



**LevelOne**

**FBR-1417TX**

**Broadband Router**

**w/VPN/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

<b>CHAPTER 1 INTRODUCTION.....</b>	<b>5</b>
FUNCTIONS AND FEATURES .....	5
PACKING LIST .....	7
<b>CHAPTER 2 HARDWARE INSTALLATION.....</b>	<b>8</b>
2.1 PANEL LAYOUT .....	8
2.2 PROCEDURE FOR HARDWARE INSTALLATION .....	10
<b>CHAPTER 3 NETWORK SETTINGS AND SOFTWARE INSTALLATION</b>	<b>11</b>
3.1 MAKE CORRECT NETWORK SETTINGS OF YOUR COMPUTER .....	11
3.2 INSTALL THE SOFTWARE INTO YOUR COMPUTERS .....	12
<b>CHAPTER 4 CONFIGURING BROADBAND ROUTER .....</b>	<b>14</b>
4.1 START-UP AND LOG IN.....	15
4.2 STATUS .....	16
4.3 WIZARD .....	17
4.4 BASIC SETTING .....	18
4.4.1 Primary Setup – WAN Type, Virtual Computers .....	19
4.5 FORWARDING RULES .....	25
4.5.1 Virtual Server .....	25
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
4.6.5 VPN setting .....	41
4.6.6 Miscellaneous Items .....	50
4.7 ADVANCED SETTINGS .....	52
4.7.1 System Time.....	52
4.7.2 System Log .....	54
4.7.3 Dynamic DNS.....	55
4.7.4 SNMP Setting .....	57
4.7.5 Routing Table .....	59
4.7.6 Schedule Rule.....	61
4.8 TOOLBOX.....	65

<b>CHAPTER 5 PRINT SERVER .....</b>	<b>70</b>
5.1 CONFIGURING ON WINDOWS 95/98 PLATFORMS .....	70
5.2 CONFIGURING ON WINDOWS NT PLATFORMS .....	73
5.3 CONFIGURING ON WINDOWS 2000 AND XP PLATFORMS.....	74
5.4 CONFIGURING ON UNIX-LIKE BASED PLATFORMS .....	79
5.5 CONFIGURING ON APPLE PC .....	84
<b>APPENDIX A TCP/IP CONFIGURATION FOR WINDOWS 95/98.....</b>	<b>86</b>
<b>APPENDIX B WIN 2000/XP IPSEC SETTING GUIDE .....</b>	<b>92</b>
<b>APPENDIX C PPTP AND L2TP CONFIGURATIONS.....</b>	<b>129</b>
<b>APPENDIX D RESET TO FACTORY DEFAULT .....</b>	<b>135</b>
RESET TO FACTORY DEFAULT.....	135

## **Chapter 1 Introduction**

Congratulations on your purchase of this outstanding LevelOne FBR-1417TX 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**

##### **I Broadband modem and NAT Router**

Connects multiple computers to a broadband (cable or DSL) modem or an Ethernet router to surf the Internet.

##### **I Auto-sensing Ethernet Switch**

Equipped with a 4-port auto-sensing Ethernet switch.

##### **I Printer sharing**

Embedded a print server to allow all of the networked computers to share one printer. Built-in USB(parallel) host to connect to USB (parallel)printer for printer sharing

##### **I Wan type supported**

The router supports some wan types, Static ,Dynamic, PPPoE ,PPTP ,and L2TP etc.

##### **I Firewall**

All unwanted packets from outside intruders are blocked to protect your Intranet.

##### **I DHCP server supported**

All of the networked computers can retrieve TCP/IP settings automatically from this product.

##### **I Web-based configuring**

Configurable through any networked computer's web browser using Netscape or Internet Explorer.

##### **I Virtual Server supported**

Enables you to expose WWW, FTP and other services on your LAN to be accessible to Internet users.

##### **I 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.

**I 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.

**I Statistics of WAN Supported**

Enables you to monitor inbound and outbound packets

## **Security functions**

**I 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.

**I Domain Filter Supported**

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

**I URL Blocking Supported**

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

**I VPN Servers**

The router has three vpn server, IPSEC (Dynamic vpn ),PPTP,L2TP.

**I VPN Pass-through**

The router also support vpn pass-through.

**I SPI Mode Supported**

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

**I DoS Attack Detection Supported**

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

## **Advanced functions**

**I System time Supported**

Allow you to synchronize system time with network time server.

**I E-mail Alert Supported**

The router can send its info by mail.

**I Dynamic dns Supported**

At present,the router has 3 ddns.dyndns,TZO.com and dhs.org.

**I SNMP Supported**

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

**I    Routing Table Supported**

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

**I    Schedule Rule supported**

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

**Other functions**

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

The router also supports this function. The applications: X-box, Msn Messenger.

**Packing List**

- I    FBR-1417TX
- I    Installation CD-ROM with user`s manual
- I    Power adapter
- I    CAT-5 cable
- I    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 D Reset to factory default.



### 2.1.2. Rear Panel

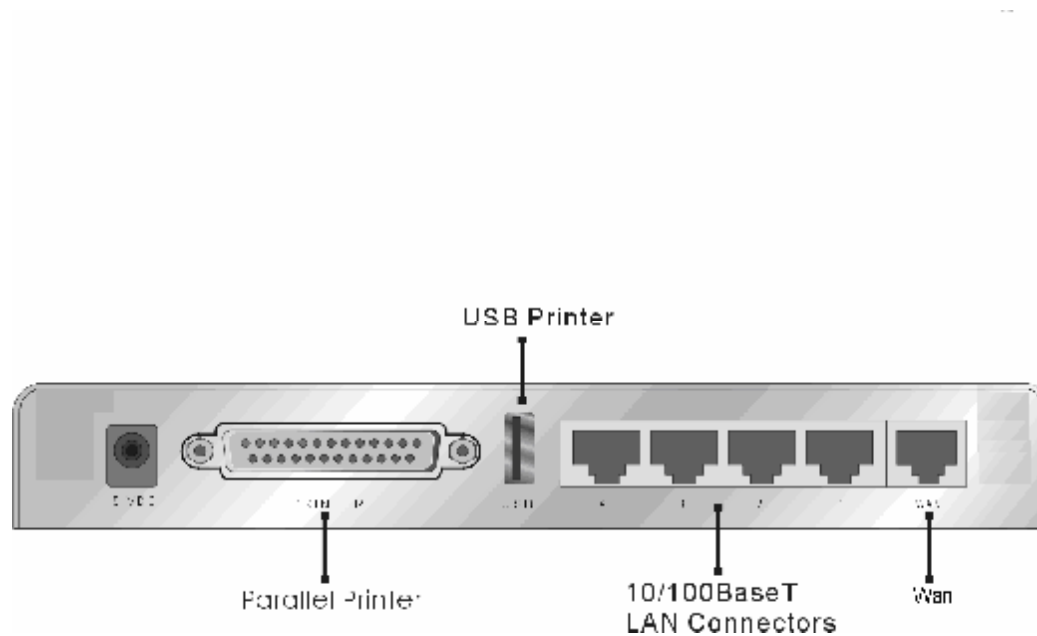


Figure 2-2 Rear Panel

Ports:

Port	Description
<b>5VDC</b>	Power inlet
<b>WAN</b>	the port where you will connect your cable (or DSL) modem or Ethernet router.
<b>Port 1-4</b>	the ports where you will connect networked computers and other devices.
<b>USB</b>	USB Ports for USB printer.
<b>PRINTER</b>	Printer Port

## **2.2 Procedure for Hardware Installation**

### **1. Decide where to place your Broadband Router**

You can place your Broadband Router 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.

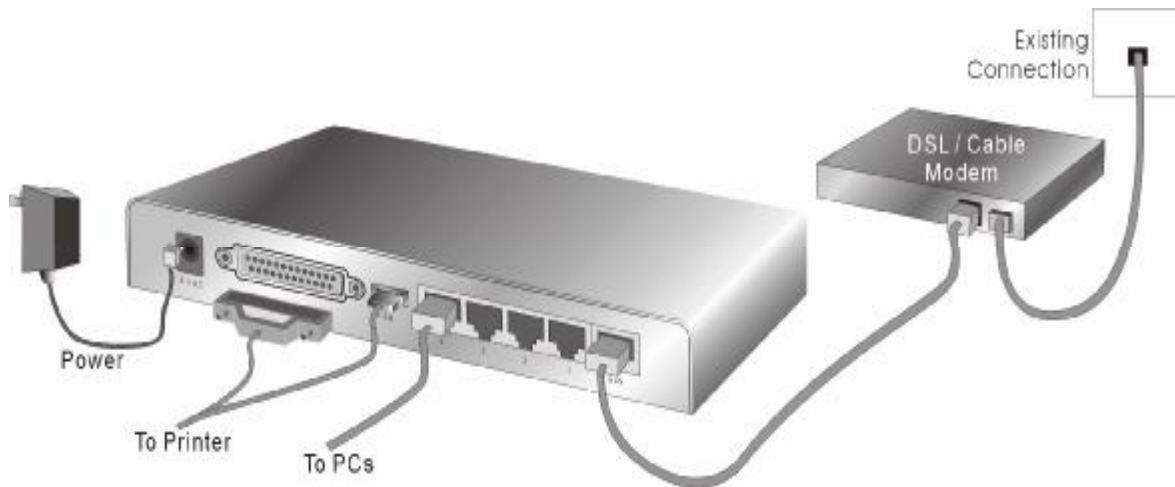


Figure 2-3 Setup of LAN and WAN connections for this product.

### **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 indicators Status LED will be lighted ON for about 10 seconds, and then it will be flashed 3 times to indicate that the self-test operation has finished. Finally, the Status LED 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 FBR-1417TX 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?

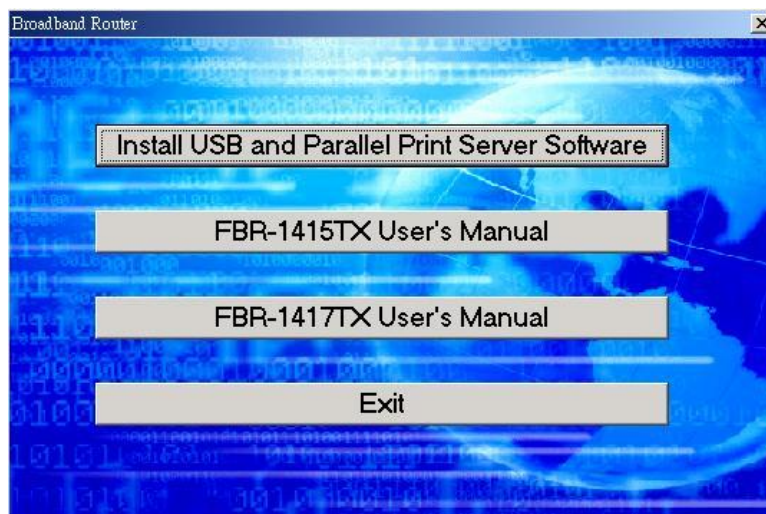
**Tip:** If the IP address of this product is 192.168.123.254, the IP address of your computer must be 192.168.123.X and default gateway must be 192.168.123.254.

## 3.2 Install the Software into Your Computers

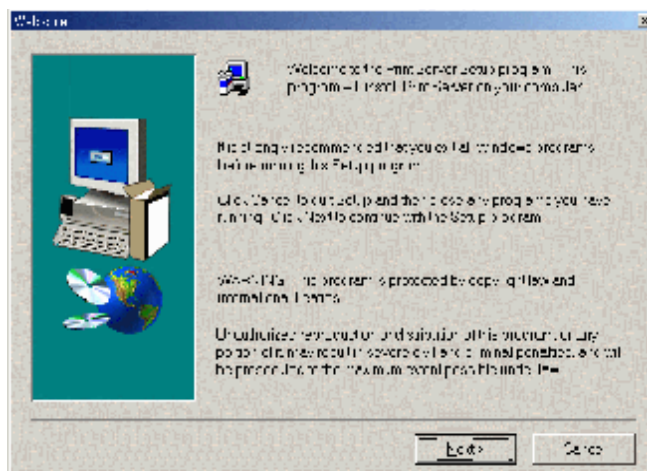
Skip this section if you do not want to use the print server function of this product.

**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.

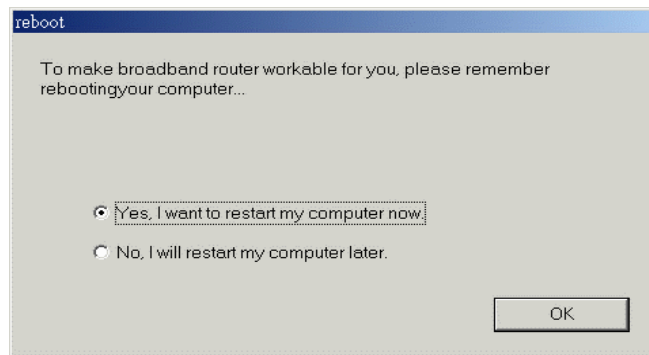


Step 2: Click on the **Install USB and Parallel Print Server Software** button. Wait until the following **Welcome** dialog to appear, and click on the **Next** button.



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.

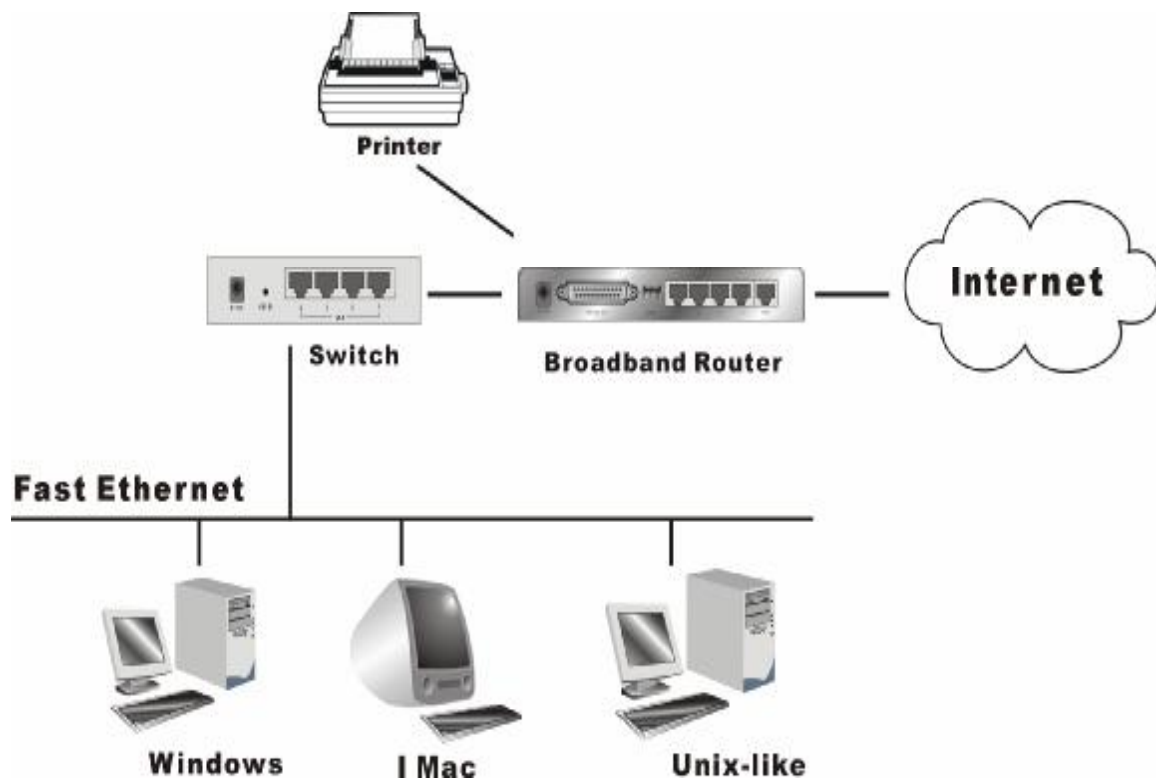


Step 4: After rebooting your computer, the software installation procedure is finished.

Now, you can configure the FBR-1417TX (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.

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 displays the 'levelOne Broadband Router Configuration' web interface. The left sidebar shows the 'Status' menu. The main content area is titled 'System Status' and contains three tables.

**System Status**

Item	WAN Status	Sidenote
Remaining Lease Time	00:00:00	Reconfiguring...
IP Address	0.0.0.0	
Subnet Mask	255.255.255.0	
Gateway	0.0.0.0	
Domain Name Server	168.95.192.1, 168.95.1.1	

**Peripheral Status**

Item	Peripheral Status	Sidenote
Printer(DB25)	Not ready	
Printer(USB)	Not ready	

**Statistics of WAN**

	Inbound	Outbound
Octets	403170	70372
Unicast Packets	534	568
Non-unicast Packets	32	39

Current Time: 06/04/2004 02:24:47

Device Time: 06/04/2004 02:25:11

Buttons: View Log..., Clients List..., Help, Refresh

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.

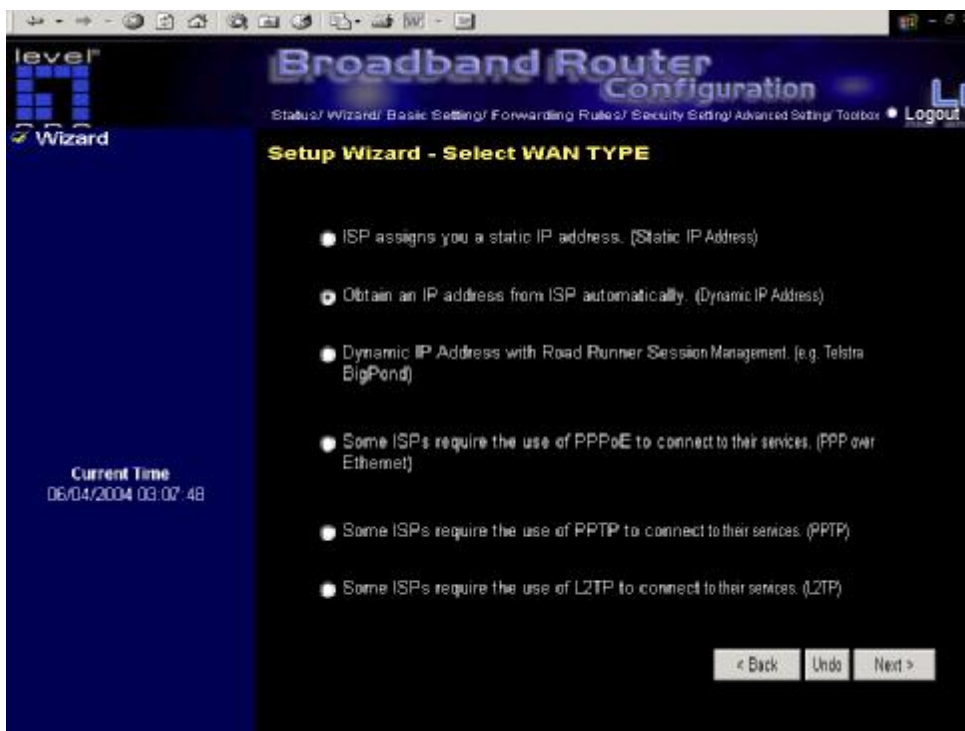
B. Statistics of WAN: enables you to monitor inbound and outbound packets



### 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

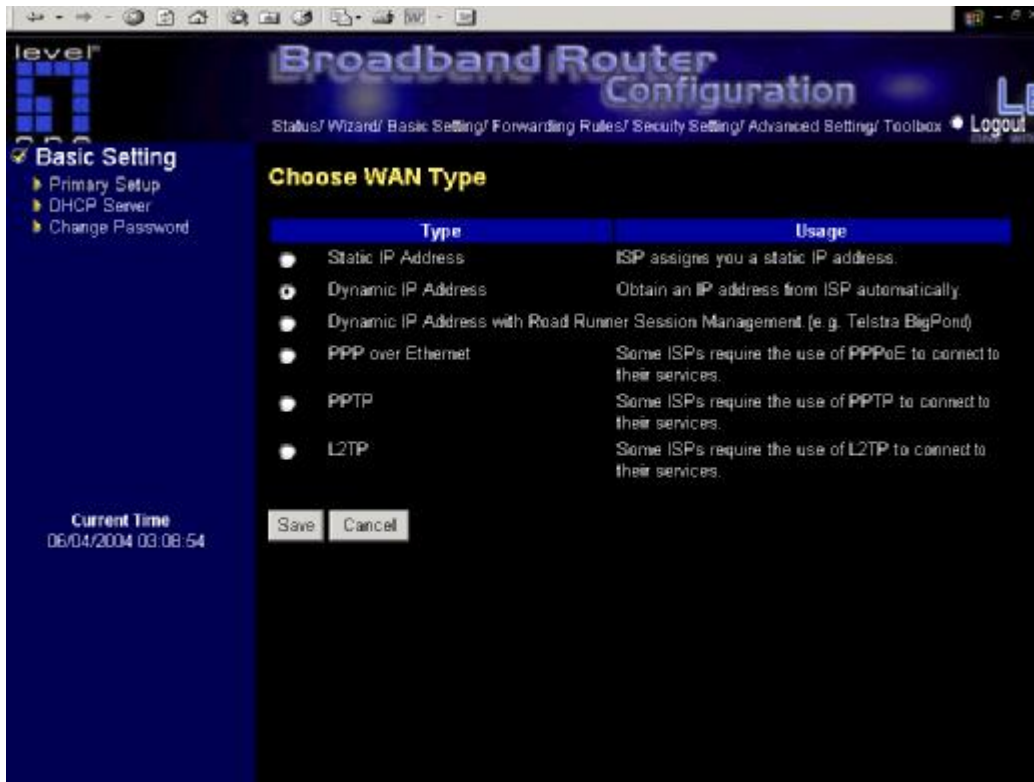
The screenshot shows the LevelOne Broadband Router Configuration web interface. The left sidebar contains a navigation menu with 'Basic Setting' selected, which includes 'Primary Setup', 'DHCP Server', and 'Change Password'. The main content area is titled 'Primary Setup' and contains a table with configuration items. The 'WAN Type' is set to 'Dynamic IP Address' with a 'Change...' button next to it. Other settings include LAN IP Address (192.168.123.254), Host Name (optional), WAN's MAC Address (00-60-18-21-BB-3B) with a 'Clone MAC' button, and a checkbox for 'Renew IP Forever' which is checked and labeled 'Enable (Auto-reconnect)'. At the bottom of the main area are buttons for 'Save', 'Undo', 'Virtual Computers...', and 'Help'. The bottom left of the sidebar shows the 'Current Time' as '06/04/2004 03:08:44'.

Item	Setting
LAN IP Address	192.168.123.254
WAN Type	Dynamic IP Address <a href="#">Change...</a>
Host Name	<input type="text"/> (optional)
WAN's MAC Address	00-60-18-21-BB-3B <a href="#">Clone MAC</a>
Renew IP Forever	<input checked="" type="checkbox"/> Enable (Auto-reconnect)

Save Undo Virtual Computers... Help

Current Time  
06/04/2004 03:08:44

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 Virtual Computers

The screenshot shows the LevelOne Broadband Router Configuration web interface. The title bar reads "levelOne Broadband Router Configuration". Below the title, there is a navigation menu with links: Status, Wizard, Basic Setting, Forwarding Rules, Security Setting, Advanced Setting, Toolbox, and Logout. The "Basic Setting" section is selected and expanded, showing sub-links: Primary Setup, DHCP Server, and Change Password. The main content area is titled "Virtual Computers" and contains a table with the following columns: ID, Global IP, Local IP, and Enable. The table has five rows, each with an ID from 1 to 5. The "Global IP" column contains empty text boxes. The "Local IP" column contains the text "192.168.123." followed by empty text boxes. The "Enable" column contains checkboxes, all of which are currently unchecked. Below the table, there are three buttons: Save, Undo, and Help. In the bottom left corner, the "Current Time" is displayed as "06/04/2004 03:11:53".

ID	Global IP	Local IP	Enable
1		192.168.123.	<input type="checkbox"/>
2		192.168.123.	<input type="checkbox"/>
3		192.168.123.	<input type="checkbox"/>
4		192.168.123.	<input type="checkbox"/>
5		192.168.123.	<input type="checkbox"/>

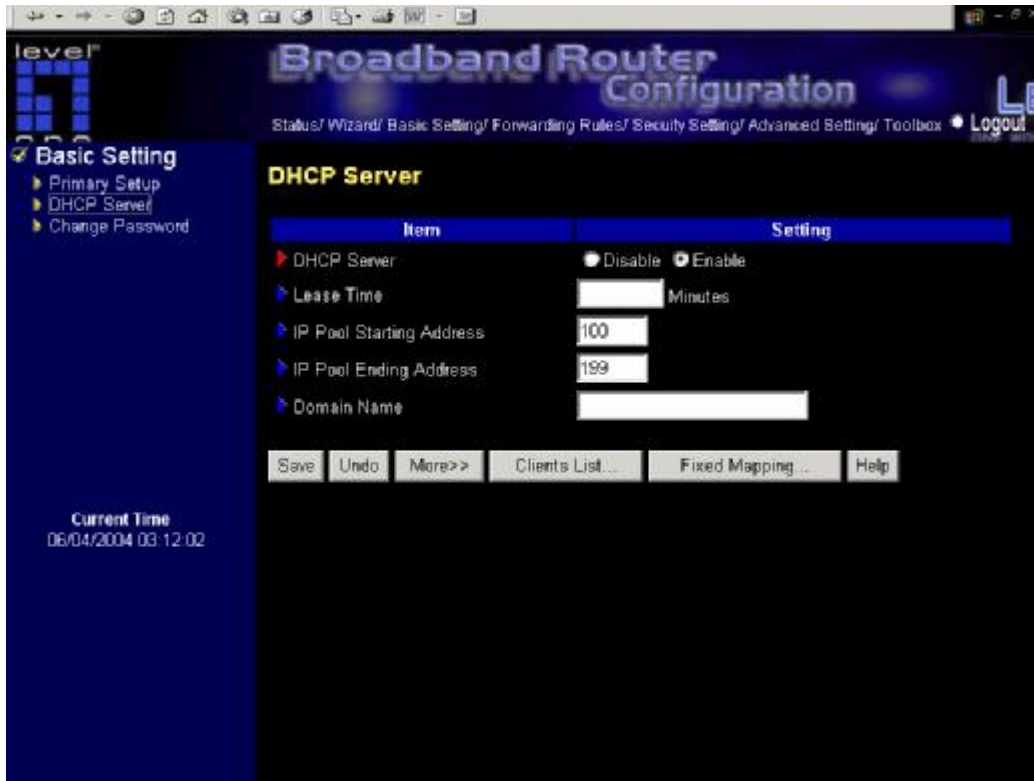
Save Undo Help

Current Time  
06/04/2004 03:11:53

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



The screenshot shows the LevelOne Broadband Router Configuration web interface. The left sidebar contains a navigation menu with 'Basic Setting' selected, which includes 'Primary Setup', 'DHCP Server', and 'Change Password'. The main content area is titled 'Change Password' and features a table with two columns: 'Item' and 'Setting'. The table contains three rows for 'Old Password', 'New Password', and 'Reconfirm', each with an adjacent text input field. Below the table are 'Save' and 'Undo' buttons. At the bottom left, the 'Current Time' is displayed as '06/04/2004 03:12:43'. The top of the interface includes a breadcrumb trail: 'Status / Wizard / Basic Setting / Forwarding Rules / Security Setting / Advanced Setting / Toolbox', and a 'Logout' link.

Item	Setting
Old Password	<input type="text"/>
New Password	<input type="text"/>
Reconfirm	<input type="text"/>

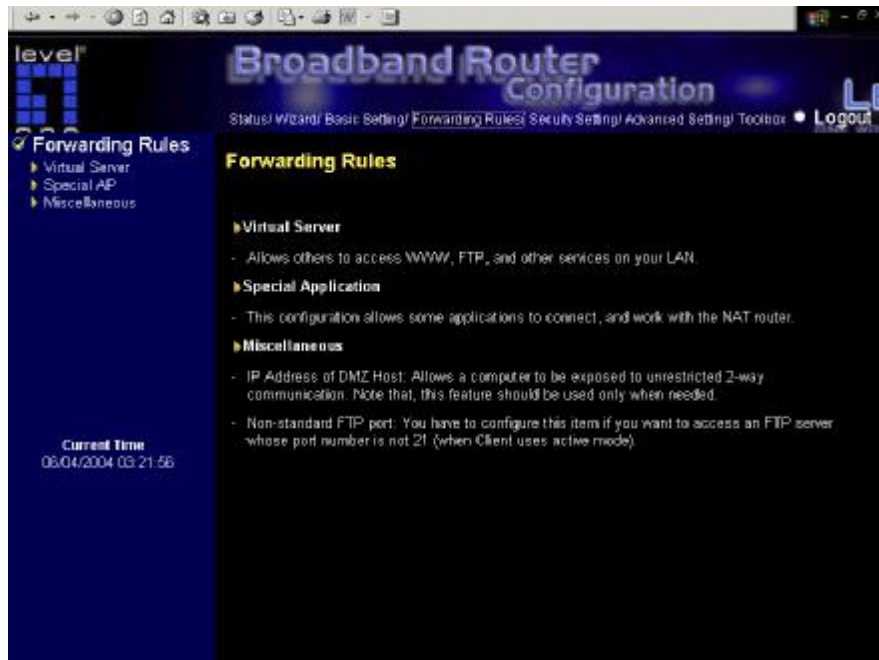
Save Undo

Current Time  
06/04/2004 03:12:43

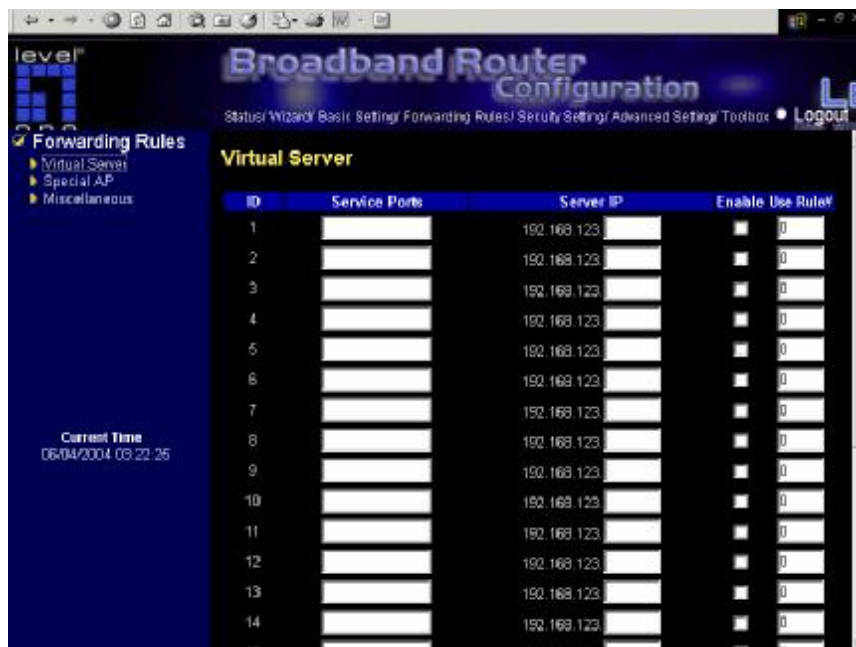
You can change Password here. We **strongly** recommend you to change the system password for security reason.



## 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

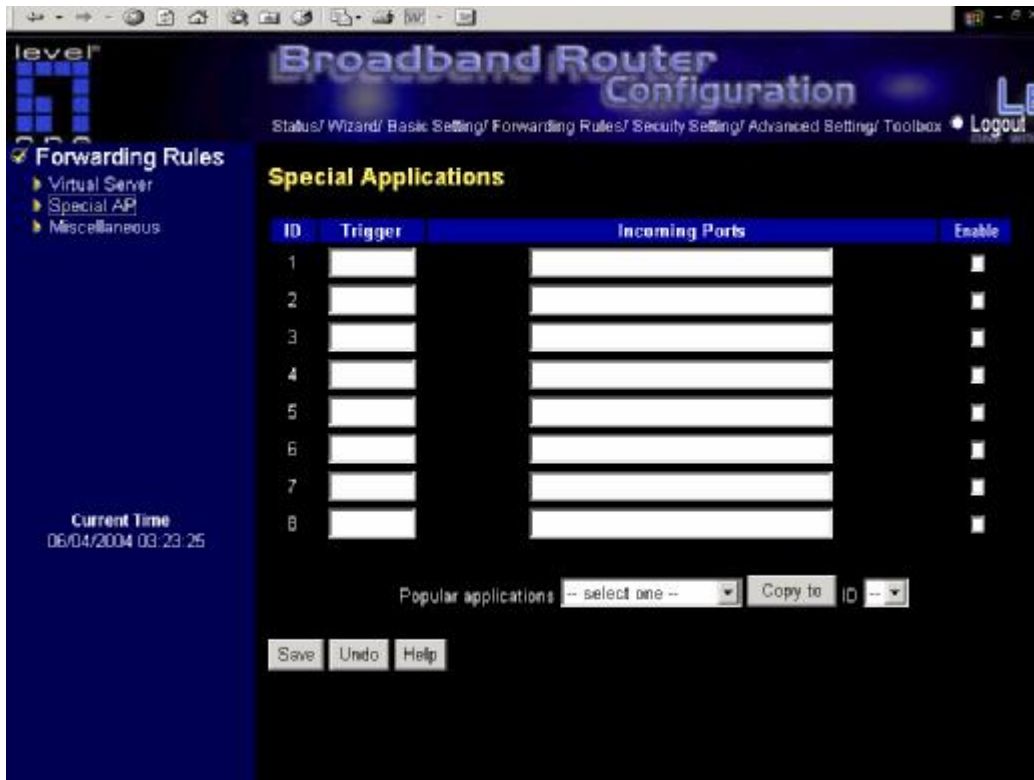
behind this product are invisible to the outside world. If you wish, you can make some of them accessible by enabling the Virtual Server Mapping.

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



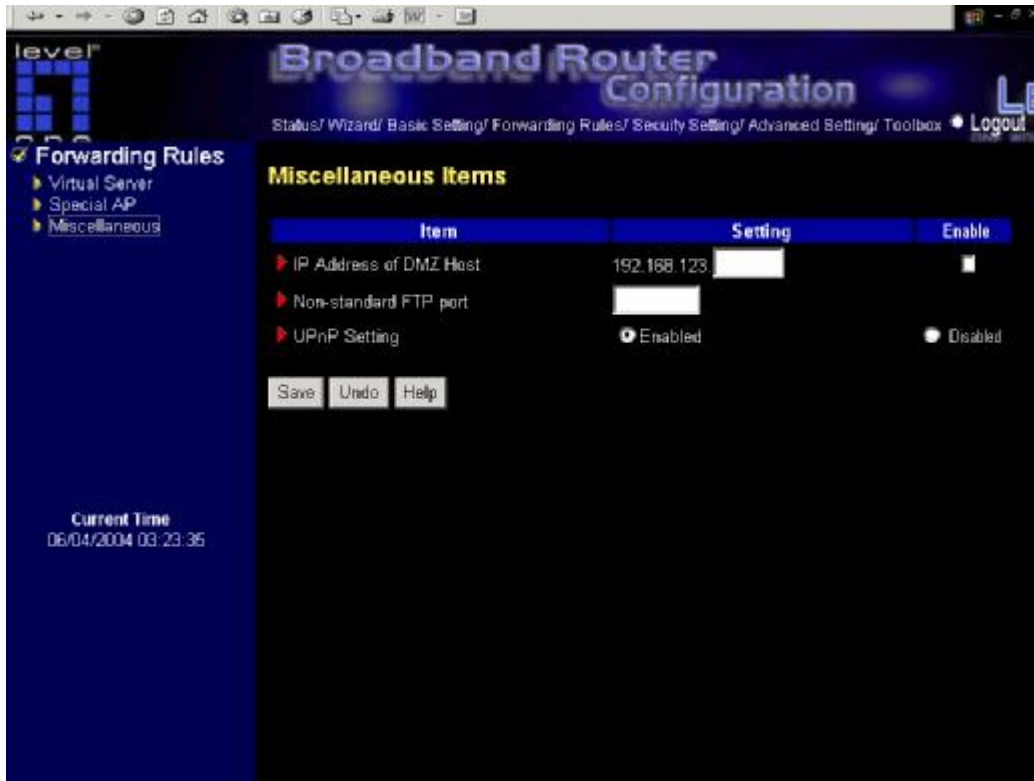
Some applications require multiple connections, like Internet games, Video conferencing, Internet telephony, etc. Because of the firewall function, these applications cannot work with a pure NAT router. The **Special Applications** feature allows some of these applications to work with this product.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

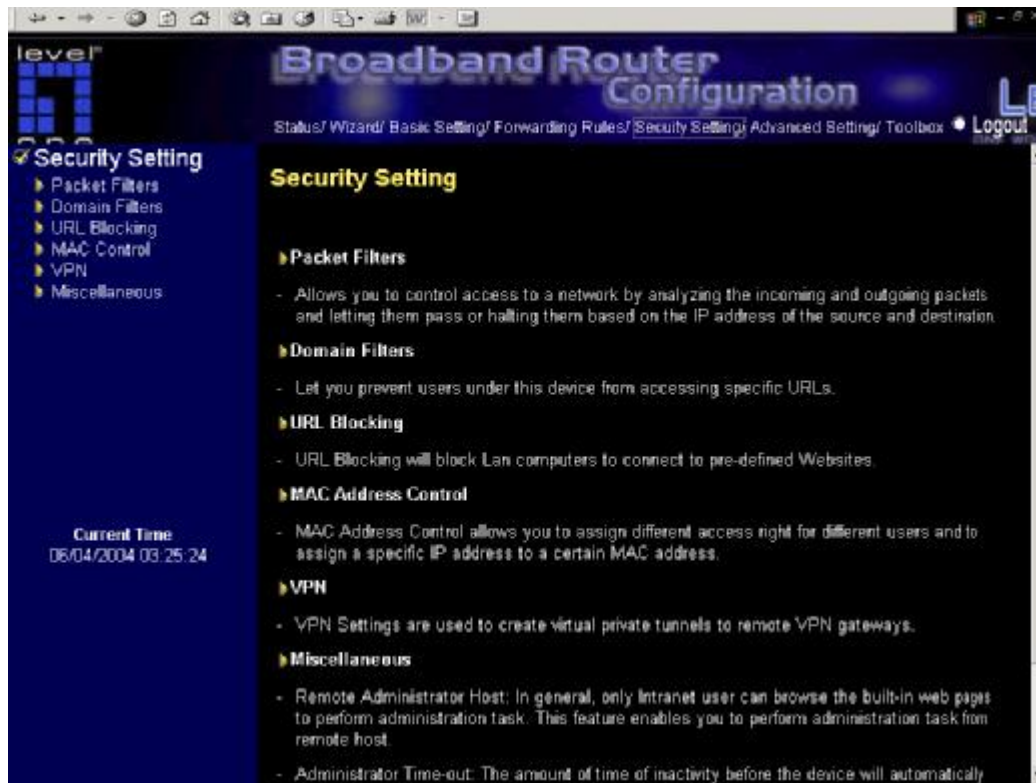
#### Non-standard FTP port

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.

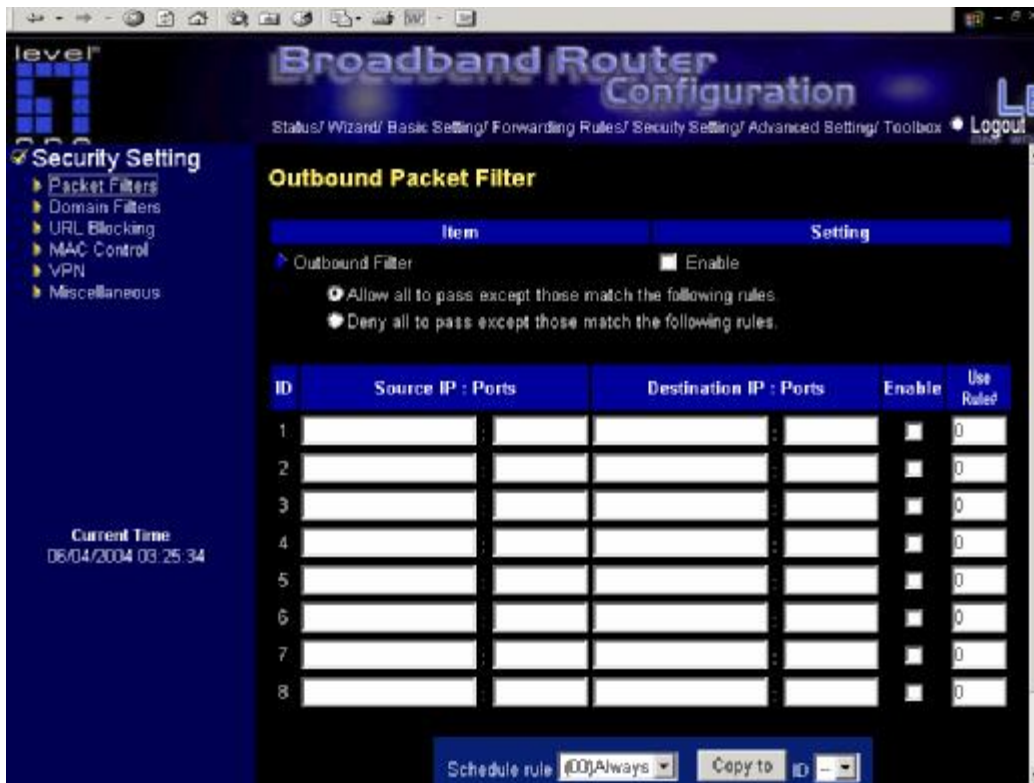
#### UPnP Setting

You can check the buttons to enable or disable the UPnP function of FBR-1417TX.

## 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**.

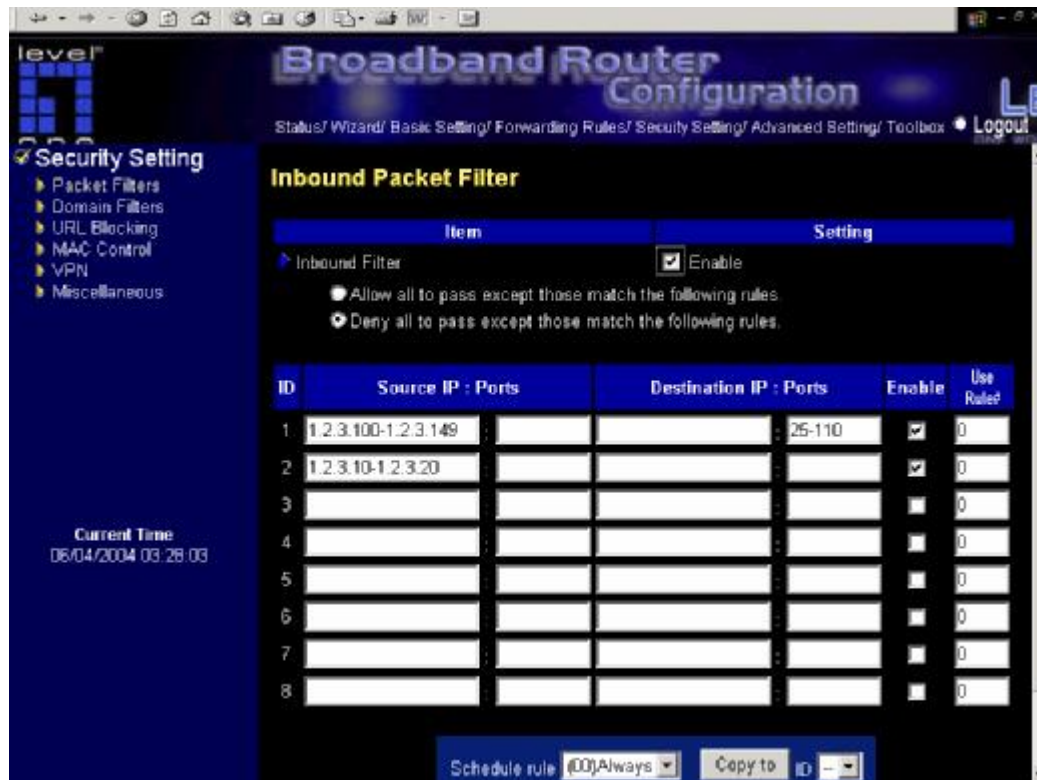
Each rule can be enabled or disabled individually.

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:**

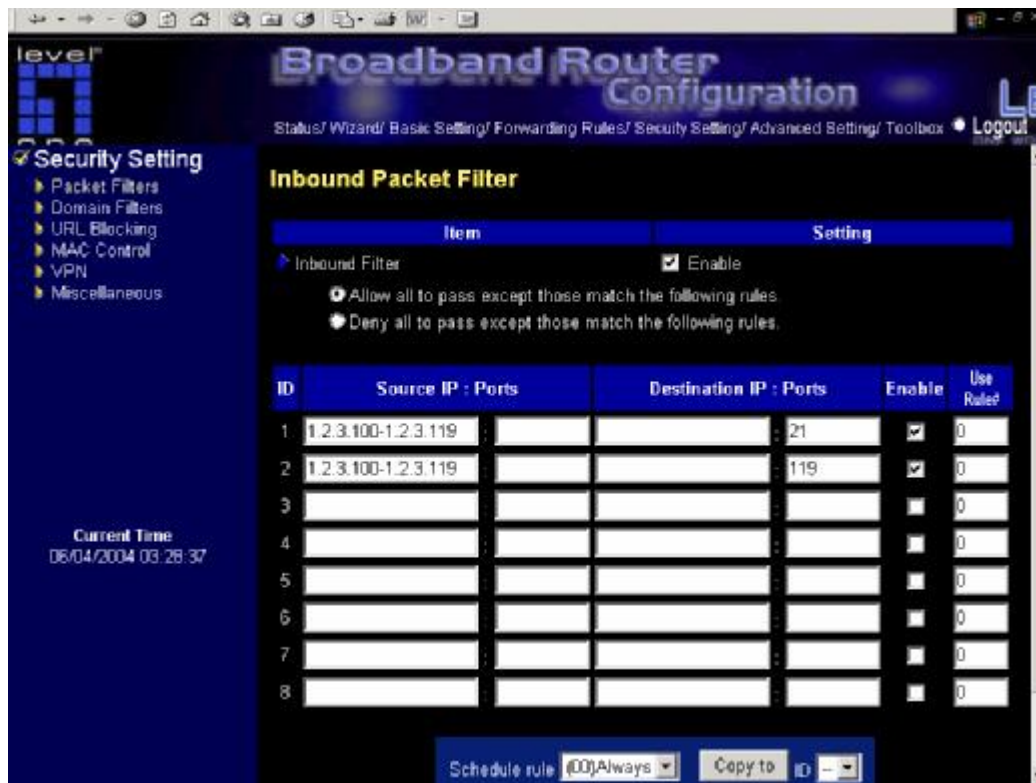


(1.2.3.100-1.2.3.149) They are allow to send mail (port 25), receive mail (port 110), and browse your web server as above (port 80)

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

Others are all blocked.

**Example 2:**



(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.

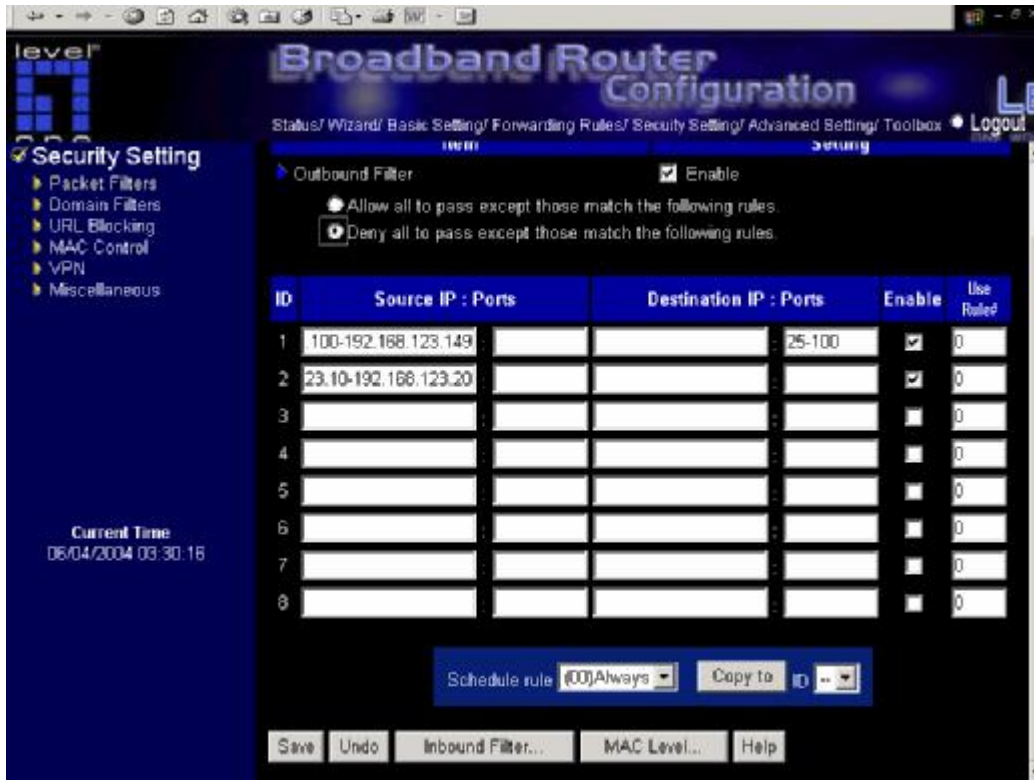
After **Inbound Packet Filter** setting is configured, click the **save** button.



Outbound Filter:

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

**Example 1:**

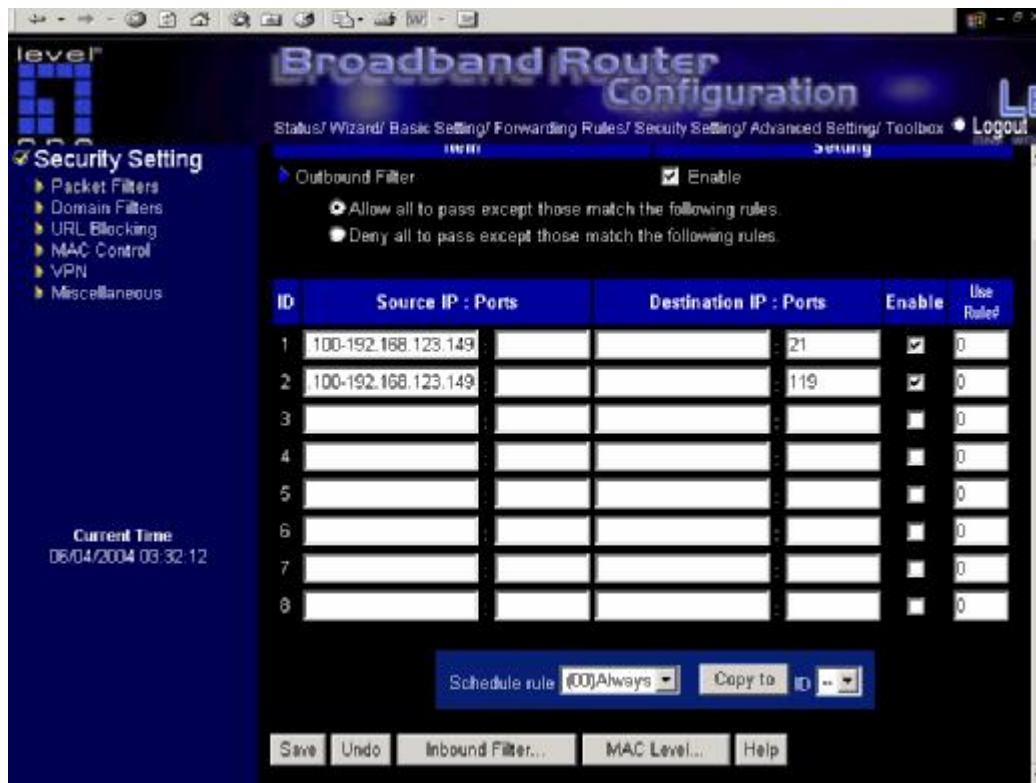


(192.168.123.100-192.168.123.149) They are allowed to send mail (port 25), receive mail (port 110), and browse Internet (port 80); port 53 (DNS) is necessary to resolve the domain name.

(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

The screenshot shows the 'Domain Filter' configuration page in the LevelOne Broadband Router Configuration utility. The left sidebar shows 'Security Setting' with sub-items: Packet Filters, Domain Filters (selected), URL Blocking, MAC Control, VPN, and Miscellaneous. The main area has a 'Domain Filter' title and three settings: 'Domain Filter' (checked), 'Log DNS Query' (checked), and 'Privilege IP Addresses Range' (From 0 To 0). Below these is a table with 10 rows for domain suffixes. Each row has columns for ID, Domain Suffix, Action (Drop and Log checkboxes), and an Enable checkbox. The last row is labeled '\* (all others)'.

ID	Domain Suffix	Action	Enable
1		<input type="checkbox"/> Drop <input type="checkbox"/> Log	<input type="checkbox"/>
2		<input type="checkbox"/> Drop <input type="checkbox"/> Log	<input type="checkbox"/>
3		<input type="checkbox"/> Drop <input type="checkbox"/> Log	<input type="checkbox"/>
4		<input type="checkbox"/> Drop <input type="checkbox"/> Log	<input type="checkbox"/>
5		<input type="checkbox"/> Drop <input type="checkbox"/> Log	<input type="checkbox"/>
6		<input type="checkbox"/> Drop <input type="checkbox"/> Log	<input type="checkbox"/>
7		<input type="checkbox"/> Drop <input type="checkbox"/> Log	<input type="checkbox"/>
8		<input type="checkbox"/> Drop <input type="checkbox"/> Log	<input type="checkbox"/>
9		<input type="checkbox"/> Drop <input type="checkbox"/> Log	<input type="checkbox"/>
10	* (all others)	<input type="checkbox"/> Drop <input type="checkbox"/> Log	<input type="checkbox"/>

### 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

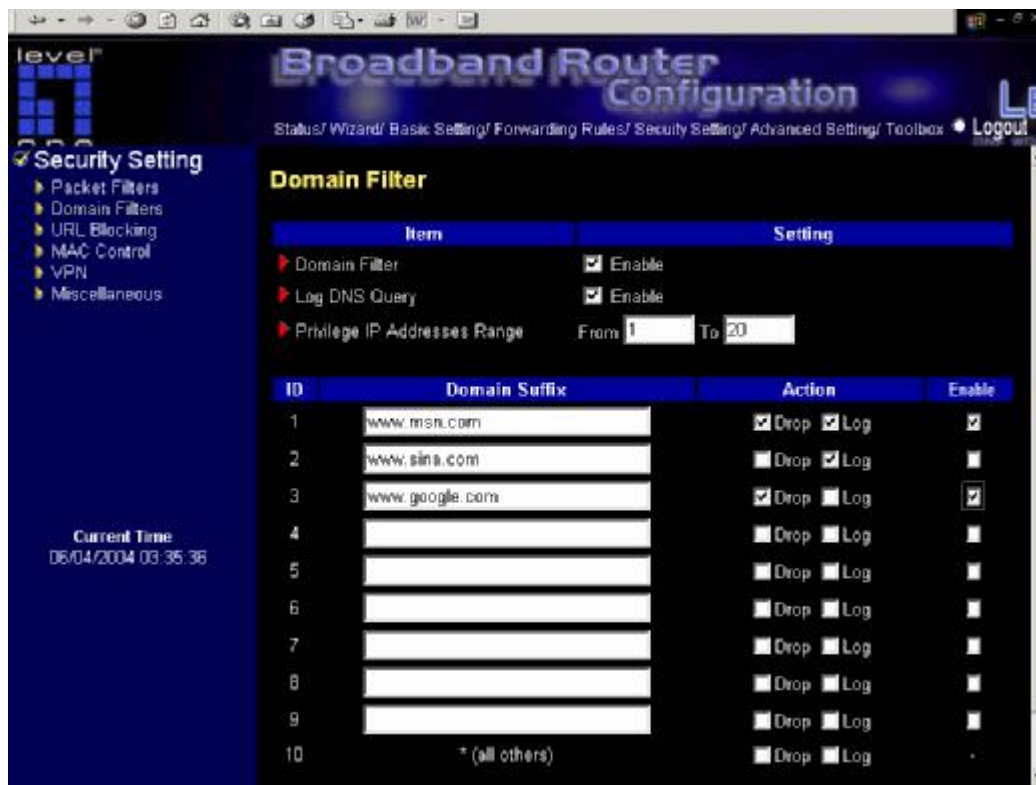
When someone is accessing the URL met the domain-suffix, what kind of action you want.

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

#### Enable

Check to enable each rule.

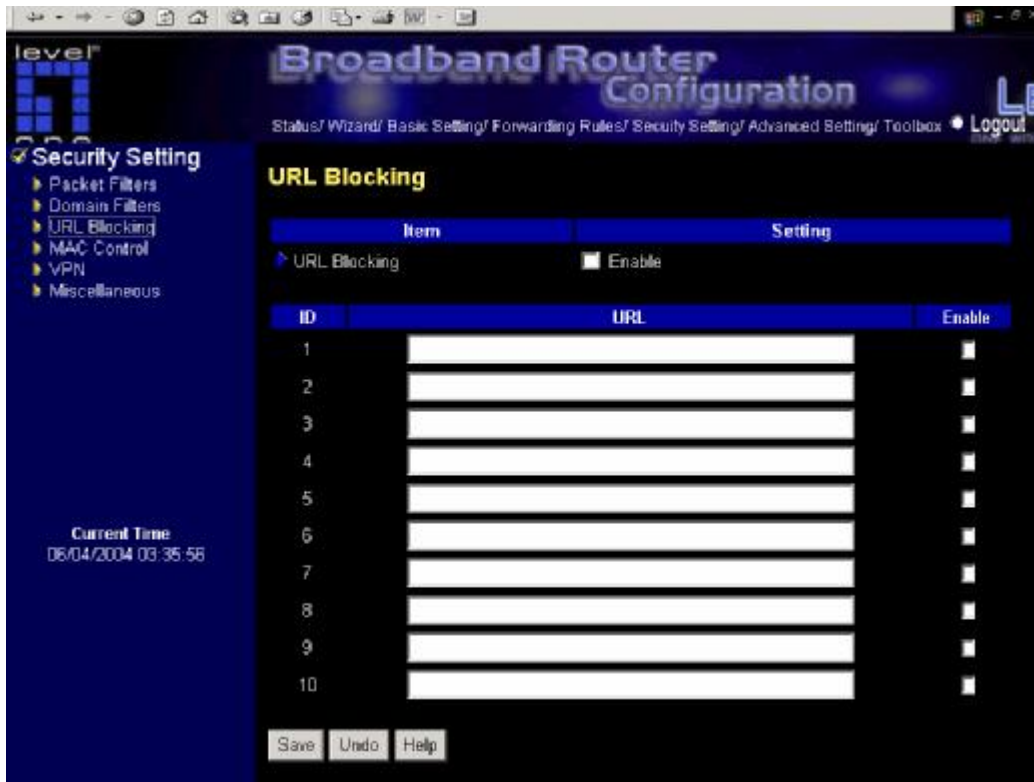
Example:



In this example:

1. URL include “[www.msn.com](http://www.msn.com)” will be blocked, and the action will be record in log-file.
2. URL include “[www.sina.com](http://www.sina.com)” will not be blocked, but the action will be record in log-file.
3. URL include “[www.google.com](http://www.google.com)” will be blocked, but the action will not be record in log-file.
4. IP address X.X.X.1~ X.X.X.20 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 “msn” will be blocked, and the action will be record in log-file.
- 2.URL include “sina” will be blocked, and the action will be record in log-file
- 3.URL include “cnnsi” will be blocked, and the action will be record in log-file.
4. URL include “espn” will be blocked, and the action will be record in log-file

#### 4.6.4 MAC Address Control

The screenshot shows the 'Broadband Router Configuration' interface for a LevelOne router. The 'Security Setting' menu is open, and 'MAC Address Control' is selected. The 'MAC Address Control' section has a checkbox for 'Enable' which is checked. Below it, the 'Connection control' checkbox is also checked, with a dropdown menu set to 'allow'. A table with 4 rows and 4 columns (ID, MAC Address, IP Address, C) is displayed. The 'C' column has checkboxes. Below the table is a 'DHCP clients' dropdown menu set to '-- select one --' and a 'Copy to' dropdown menu set to 'ID'. At the bottom are buttons for '<< Previous', 'Next >>', 'Save', 'Undo', and 'Help'.

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

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

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

-- select one --

Copy to

ID

--

<< Previous

Next >>

Save

Undo

Help

"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 --

Copy to

ID

--

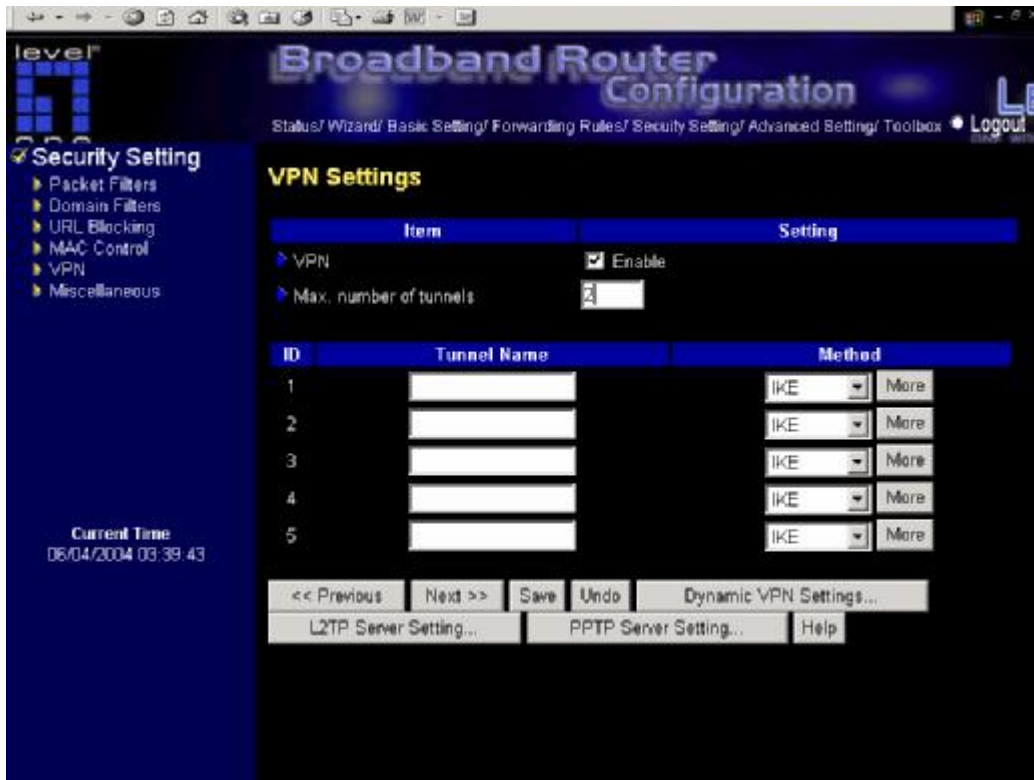
You can select a specific client in the "DHCP clients" Combobox, and then click on the "Copy to" button to copy the MAC address of the client you select to the ID selected in the "ID" Combobox.

### 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.

#### 4.6.5.1 VPN Settings – IPSEC

The screenshot shows the 'Broadband Router Configuration' web interface. The left sidebar has a 'Security Setting' menu with options: Packet Filters, Domain Filters, URL Blocking, MAC Control, VPN, and Miscellaneous. The main content area is titled 'VPN Settings - Tunnel 1 - IKE'. It contains a table with two columns: 'Item' and 'Setting'. The items and their corresponding settings are:

Item	Setting
Tunnel Name	<input type="text"/>
Local Subnet	<input type="text" value="0.0.0.0"/>
Local Netmask	<input type="text" value="0.0.0.0"/>
Remote Subnet	<input type="text" value="0.0.0.0"/>
Remote Netmask	<input type="text" value="0.0.0.0"/>
Remote Gateway	<input type="text"/>
Preshare Key	<input type="text"/>
IKE Proposal index	<input type="button" value="Select IKE Proposal..."/>
IPSec Proposal index	<input type="button" value="Select IPSec Proposal..."/>

At the bottom of the form, there are buttons for 'Save', 'Undo', 'Back', and 'Help', followed by the text 'No change!'. The current time is displayed as '06/04/2004 03:41:00'.

#### 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

The screenshot shows the 'Broadband Router Configuration' interface. The left sidebar has a 'Security Setting' menu with options: Packet Filters, Domain Filters, URL Blocking, MAC Control, VPN, and Miscellaneous. The main content area is titled 'VPN Settings - Tunnel 1 - Set IKE Proposal'. It features a table with columns: ID, Proposal Name, DH Group, Encrypt. algorithm, Auth. algorithm, Life Time, and Life Time Unit. The table contains 10 rows, all with 'Group 1' for DH Group, '3DES' for Encrypt. algorithm, and 'SHA1' for Auth. algorithm. The Life Time is set to '0' and the Life Time Unit is 'Sec'. Above the table, there is an 'IKE Proposal Index' section with a dropdown menu showing '- Empty -' and a 'Remove' button. The top navigation bar includes links for Status, Wizard, Basic Setting, Forwarding Rules, Security Setting, Advanced Setting, and Toolbox, along with a Logout button. The bottom left corner shows the 'Current Time' as 06/04/2004 03:41:57.

ID	Proposal Name	DH Group	Encrypt. algorithm	Auth. algorithm	Life Time	Life Time Unit
1		Group 1	3DES	SHA1	0	Sec
2		Group 1	3DES	SHA1	0	Sec
3		Group 1	3DES	SHA1	0	Sec
4		Group 1	3DES	SHA1	0	Sec
5		Group 1	3DES	SHA1	0	Sec
6		Group 1	3DES	SHA1	0	Sec
7		Group 1	3DES	SHA1	0	Sec
8		Group 1	3DES	SHA1	0	Sec
9		Group 1	3DES	SHA1	0	Sec
10		Group 1	3DES	SHA1	0	Sec

### 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

The screenshot shows the 'VPN Settings - Tunnel 1 - Set IPSec Proposal' configuration page. On the left is a sidebar with 'Security Setting' expanded, showing options like Packet Filters, Domain Filters, URL Blocking, MAC Control, VPN, and Miscellaneous. The main area has a title bar with navigation links (Status/Wizard/Basic Setting/Forwarding Rules/Security Setting/Advanced Setting/Toolbox) and a 'Logout' button. Below the title is a table for the 'IPSec Proposal index' with columns 'Item' and 'Setting'. The 'Item' column contains a dropdown menu currently showing '- Empty -' and a 'Remove' button. Below this is a table of 10 available proposals.

ID	Proposal Name	DH Group	Encap. protocol	Encrypt. algorithm	Auth. algorithm	Life Time	Life Time Unit
1		None	ESP	3DES	None	0	Sec.
2		None	ESP	3DES	None	0	Sec.
3		None	ESP	3DES	None	0	Sec.
4		None	ESP	3DES	None	0	Sec.
5		None	ESP	3DES	None	0	Sec.
6		None	ESP	3DES	None	0	Sec.
7		None	ESP	3DES	None	0	Sec.
8		None	ESP	3DES	None	0	Sec.
9		None	ESP	3DES	None	0	Sec.
10		None	ESP	3DES	None	0	Sec.

Current Time: 06/04/2004 03:42:30

### **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.

#### 4.6.5.2 VPN Settings - Dynamic VPN Tunnel

The screenshot shows the LevelOne Broadband Router Configuration interface. The left sidebar contains a 'Security Setting' menu with options: Packet Filters, Domain Filters, URL Blocking, MAC Control, VPN, and Miscellaneous. The main content area is titled 'VPN Settings - Dynamic VPN Tunnel'. It features a table with two columns: 'Item' and 'Setting'. The table contains the following rows:

Item	Setting
Tunnel Name	<input type="text"/>
Dynamic VPN	<input checked="" type="checkbox"/> Enable
Local Subnet	<input type="text" value="0.0.0.0"/>
Local Netmask	<input type="text" value="0.0.0.0"/>
Preshare Key	<input type="text"/>
IKE Proposal index	Select IKE Proposal...
IPSec Proposal index	Select IPSec Proposal...

Below the table are buttons for 'Save', 'Undo', 'Back', and 'Help'. In the bottom left corner, the 'Current Time' is displayed as '06/04/2004 03:43:07'.

When using **VPN Dynamic IP Setting**, this router is working as a Dynamic VPN server. Dynamic VPN Server will not check VPN client IP information, so user can build VPN tunnel with VPN gateway from any remote host regardless of its IP information.

#### 4.6.5.3 VPN Settings – L2TP Server

The screenshot shows the Level1 Broadband Router Configuration interface. The left sidebar contains a 'Security Setting' menu with options: Packet Filters, Domain Filters, URL Blocking, MAC Control, VPN, and Miscellaneous. The main content area is titled 'VPN Settings - L2TP Server'. It includes a table for configuration settings and a table for tunnel details.

Item	Setting
L2TP Server	<input type="checkbox"/> Enable
Virtual IP of L2TP Server	10 . 0 . 1 . 1
Authentication Protocol	<input checked="" type="radio"/> PAP <input type="radio"/> CHAP <input type="radio"/> MSCHAP

ID	Tunnel Name	User Name	Password
1			
2			
3			
4			
5			

Buttons: Save, Undo, Back, Help

Current Time: 06/04/2004 09:43:41

**L2TP** (Layer2 Tunneling protocol) combine features of both Point-to-Point Tunneling Protocol (PPTP) and Layer 2 Forwarding (L2F) technology. L2TP provides security for a virtual private network (VPN) connection from the remote user to the corporate LAN.

User can build up to five L2TP tunnels for L2TP clients. Each tunnel can accept more than one client. User is required to configure Virtual IP of L2TP Server, Authentication Protocol, L2TP Tunnel Name and User Account, Password.

**Virtual IP of L2TP Server:** L2TP server's virtual IP. User must assign a virtual IP for L2TP Server.

**Authentication Protocol:** Protocols that Clients can use to authenticate to Server.

**L2TP Tunnel, Username and Password:** Each tunnel defined a username and password that clients can use to connect to L2TP Server.



#### 4.6.5.4 VPN Settings – PPTP Server

PPTP (Point-to-Point Tunneling Protocol) is a tunneling

The screenshot shows the 'level1 Broadband Router Configuration' web interface. The left sidebar has a 'Security Setting' menu with options: Packet Filters, Domain Filters, URL Blocking, MAC Control, VPN, and Miscellaneous. The main content area is titled 'VPN Settings - PPTP Server'. It contains a table with two columns: 'Item' and 'Setting'. The 'PPTP Server' item has an 'Enable' checkbox. The 'Virtual IP of PPTP Server' item has four input fields with values 10, 0, 0, and 1. The 'Authentication Protocol' item has three radio buttons: PAP (selected), CHAP, and MSCHAP. Below this is a table with four columns: ID, Tunnel Name, User Name, and Password. There are five rows for ID 1 through 5, each with empty input fields. At the bottom are buttons for Save, Undo, Back, and Help. A 'Current Time' display shows '06/04/2004 03:44:00'.

Item	Setting
PPTP Server	<input type="checkbox"/> Enable
Virtual IP of PPTP Server	10 0 0 1
Authentication Protocol	<input checked="" type="radio"/> PAP <input type="radio"/> CHAP <input type="radio"/> MSCHAP

ID	Tunnel Name	User Name	Password
1			
2			
3			
4			
5			

Save Undo Back Help

Current Time: 06/04/2004 03:44:00

protocol for connecting clients and servers. PPTP can be used to create a Virtual Private Network (VPN) between the remote user and the corporate LAN.

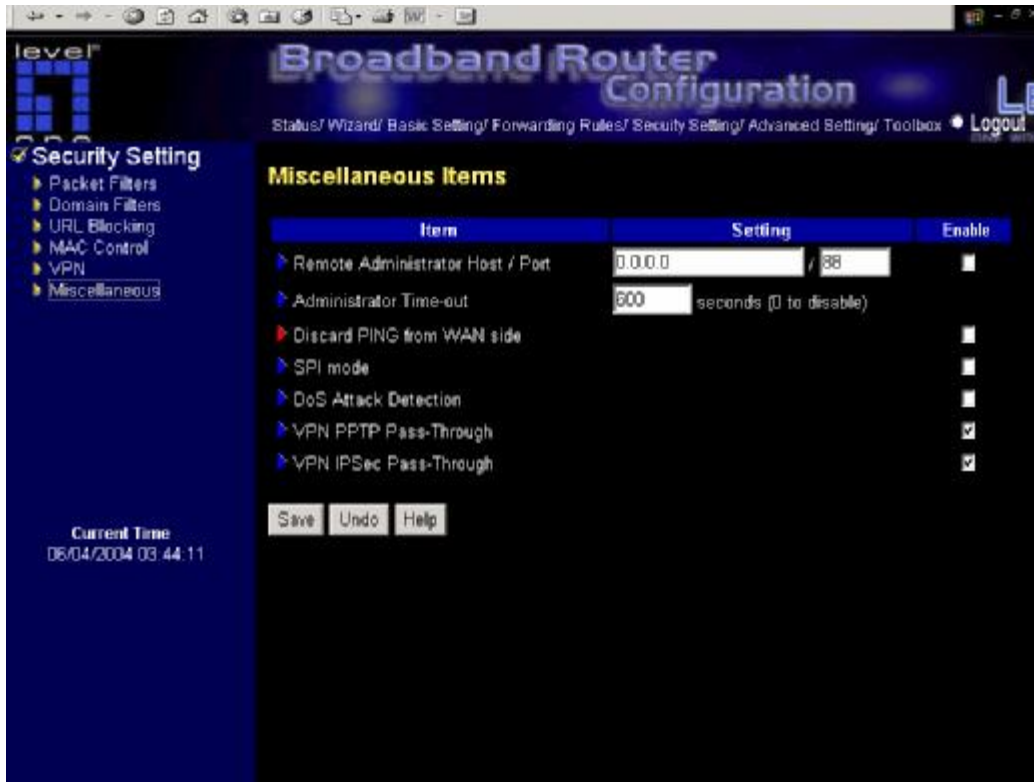
User can build up to five PPTP tunnels for PPTP clients. Each tunnel can accept more than one client. User is required to configure Virtual IP of PPTP Server, Authentication Protocol, PPTP Tunnel Name and User Account, Password.

**Virtual IP of PPTP Server:** PPTP server's virtual IP. User must assign a virtual IP for PPTP Server.

**Authentication Protocol:** Protocols that Clients can use to authenticate to Server.

**PPTP Tunnel Name, Username and Password:** Each tunnel defined a username and password that clients can use to connect to PPTP Server.

#### 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**

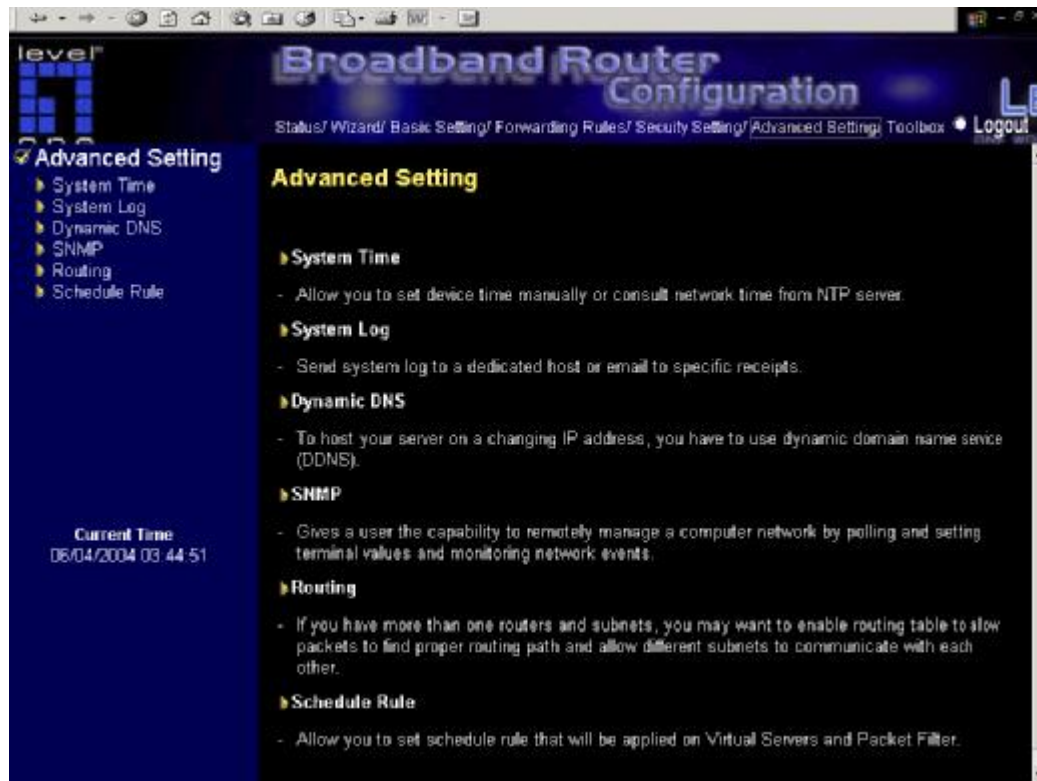
When this feature is enabled, the router will detect and log the DoS attack comes from the Internet.

Currently, the router can detect the following DoS attack: SYN Attack, WinNuke, Port Scan, Ping of Death, Land Attack etc.

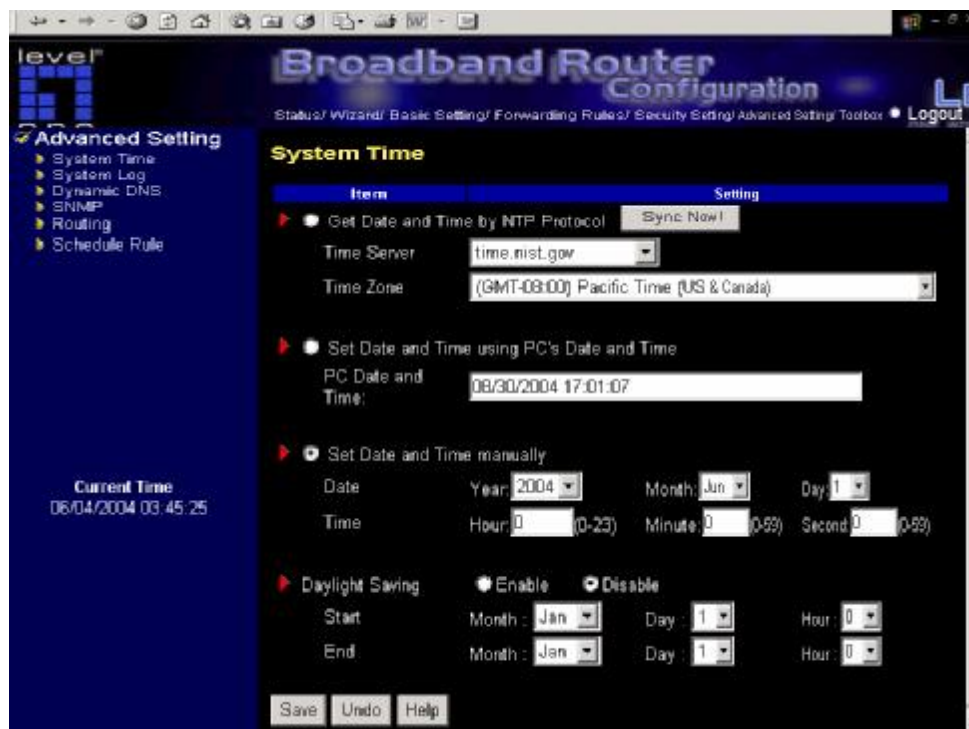
#### **VPN PPTP/IPSec Pass-Through**

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

Item	Setting	Enable
IP Address of Syslog Server	192.168.123.	<input type="checkbox"/>
E-mail Alert	<input type="button" value="Send Mail Now"/>	<input type="checkbox"/>
SMTP Server IP/Port	<input type="text"/>	
E-mail addresses	<input type="text"/>	
E-mail Subject	<input type="text"/>	

View Log... Save Undo Help

Current Time: 06/04/2004 03:45:49

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".

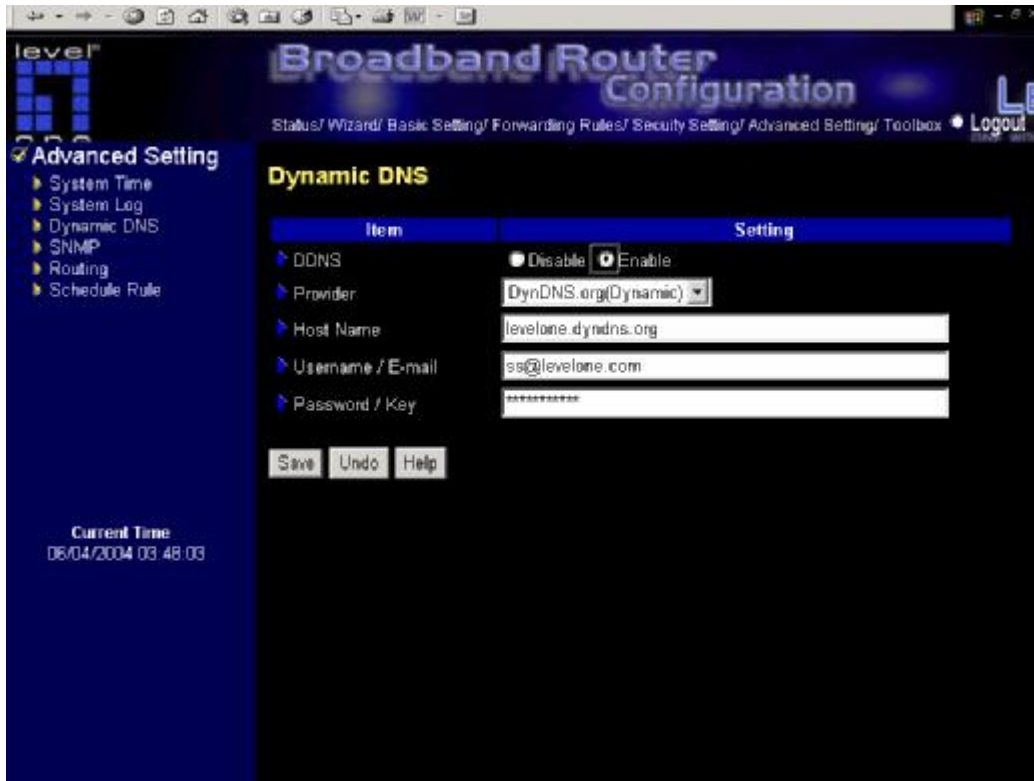
### E-mail addresses

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:**

The screenshot shows the 'level1 Broadband Router Configuration' web interface. The left sidebar lists navigation options: 'Advanced Setting' (selected), 'System Time', 'System Log', 'Dynamic DNS', 'SNMP', 'Routing', and 'Schedule Rule'. The main content area is titled 'Dynamic DNS' and contains a table with two columns: 'Item' and 'Setting'.

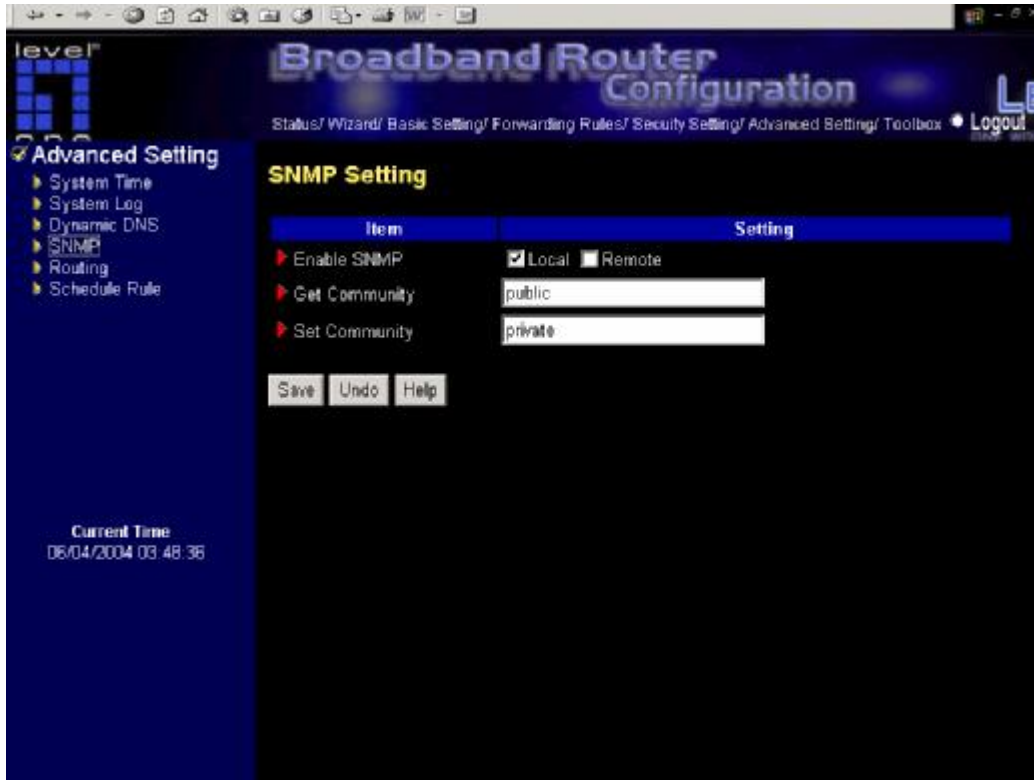
Item	Setting
DDNS	<input type="radio"/> Disable <input checked="" type="radio"/> Enable
Provider	DynDNS.org(Dynamic)
Host Name	levelone.dyndns.org
Username / E-mail	ss@levelone.com
Password / Key	*****

Below the table are three buttons: 'Save', 'Undo', and 'Help'. At the bottom left of the interface, the 'Current Time' is displayed as '06/04/2004 03:47:53'. The top navigation bar includes links for 'Status', 'Wizard', 'Basic Setting', 'Forwarding Rules', 'Security Setting', 'Advanced Setting', 'Toolbox', and a 'Logout' button.

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"

## 4.7.5 Routing Table

The screenshot shows the 'Broadband Router Configuration' interface. On the left is a sidebar with 'Advanced Setting' expanded, showing options like System Time, System Log, Dynamic DNS, SNMP, Routing, and Schedule Rule. The main area is titled 'Routing Table'. It has a sub-header with 'Item' and 'Setting'. Under 'Item', there are radio buttons for 'RIP' (selected), 'Static Routing', 'Disable', 'RIPv1', and 'RIPv2'. Below this is a table with 8 rows and 6 columns: ID, Destination, Subnet Mask, Gateway, Hop, and Enable. The table is currently empty. At the bottom of the table are buttons for 'Save', 'Undo', and 'Help'. The current time is displayed as 06/04/2004 03:58:44.

ID	Destination	Subnet Mask	Gateway	Hop	Enable
1					<input type="checkbox"/>
2					<input 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"/>

**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.

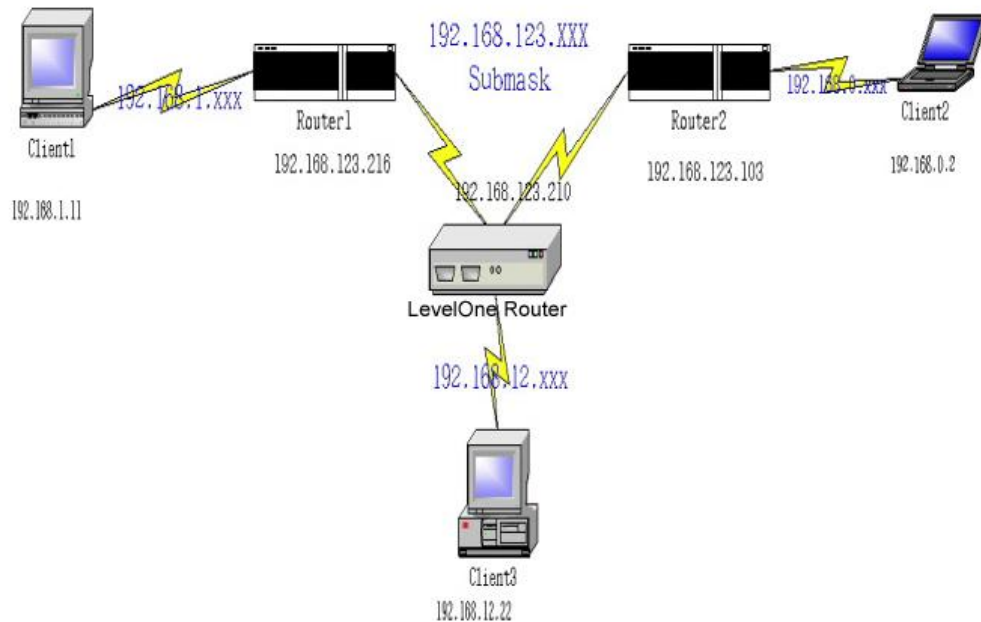
### Dynamic Routing

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	✓
192.168.0.0	255.255.255.0	192.168.123.103	1	✓

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

**level1 Broadband Router Configuration**

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

**Advanced Setting**

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

**Schedule Rule Setting**

Name of Rule 1: ftp time

Week Day	Start Time (hh:mm)		End Time (hh:mm)	
Sunday				
Monday				
Tuesday				
Wednesday				
Thursday				
Friday				
Saturday				
Every Day	14	10	16	20

Current Time: 06/04/2004 03:45:16

Save Undo Help back

After configure Rule 1à



#### Schedule Enable

Selected if you want to Enable the Scheduler.

#### Edit

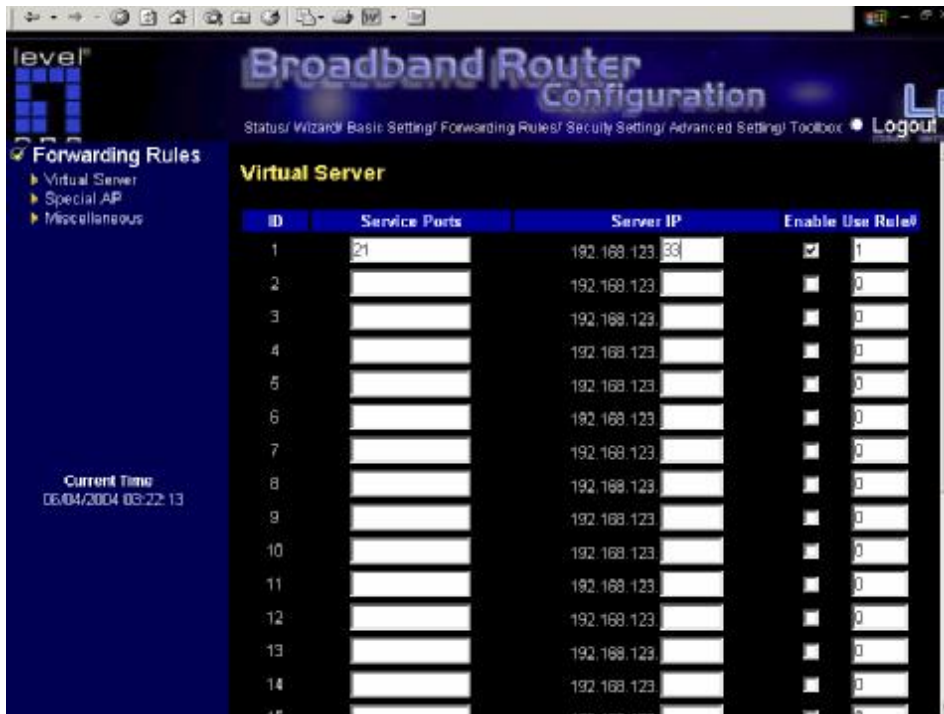
To edit the schedule rule.

#### Delete

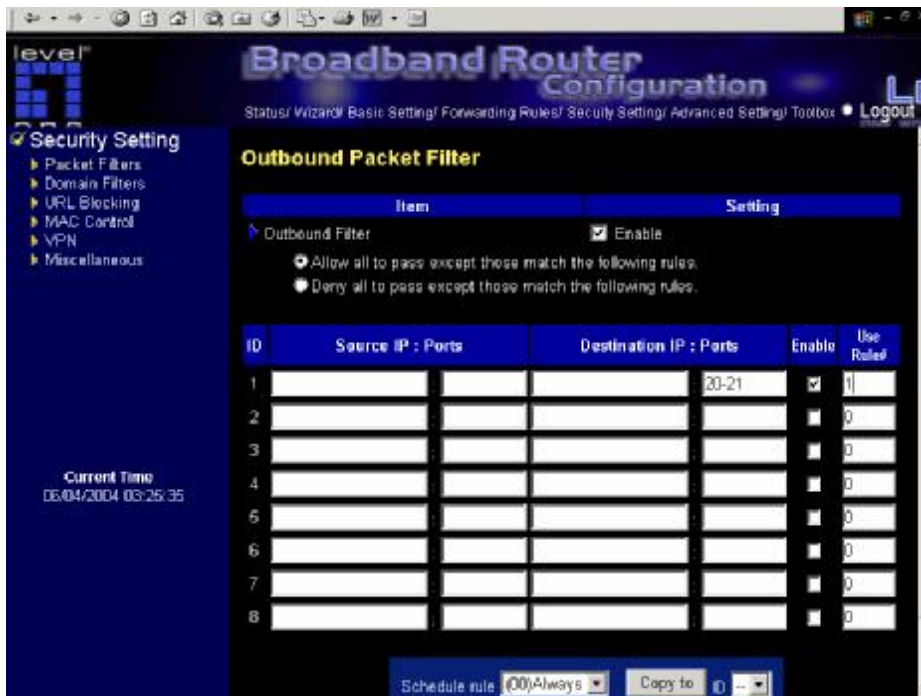
To delete the schedule rule, and the rule# of the rules behind the deleted one will decrease one automatically.

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

Example1: **Virtual Server** – Apply Rule#1 (ftp time: everyday 14:10 to 16:20)

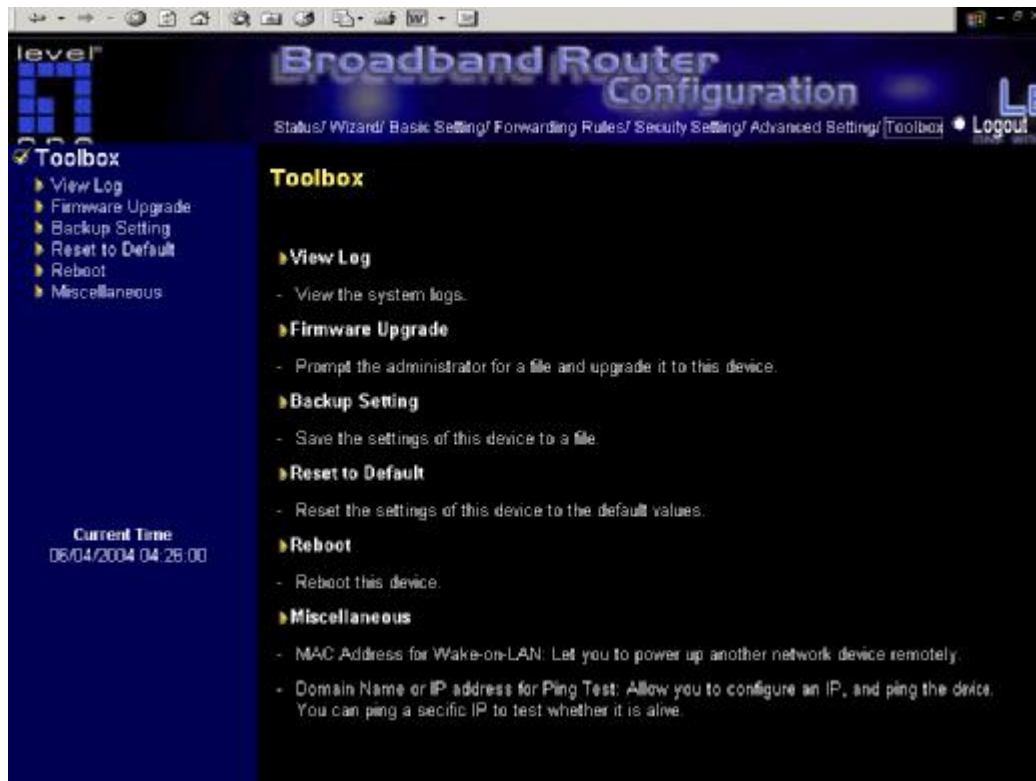


Example2: **Packet Filter** – Apply Rule#1 (ftp time: everyday 14:10 to 16:20).





## 4.8 Toolbox

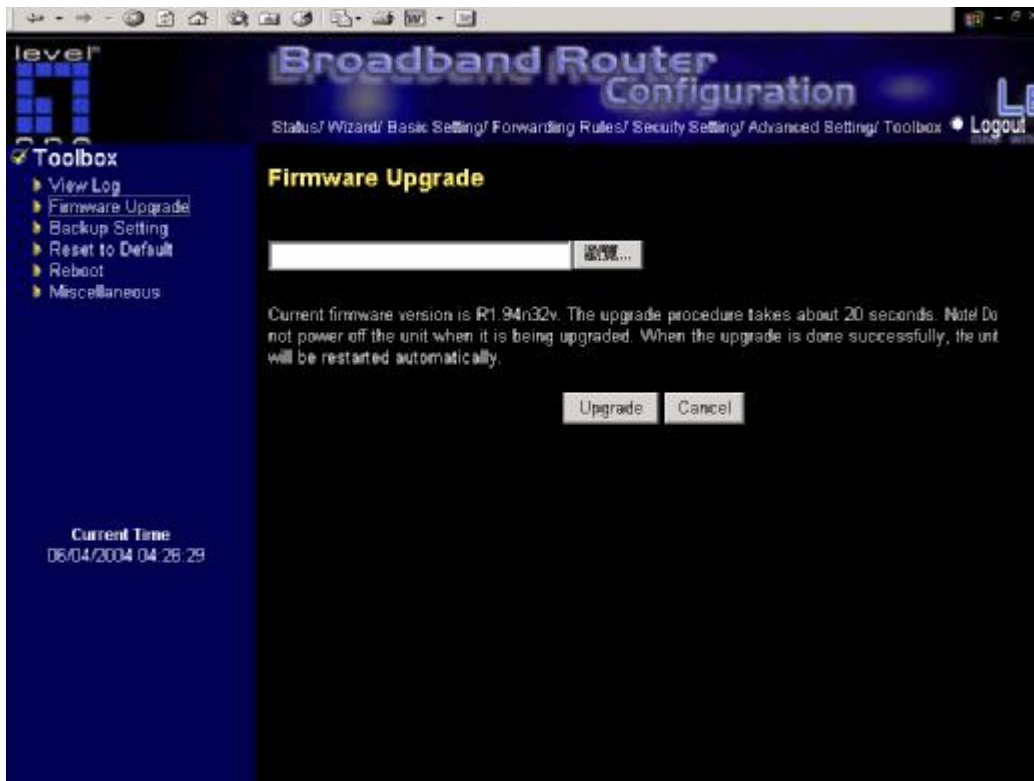


#### 4.8.1 System Log



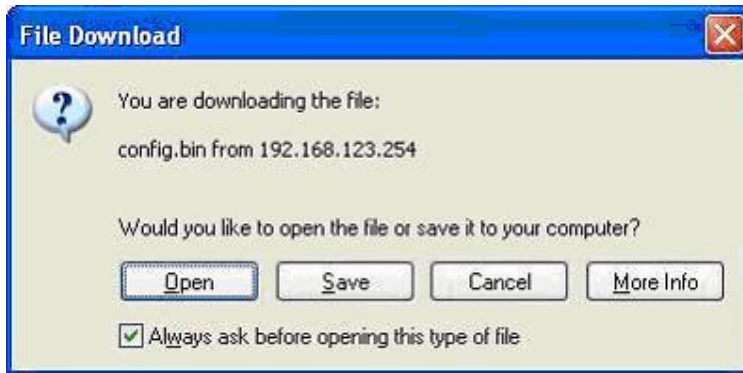
You can View system log by clicking the **View Log** button

## 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



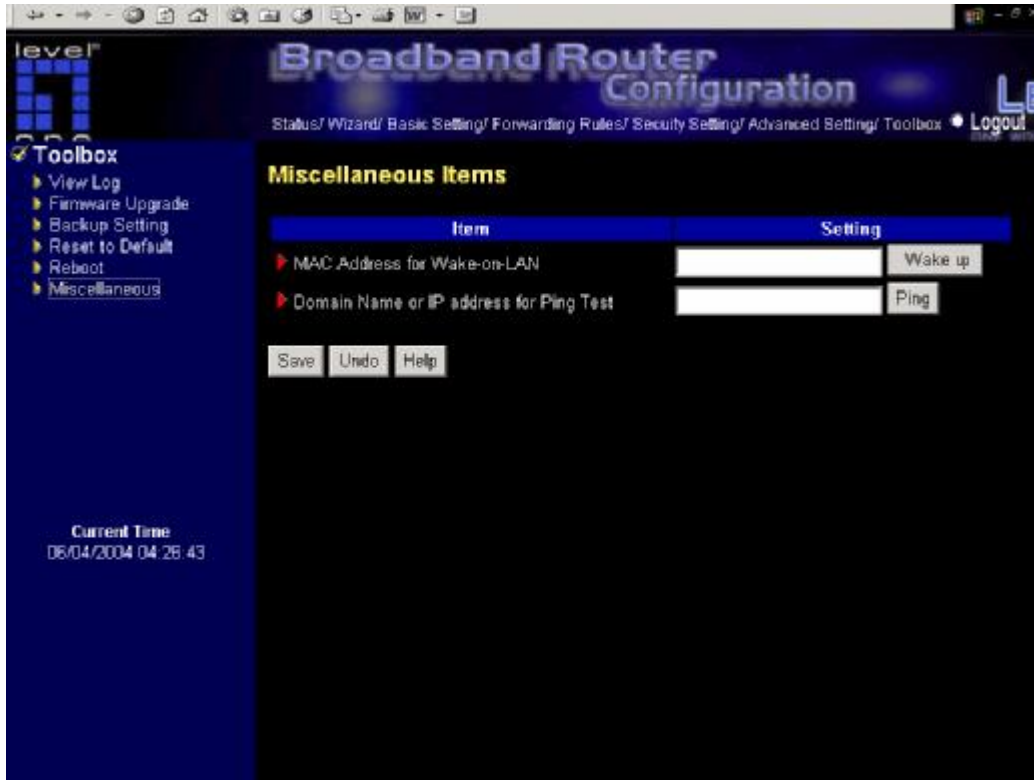
You can also reset this product to factory default by clicking the **Reset to default** button.

#### 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

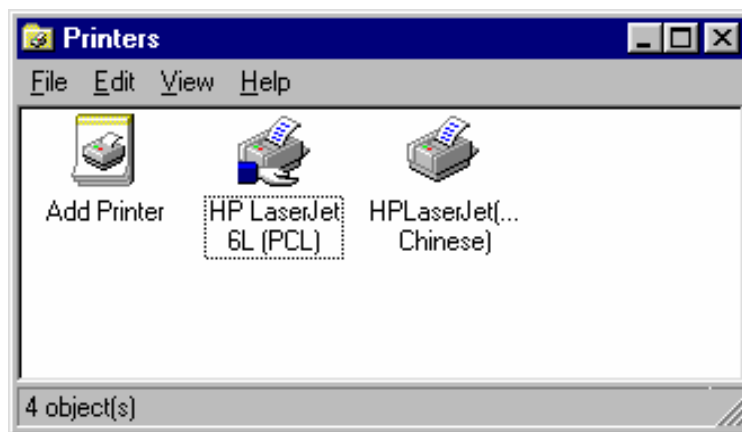
Allow you to configure an IP, and ping the device. You can ping a specific IP to test whether it is alive.

## Chapter 5 Print 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.)

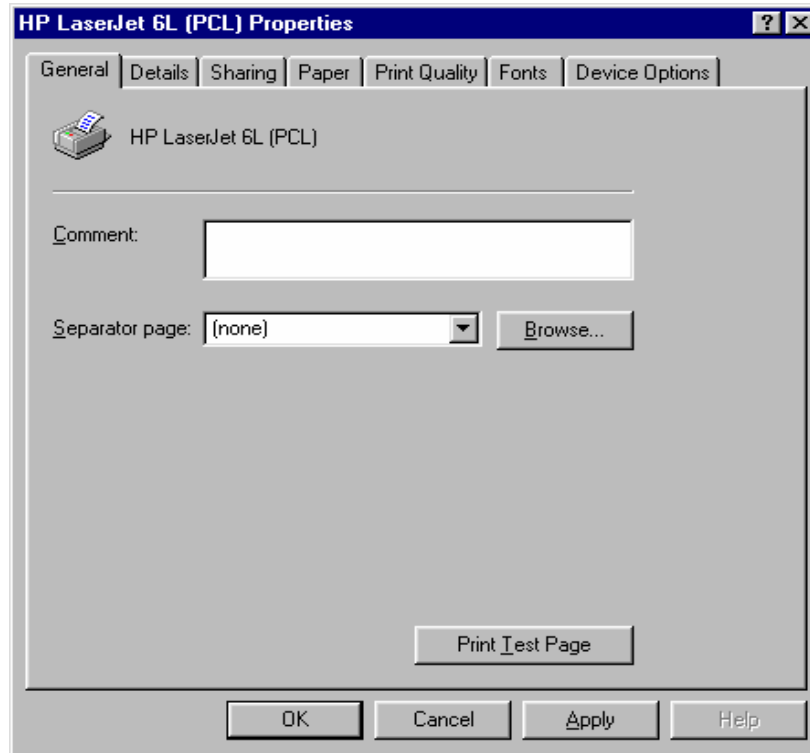
### 5.1 Configuring on Windows 95/98 Platforms

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:

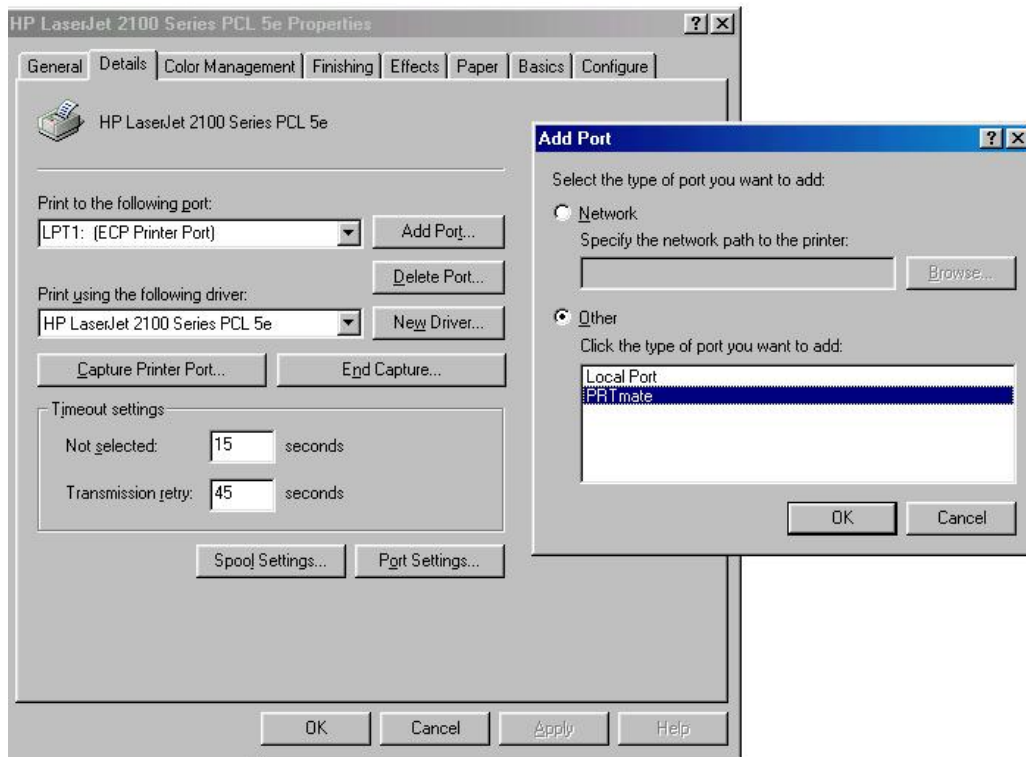


Now, you can configure the print server of this product:

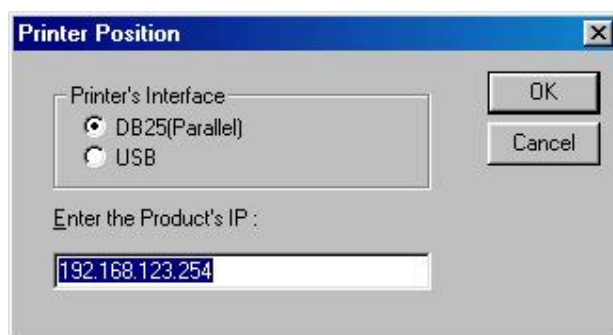
1. Find out the corresponding icon of your server printer, for example, the **HP LaserJet 6L**. Click the mouse's right button on that icon, and then select the **Properties** item:



2. Click the **Details** item:



3. Choose the "PRTmate: (All-in-1)" from the list attached at the **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 **Port Settings**:



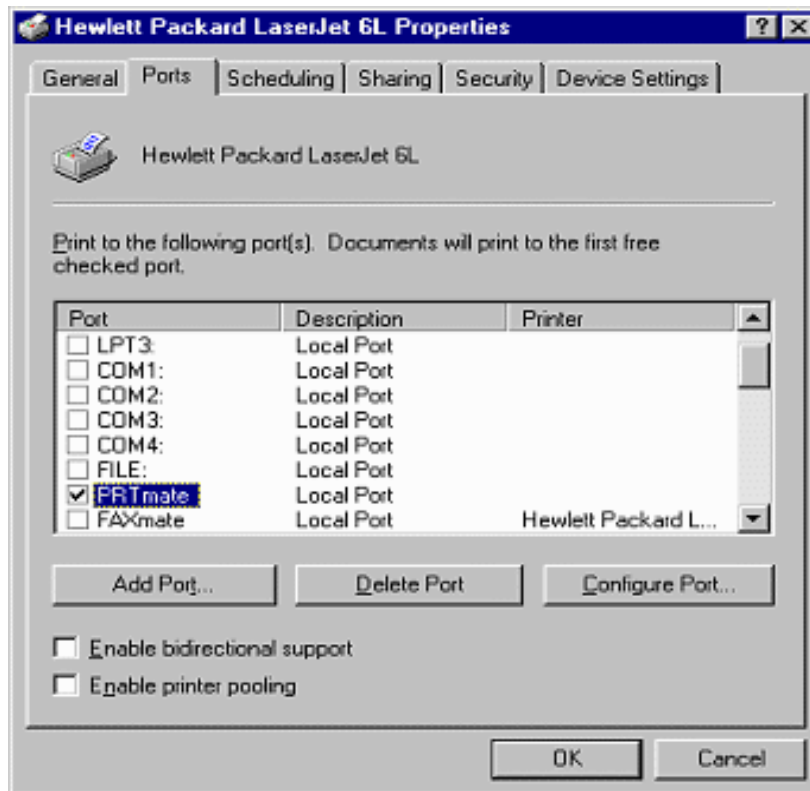
Type in the IP address of this product and then click the **OK** button.

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**:



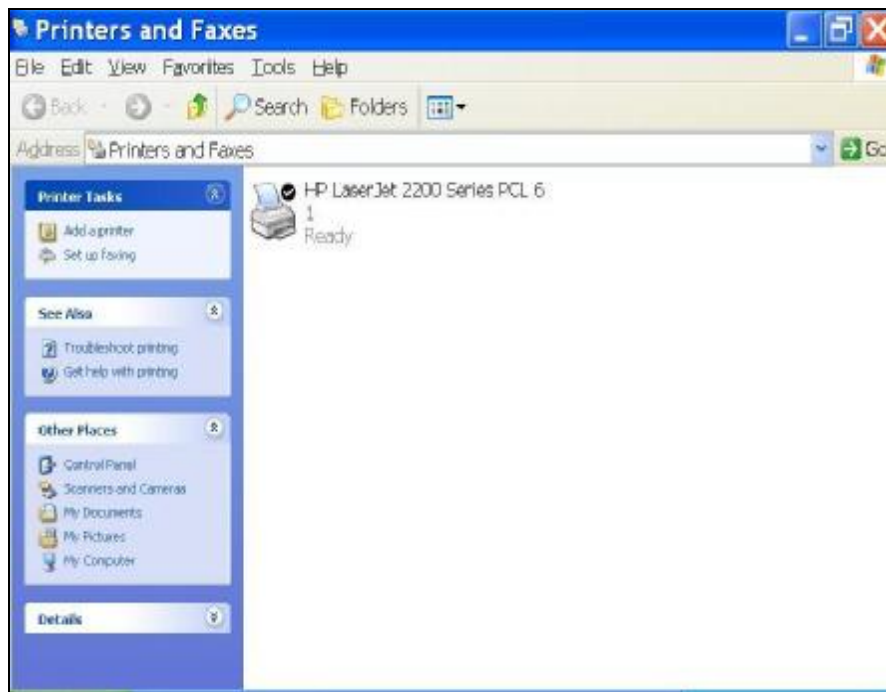
Compared to the procedure in last section, the selection of **Details** is equivalent to the selection of **Ports**, and **Port Settings** is equivalent to **Configure Port**.

### 5.3 Configuring on Windows 2000 and XP Platforms

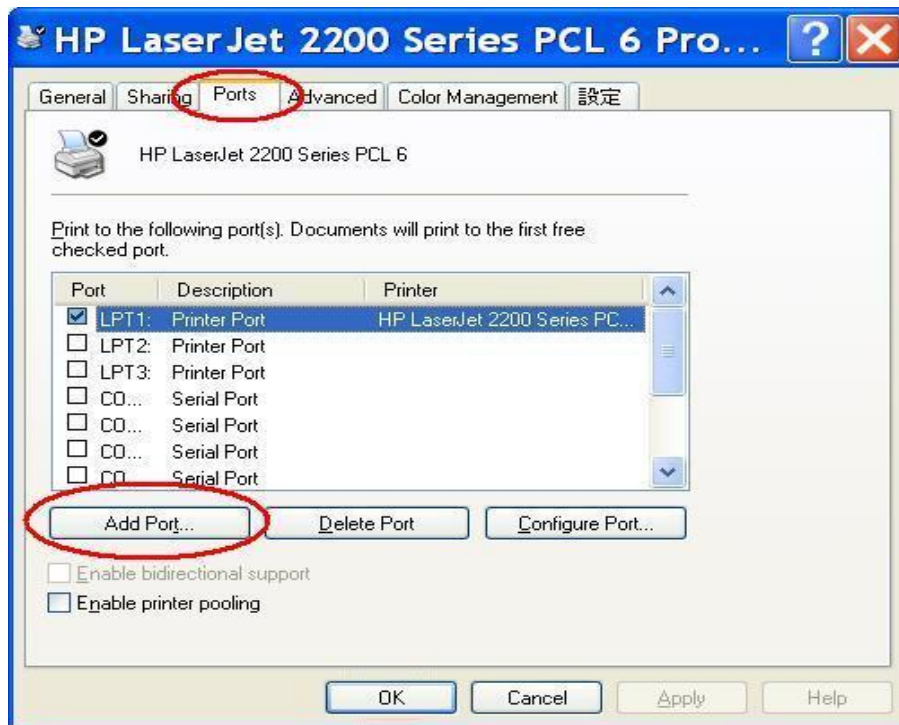
Windows 2000 and XP have built-in LPR client, users could utilize this feature to Print.

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

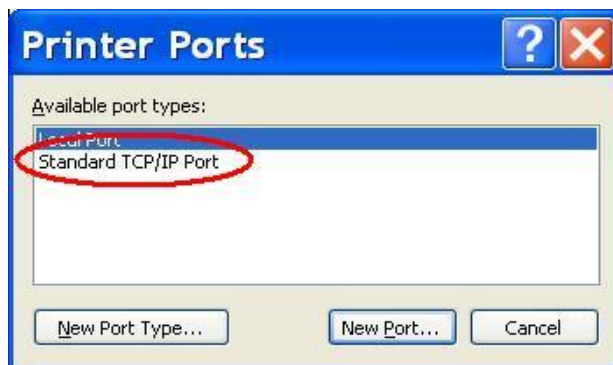
1.Open Printers and Faxes.



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

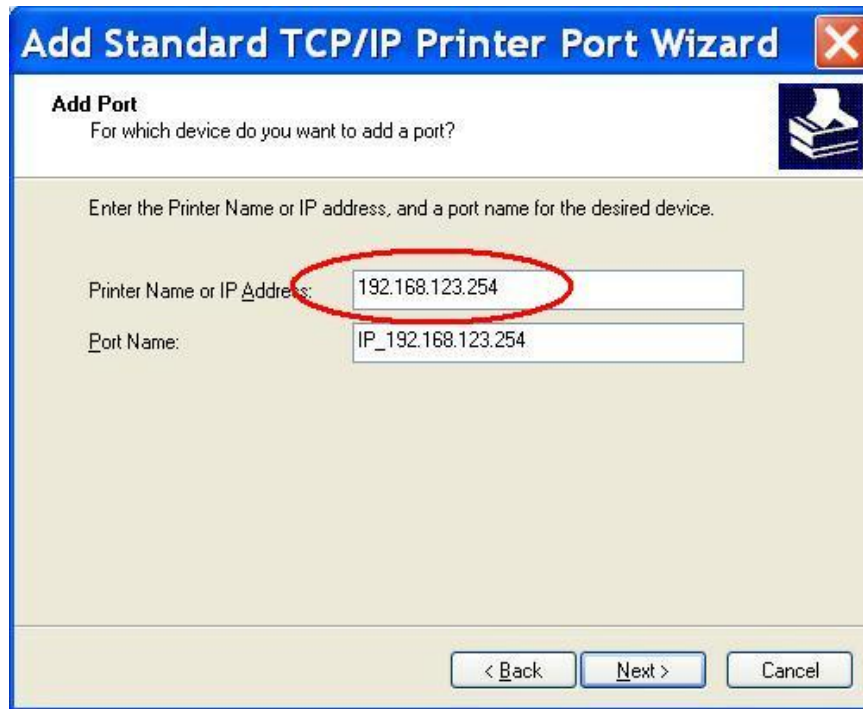


3. Select “Standard TCP/IP Port”, and then click “New Port...”



4. Click Next and then provide the following information:

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



The screenshot shows the 'Add Standard TCP/IP Printer Port Wizard' dialog box, specifically the 'Add Port' step. The title bar reads 'Add Standard TCP/IP Printer Port Wizard' with a red 'X' icon. The main heading is 'Add Port' with a subtext 'For which device do you want to add a port?'. Below this, it says 'Enter the Printer Name or IP address, and a port name for the desired device.' There are two input fields: 'Printer Name or IP Address:' containing '192.168.123.254' and 'Port Name:' containing 'IP\_192.168.123.254'. The IP address field is circled in red. At the bottom, there are three buttons: '< Back', 'Next >', and 'Cancel'.

3. Select Custom, then click "Settings..."



The screenshot shows the 'Add Standard TCP/IP Printer Port Wizard' dialog box, specifically the 'Additional Port Information Required' step. The title bar reads 'Add Standard TCP/IP Printer Port Wizard' with a red 'X' icon. The main heading is 'Additional Port Information Required' with a subtext 'The device could not be identified.' Below this, it says 'The device is not found on the network. Be sure that:' followed by a list of four items: 1. The device is turned on. 2. The network is connected. 3. The device is properly configured. 4. The address on the previous page is correct. It then says 'If you think the address is not correct, click Back to return to the previous page. Then correct the address and perform another search on the network. If you are sure the address is correct, select the device type below.' There are two radio buttons: 'Standard' (selected) and 'Custom' (selected). The 'Custom' radio button is circled in red. Next to the 'Custom' radio button is a button labeled 'Settings...'. At the bottom, there are three buttons: '< Back', 'Next >', and 'Cancel'.

6. Select "LPR", type "lp" lowercase letter in "Queue Name:"

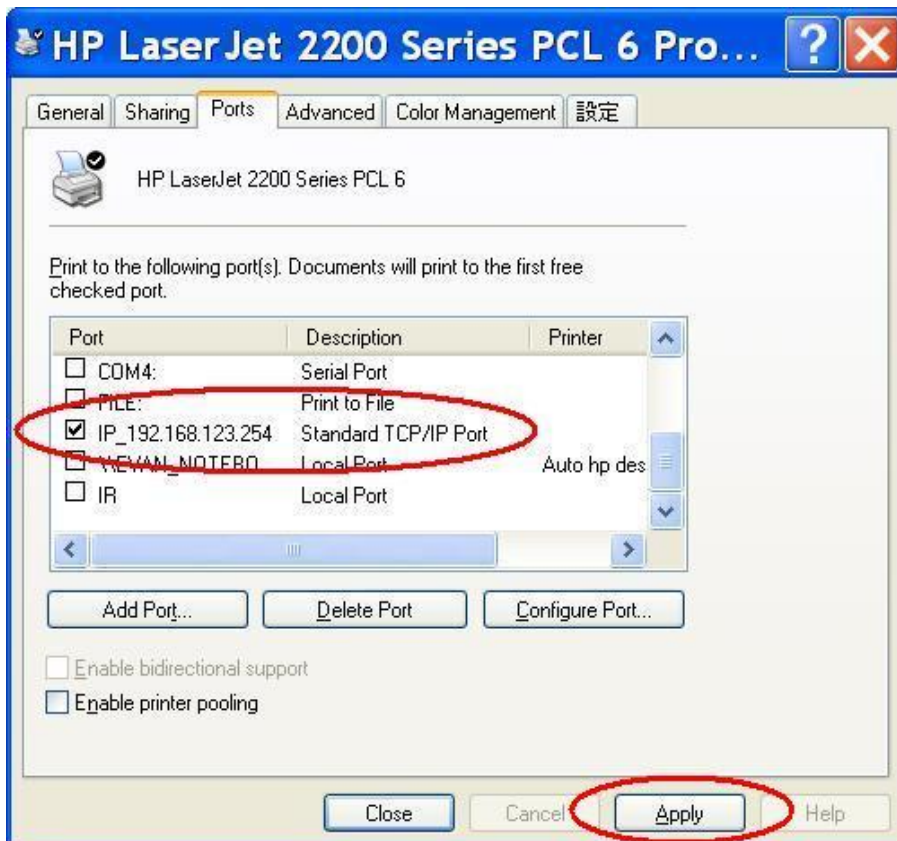
And enable "LPR Byte Counting Enabled".

The screenshot 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. The "SNMP Status Enabled" checkbox is unchecked. The "Community Name" is "public" and the "SNMP Device Index" is "1". At the bottom are "OK" and "Cancel" buttons.

Port Settings	
Port Name:	IP_192.168.123.254
Printer Name or IP Address:	192.168.123.254
Protocol	
<input type="radio"/> Raw	<input checked="" type="radio"/> LPR
Raw Settings	
Port Number:	9100
LPR Settings	
Queue Name:	lp
<input checked="" type="checkbox"/> LPR Byte Counting Enabled	
<input type="checkbox"/> SNMP Status Enabled	
Community Name:	public
SNMP Device Index:	1

OK Cancel

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

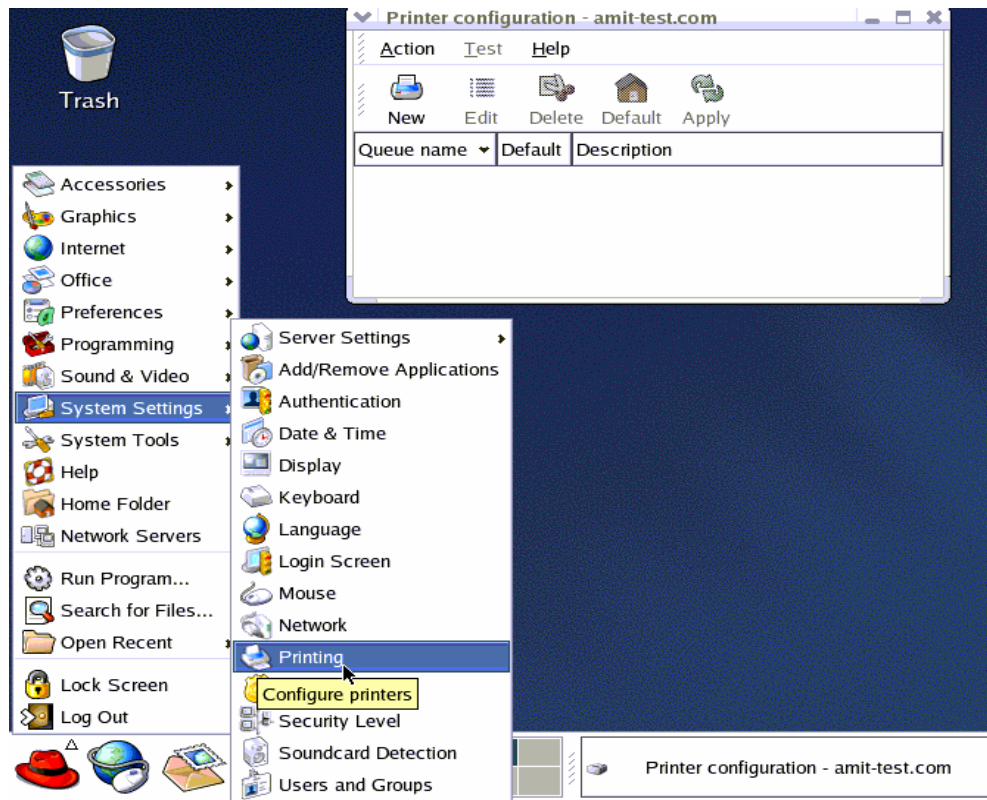
### 2.Use USB to print

Queue Name: lpUSB0

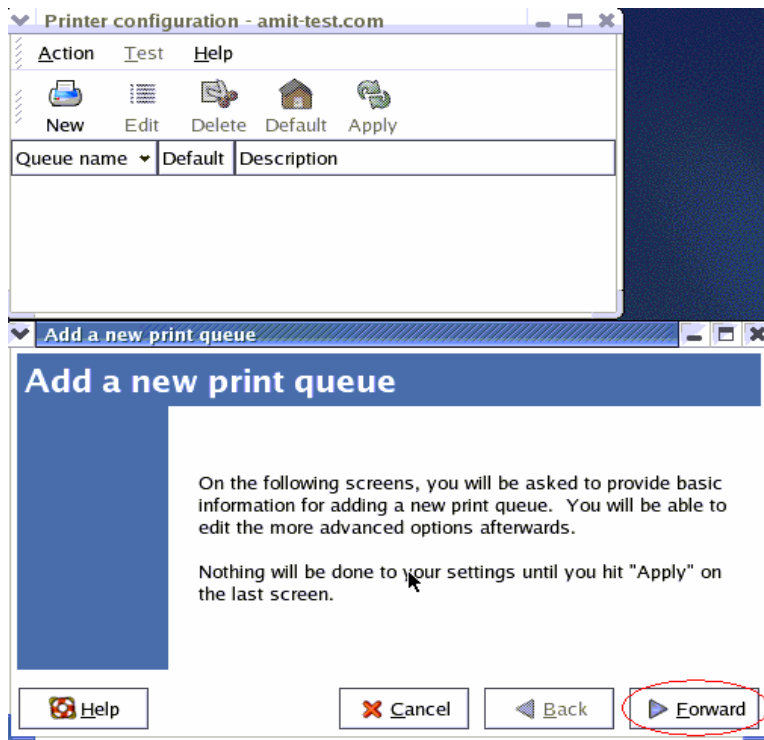
In X-Windows, for example, In Redhat Platforms,

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.

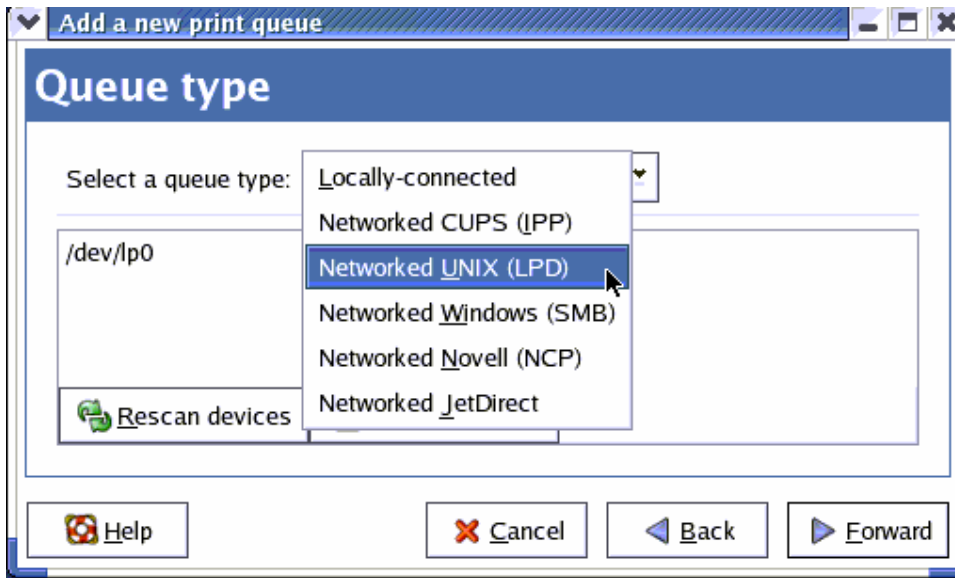


1. Enter the Pinter Name, Comments then forward.

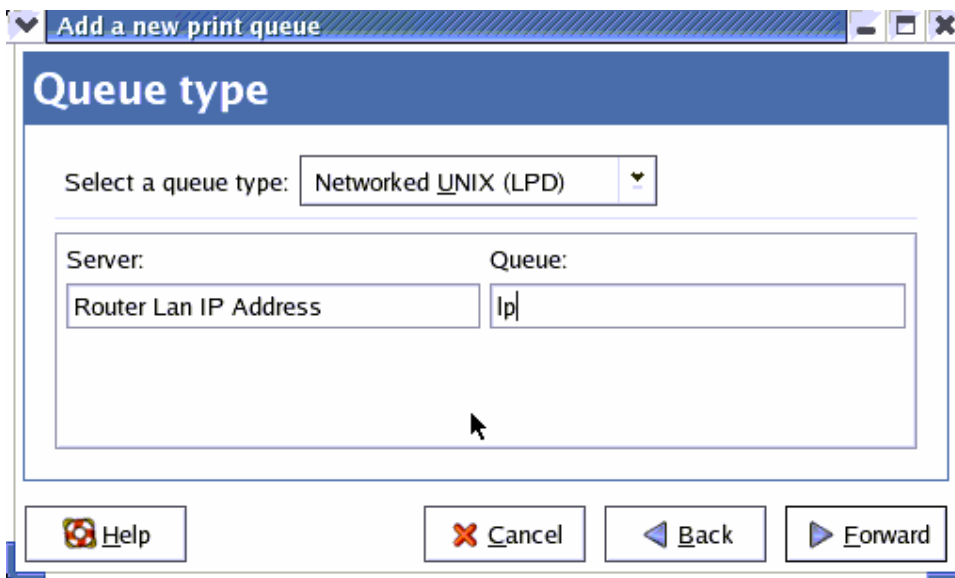
The image shows the 'Add a new print queue' dialog box at the 'Queue name' step. The dialog has a title bar 'Add a new print queue' and a blue header 'Queue name'. The main content area contains the text: 'Please enter a name for this queue. Choose a short name that begins with a letter and contains no spaces.' Below this is a text input field labeled 'Name:' containing the text 'printertest'. Further down, it says 'About' and 'If you like, you can enter a description of the printer to help you identify it more easily.' Below this is a text input field labeled 'Short description:' containing the text 'test'. At the bottom of the dialog are four buttons: 'Help' (with a question mark icon), 'Cancel' (with a red X icon), 'Back' (with a left arrow icon), and 'Forward' (with a right arrow icon).

4. Select LPD protocol and then forward.

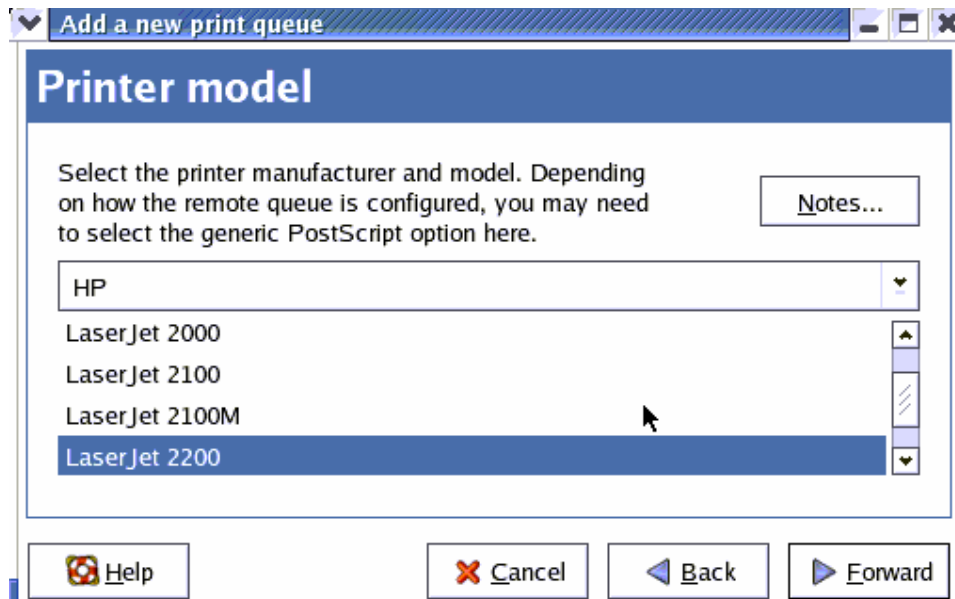




5. Enter Router LAN IP Address and the queue name "lp". Then forward.



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

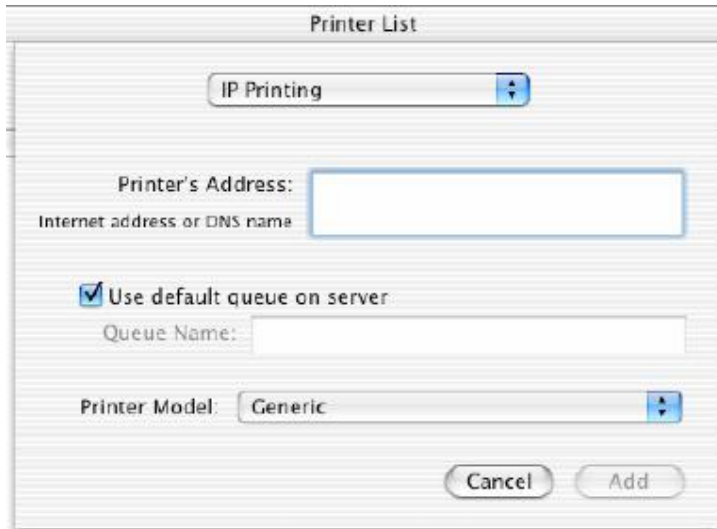
```
#mkdir /var/spool/lpd/lp
```

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

```
#man printcap
```

## 5.5 Configuring on Apple PC

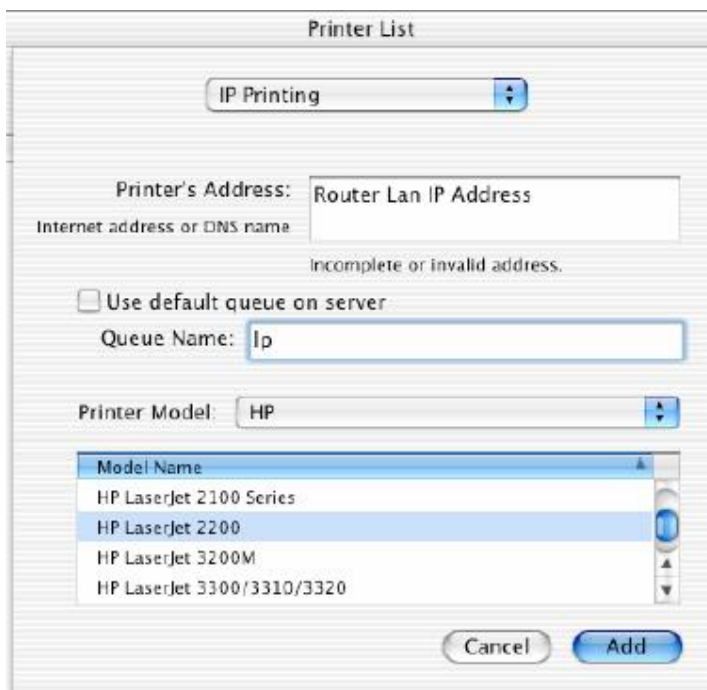
1.First, go to Printer center (Printer list) and add printer



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

3.Disable “[Default Queue of Server.](#)” And fill in ‘[Ip](#)’ 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**

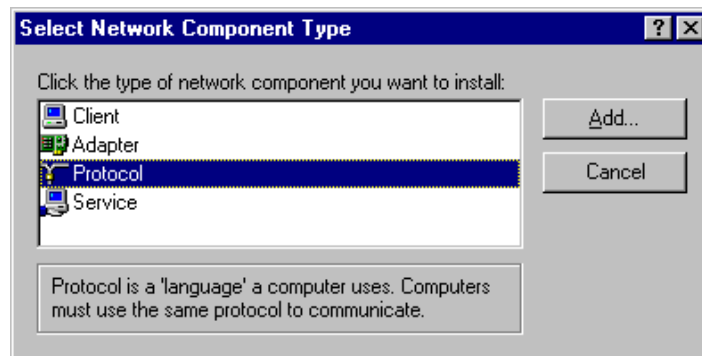
**Queue Name: lpUSB0**

## Appendix A TCP/IP Configuration for Windows 95/98

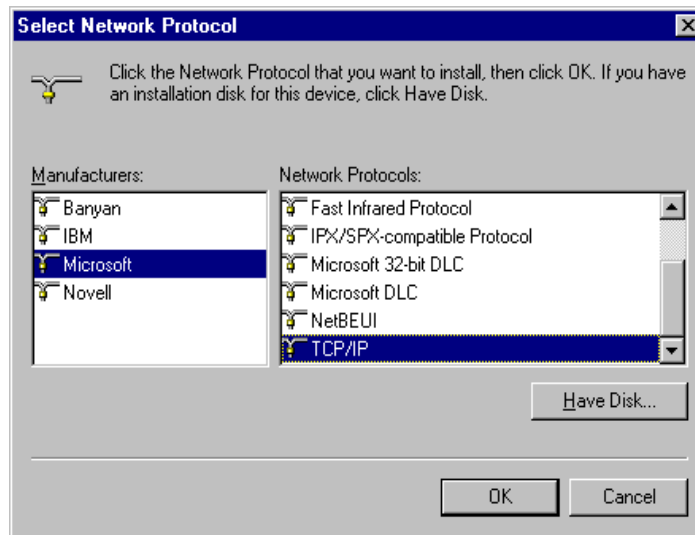
This section introduces you how to install TCP/IP protocol into your personal computer. And suppose you have been successfully installed one network card on your personal computer. If not, please refer to your network card manual. Moreover, the Section B.2 tells you how to set TCP/IP values for working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



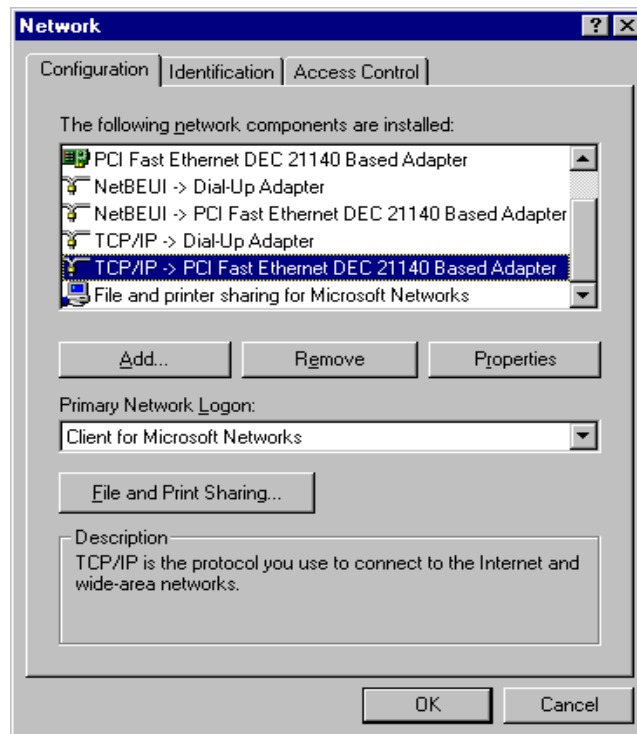
5. Select **Microsoft** item in the manufactures list. And choose **TCP/IP** in the Network Protocols.  
Click **OK** button to return to Network window.



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:



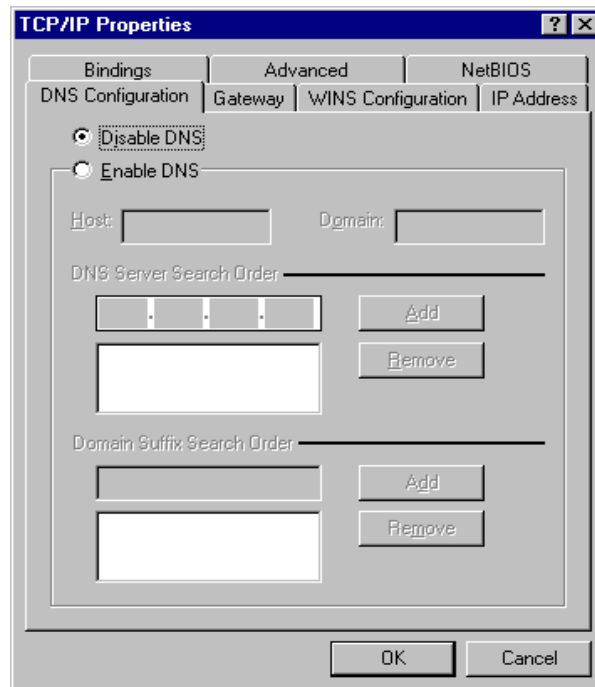
- a. Select **Obtain an IP address automatically** in the IP Address tab.

The screenshot shows the 'TCP/IP Properties' dialog box with the 'IP Address' tab selected. The dialog has a title bar with a question mark and a close button. Below the title bar are four tabs: 'Bindings', 'Advanced', 'NetBIOS', and 'IP Address'. The 'IP Address' tab is active, showing a text area with instructions: 'An IP address can be automatically assigned to this computer. If your network does not automatically assign IP addresses, ask your network administrator for an address, and then type it in the space below.' Below this text are two radio buttons. The first radio button, labeled 'Obtain an IP address automatically', is selected. The second radio button, labeled 'Specify an IP address:', is unselected. Below the second radio button is a group box containing two input fields: 'IP Address:' and 'Subnet Mask:'. Each input field is a four-part dotted box. At the bottom of the dialog are 'OK' and 'Cancel' buttons.

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

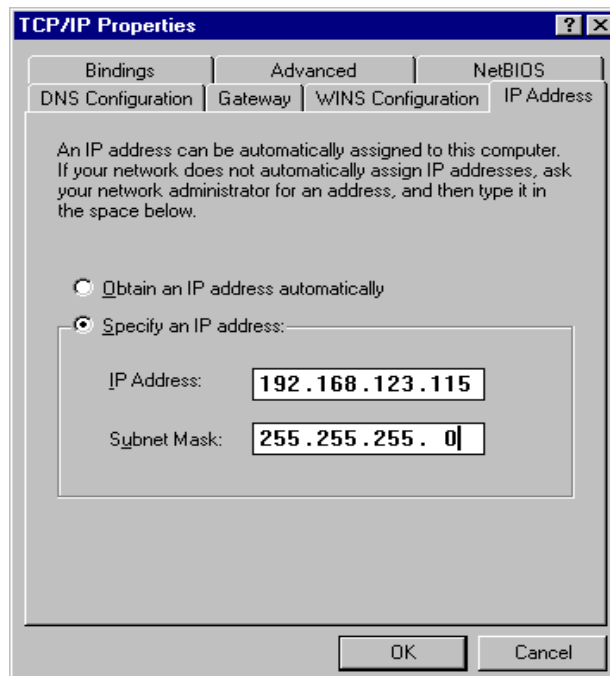
The screenshot shows the 'TCP/IP Properties' dialog box with the 'Gateway' tab selected. The dialog has a title bar with a question mark and a close button. Below the title bar are four tabs: 'Bindings', 'Advanced', 'NetBIOS', and 'Gateway'. The 'Gateway' tab is active, showing a text area with instructions: 'The first gateway in the Installed Gateway list will be the default. The address order in the list will be the order in which these machines are used.' Below this text is a section labeled 'New gateway:' with a four-part dotted input field and an 'Add' button. Below this is a section labeled 'Installed gateways:' with an empty list box and a 'Remove' button. At the bottom of the dialog are 'OK' and 'Cancel' buttons.

- 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.

The screenshot shows the 'TCP/IP Properties' dialog box with the 'Gateway' tab selected. The 'New gateway' field contains the IP address '192.168.123.254'. Below it, the 'Installed gateways' list is empty. The 'Add' button is visible next to the 'New gateway' field, and the 'Remove' button is next to the 'Installed gateways' list. The 'OK' and 'Cancel' buttons are at the bottom.

- 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.

The screenshot shows the 'TCP/IP Properties' dialog box with the 'DNS Configuration' tab selected. The 'Enable DNS' radio button is selected. The 'Host' field contains 'MyComputer' and the 'Domain' field is empty. The 'DNS Server Search Order' list contains the IP address '168.95.1.1'. The 'Add' button is visible next to the 'DNS Server Search Order' list, and the 'Remove' button is next to the list. The 'Domain Suffix Search Order' list is empty. The 'Add' and 'Remove' buttons are visible next to the 'Domain Suffix Search Order' list. The 'OK' and 'Cancel' buttons are at the bottom.

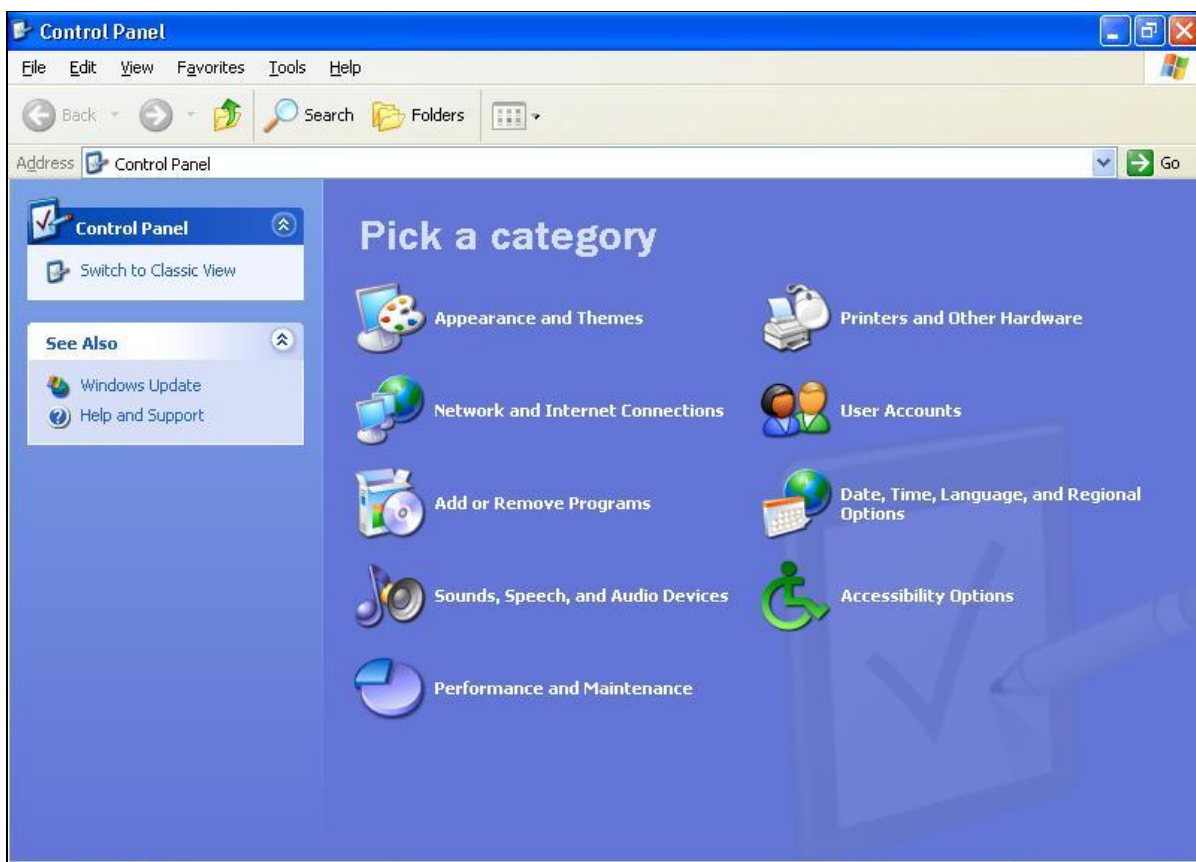
## Appendix B Win 2000/XP IPSEC Setting guide

**Example: Win XP/2000 à VPN Router**

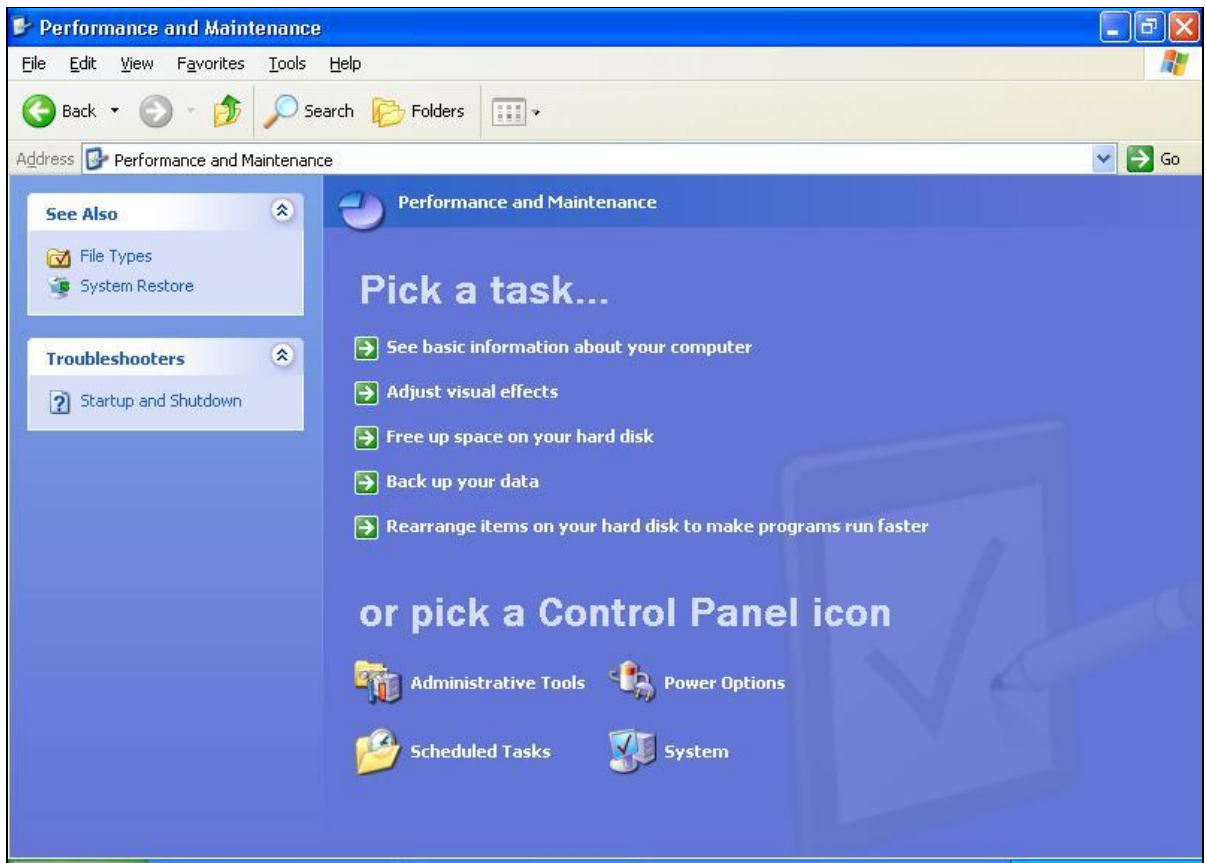
(Configuration on WIN 2000 is similar to XP)

1. On Win 2000/XP, click **[Start]** button, select **[Run]**, type **secpol.msc** in the field, then click **[Run]** à Goto **\*\*Local Security Policy Settings\*\*** page

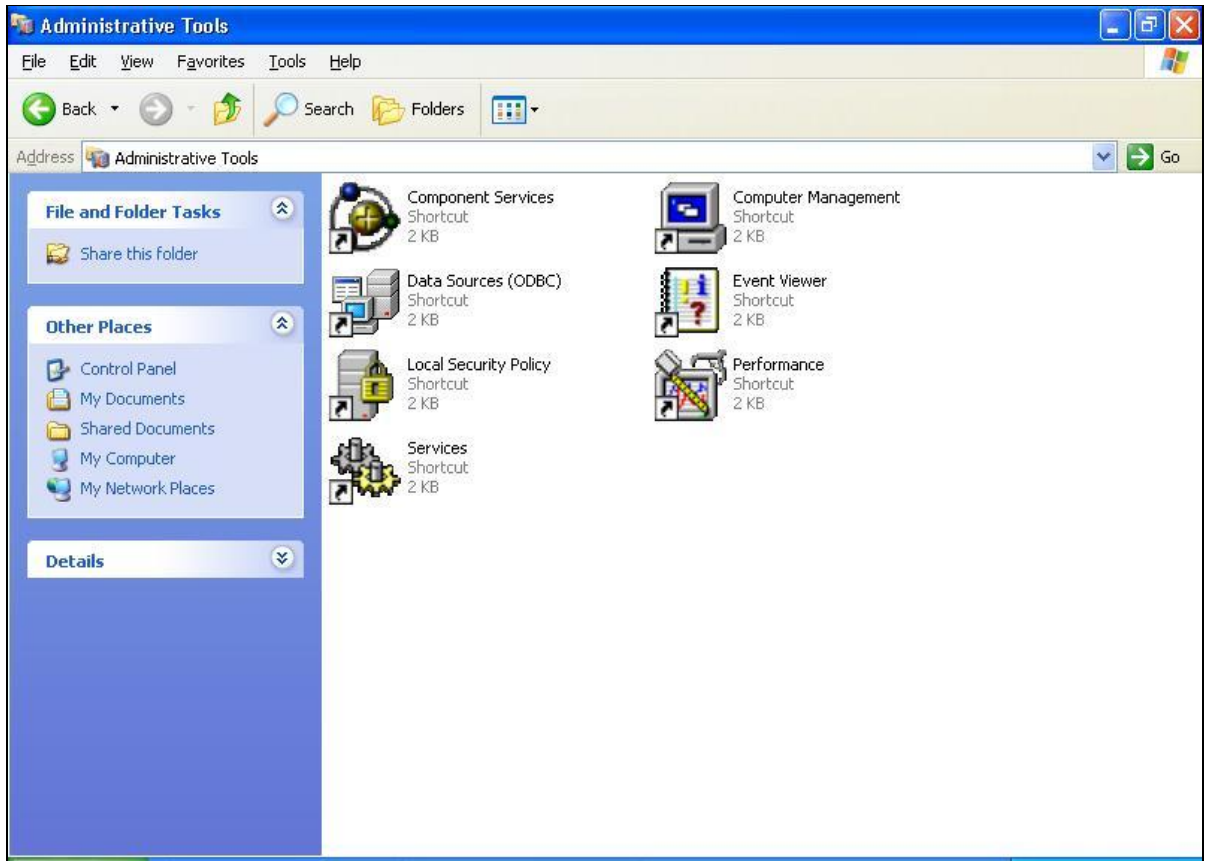
2. Or in Win XP, Click **[Control Pannel]**



Double-click **[Performance and Maintenance]**

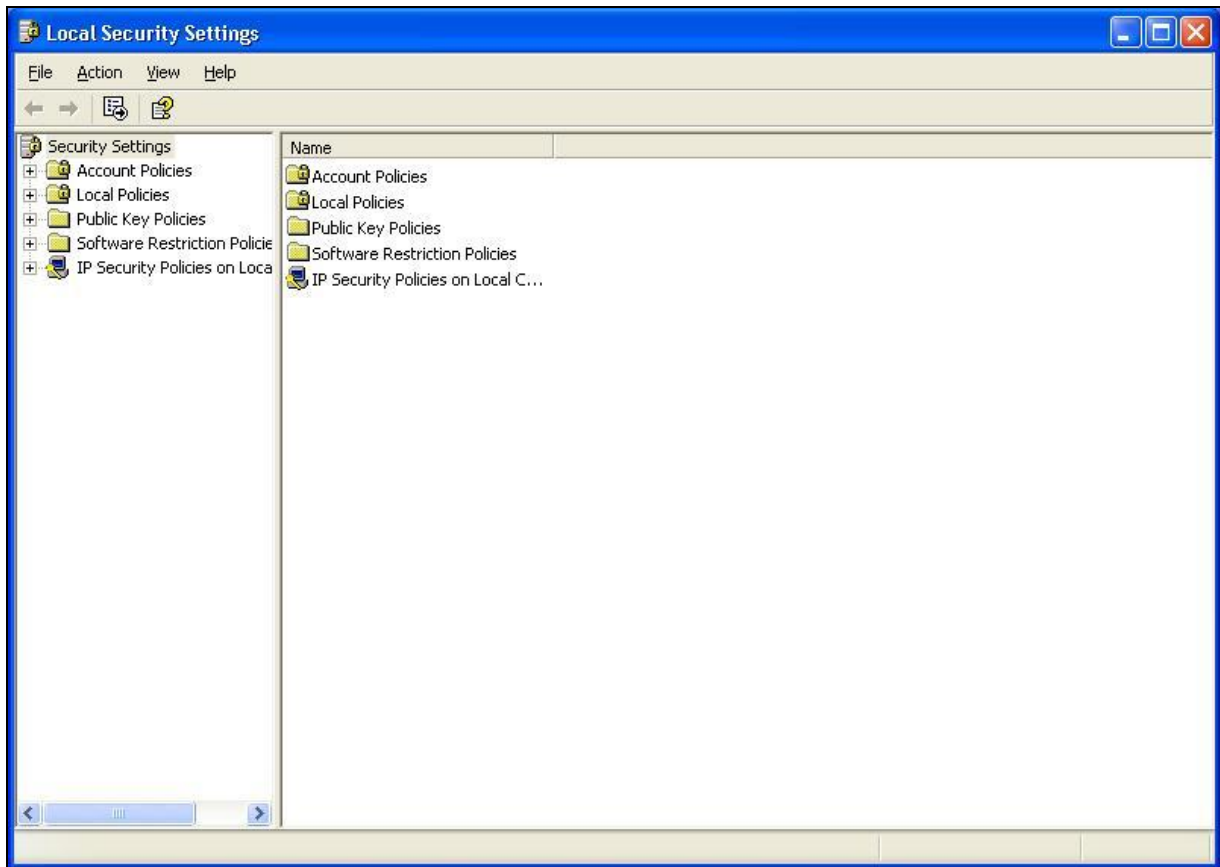


Double-click [Administrative Tools]



## Local Security Policy Settings

Double-click [Local Security Policy]

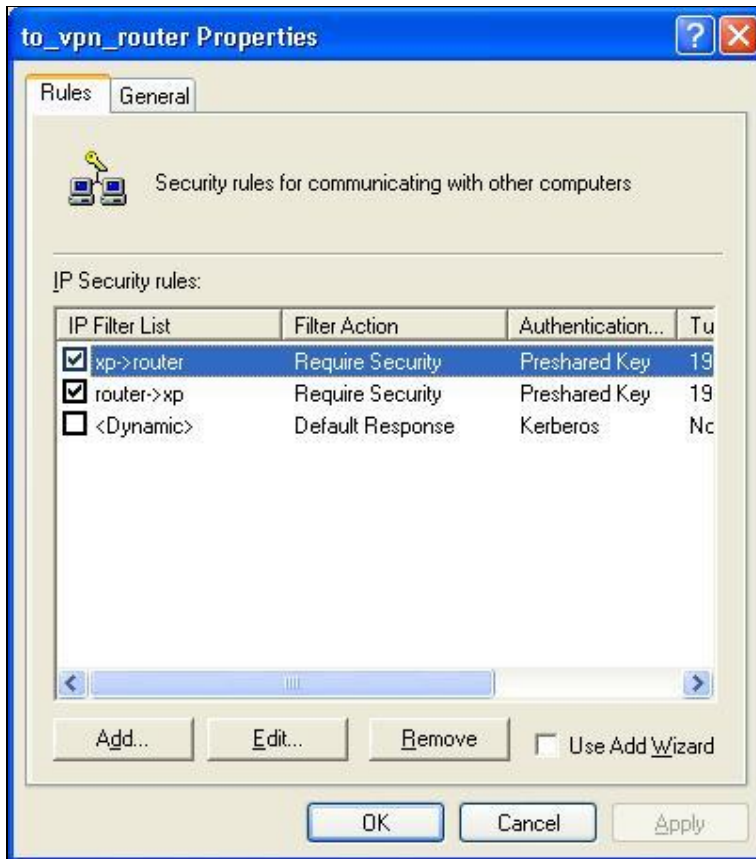


Right-click **[IP Security Policies on Local Computer]**, and click **[Create IP Security Policy]**.

Click the **[Next]** button, enter your policy's name (Here it is **to\_vpn\_router**). Then, click **[Next]**.

Dis-select the **[Activate the default response rule]** check box, and click **[Next]** button.

Click **[Finish]** button, make sure **[Edit]** check box is checked.

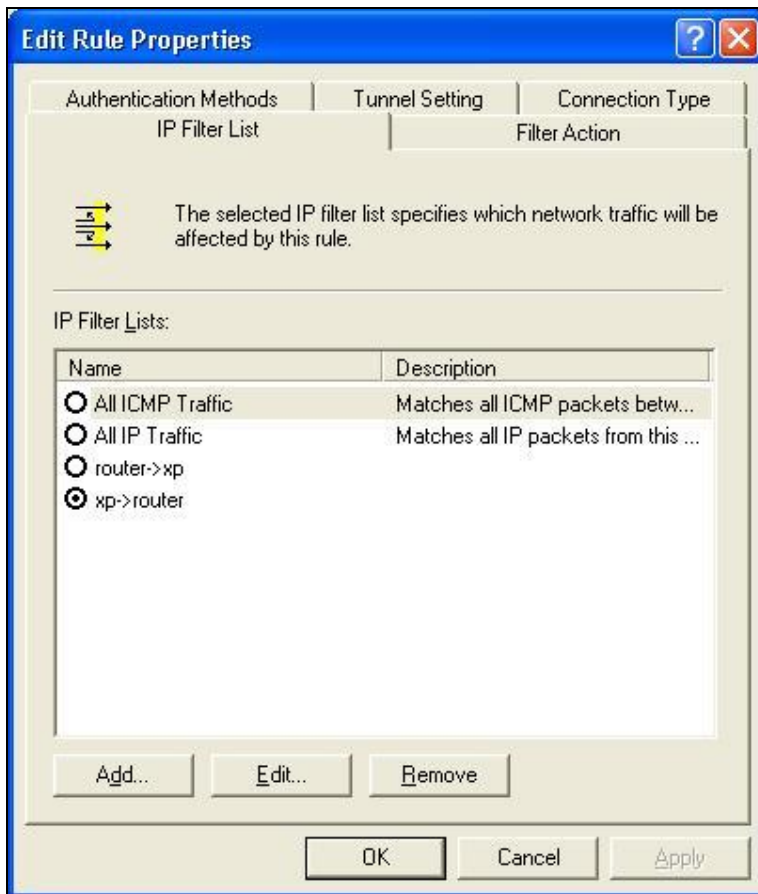


## Build 2 Filter Lists: “xp->router” and “router->xp”

### Filter List 1: xp-> router

In the “new policy’s properties” screen, select [Use Add Wizard] check box, and then click [Add] button to create a new rule.





click [Add] button

**IP Filter List**

An IP filter list is composed of multiple filters. In this way, multiple subnets, IP addresses and protocols can be combined into one IP filter.

Name:

Description:

Filters: ☐ Use Add Wizard

Mirrored	Description	Protocol	Source Port	Destination
No		ANY	ANY	ANY

Enter a name, for example: **xp->router**  
 and dis-select **[Use Add Wizard]** check box. Click **[Add]** button.

**Filter Properties**

Addressing | Protocol | Description

Source address:

A specific IP Address

IP Address: 192 . 168 . 1 . 1

Subnet mask: 255 . 255 . 255 . 255

Destination address:

A specific IP Subnet

IP address: 192 . 168 . 123 . 0

Subnet mask: 255 . 255 . 255 . 0

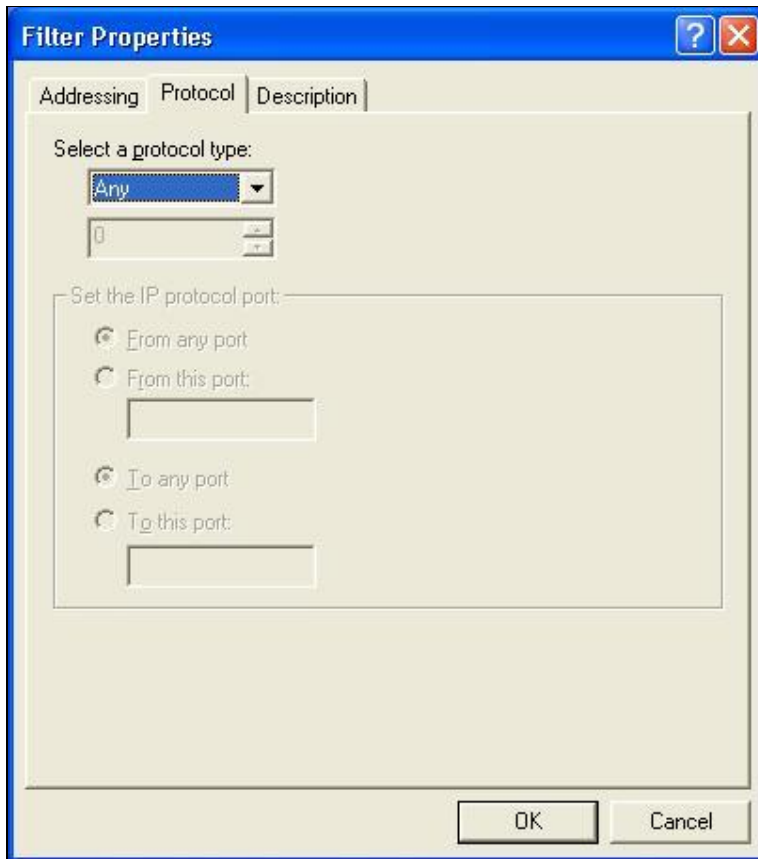
☐ Mirrored. Also match packets with the exact opposite source and destination addresses.

OK Cancel

In the Source address field, select [**A specific IP Address**].  
and fill in IP Address: **192.168.1.1**

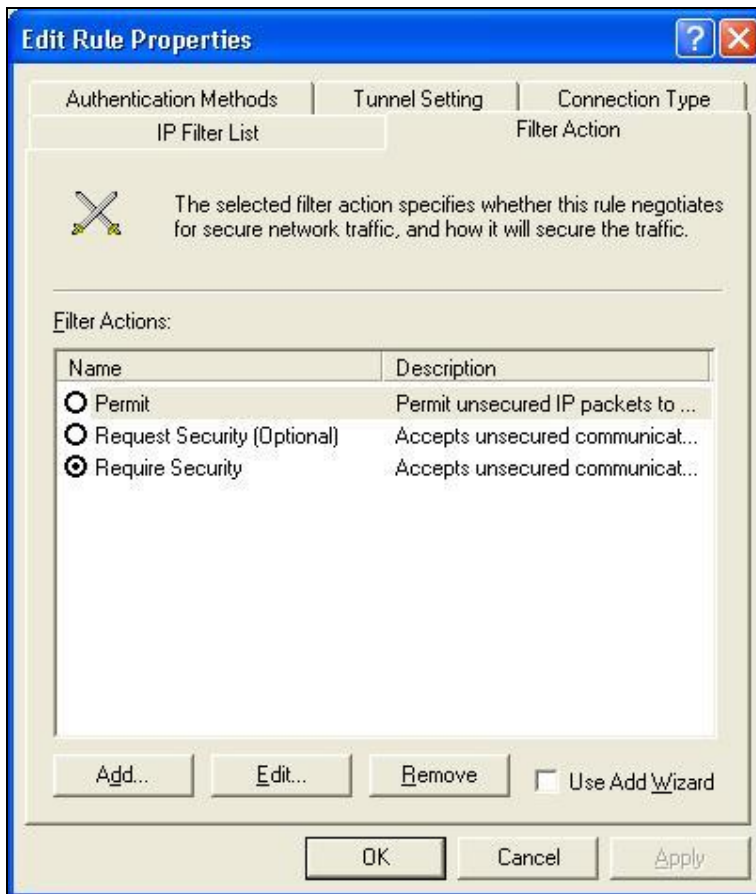
In the Destination address field, select [**A specific IP Subnet**], fill in  
IP Address: **192.168.123.0** and Subnet mask: **255.255.255.0**.

If you want to select a protocol for your filter, click [**Protocol**] page.

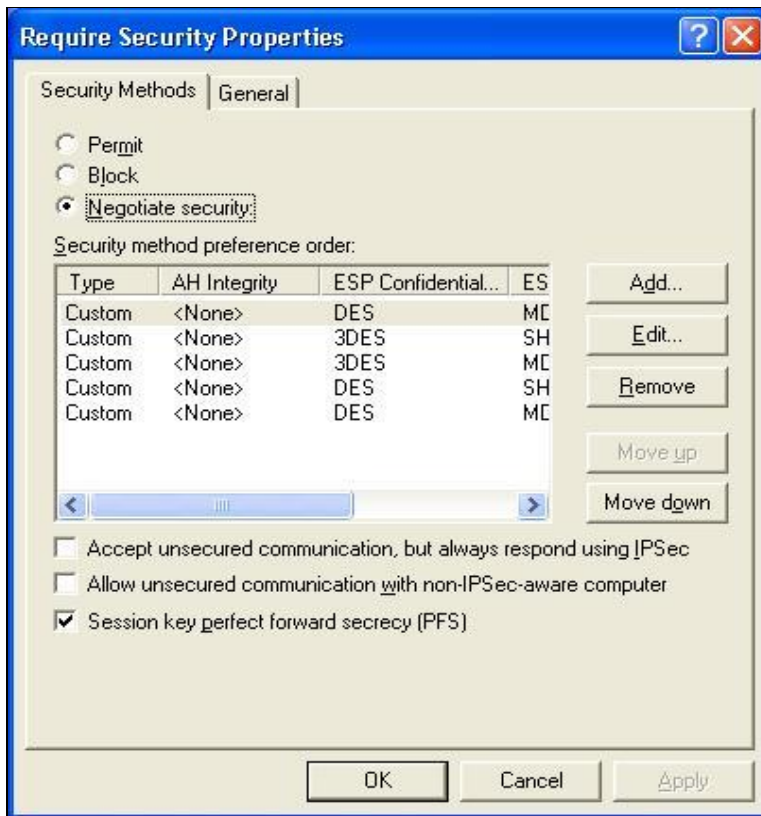


The image shows a Windows-style dialog box titled "Filter Properties". It has a blue title bar with a question mark icon and a close button (X). Below the title bar are three tabs: "Addressing", "Protocol", and "Description". The "Protocol" tab is currently selected. Inside the dialog, under the "Protocol" tab, there is a section titled "Select a protocol type:". Below this title is a dropdown menu showing "Any" and a small downward arrow. Below the dropdown is a text box containing the number "0". Below this is another section titled "Set the IP protocol port:". This section contains four radio button options: "From any port" (which is selected), "From this port:" (with an empty text box below it), "To any port" (which is also selected), and "To this port:" (with an empty text box below it). At the bottom right of the dialog are two buttons: "OK" and "Cancel".

Click **[OK]** button. Then click **[OK]** button on the “**IP Filter List**” page.

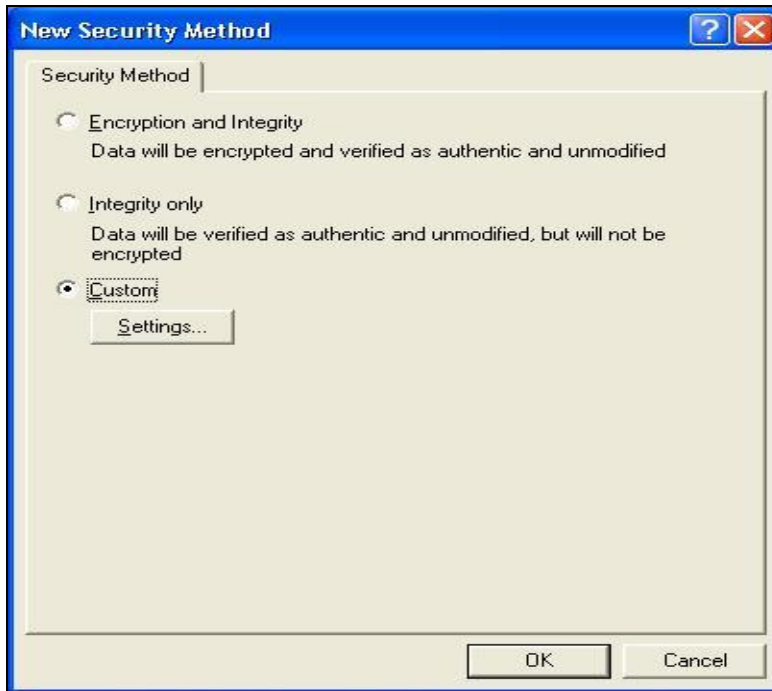


select **[Filter Action]**, select **[Require Security]**, then  
click **[Edit]** button.

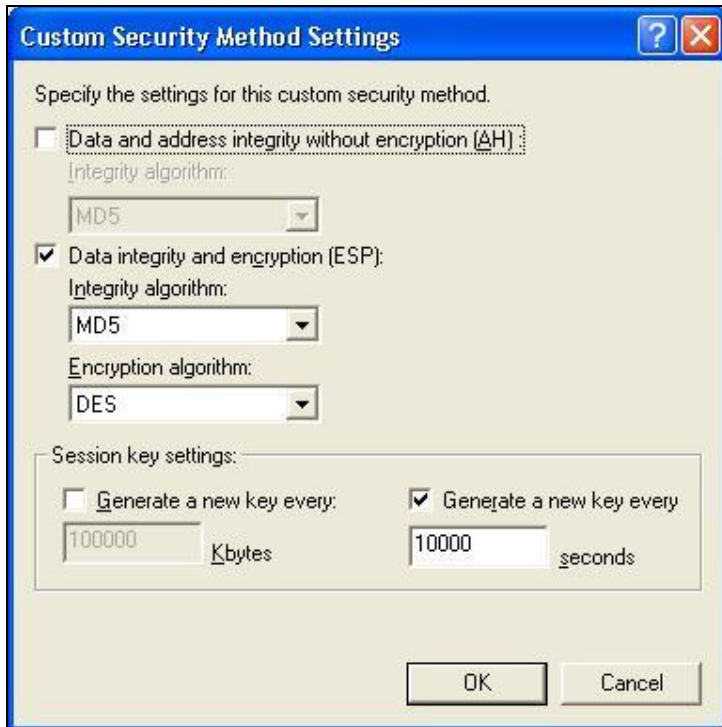


select [Negotiate security], Select [Session key Perfect Forward Secrecy (PFS)]

click [Edit] button.



select [**Custom**] button



Select **[Data integrity and encryption (ESP)]**

Configure “**Integrity algorithm**”: **[MD5]**

Configure “**Encryption algorithm**”: **[DES]**

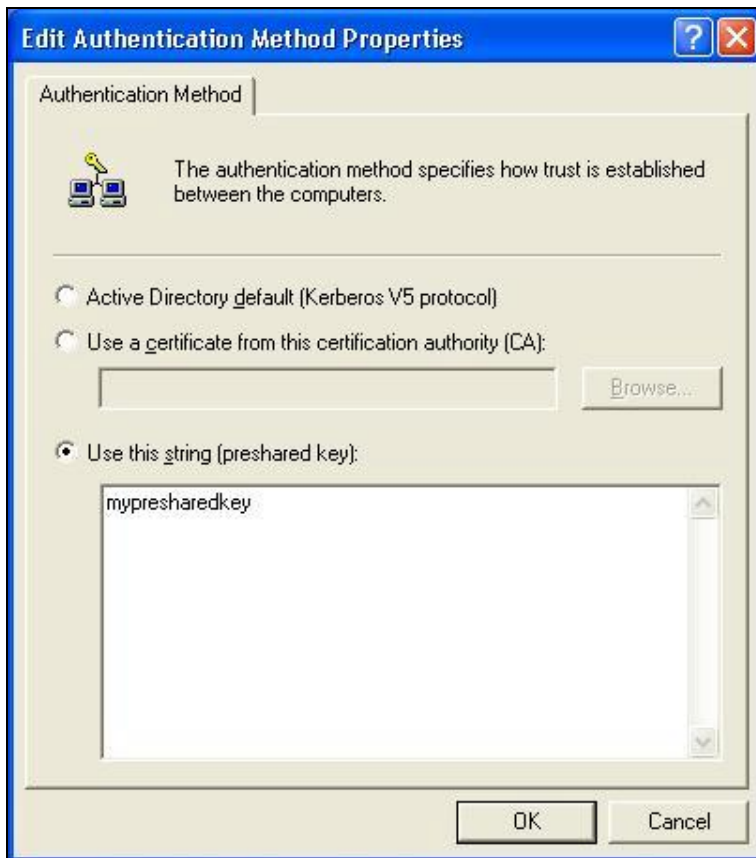
Configure “**Generate a new key every [10000] seconds**”

Click **[OK]** button





select [**Authentication Methods**] page, click [**Add**] button.



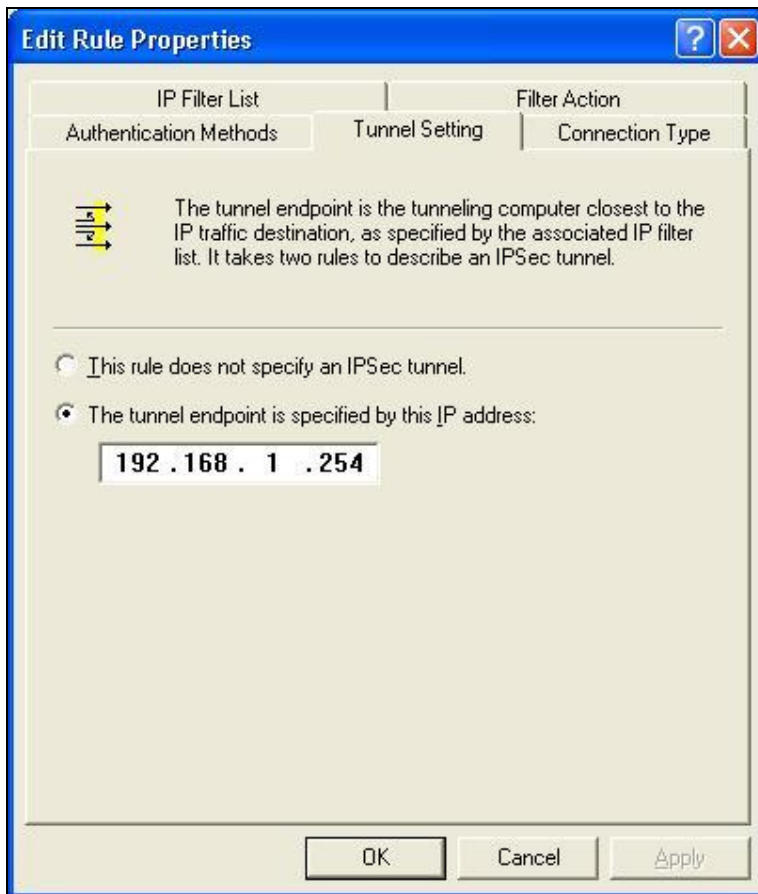
select **[Use this string to protect the key exchange (preshared key)]**,

and enter your preshared key string, such as

**mypresharedkey**. Click **[OK]** button.

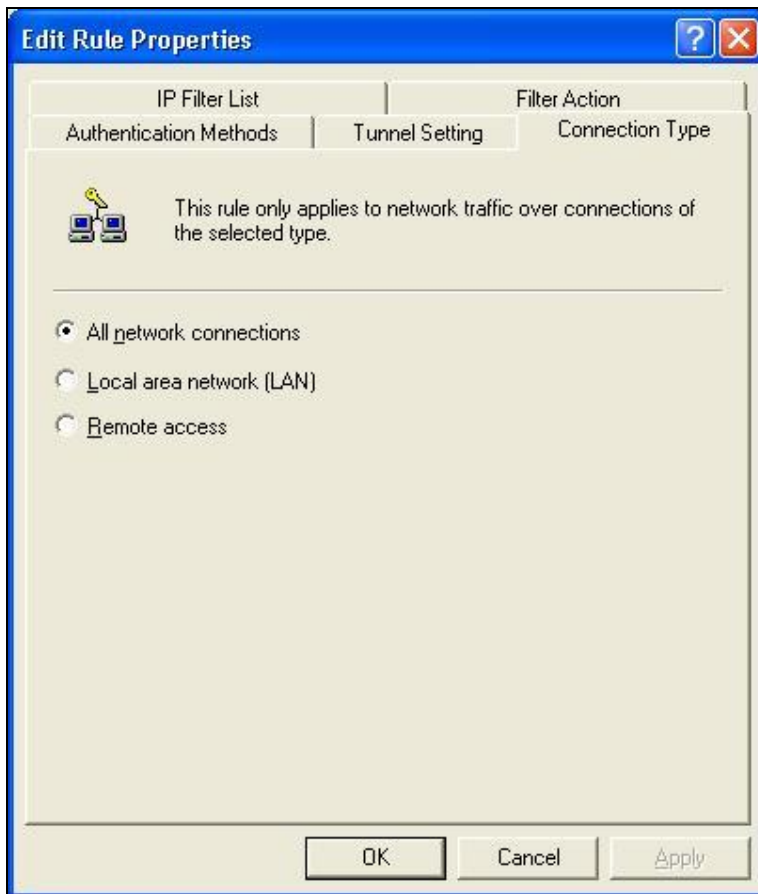
Click **[OK]** button on **[Authentication Methods]** page.

Select **[Tunnel Setting]**



configure [The tunnel endpoint is specified by this IP address]: 192.168.1.254

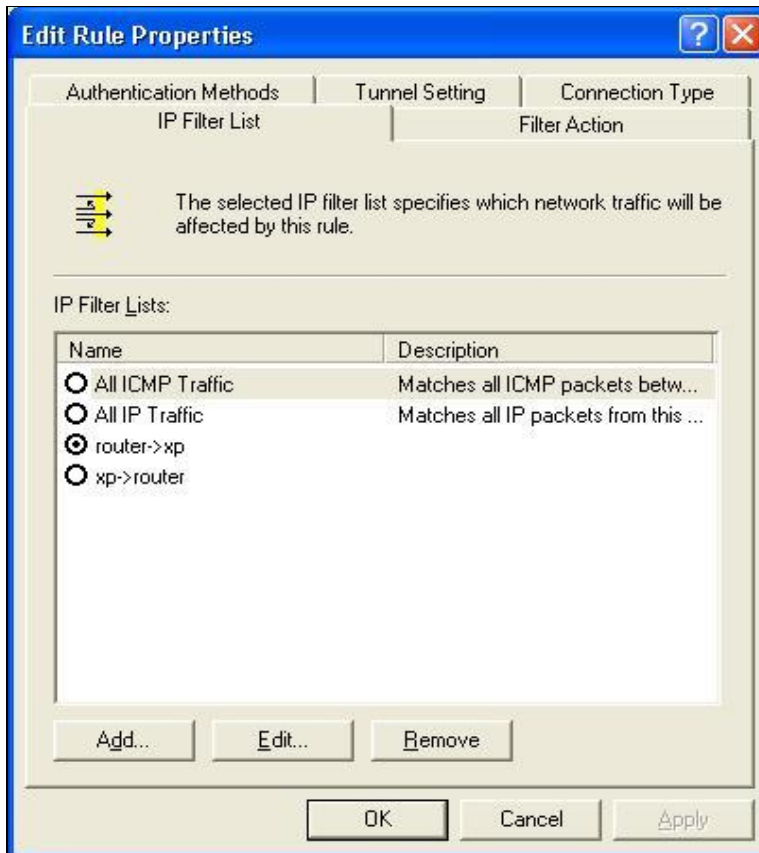
Select [Connection Type]



select **[All network connections]**

#### **Tunnel 2: router->xp**

In the “**new policy’s properties**” page, dis-select **[Use Add Wizard]** check box, and then click **[Add]** button to create a new rule.



click **[Add]** button

**IP Filter List**

An IP filter list is composed of multiple filters. In this way, multiple subnets, IP addresses and protocols can be combined into one IP filter.

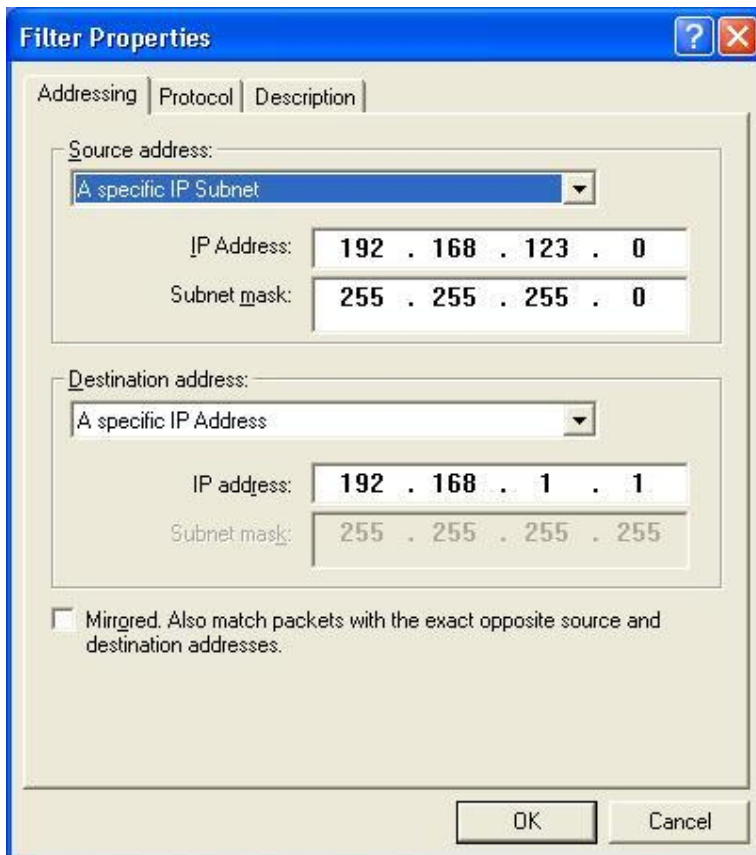
Name:

Description:

Filters: ☐ Use Add Wizard

Mirrored	Description	Protocol	Source Port	Destination
No		ANY	ANY	ANY

Enter a name, such as **router->xp**  
and dis-select **[Use Add Wizard]** check box. Click **[Add]** button.

The image shows a 'Filter Properties' dialog box with a blue title bar and standard window controls. It has three tabs: 'Addressing' (selected), 'Protocol', and 'Description'. The 'Addressing' tab contains two main sections. The first section, 'Source address:', has a dropdown menu set to 'A specific IP Subnet'. Below it are two input fields: 'IP Address' with the value '192 . 168 . 123 . 0' and 'Subnet mask' with the value '255 . 255 . 255 . 0'. The second section, 'Destination address:', has a dropdown menu set to 'A specific IP Address'. Below it are two input fields: 'IP address' with the value '192 . 168 . 1 . 1' and 'Subnet mask' with the value '255 . 255 . 255 . 255'. At the bottom of the dialog is a checkbox labeled 'Mirrored. Also match packets with the exact opposite source and destination addresses.' which is currently unchecked. At the very bottom are 'OK' and 'Cancel' buttons.

**Filter Properties**

Addressing | Protocol | Description

Source address:

A specific IP Subnet

IP Address: 192 . 168 . 123 . 0

Subnet mask: 255 . 255 . 255 . 0

Destination address:

A specific IP Address

IP address: 192 . 168 . 1 . 1

Subnet mask: 255 . 255 . 255 . 255

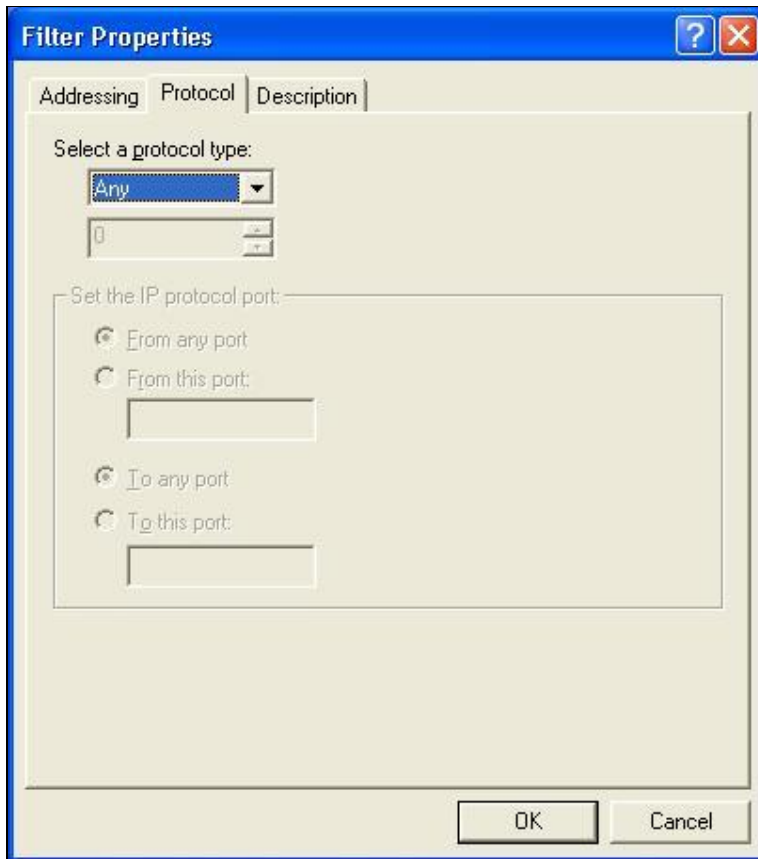
☐ Mirrored. Also match packets with the exact opposite source and destination addresses.

OK Cancel

In the Source address field, select [**A specific IP Subnet**]. fill in  
IP Address: **192.168.123.0** and Subnet mask: **255.255.255.0**.

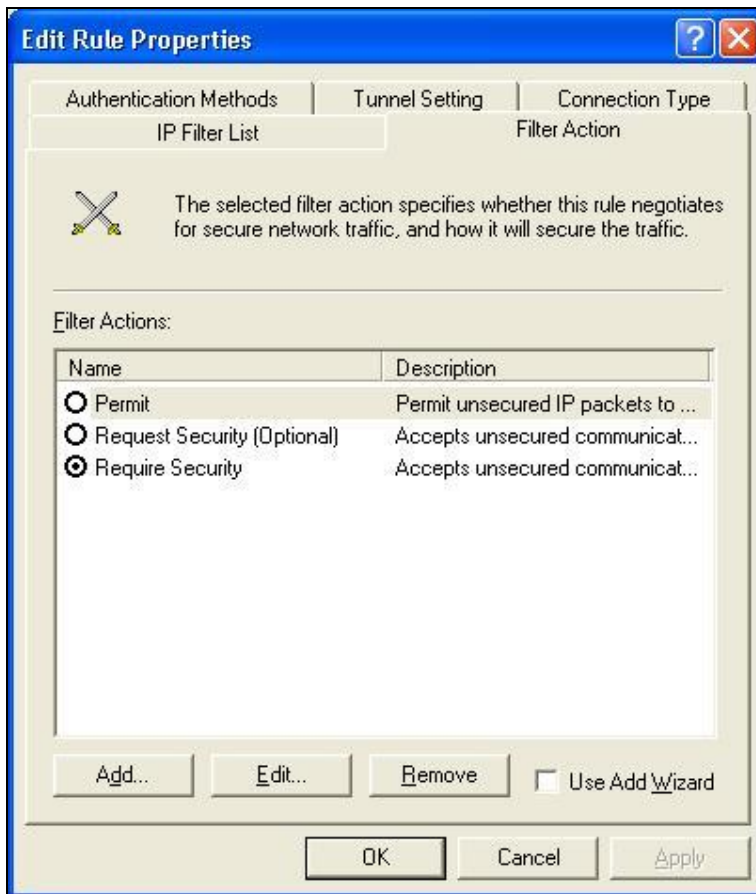
In the Destination address field, select [**A specific IP Address**],  
and fill in IP Address: **192.168.1.1**

If you want to select a protocol for your filter, click [**Protocol**] page.

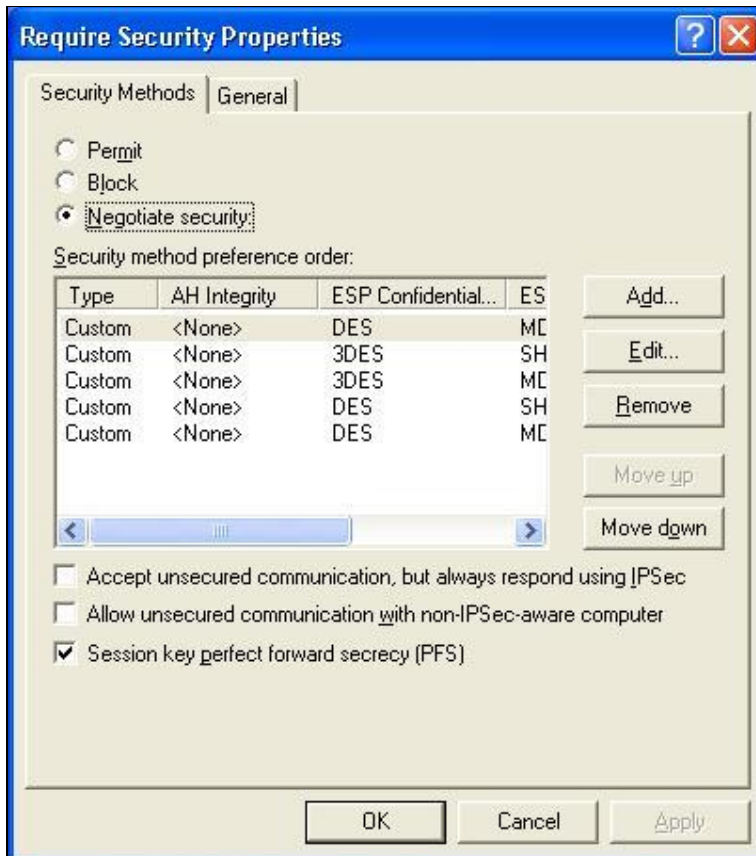


Click **[OK]** button. Then click **[OK]** button on **[IP Filter List]** window.

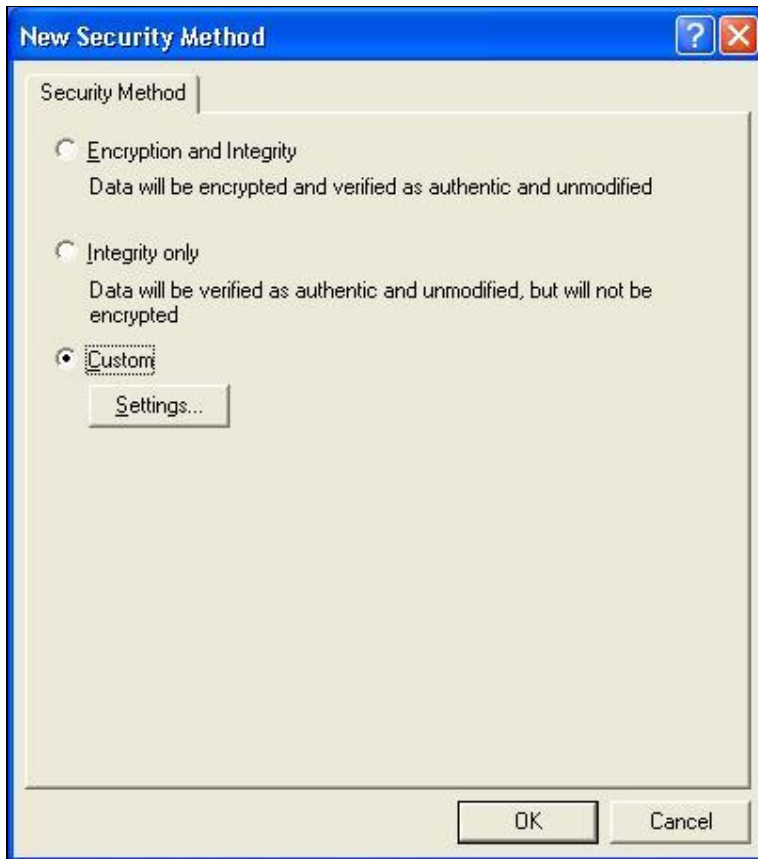




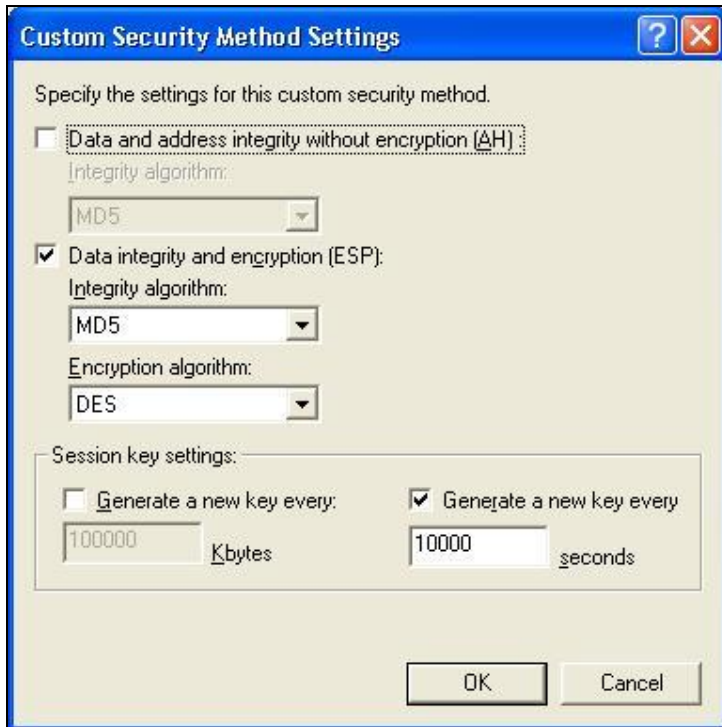
select **[Filter Action tab]**, select **[Require Security]**, then  
click **[Edit]** button.



select **[Negotiate security]**, Select **[Session key Perfect Forward Secrecy (PFS)]**  
 click **[Edit]** button.



select [**Custom**] button



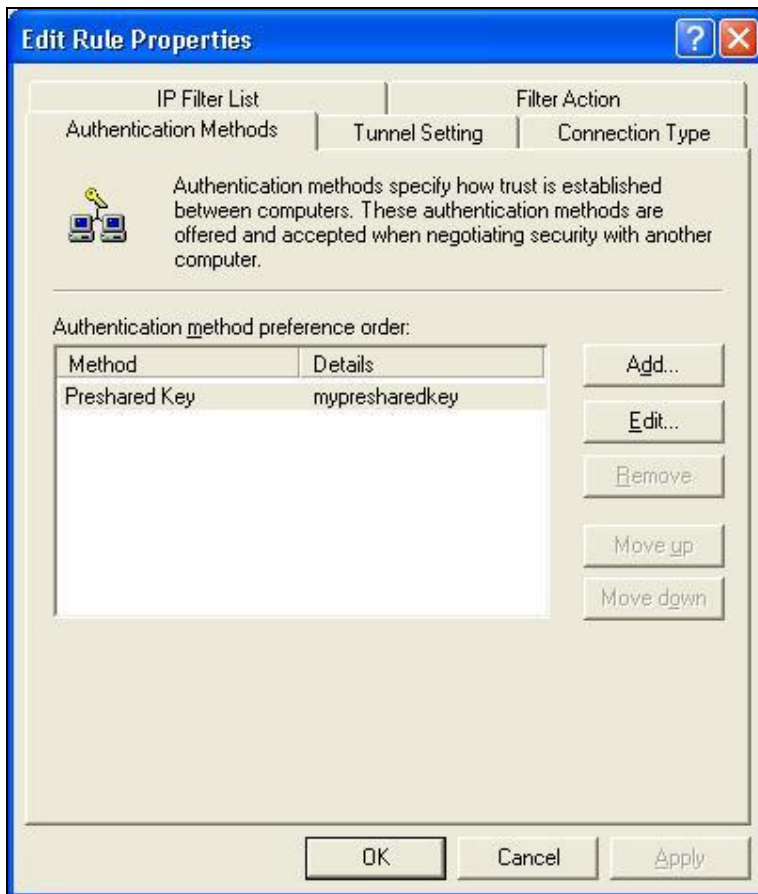
Select **[Data integrity and encryption (ESP)]**

Configure “**Integrity algorithm**”: **[MD5]**

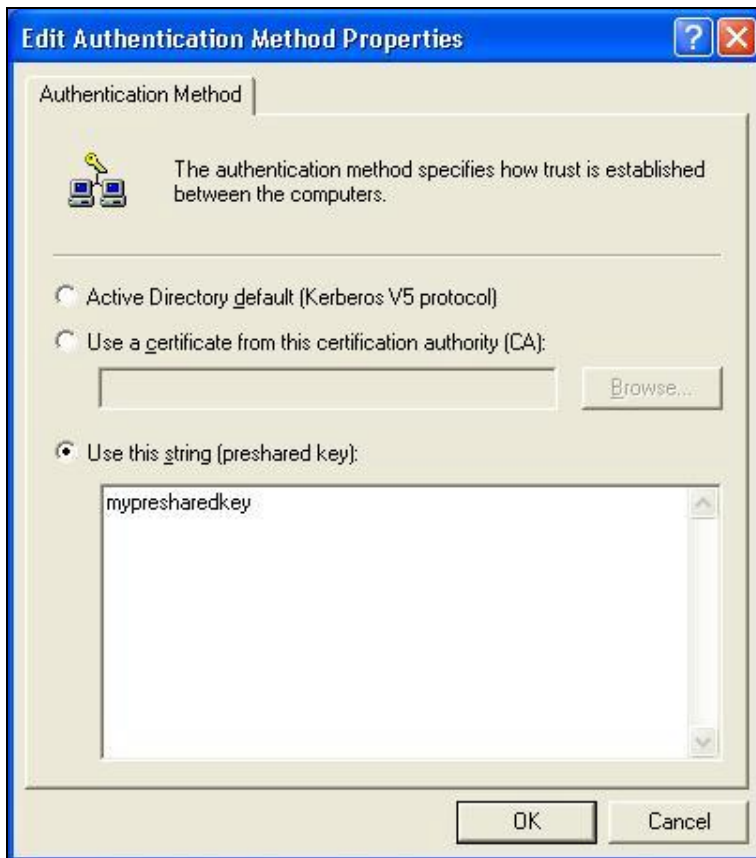
Configure “**Encryption algorithm**”: **[DES]**

Configure “**Generate a new key every [10000] seconds**”

Click **[OK]** button



select **[Authentication Methods]** page, click **[Add]** button.



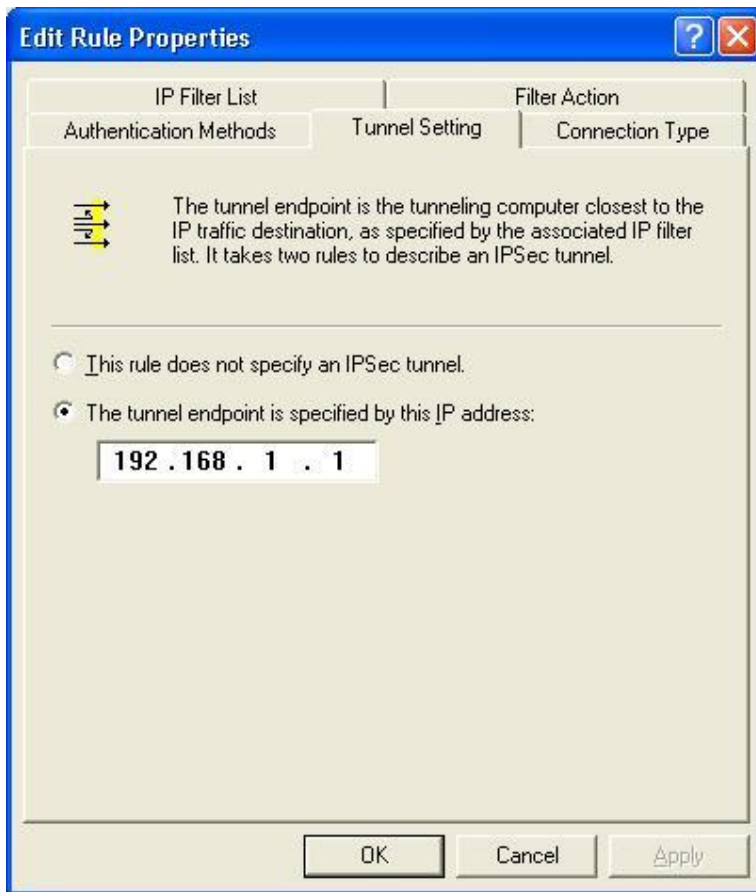
select **[Use this string to protect the key exchange (preshared key)]**,

and enter the preshared key string, such as

**mypresharedkey**. Click **[OK]** button.

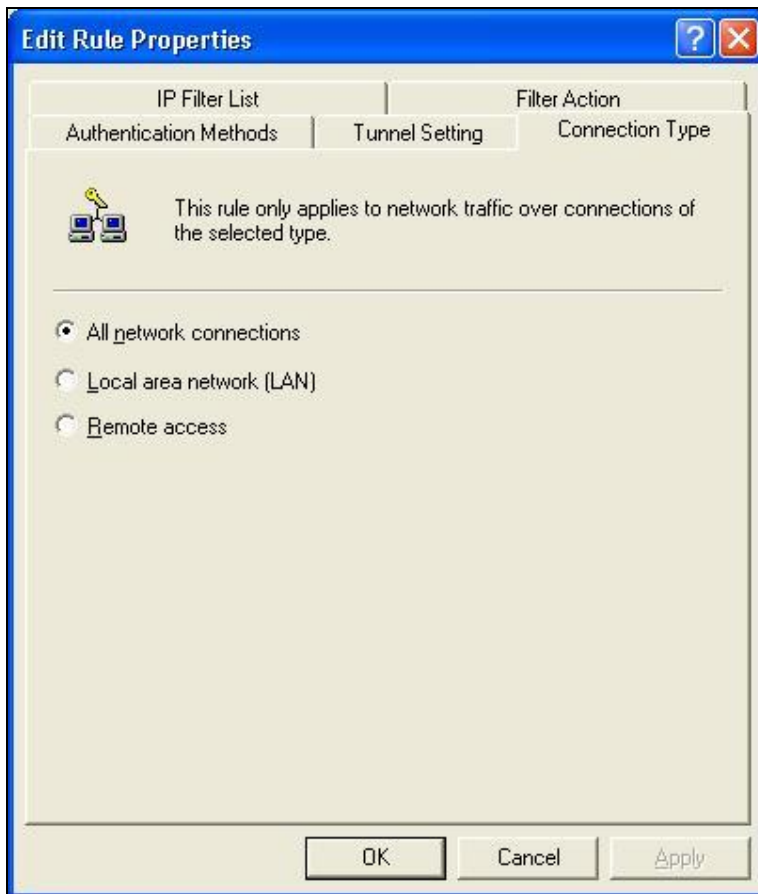
Click **[OK]** button on **[Authentication Methods]** page.

Select **[Tunnel Setting]**



Configure [**The tunnel endpoint is specified by this IP address**]: **192.168.1.1**

Select [**Connection Type**]



select [All network connections]

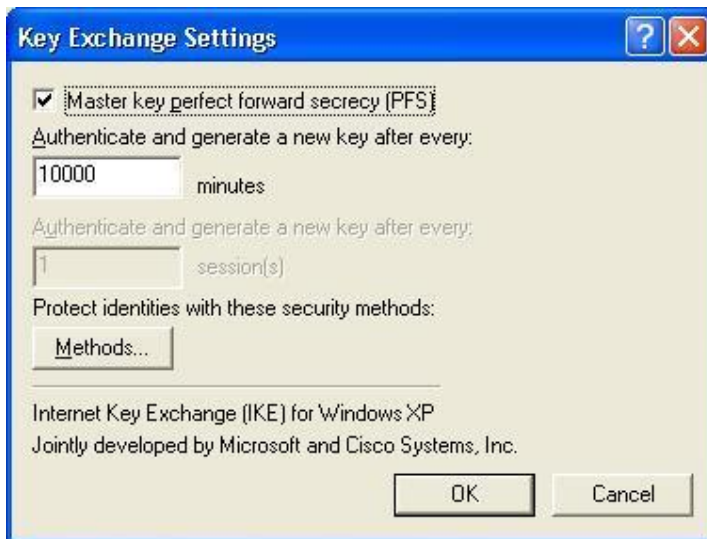


## Configure IKE properties

Select **[General]**



Click **[Advanced...]**



enable “**Master key perfect forward security (PFS)**”

configure “**Authenticate and generate a new key after every [10000] seconds**”

click [**Methods...**]



click [**Add**] button



Configure “**Integrity algorithm**”: [SHA1]

Configure “**Encryption algorithm**”: [3DES]

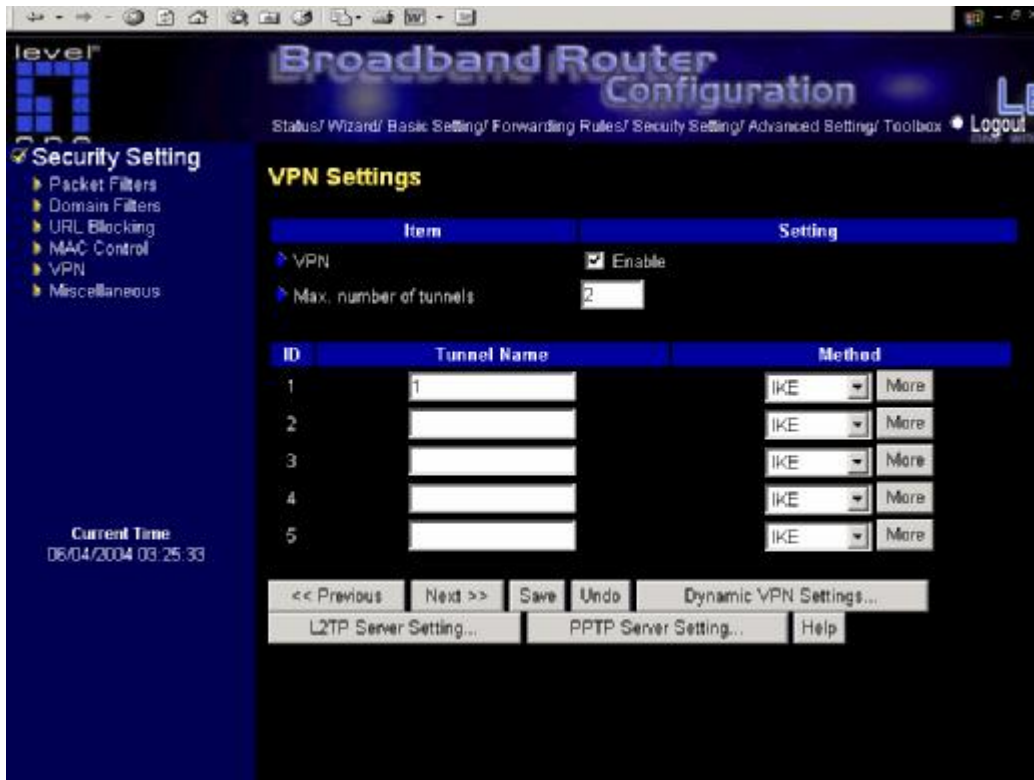
Configure “**Diffie-Hellman group**”: [Medium (2)]

Settings on VPN router

**VPN Router:** Wan IP address:192.168.1.254

Lan IP address:192.168.123.254

**PC:** 192.168.123.123



#### VPN Settings:

VPN: Enable

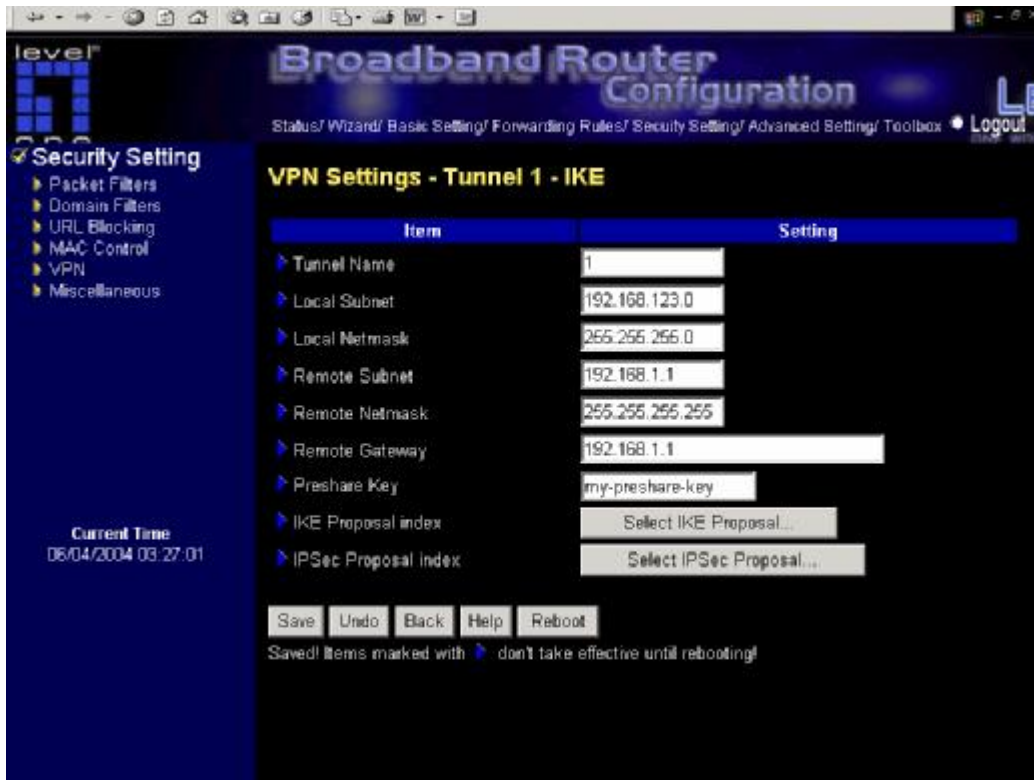
Max. number of tunnels: 2

ID: 1

Tunnel Name: 1

Method: IKE

Press **"More"**à



#### VPN Settings - Tunnel 1 – IKE

Tunnel:1

Local Subnet:192.168.123.0

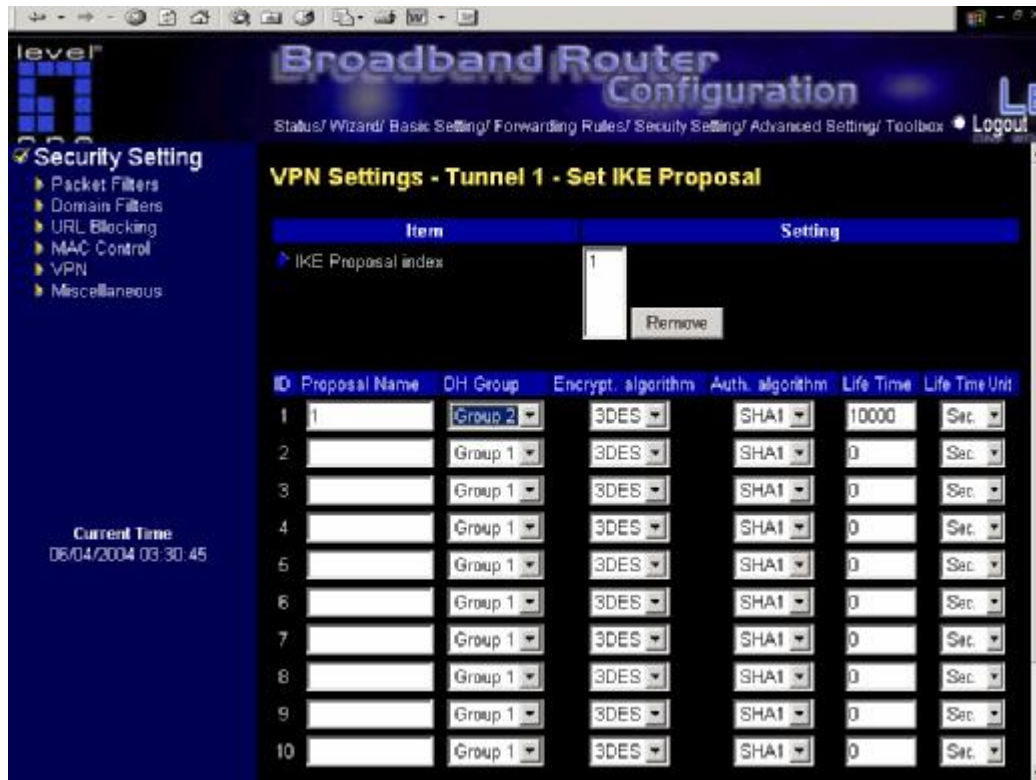
Local Netmask:255.255.255.0

Remote Subnet:192.168.1.1

Remote Netmask:255.255.255.255

Remote Gateway:192.168.1.1

Preshare Key: my-preshare-key



#### VPN Settings - Tunnel 1 - Set IKE Proposal

ID: 1

Proposal Name: 1

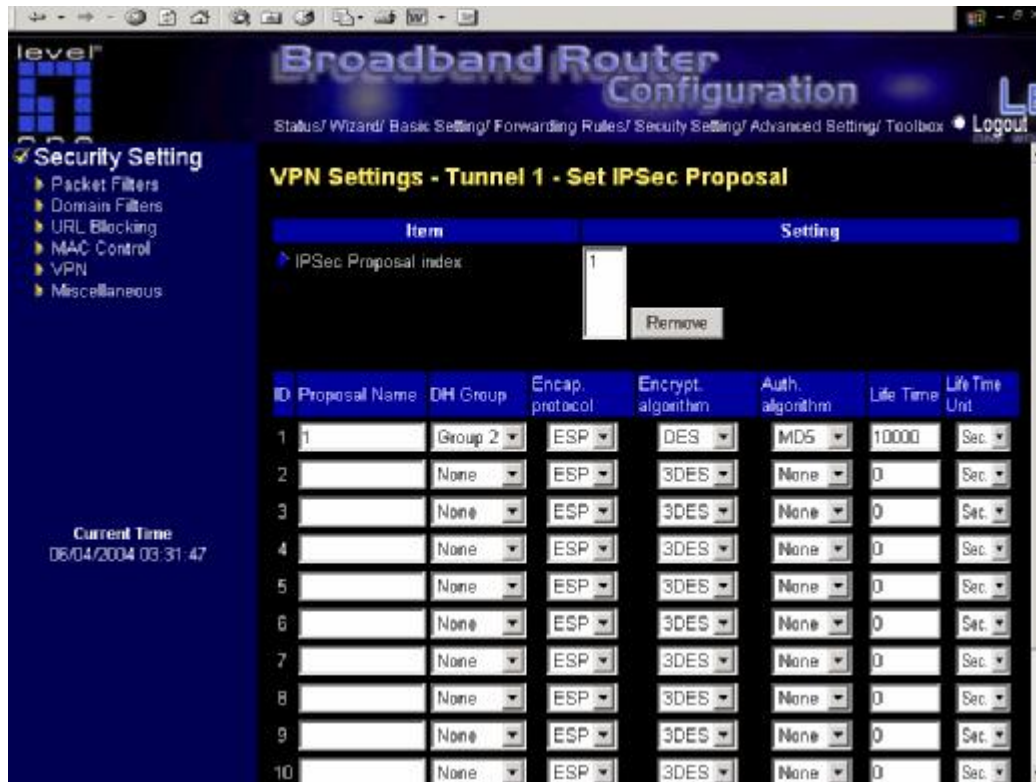
DH Group: Group2

Encrypt. Algorithm: 3DES

Auth. Algorithm: SHA1

Life Time: 10000

Life Time Unit: Sec.



### VPN Settings - Tunnel 1 - Set IPsec Proposal

ID: 1

Proposal Name: proposal1

DH Group: Group2

Encap. Protocol: ESP

Encrypt. Algorithm: DES

Auth. Algorithm: MD5

Life Time: 10000

Life Time Unit: Sec.

## System Log

WAN Type: Static IP Address

Display time: Tuesday, April 01, 2003 9:28:40 AM

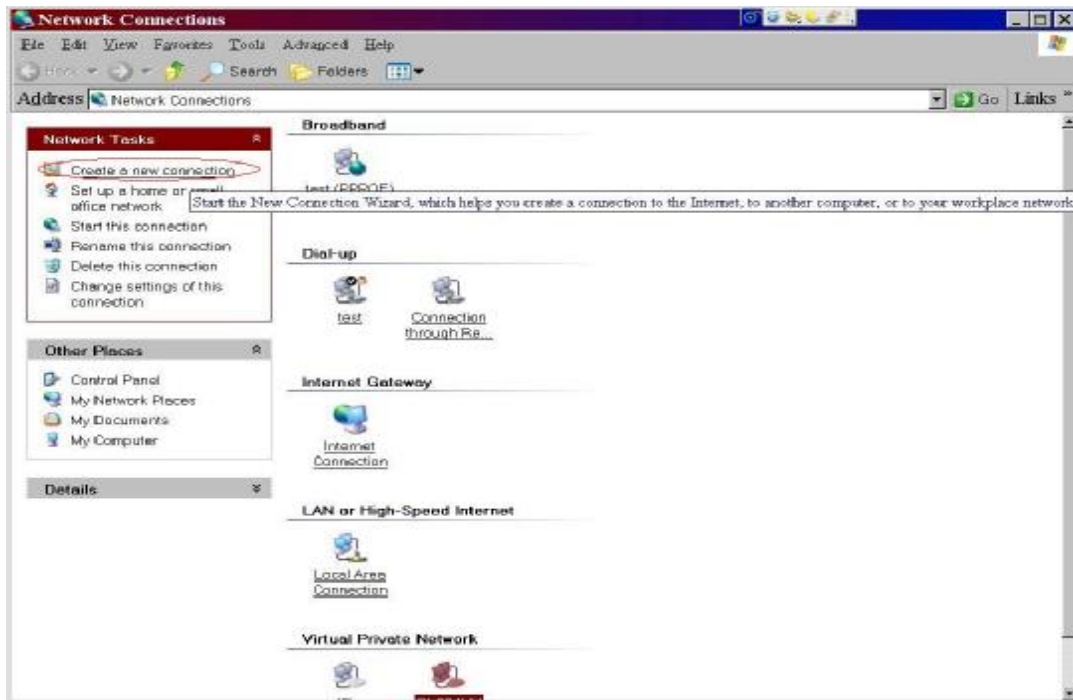
```
Tuesday, April 01, 2003 9:28:34 AM 192.168.123.197 login successful
*
* Initial IKE.
* <--M1 (INIT) [88]    -->M2 (RESP) [80]
*
* in:0 (0) out:36 (24)
*    -->M4 (KEYRESP) [156]
*    -->M6 (IDRESP) [40]
*    [192.168.1.1] <--> [192.168.1.254] Phase1 established
*    -->Q2 (QRESP) [264]
*
* in:268435457 (10000001) out:2054219905 (7a70e881)
*    Inbound 16777232 (1000010)
*    Outbound 2054219905 (7a70e881)
*
*    [192.168.1.1] <--> [192.168.1.254] Phase2 (IPSEC SA) established
*
* QM Notify:ISAKMP_NMT_CONNECTED
*
* IKE daemon start up.
*    -->INFO[84]
*
* IKE daemon start up.
Tuesday, April 01, 2003 9:28:19 AM 192.168.123.114 login successful
```

User can view VPN connection process in “**System Log**” page, and correct their settings. Phase1 is related to **IKE** settings, Phase2 is related to **IPSEC** settings.

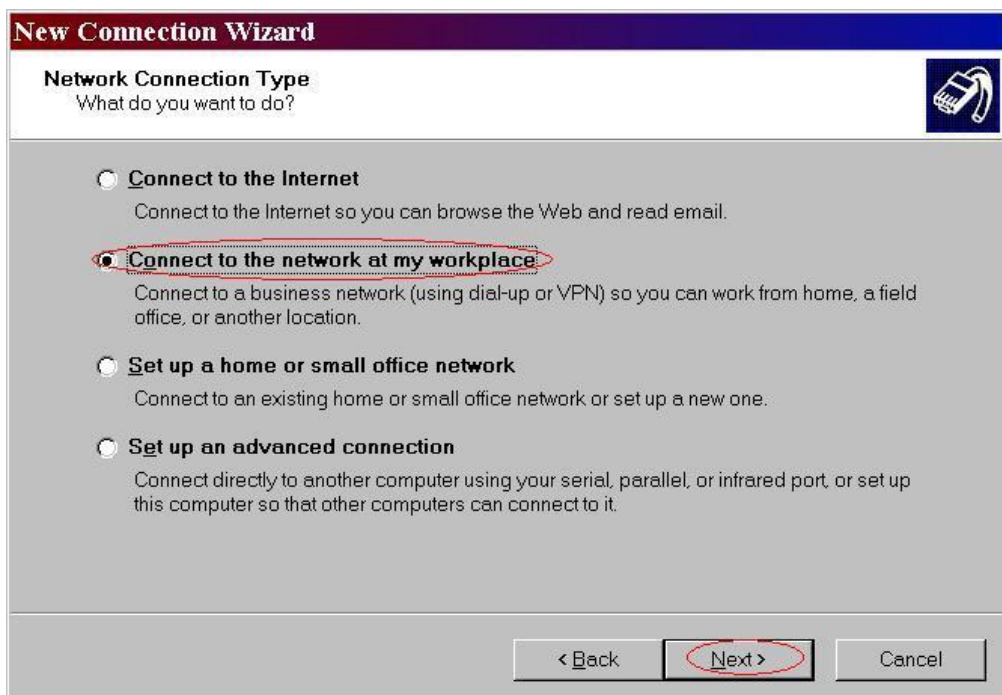


## Appendix C PPTP and L2TP Configurations

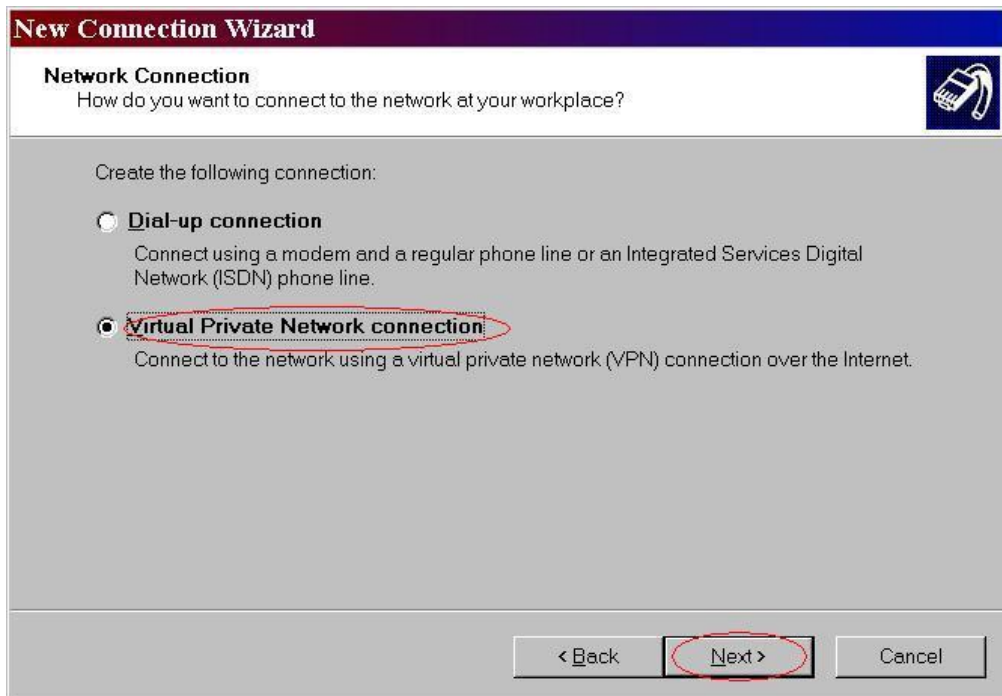
1. First, please go to the Network connection



2. Connect to network at my workplace



### 3. Choose Virtual Private Network



**New Connection Wizard**

**Network Connection**  
How do you want to connect to the network at your workplace?

Create the following connection:

- ☐ **Dial-up connection**  
Connect using a modem and a regular phone line or an Integrated Services Digital Network (ISDN) phone line.
- ☒ **Virtual Private Network connection**  
Connect to the network using a virtual private network (VPN) connection over the Internet.

< Back   Next >   Cancel

### 4. Do not dial to initial connection



**New Connection Wizard**

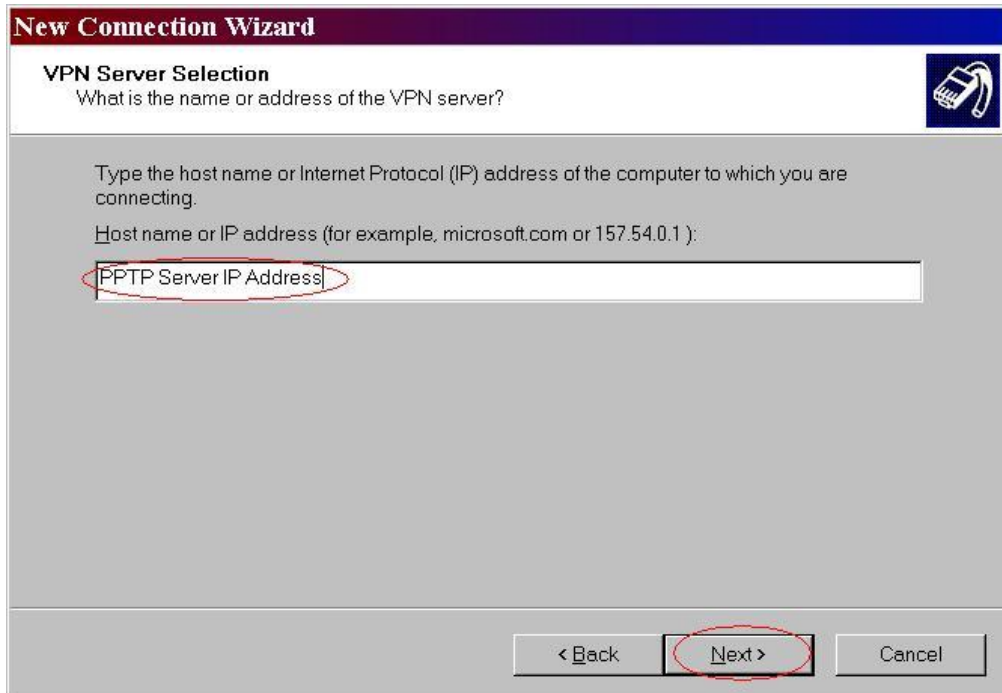
**Public Network**  
Windows can make sure the public network is connected first.

Windows can automatically dial the initial connection to the Internet or other public network, before establishing the virtual connection.

- ☒ **Do not dial the initial connection.**
- ☐ **Automatically dial this initial connection:**

< Back   Next >   Cancel

## 5. INPUT THE ROUTER WAN IP ADDRESS



**New Connection Wizard**

**VPN Server Selection**  
What is the name or address of the VPN server?

Type the host name or Internet Protocol (IP) address of the computer to which you are connecting.  
Host name or IP address (for example, microsoft.com or 157.54.0.1):

PPTP Server IP Address

< Back   **Next >**   Cancel

This screenshot shows the 'New Connection Wizard' window with the 'VPN Server Selection' step. The title bar reads 'New Connection Wizard'. Below the title bar, the section is 'VPN Server Selection' with a sub-question 'What is the name or address of the VPN server?'. A text box contains 'PPTP Server IP Address', which is circled in red. Below the text box are three buttons: '< Back', 'Next >' (circled in red), and 'Cancel'.

6. Then ok, please input username and password as you setup in the router.



**Connect PPTP**

User name: PPTP user name

Password: .....

☐ Save this user name and password for the following users:

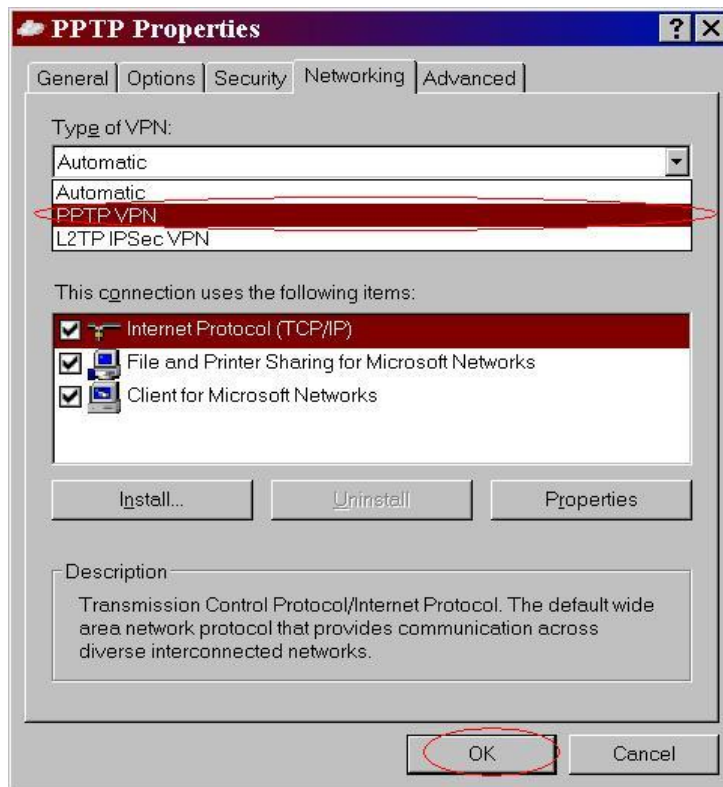
☒ Me only

☐ Anyone who uses this computer

Connect   Cancel   **Properties**   Help

This screenshot shows the 'Connect PPTP' window. The title bar reads 'Connect PPTP'. The main area features an illustration of two laptops connected by a globe. Below the illustration are two text boxes: 'User name:' containing 'PPTP user name' (circled in red) and 'Password:' containing a series of dots (circled in red). Below these is a checkbox labeled 'Save this user name and password for the following users:' with two radio button options: 'Me only' (selected) and 'Anyone who uses this computer'. At the bottom are four buttons: 'Connect', 'Cancel', 'Properties' (circled in red), and 'Help'.

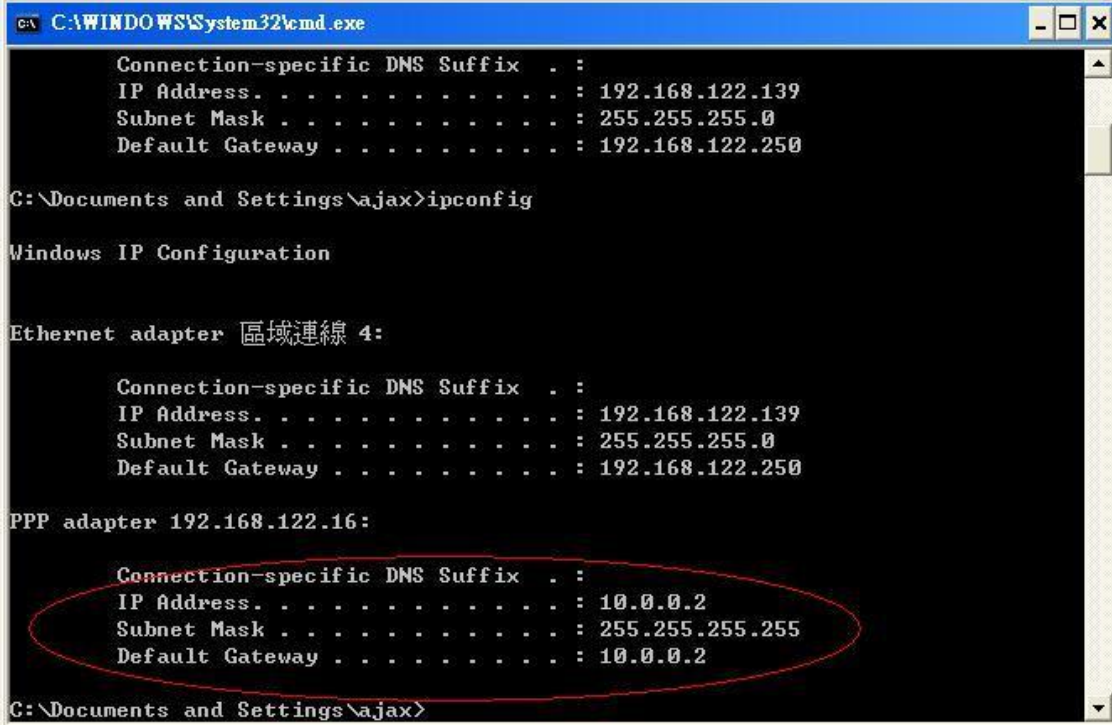
## 7. SELECT THE TYPE OF VPN



However, you should add the Authentication Protocol in advanced(Custom setting) of Security option, like below to support pap, chap, mschap.

If successfully, we will see:

This time, the client in the internet can ping any pcs in the lan(192.168.123.x)



```
C:\WINDOWS\System32\cmd.exe

Connection-specific DNS Suffix . : 
IP Address. . . . . : 192.168.122.139
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.122.250

C:\Documents and Settings\ajax>ipconfig

Windows IP Configuration

Ethernet adapter 區域連線 4:

    Connection-specific DNS Suffix  . : 
    IP Address. . . . . : 192.168.122.139
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.122.250

PPP adapter 192.168.122.16:

    Connection-specific DNS Suffix  . : 
    IP Address. . . . . : 10.0.0.2
    Subnet Mask . . . . . : 255.255.255.255
    Default Gateway . . . . . : 10.0.0.2

C:\Documents and Settings\ajax>
```

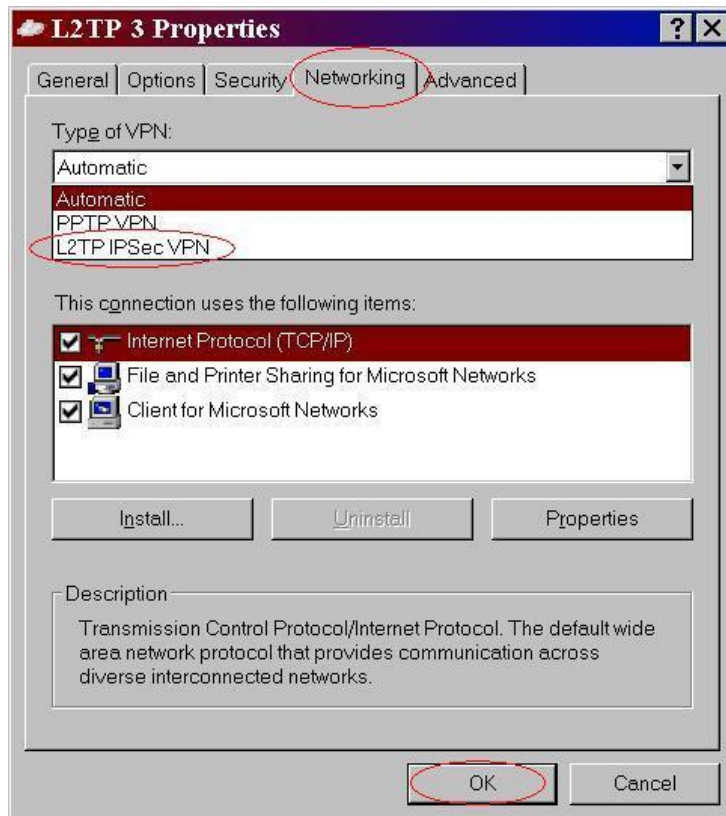
## L2TP

However, the router is the also vpn-l2tp server and supports three Authentication Protocols, PAP, CHAP and MSCAP.

And the settings are similar with PPTP. But MS-operating systems, like winxp win2000 will not find The type of vpn “L2tp”.We can use this files(disableipsec.zip) to enable it.

<http://support.iglou.com/fom-serve/cache/473.html>

Then We will see L2tp IPSEC VPN and choose it:



**THEN THE STEPS REFER TO PPTP SETTINGS.**

## **Appendix D   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 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), and then release the button. The RESTORE process is completed.