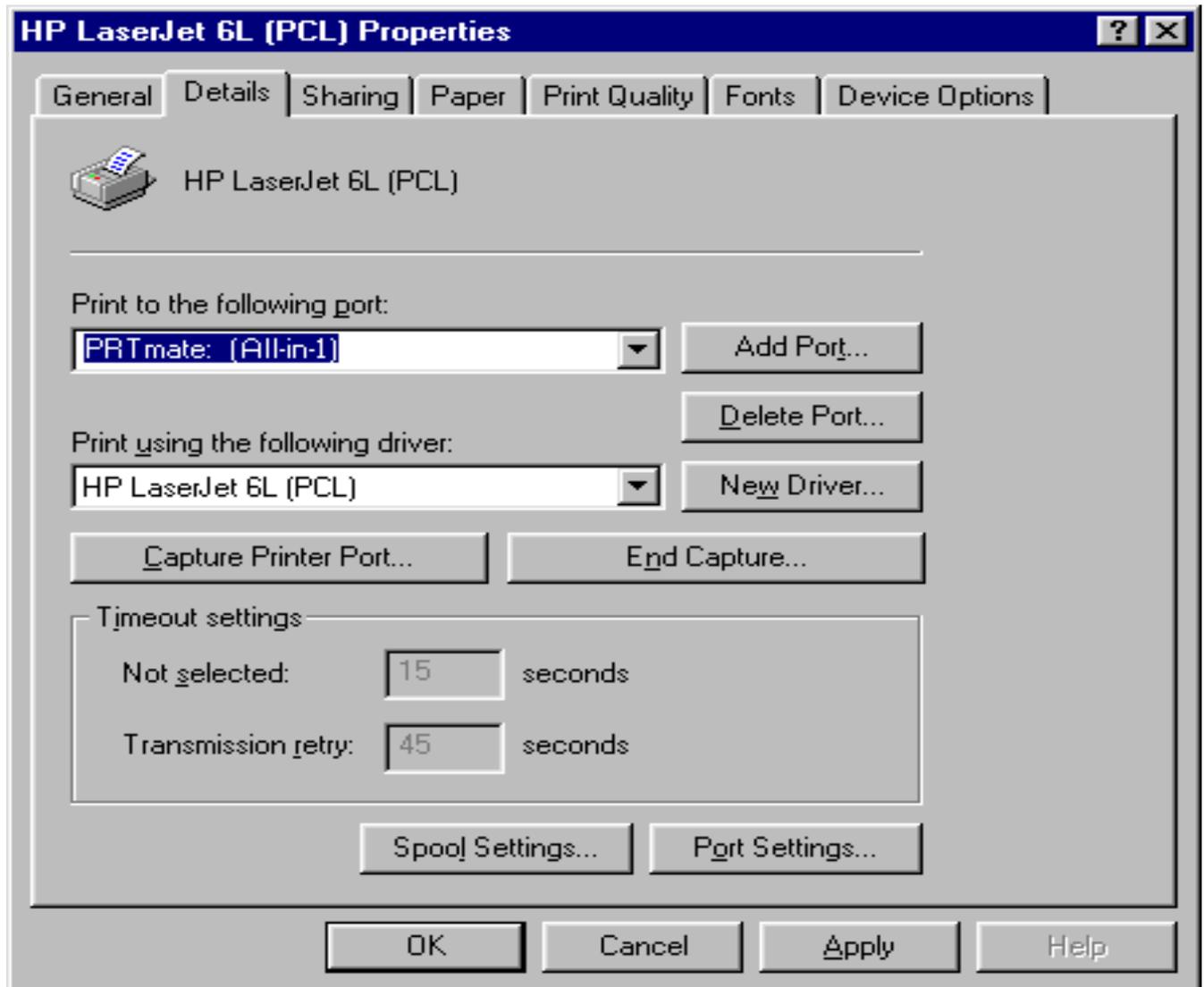


Now, you can configure the print server of this product:

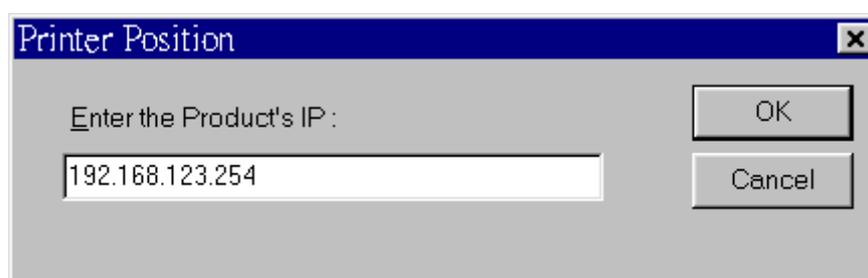
1. Find out the corresponding icon of your *server printer*, for example, the **HP LaserJet 6L**. Click the mouse's right button on that icon, and then select the *Properties* item:



2. Click the *Details* item:



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

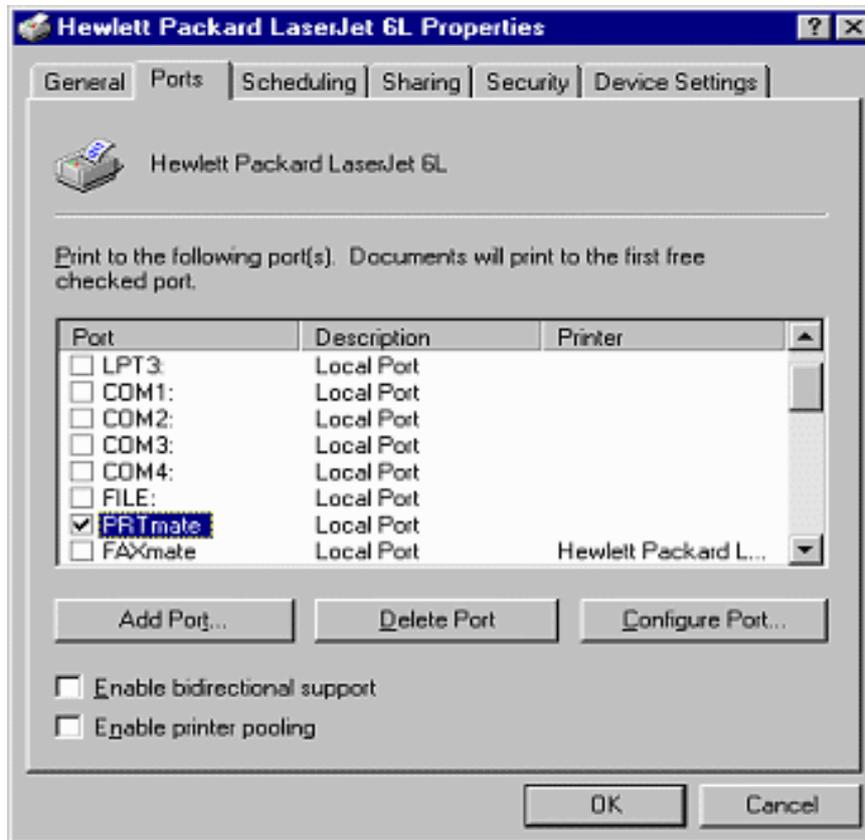


Type in the IP address of this product and then click the **OK** button.

5. 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*:



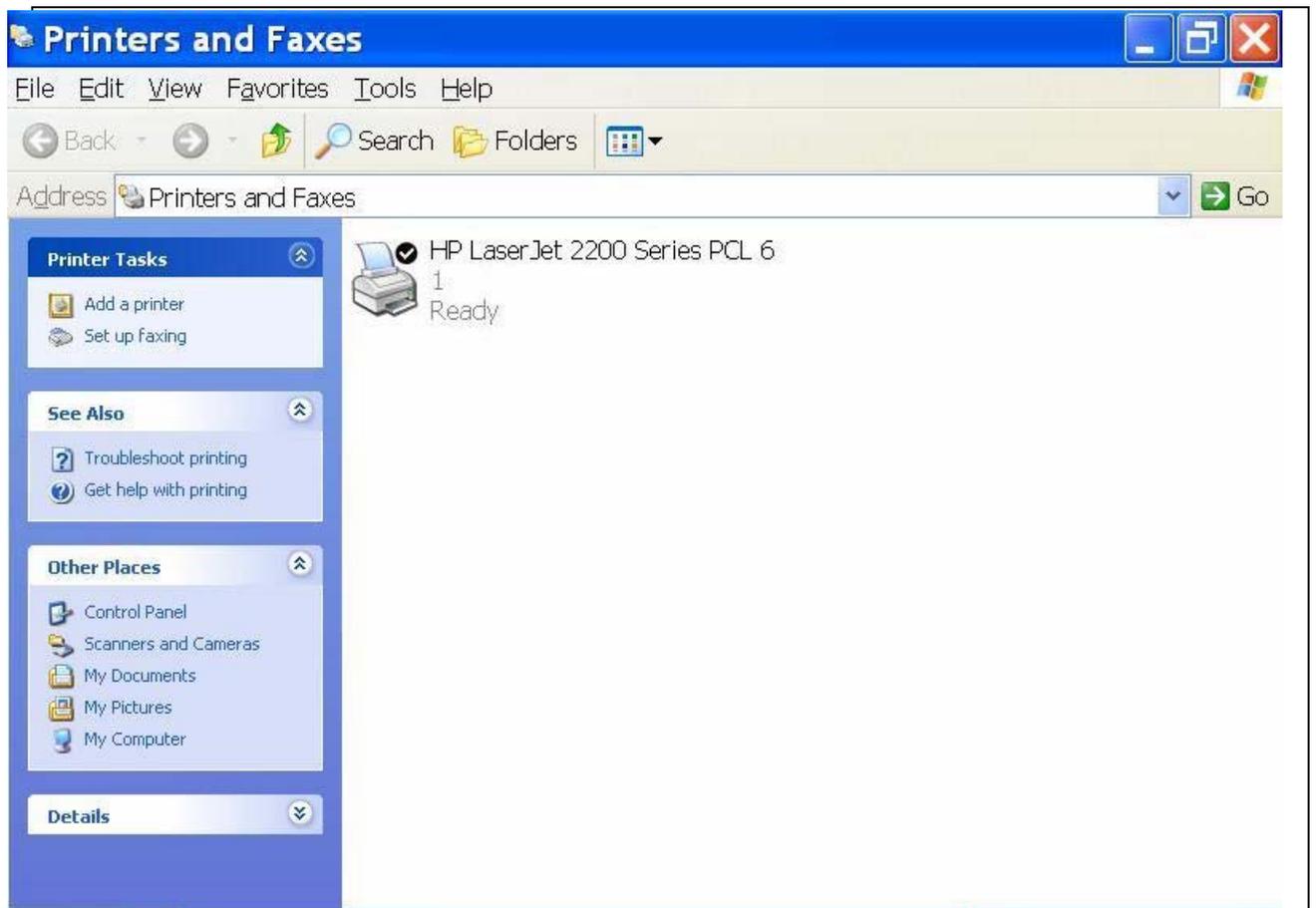
Compared to the procedure in last section, the selection of *Details* is equivalent to the selection of *Ports*, and *Port Settings* is equivalent to *Configure Port*.

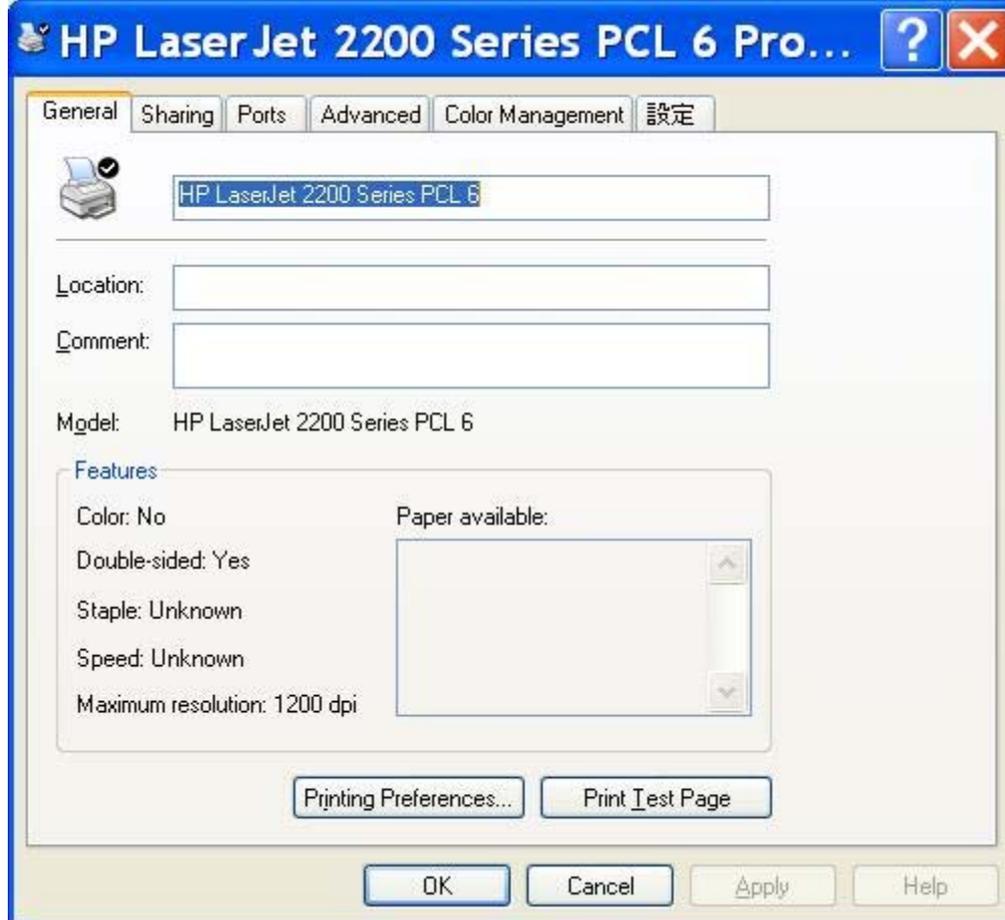
5.3 Configuring on Windows 2000 and XP Platforms

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

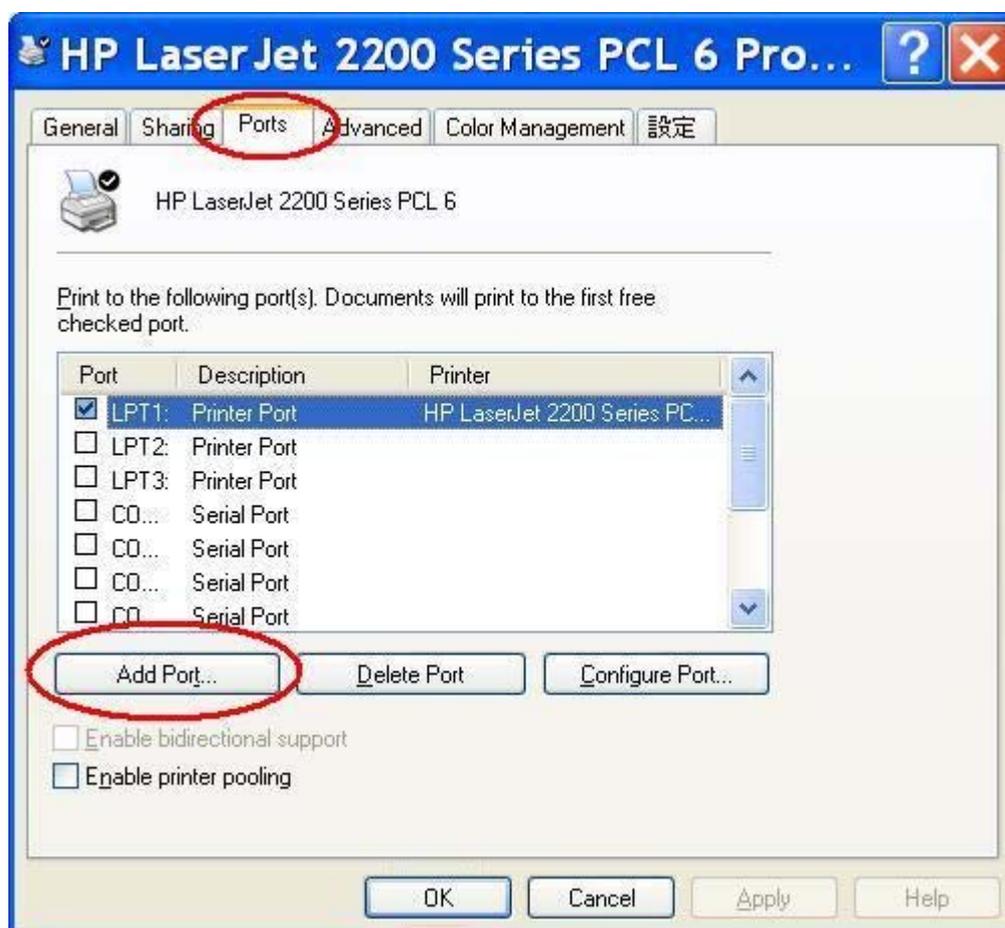
You have to install your Printer Driver on LPT1 or other ports before you proceed the following sequence.

1. Open Printers and Faxes.

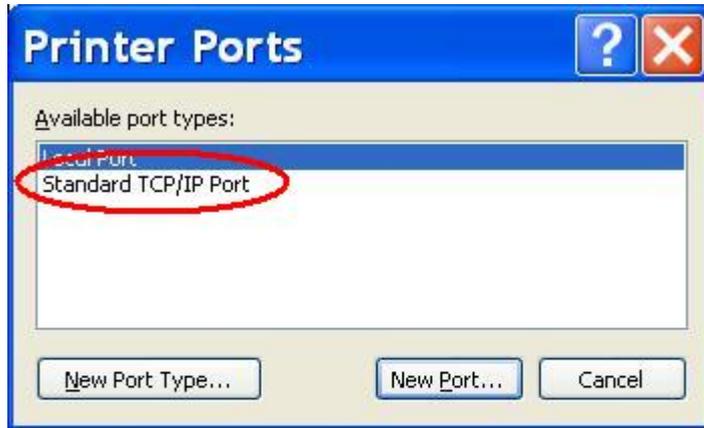




2. Select "Ports" page, Click "Add Port..."

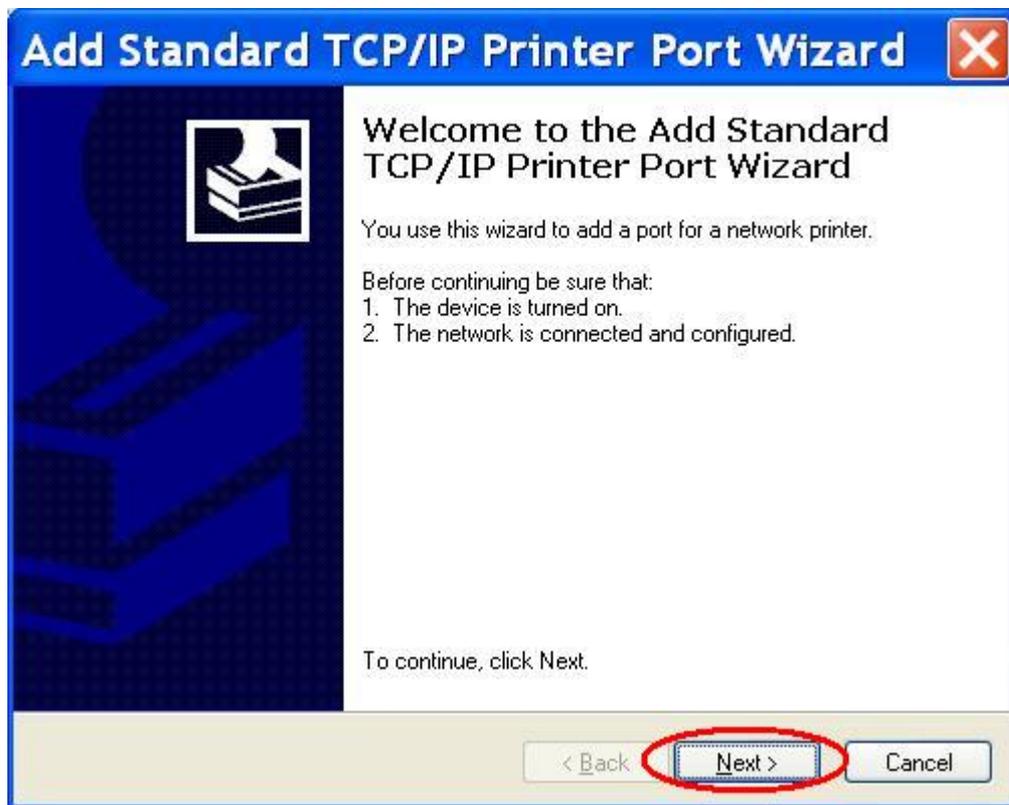


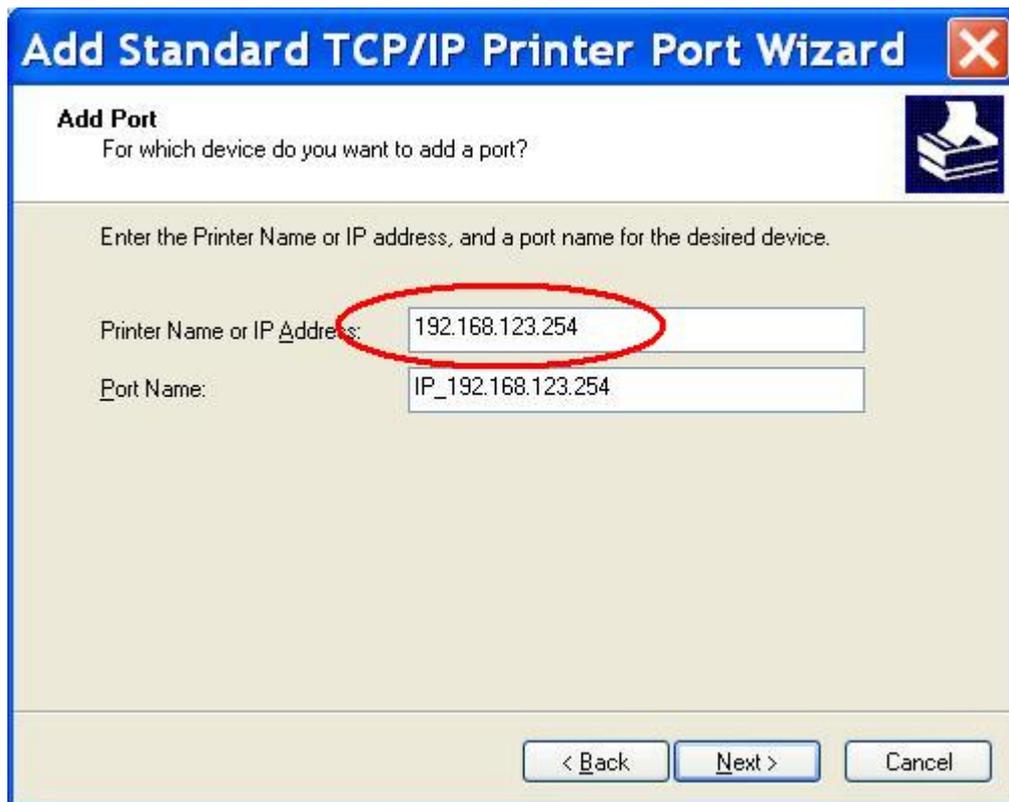
3. Select “Standard TCP/IP Port”, and then click “New Port...”



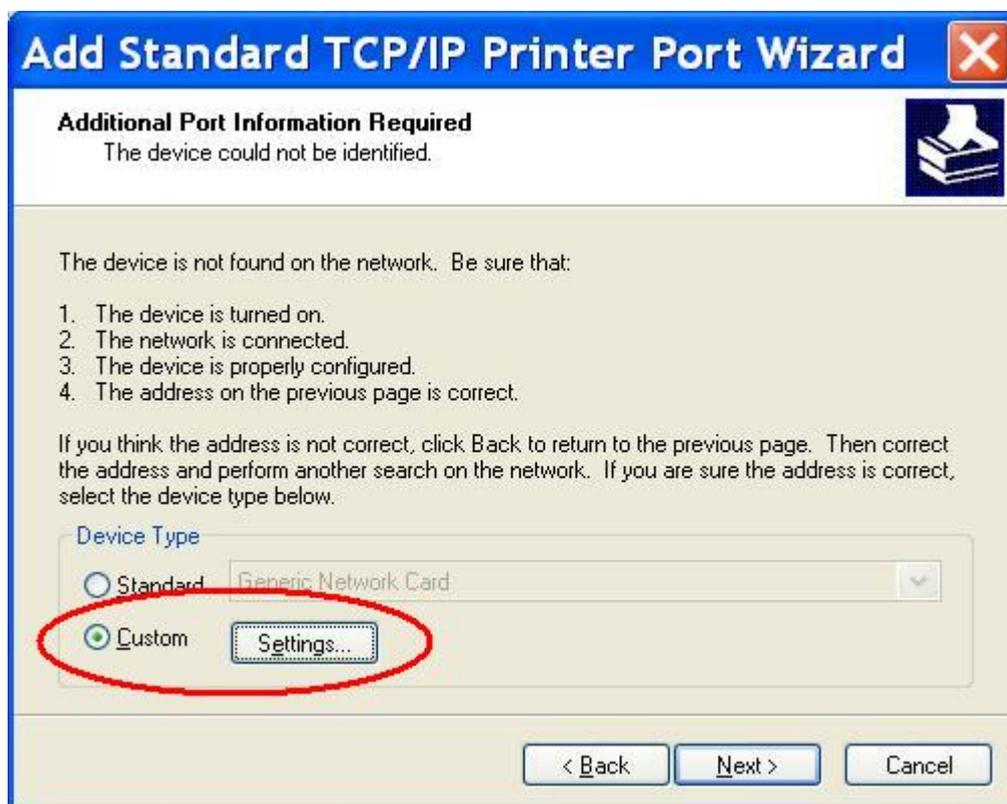
4. Click Next and then provide the following information:

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





5. Select Custom, then click “Settings...”

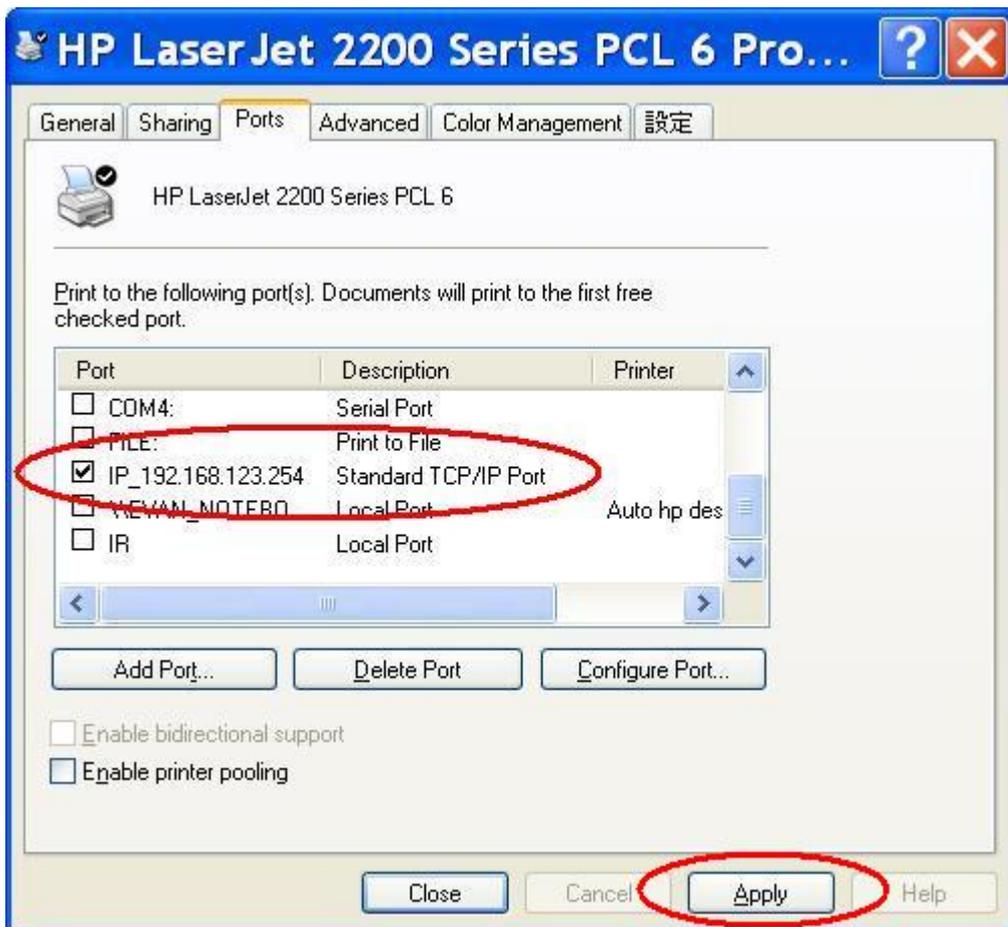


6. Select “LPR”, type ” **lp**“ lowercase letter in “Queue Name:”

And enable “LPR Byte Counting Enabled”.

The image shows a Windows-style dialog box titled "Configure Standard TCP/IP P...". It has a "Port Settings" tab selected. The "Port Name" field contains "IP_192.168.123.254" and the "Printer Name or IP Address" field contains "192.168.123.254". Under the "Protocol" section, the "LPR" radio button is selected and circled in red. Below this, the "Raw Settings" section has a "Port Number" of "9100". The "LPR Settings" section has a "Queue Name" of "lp" circled in red, and the "LPR Byte Counting Enabled" checkbox is checked. There is also an unchecked "SNMP Status Enabled" checkbox. At the bottom, there are "OK" and "Cancel" buttons.

7. Apply your settings



5.4 Configuring on Unix based Platforms

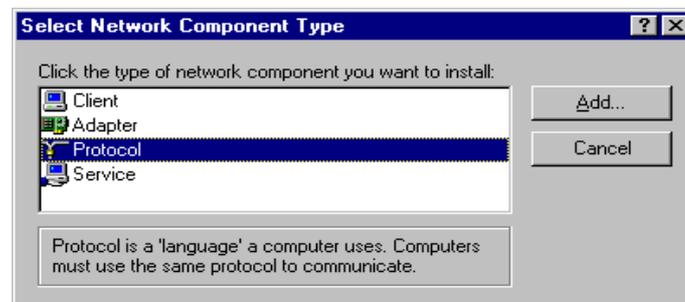
Please follow the traditional configuration procedure on Unix platforms to setup the print server of this product. The printer name is “lp.”

Appendix A TCP/IP Configuration for Windows 95/98

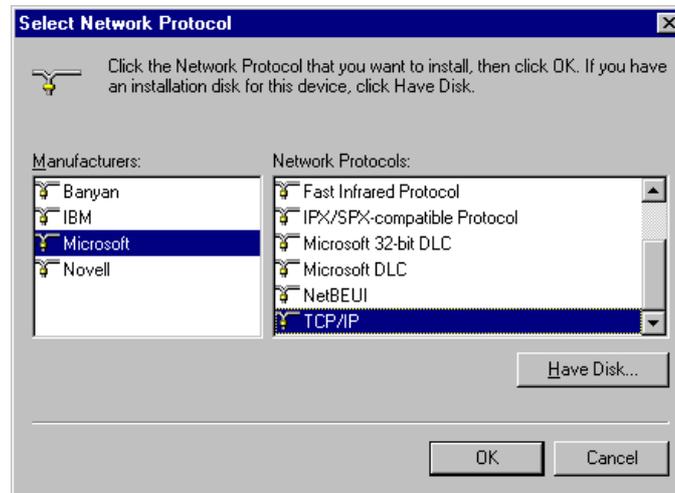
This section introduces you how to install TCP/IP protocol into your personal computer. And suppose you have been successfully installed one network card on your personal computer. If not, please refer to your network card manual. Moreover, the Section B.2 tells you how to set TCP/IP values for working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



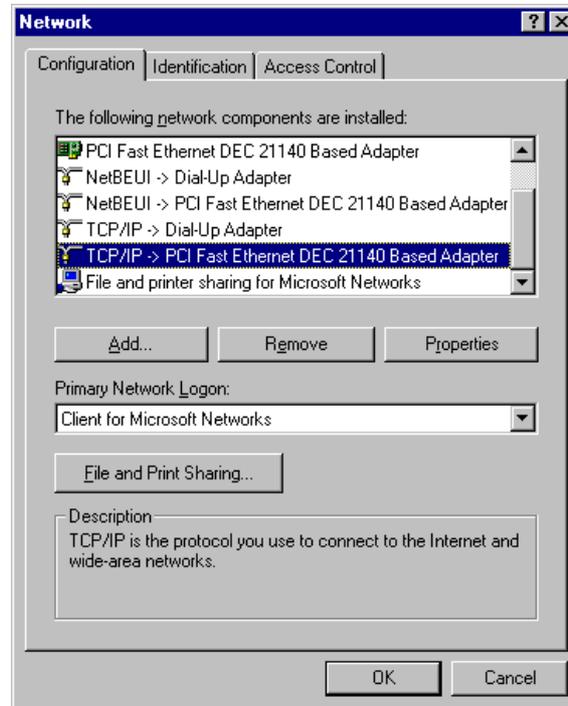
5. Select **Microsoft** item in the *manufactures* list. And choose **TCP/IP** in the *Network Protocols*. Click **OK** button to return to Network window.



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.

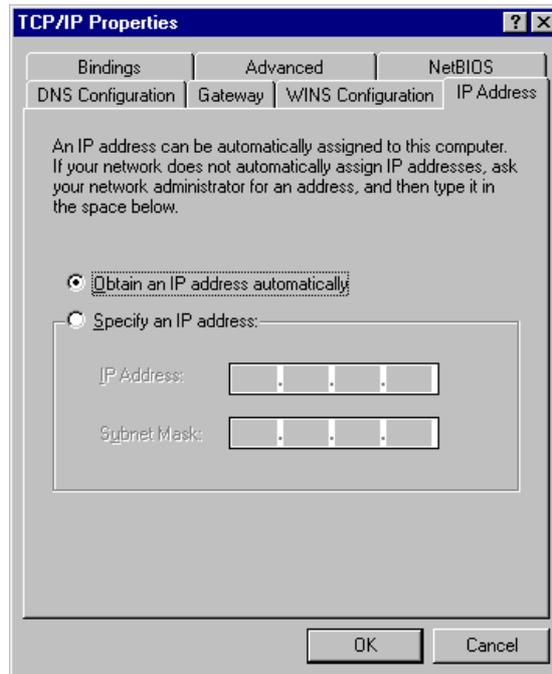
A.2 Set TCP/IP Protocol for Working with NAT Router

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.

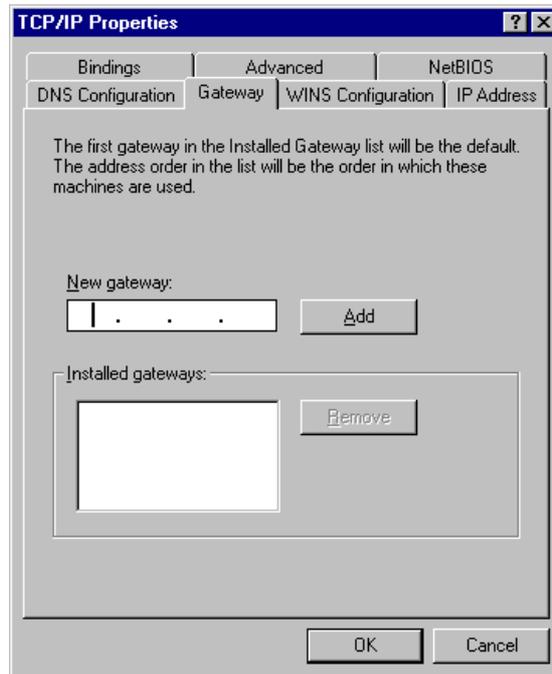


3. Click **Properties** button to set the TCP/IP protocol for this NAT Router.
4. Now, you have two setting methods:
 - A. Get IP via DHCP server

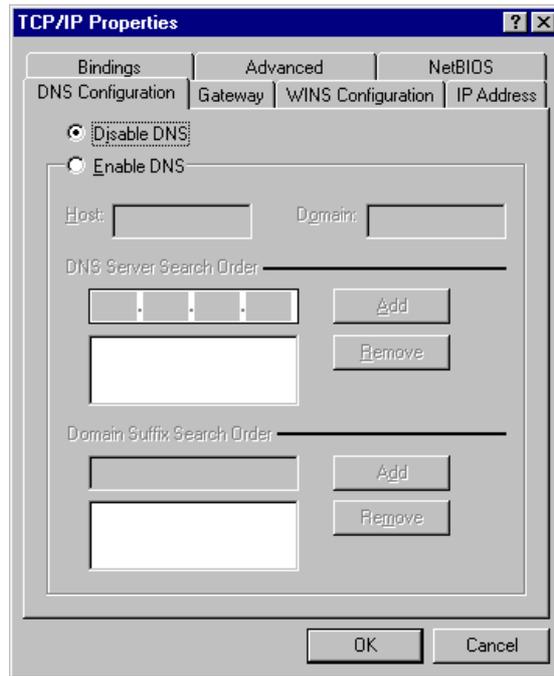
- a. Select *Obtain an IP address automatically* in the *IP Address* tab.



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

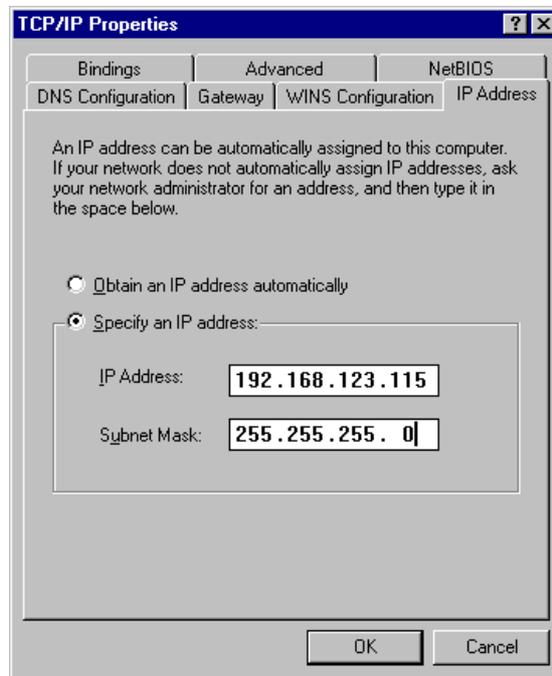


- c. Choose *Disable DNS* in the *DNS Configuration* tab.

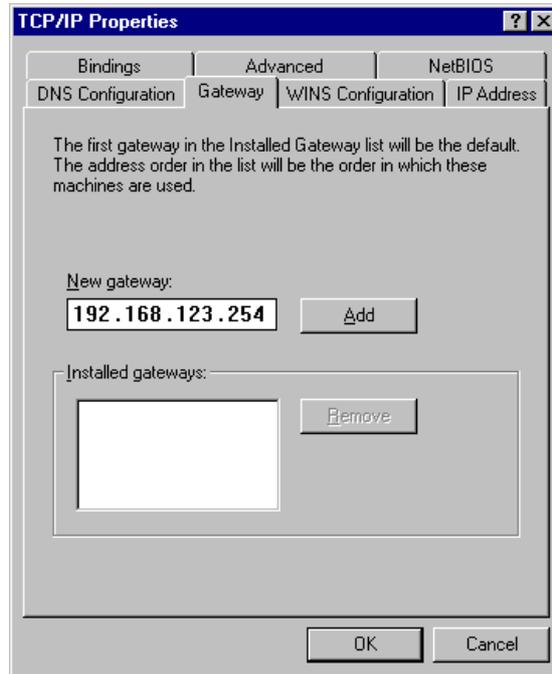


B. Configure IP manually

- 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.

