User’s Manual

Copyright

Trademarks

FCC Interference Statement

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

CE Declaration of Conformity

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

.

The specification is subject to change without notice.

Table of Contents

Chapter 1 Introduction

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

Functions and Features

Router Basic functions

- **Broadband modem and NAT Router**

  Connects multiple computers to a broadband (cable or DSL) modem or an Ethernet router to surf the Internet.
- **Auto-sensing Ethernet Switch**

  Equipped with a 4-port auto-sensing Ethernet switch.
- **Printer sharing**

  Embedded a print server to allow all of the networked computers to share one printer.

  Built-in USB (parallel) host to connect to USB (parallel) printer for printer sharing
- **WAN type supported**

  The router supports some WAN types, Static, Dynamic, PPPOE, PPTP, and Dynamic IP with Road Runner.
- **Firewall**

  All unwanted packets from outside intruders are blocked to protect your Intranet.
- **DHCP server supported**

  All of the networked computers can retrieve TCP/IP settings automatically from this product.
- **Web-based configuring**

  Configurable through any networked computer’s web browser using Netscape or Internet Explorer.
- **Virtual Server supported**

  Enables you to expose WWW, FTP and other services on your LAN to be accessible to Internet users.
- **User-Definable Application Sensing Tunnel**

  User can define the attributes to support the special applications requiring multiple connections, like Internet gaming, video conferencing, Internet telephony and so on, then this product can sense the application type and open multi-port tunnel for it.
- **DMZ Host supported**

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

- **Statistics of WAN Supported**

  Enables you to monitor inbound and outbound packets

Security functions

- **Packet filter supported**

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

  Let you prevent users under this device from accessing specific URLs.
- **URL Blocking Supported**

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

  The router has three VPN servers, IPSEC (Dynamic VPN), PPTP, and L2TP.
- **VPN Pass-through**

  The router also supports VPN pass-through.
- **SPI Mode Supported**

  When SPI Mode is enabled, the router will check every incoming packet to detect if this packet is valid.
- **DoS Attack Detection Supported**

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

Advanced functions

- **System time Supported**

  Allow you to synchronize system time with network timeserver.
- **E-mail Alert Supported**

  The router can send its info by mail.
- **Dynamic dns Supported**

  At present,the router has 3 ddns.dyndns,TZO.com and dhs.org.
- **SNMP Supported**

  Because SNMP this function has many versions, anyway, the router supports V1 and V2c.
- **Routing Table Supported**

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

- **Schedule Rule supported**

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

Other functions

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

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

Packing List

- Broadband router unit
- Installation CD-ROM
- Power adapter
- CAT-5 UTP Fast Ethernet cable

Chapter 2 Hardware Installation

2.1 Panel Layout

2.1.1. Front Panel

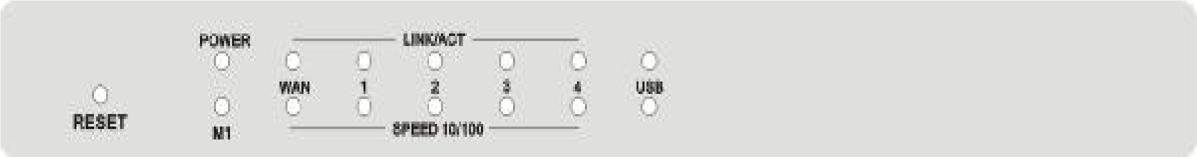


Figure 2-1 Front Panel

LED:

LED	Function	Color	Status	Description
POWER	Power indication	Green	On	Power is being applied to this product.
M1	System status 1	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	M1	Green	Flashing	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 port is linked.
			Blinking	The USB port is sending or receiving data.

※For details, please refer to Appendix D FAQ and Troubleshooting.

2.1.2. Rear Panel

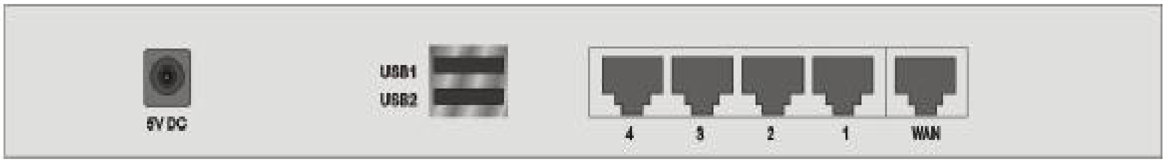


Figure 2-2 Rear Panel

Ports:

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

All technical and physical specifications are subject to changes without any prior notification. The manufacturer reserves the right to alter the product appearance from that picture.

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.

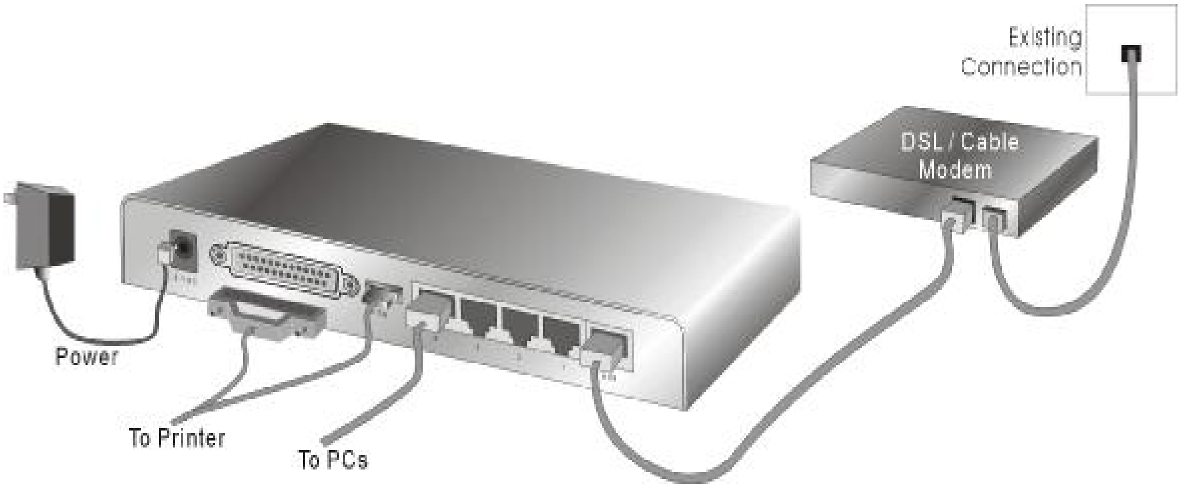


Figure 2-3 Setup of LAN and WAN connections for this product.

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 (optional)

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

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 M1 will be lighted ON for about 10 seconds, and then M1 will be flashed 3 times to indicate that the self-test operation has finished. Finally, the M1 will be continuously flashed once per second to indicate that this product is in normal operation.

Chapter 3 Network Settings and Software Installation

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

3.1 Make Correct Network Settings of Your Computer

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

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

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

```
ping 192.168.123.254
```

If the following messages appear:

```
Pinging 192.168.123.254 with 32 bytes of data:
Reply from 192.168.123.254: bytes=32 time=2ms TTL=64
```

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

```
Pinging 192.168.123.254 with 32 bytes of data:
Request timed out.
```

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

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

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

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

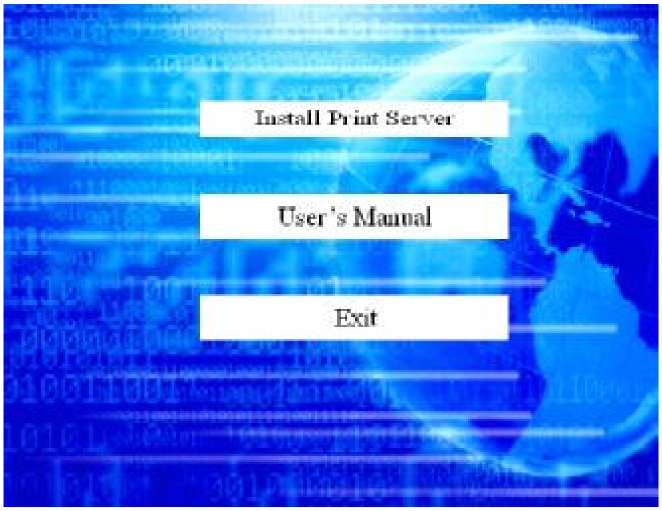
   Tip: If the IP address of this product is 192.168.123.254, the IP address of your computer must be 192.168.123.X and default gateway must be 192.168.123.254.

3.2 Install the Software into Your Computers

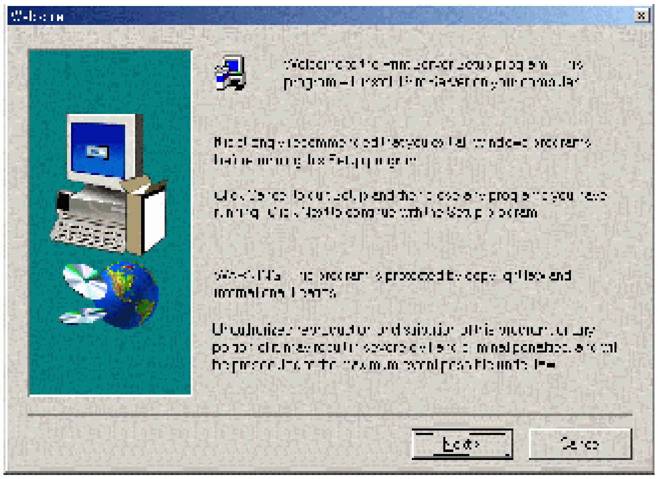
Skip this section if you do not want to use the print server function of this product.

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

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



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



Welcome to the Print Server Setup program. This program will install Print Server on your computer.

It is strongly recommended that you exit all Windows programs before running this Setup program.

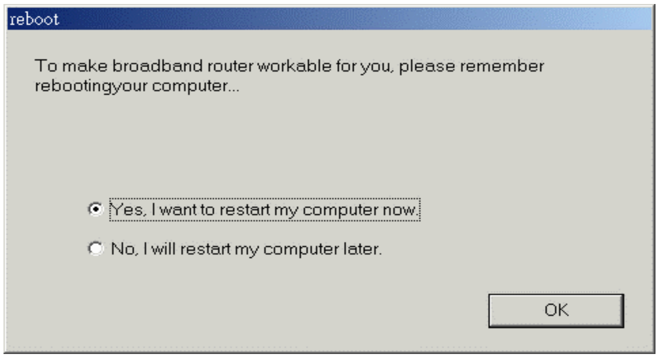
Click Cancel to quit Setup and then close any programs you have running. Click Next to continue with the Setup program.

WARNING: This program is protected by copyright law and international treaties.

Unauthorized reproduction or distribution of this program, or any portion of it, may result in severe civil and criminal penalties, and will be prosecuted to the maximum extent possible under law.

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.



reboot

To make broadband router workable for you, please remember rebootingyour computer...

● Yes, I want to restart my computer now.

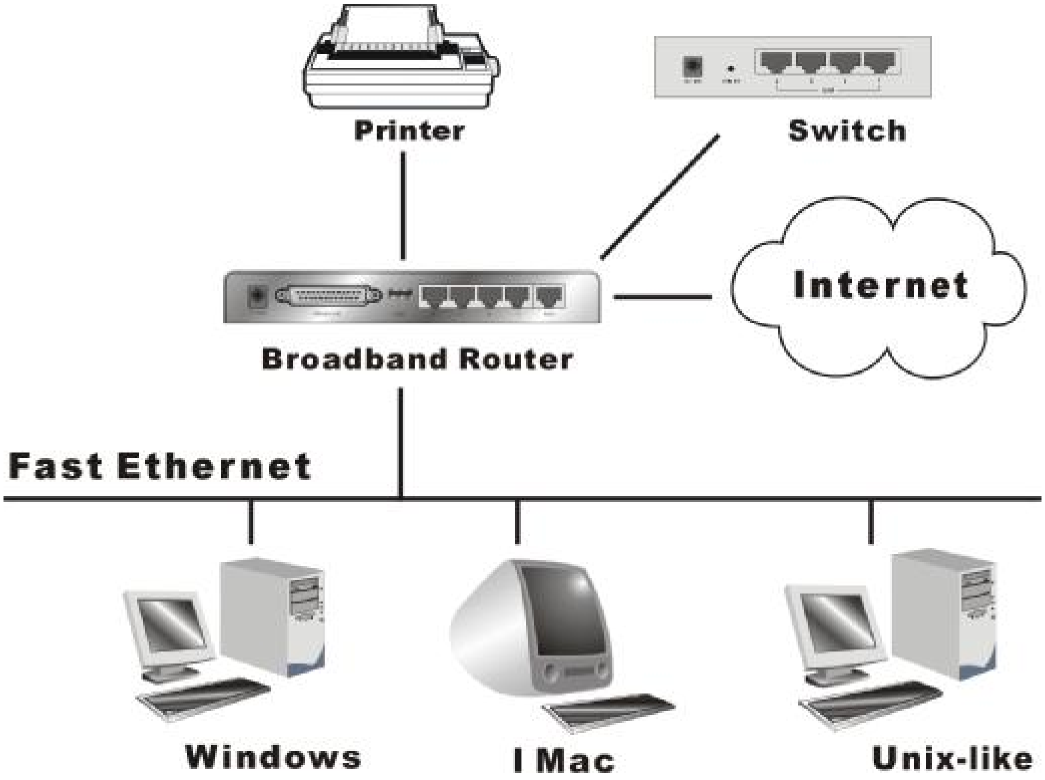
○ No, I will restart my computer later.

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

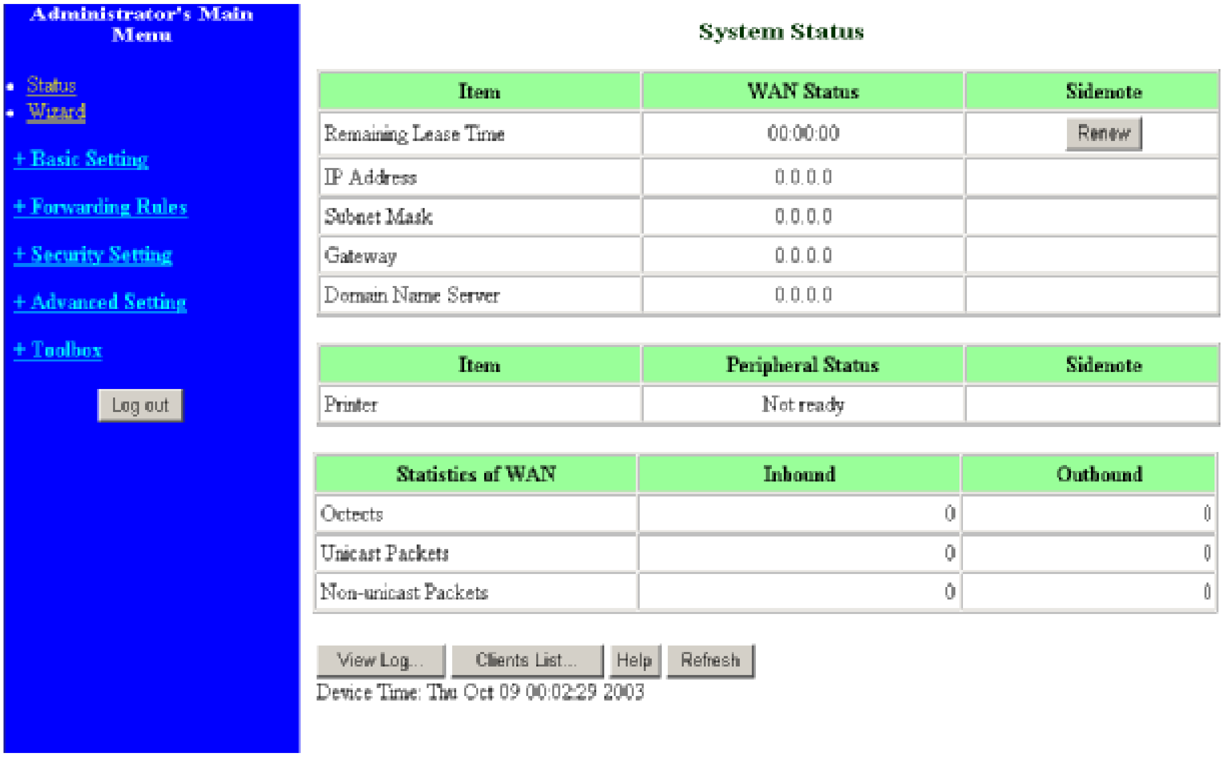
Now, you can configure the NAT Router (refer to Chapter 4) and setup the Print Server (refer to Chapter 5).

Chapter 4 Configuring 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



System Status

Item	WAN Status	Sidenote
Remaining Lease Time	00:00:00	Renew
IP Address	0.0.0.0	
Subnet Mask	0.0.0.0	
Gateway	0.0.0.0	
Domain Name Server	0.0.0.0	

Item	Peripheral Status	Sidenote
Printer	Not ready	

Statistics of WAN	Inbound	Outbound
Octects	0	0
Unicast Packets	0	0
Non-unicast Packets	0	0

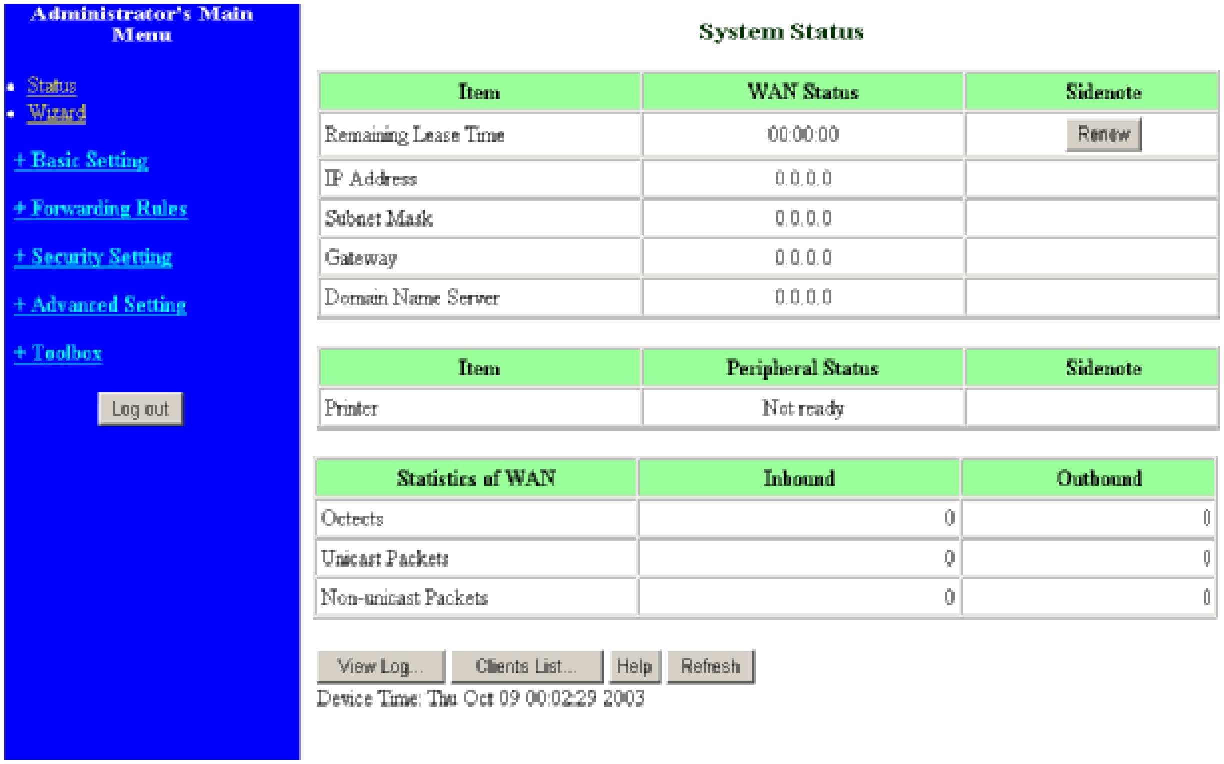
Device Time: Thu Oct 09 00:02:29 2003

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

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

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

4.2 Status



System Status

Item	WAN Status	Sidenote
Remaining Lease Time	00:00:00	Renew
IP Address	0.0.0.0	
Subnet Mask	0.0.0.0	
Gateway	0.0.0.0	
Domain Name Server	0.0.0.0	

Item	Peripheral Status	Sidenote
Printer	Not ready	

Statistics of WAN	Inbound	Outbound
Octects	0	0
Unicast Packets	0	0
Non-unicast Packets	0	0

Device Time: Thu Oct 09 00:02:29 2003

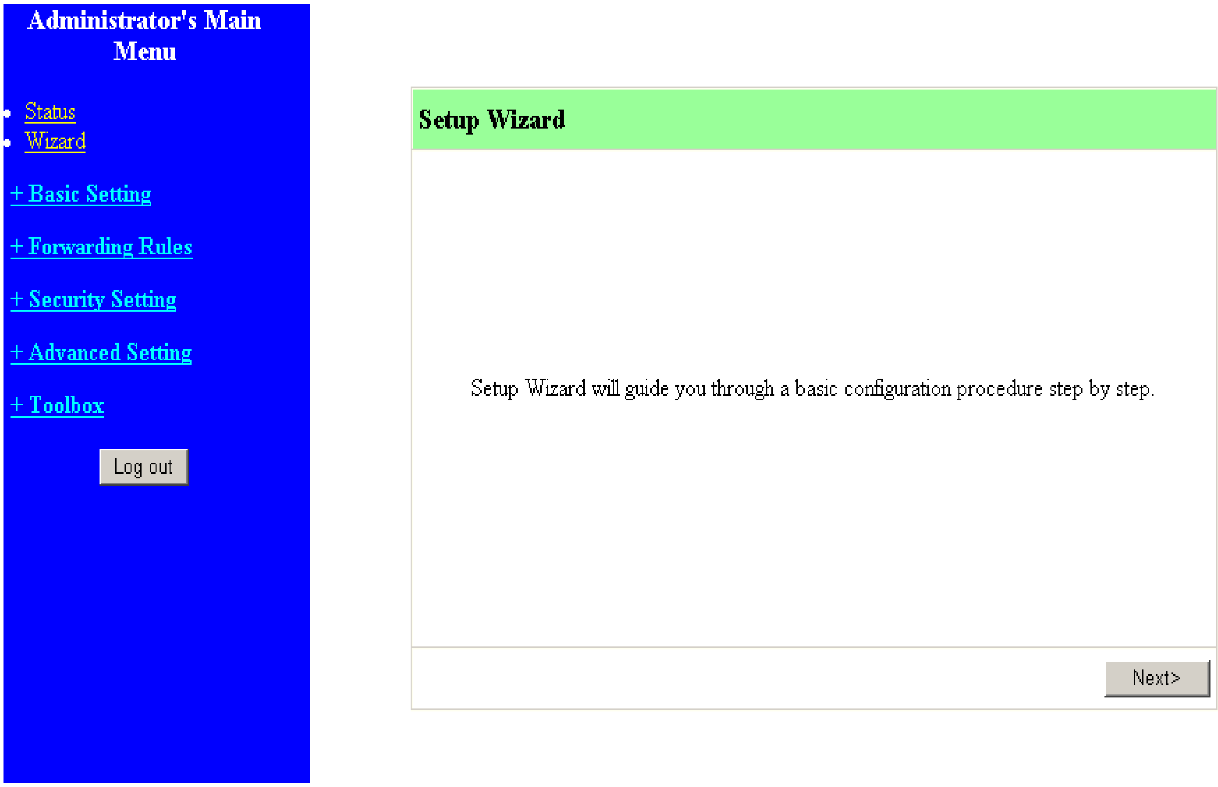
This option provides the function for observing this product's working status:

A. WAN Port Status.

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

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

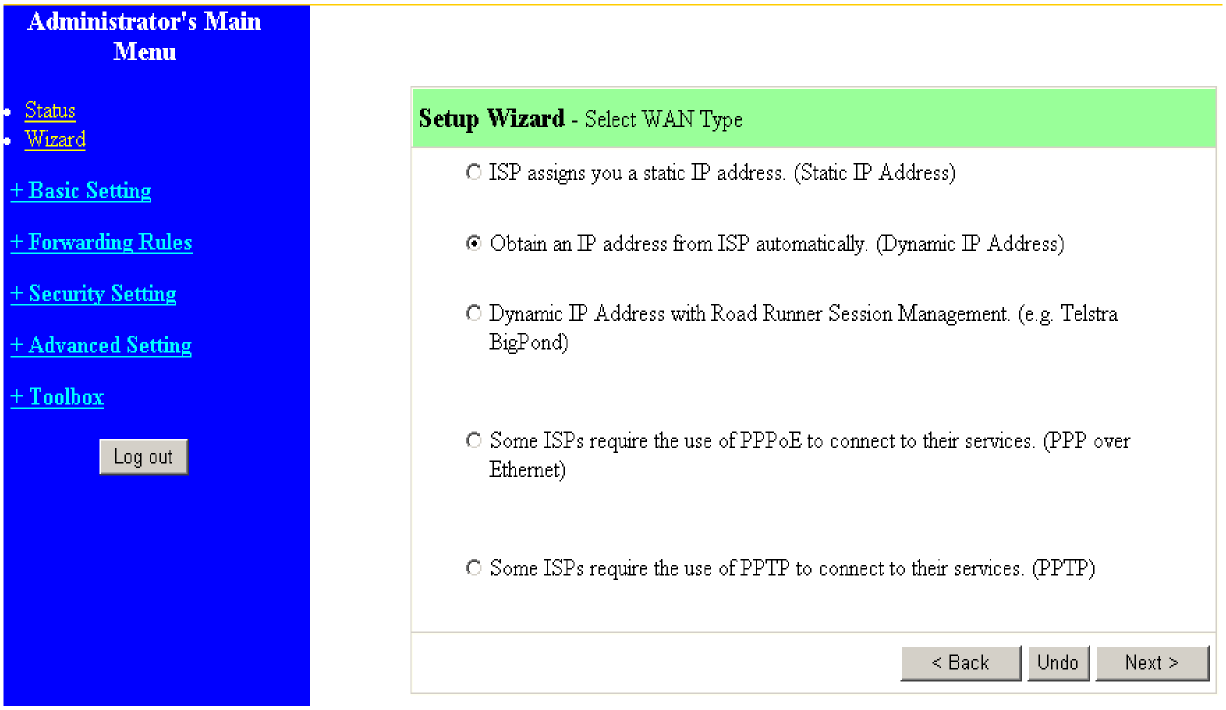
4.3 Wizard



Setup Wizard

Setup Wizard will guide you through a basic configuration procedure step by step.

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



Setup Wizard - Select WAN Type

○ ISP assigns you a static IP address. (Static IP Address)

● Obtain an IP address from ISP automatically. (Dynamic IP Address)

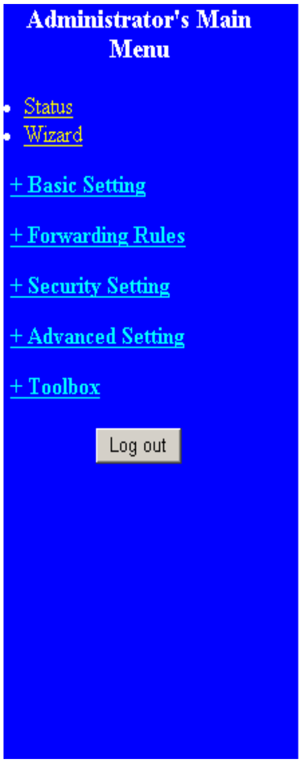
○ Dynamic IP Address with Road Runner Session Management. (e.g. Telstra BigPond)

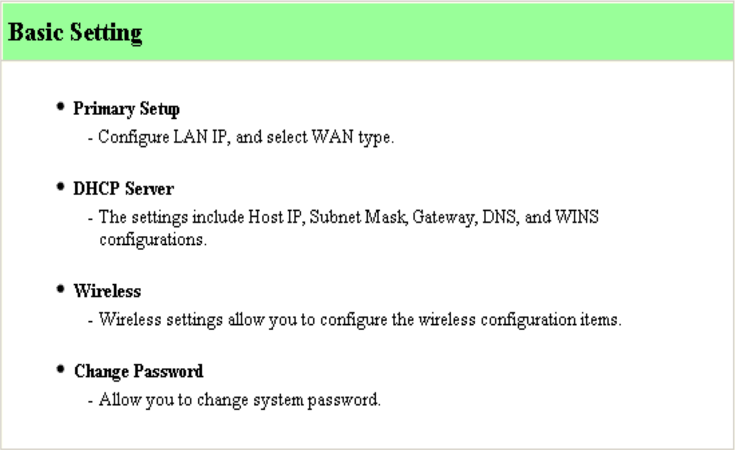
○ Some ISPs require the use of PPPoE to connect to their services. (PPP over Ethernet)

○ Some ISPs require the use of PPTP to connect to their services. (PPTP)

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

4.4 Basic Setting

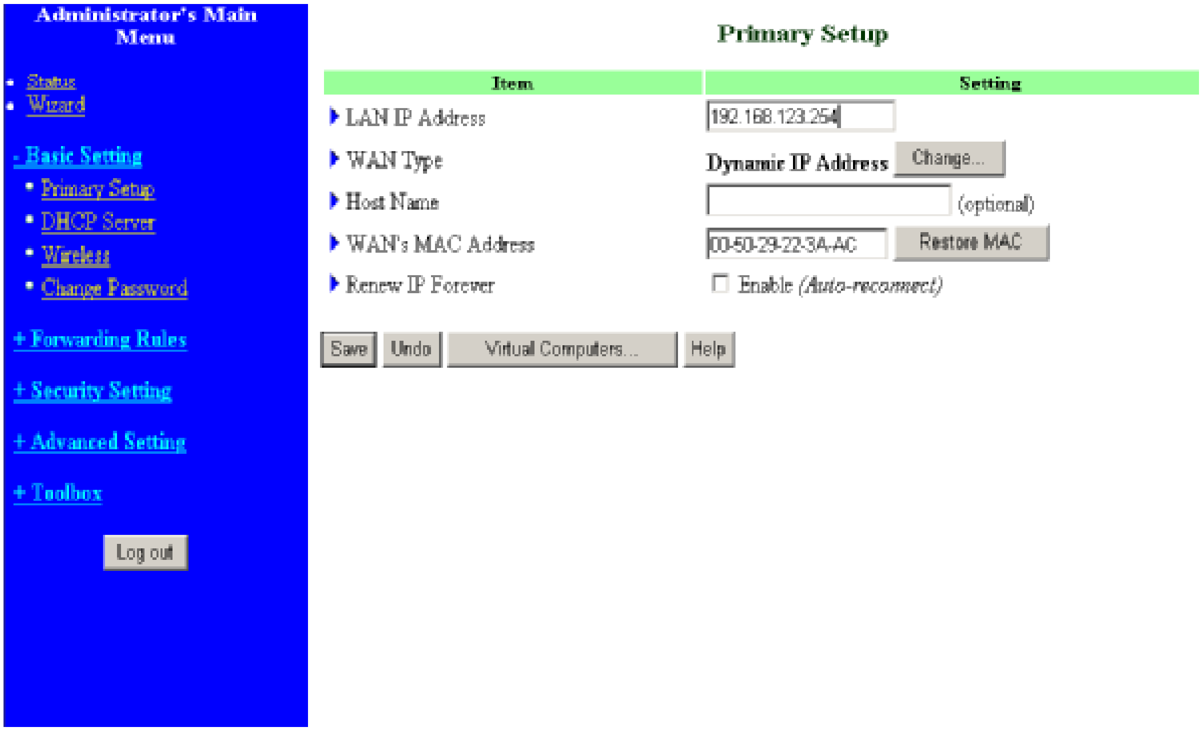




Basic Setting

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

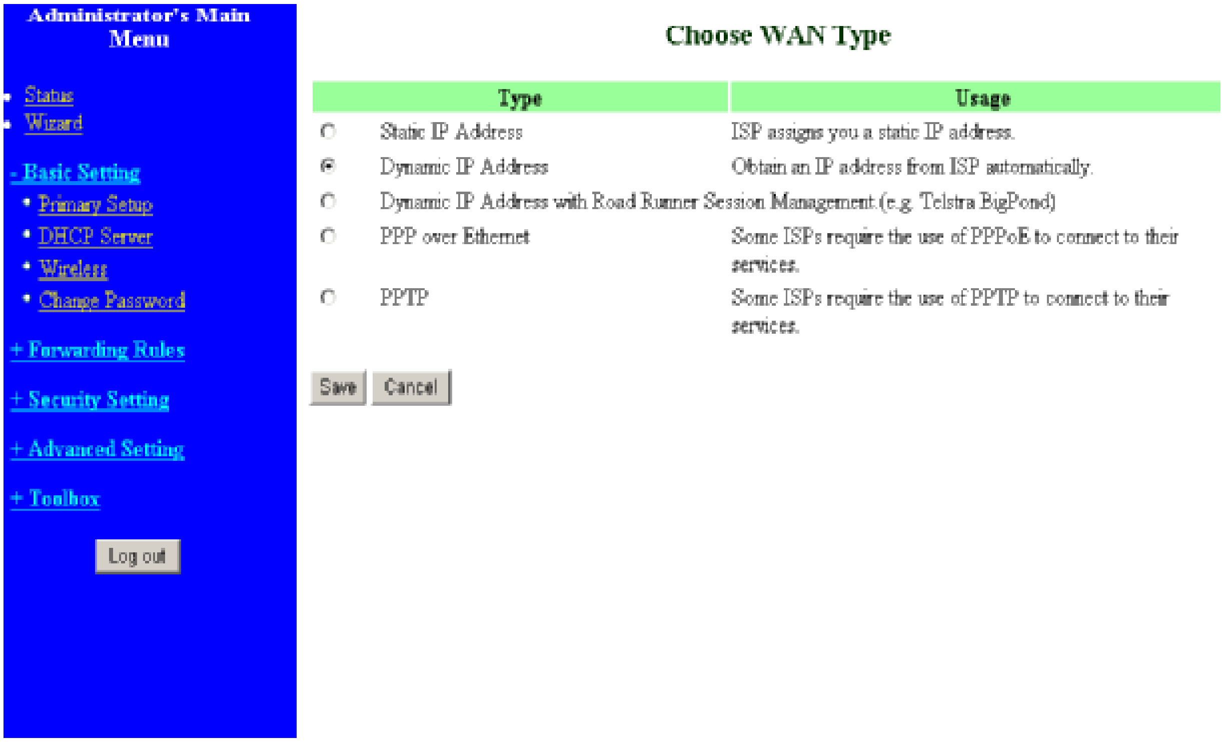
4.4.1 Primary Setup – WAN Type, Virtual Computers



Primary Setup

Item	Setting
LAN IP Address	192.168.123.254
WAN Type	Dynamic IP Address Change...
Host Name	(optional)
WAN's MAC Address	00-50-29-22-3A-AC Restore MAC
Renew IP Forever	□ Enable *(Auto-reconnect)*

Press **“Change”**



Choose WAN Type

Type	Usage
○ Static IP Address	ISP assigns you a static IP address.
● Dynamic IP Address	Obtain an IP address from ISP automatically.
○ Dynamic IP Address with Road Runner Session Management.(e.g. Telstra BigPond)	
○ PPP over Ethernet	Some ISPs require the use of PPPoE to connect to their services.
○ PPTP	Some ISPs require the use of PPTP to connect to their services.

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 renews 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. **Maximum Transmission Unit (MTU)**: Most ISP offers MTU value to users. The most common

MTU value is 1492.

4.4.1.5 PPTP

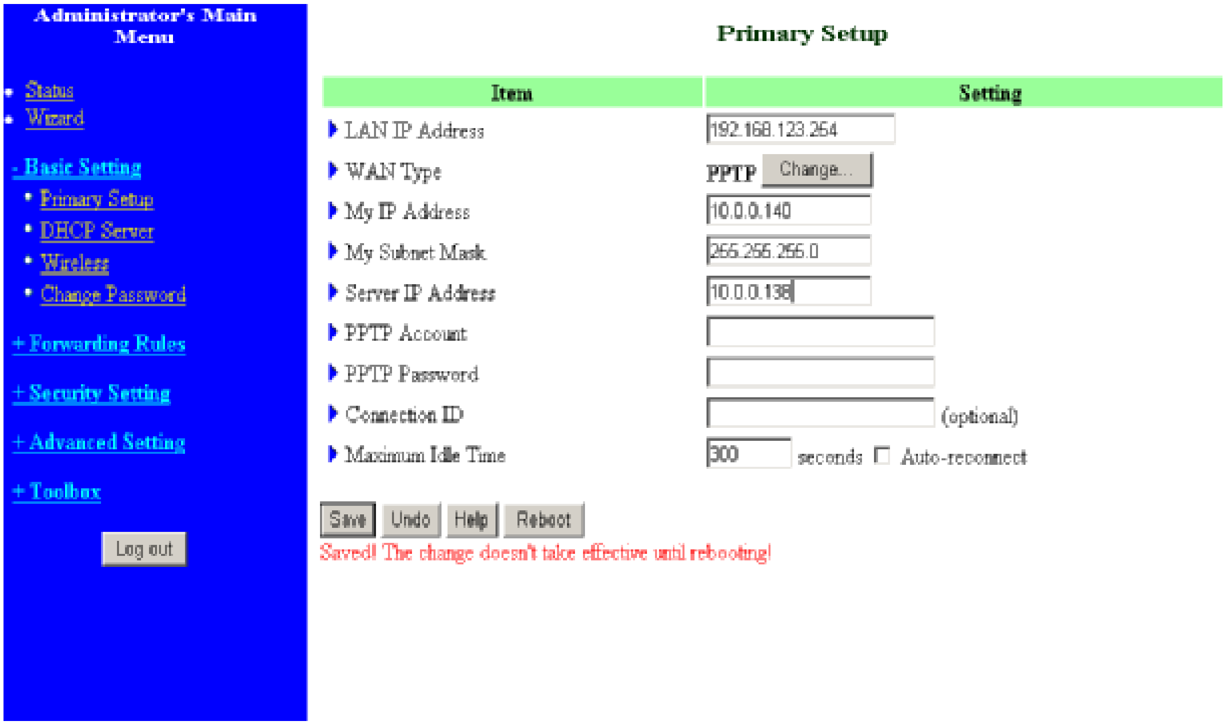
1. My IP Address and My Subnet Mask: the private IP address and subnet mask your ISP assigned to you.

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.

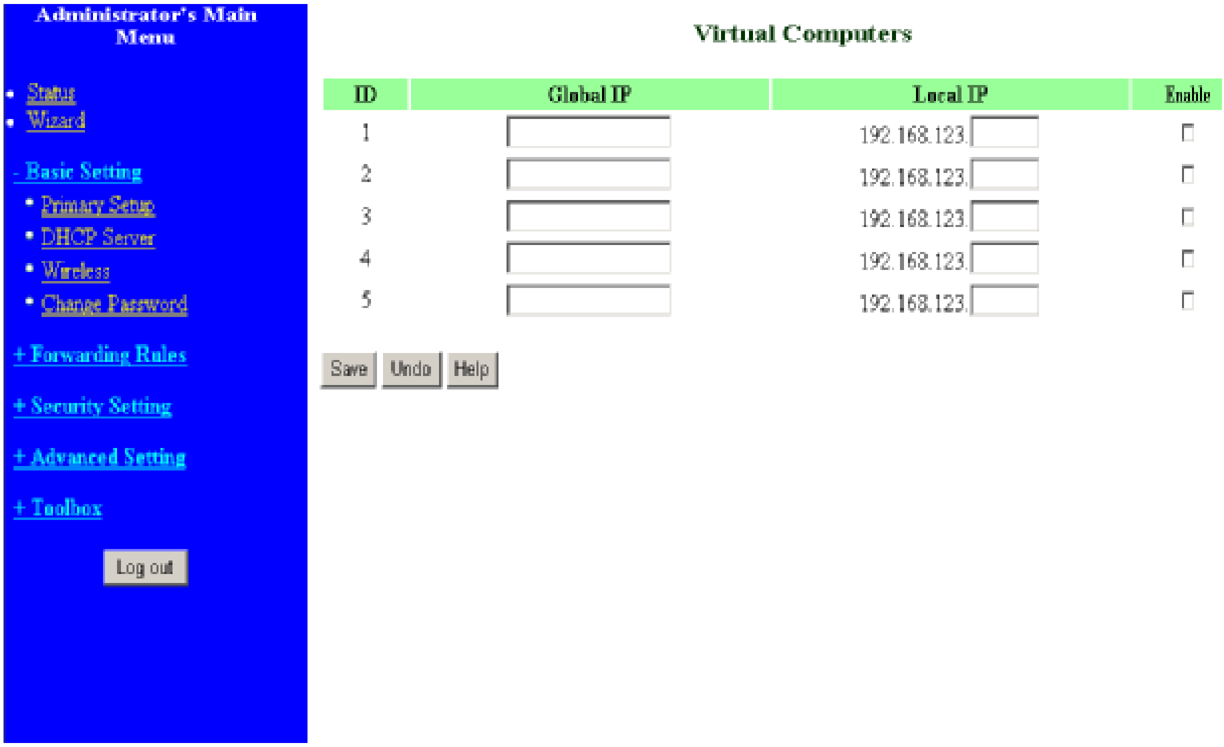


Primary Setup

Item	Setting
LAN IP Address	192.168.123.254
WAN Type	PPTP Change...
My IP Address	10.0.0.140
My Subnet Mask	255.255.255.0
Server IP Address	10.0.0.138
PPTP Account	
PPTP Password	
Connection ID	(optional)
Maximum Idle Time	300 seconds □ Auto-reconnect

Saved! The change doesn't take effective until rebooting!

4.4.1.6 Virtual Computers



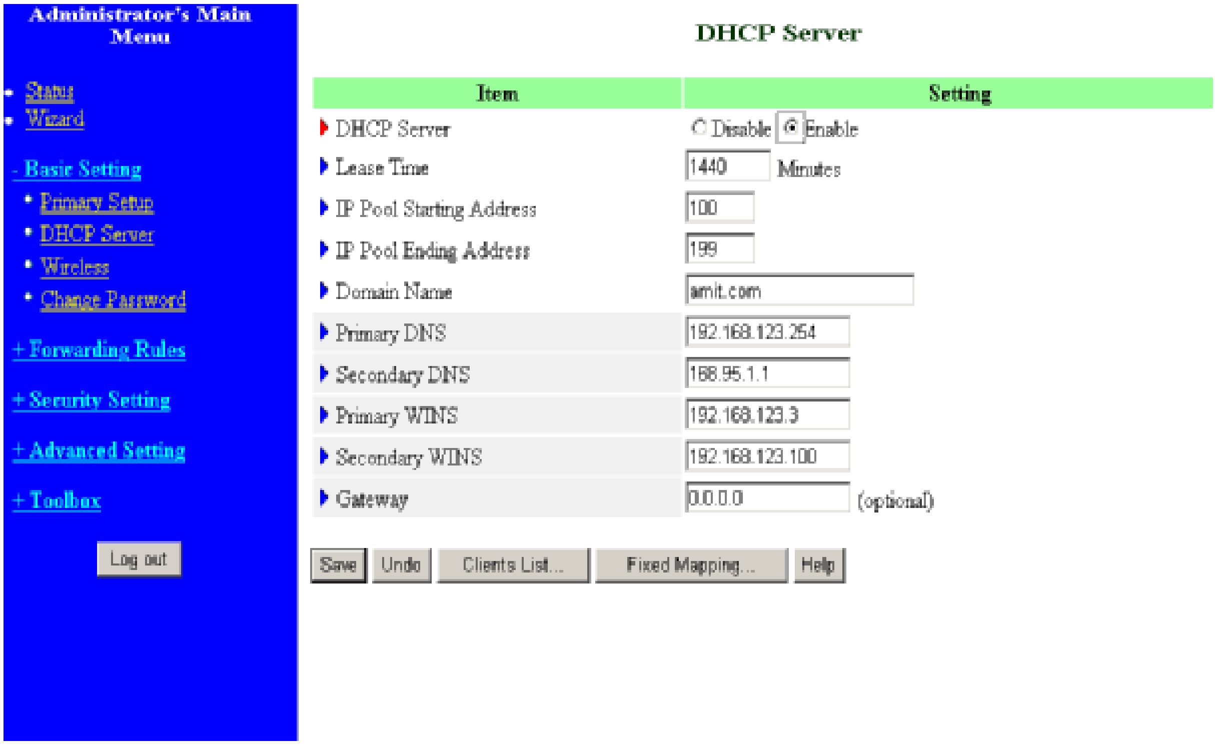
Virtual Computers

ID	Global IP	Local IP	Enable
1		192.168.123.	☐
2		192.168.123.	☐
3		192.168.123.	☐
4		192.168.123.	☐
5		192.168.123.	☐

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



DHCP Server

Item	Setting
DHCP Server	○ Disable ● Enable
Lease Time	1440 Minutes
IP Pool Starting Address	100
IP Pool Ending Address	199
Domain Name	amit.com
Primary DNS	192.168.123.254
Secondary DNS	168.95.1.1
Primary WINS	192.168.123.3
Secondary WINS	192.168.123.100
Gateway	0.0.0.0 (optional)

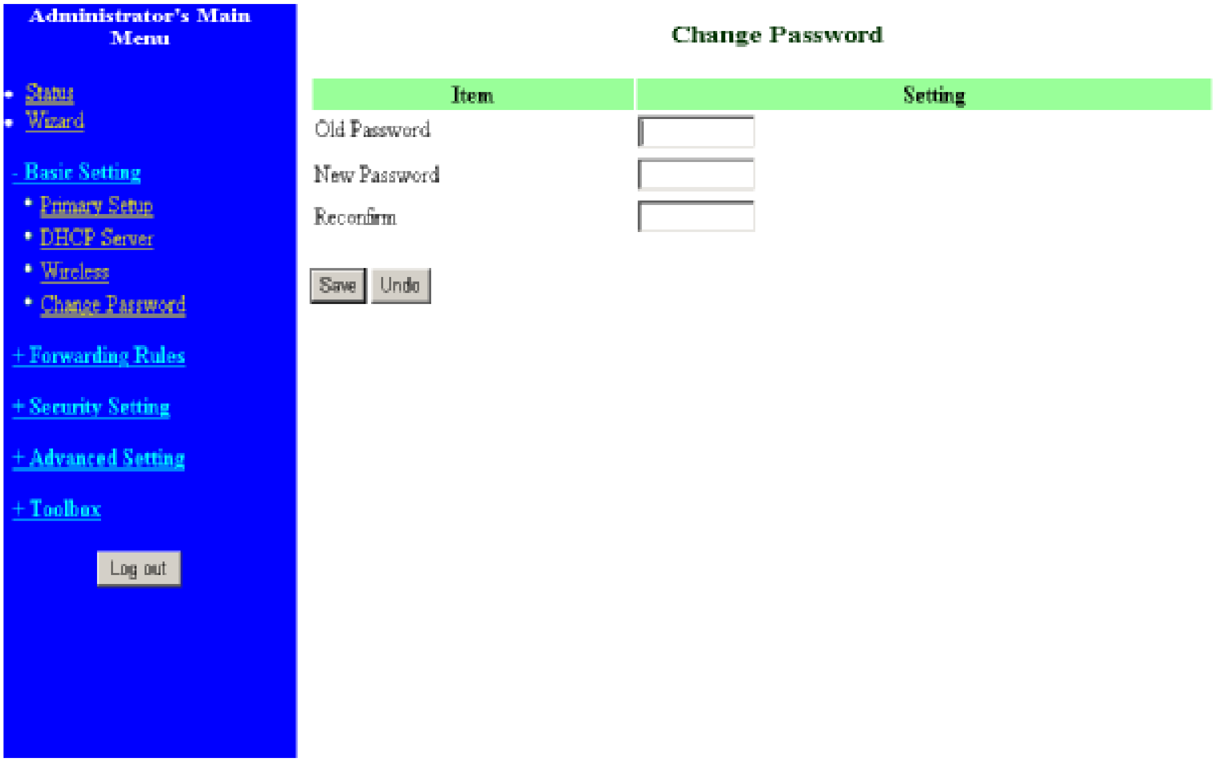
Press **"More>>"**

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

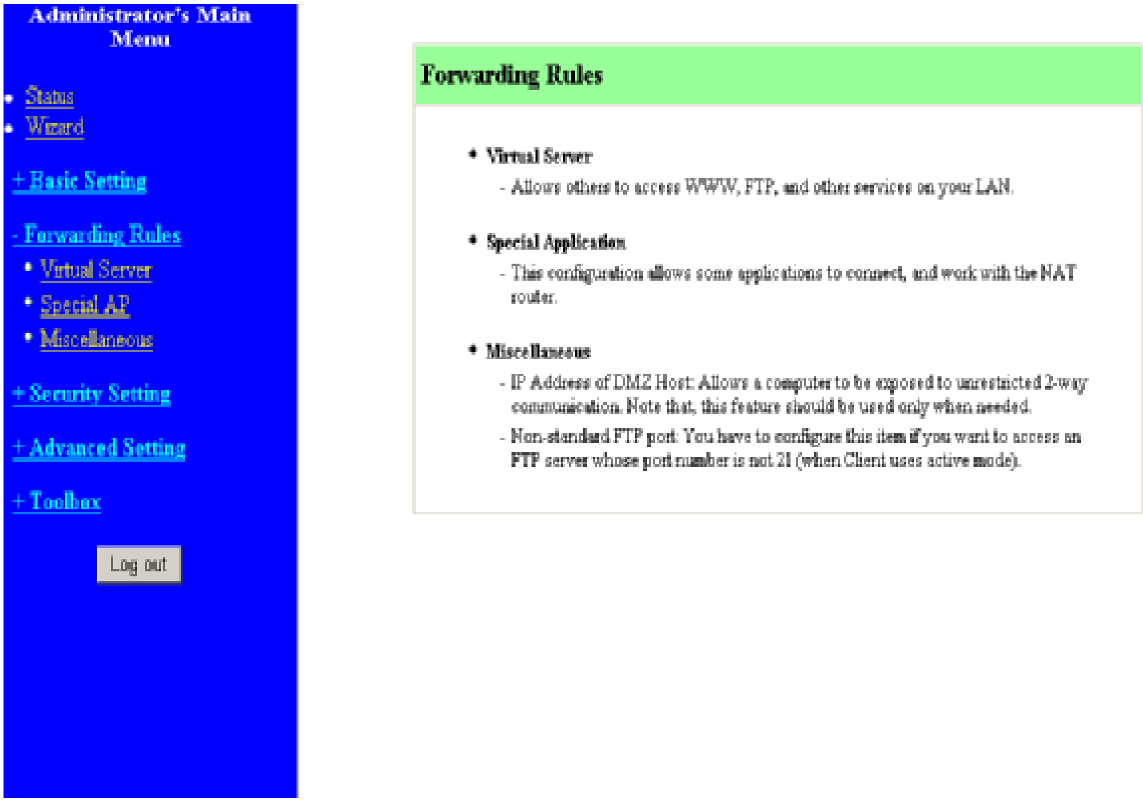


Change Password

Item	Setting
Old Password	
New Password	
Reconfirm	

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

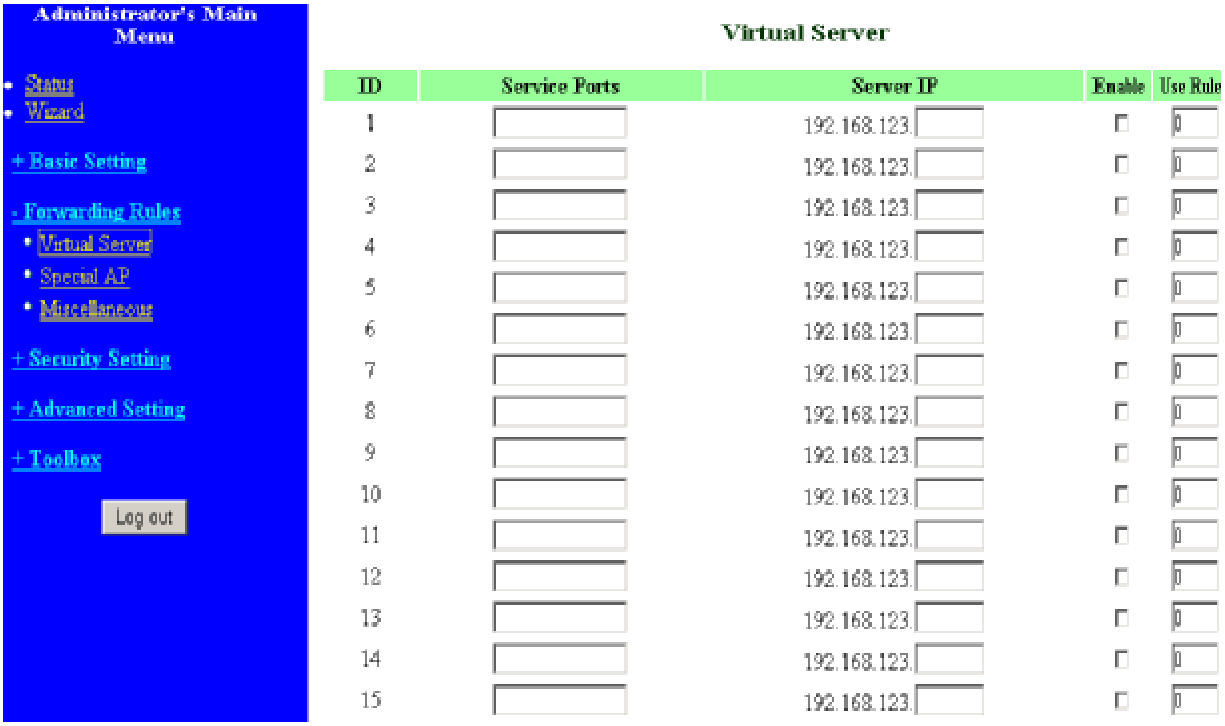
4.5 Forwarding Rules



Forwarding Rules

- **Virtual Server**
  - Allows others to access WWW, FTP, and other services on your LAN.
- **Special Application**
  - This configuration allows some applications to connect, and work with the NAT router.
- **Miscellaneous**
  - IP Address of DMZ Host: Allows a computer to be exposed to unrestricted 2-way communication. Note that, this feature should be used only when needed.
  - Non-standard FTP port: You have to configure this item if you want to access an FTP server whose port number is not 21 (when Client uses active mode).

4.5.1 Virtual Server



Virtual Server

ID	Service Ports	Server IP	Enable	Use Rule
1		192.168.123.	☐	0
2		192.168.123.	☐	0
3		192.168.123.	☐	0
4		192.168.123.	☐	0
5		192.168.123.	☐	0
6		192.168.123.	☐	0
7		192.168.123.	☐	0
8		192.168.123.	☐	0
9		192.168.123.	☐	0
10		192.168.123.	☐	0
11		192.168.123.	☐	0
12		192.168.123.	☐	0
13		192.168.123.	☐	0
14		192.168.123.	☐	0
15		192.168.123.	☐	0

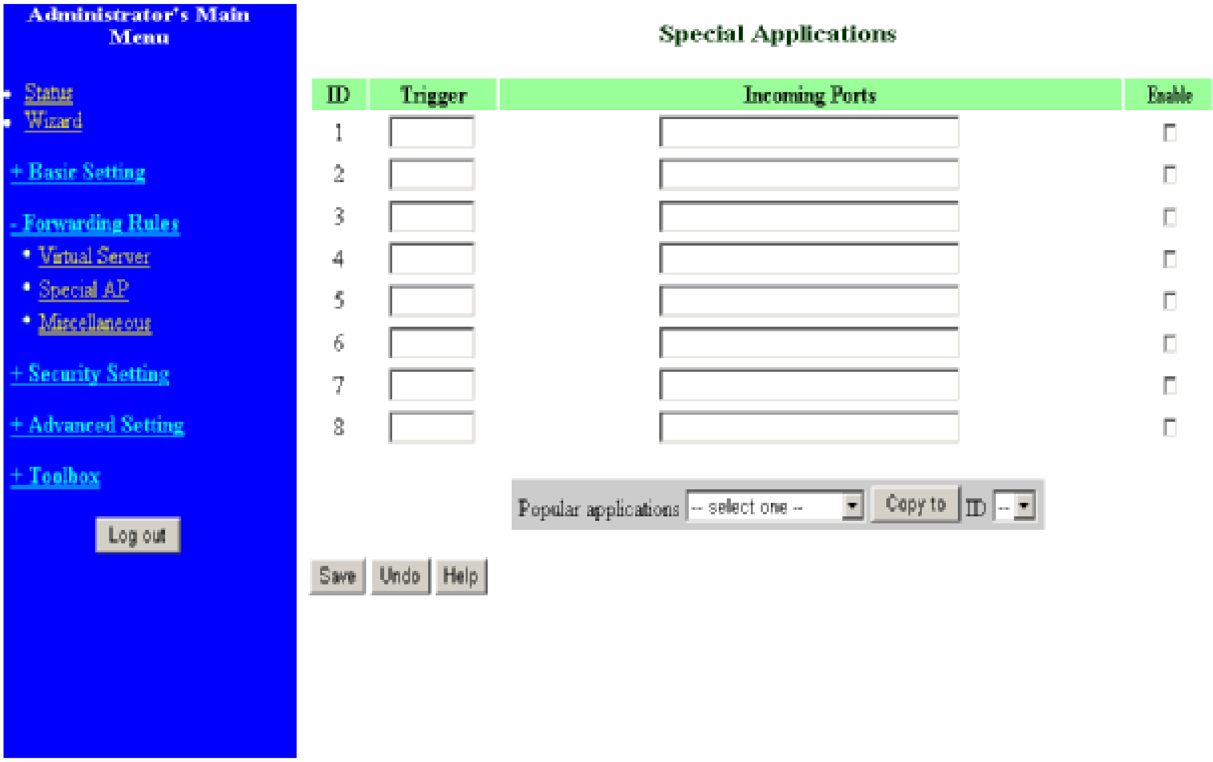
This product's NAT firewall filters out unrecognized packets to protect your Intranet, so all hosts behind this product are invisible to the outside world. If you wish, you can make some of them accessible by enabling the Virtual Server Mapping.

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



Special Applications

ID	Trigger	Incoming Ports	Enable
1			□
2			□
3			□
4			□
5			□
6			□
7			□
8			□

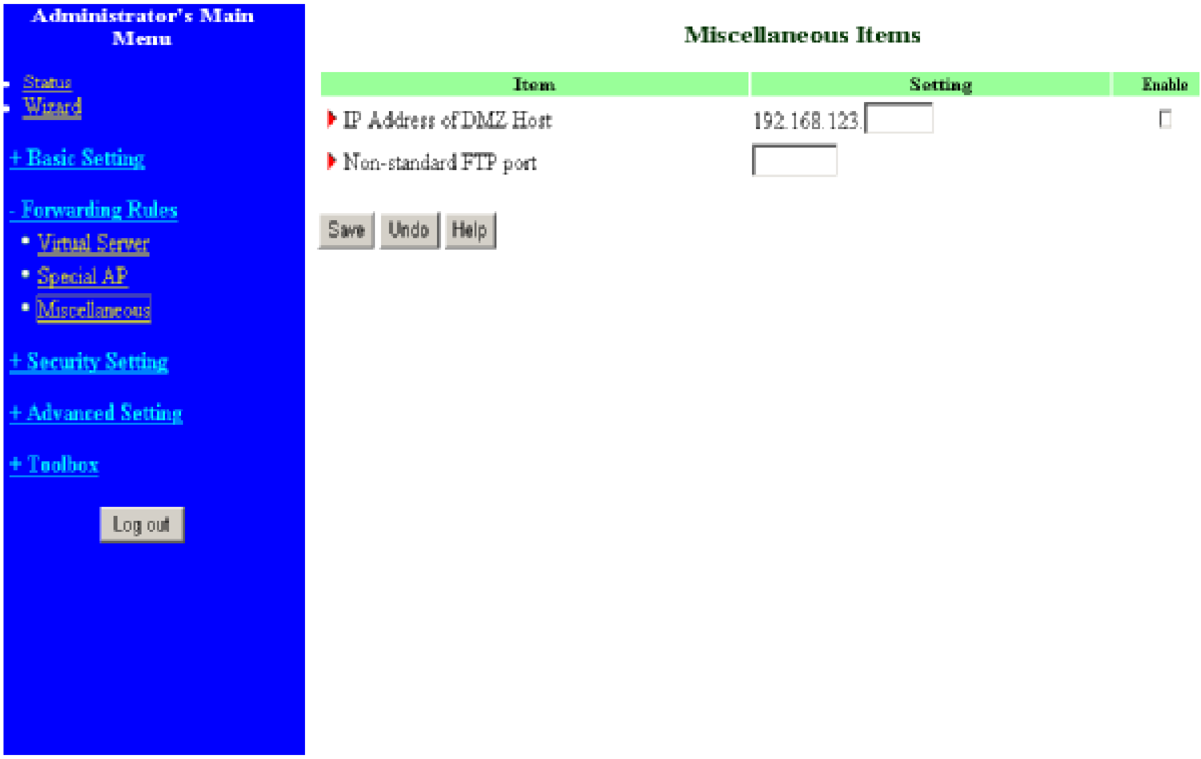
Some applications require multiple connections, like Internet games, Video conferencing, Internet telephony, etc. Because of the firewall function, these applications cannot work with a pure NAT router. The **Special Applications** feature allows some of these applications to work with this product.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



Miscellaneous Items

Item	Setting	Enable
IP Address of DMZ Host	192.168.123.	□
Non-standard FTP port		

IP Address of DMZ Host

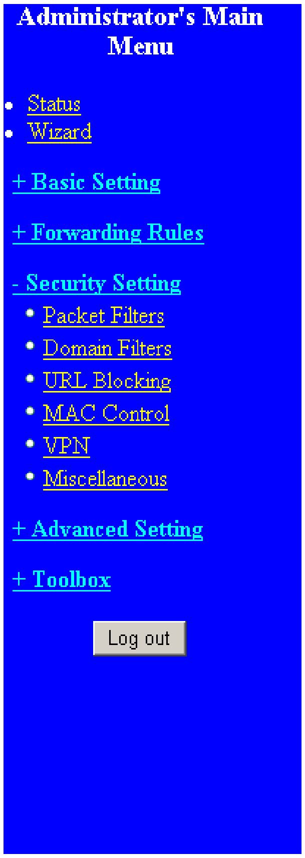
DMZ (DeMilitarized Zone) Host is a host without the protection of firewall. It allows a computer to be exposed to unrestricted 2-way communication for Internet games, Video conferencing, Internet telephony and other special applications.

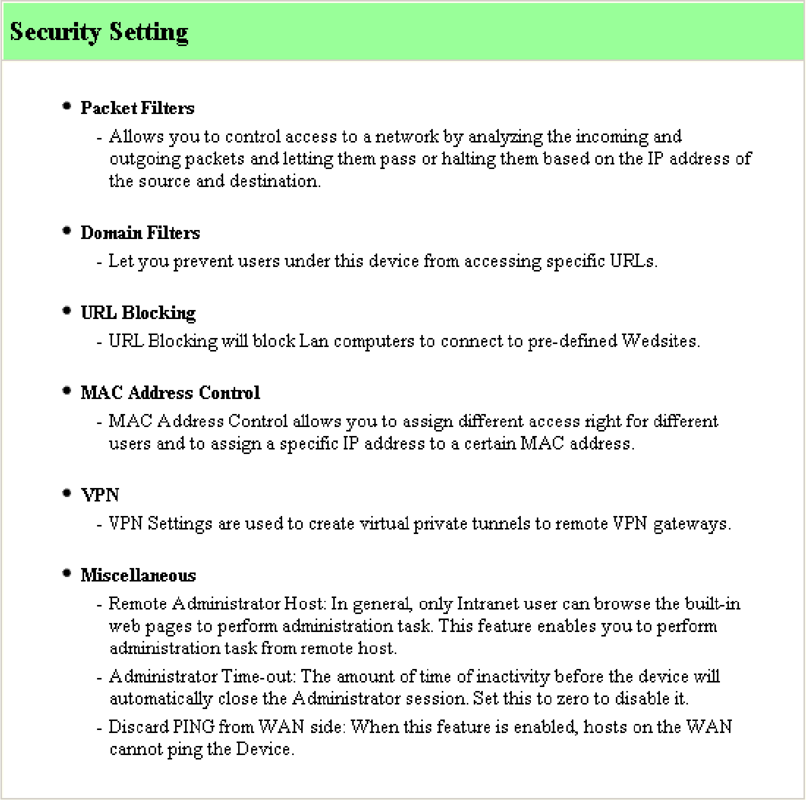
NOTE: This feature should be used only when needed.

Non-standard FTP port

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

4.6 Security Settings

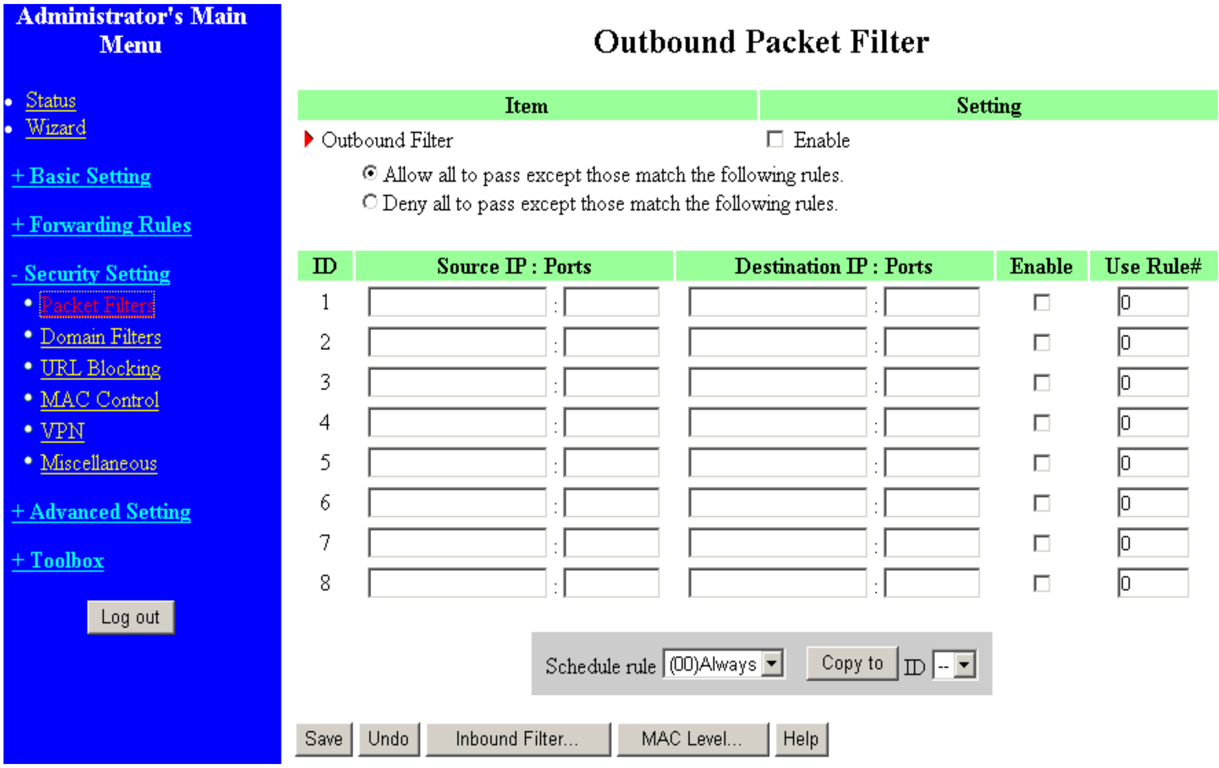




Security Setting

- **Packet Filters**
  - Allows you to control access to a network by analyzing the incoming and outgoing packets and letting them pass or halting them based on the IP address of the source and destination.
- **Domain Filters**
  - Let you prevent users under this device from accessing specific URLs.
- **URL Blocking**
  - URL Blocking will block Lan computers to connect to pre-defined Wedsites.
- **MAC Address Control**
  - MAC Address Control allows you to assign different access right for different users and to assign a specific IP address to a certain MAC address.
- **VPN**
  - VPN Settings are used to create virtual private tunnels to remote VPN gateways.
- **Miscellaneous**
  - Remote Administrator Host: In general, only Intranet user can browse the built-in web pages to perform administration task. This feature enables you to perform administration task from remote host.
  - Administrator Time-out: The amount of time of inactivity before the device will automatically close the Administrator session. Set this to zero to disable it.
  - Discard PING from WAN side: When this feature is enabled, hosts on the WAN cannot ping the Device.

4.6.1 Packet Filter



Outbound Packet Filter

Item	Setting
Outbound Filter	□ Enable

● Allow all to pass except those match the following rules.
○ Deny all to pass except those match the following rules.

ID	Source IP : Ports	Destination IP : Ports	Enable	Use Rule#
1	:	:	□	0
2	:	:	□	0
3	:	:	□	0
4	:	:	□	0
5	:	:	□	0
6	:	:	□	0
7	:	:	□	0
8	:	:	□	0

Schedule rule (00)Always Copy to ID --

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**.

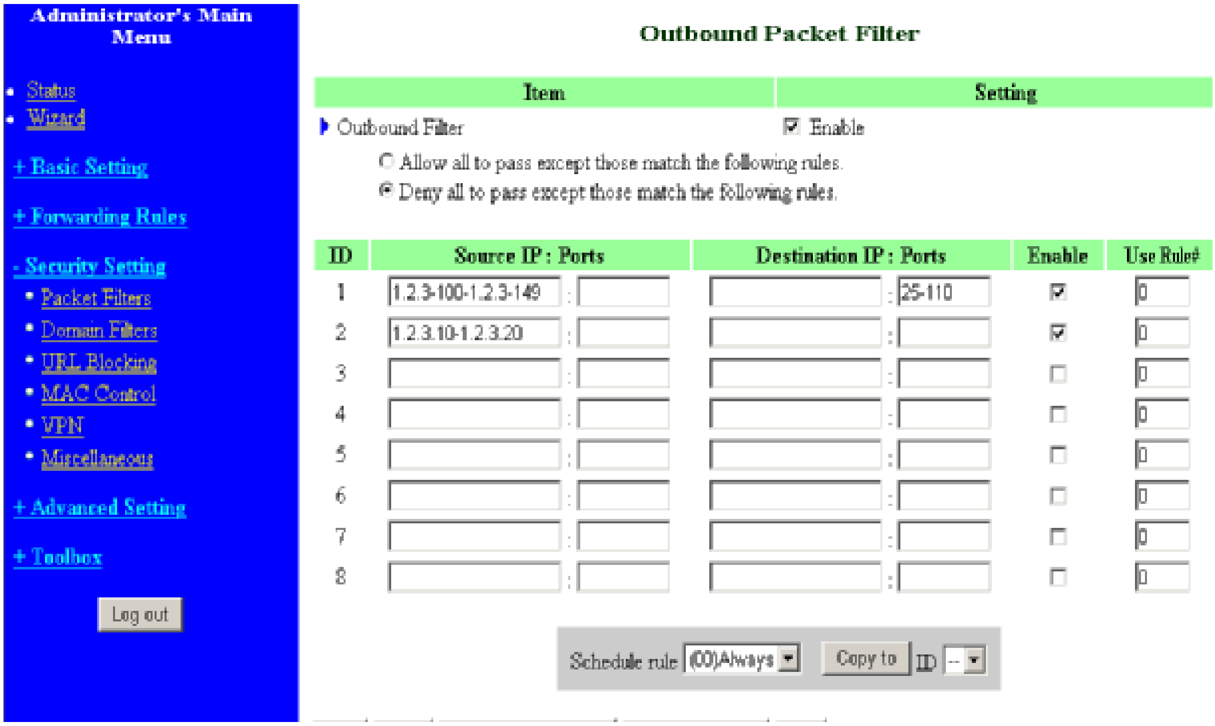
Each rule can be enabled or disabled individually.

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:



Outbound Packet Filter

Item	Setting
Outbound Filter	☑ Enable

○ Allow all to pass except those match the following rules.
● Deny all to pass except those match the following rules.

ID	Source IP : Ports		Destination IP : Ports		Enable	Use Rule#
1	1.2.3-100-1.2.3-149			25-110	☑	0
2	1.2.3.10-1.2.3.20				☑	0
3					□	0
4					□	0
5					□	0
6					□	0
7					□	0
8					□	0

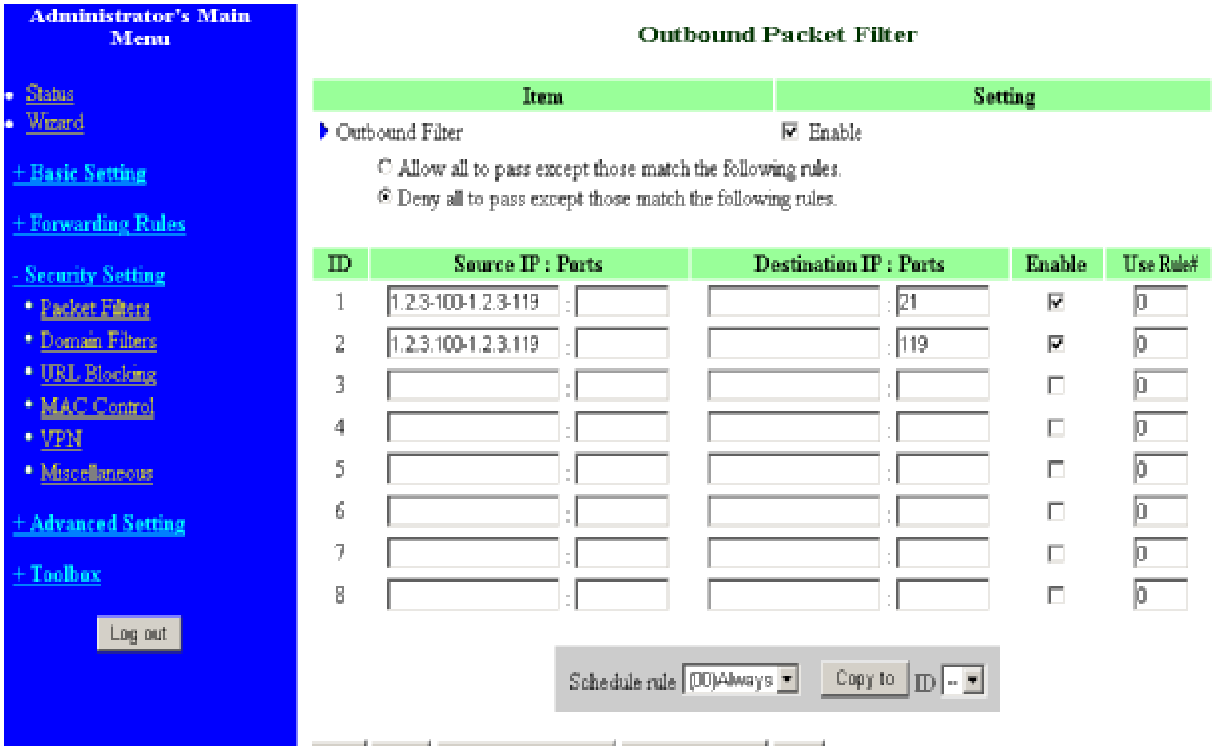
Schedule rule (00)Always ▾ Copy to ID -- ▾

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

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

Others are all blocked.

Example 2:



Outbound Packet Filter

Item	Setting
Outbound Filter	☑ Enable

○ Allow all to pass except those match the following rules.
● Deny all to pass except those match the following rules.

ID	Source IP : Ports		Destination IP : Ports		Enable	Use Rule#
1	1.2.3-100-1.2.3-119			21	☑	0
2	1.2.3.100-1.2.3.119			119	☑	0
3					☐	0
4					☐	0
5					☐	0
6					☐	0
7					☐	0
8					☐	0

Schedule rule (00)Always

(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)

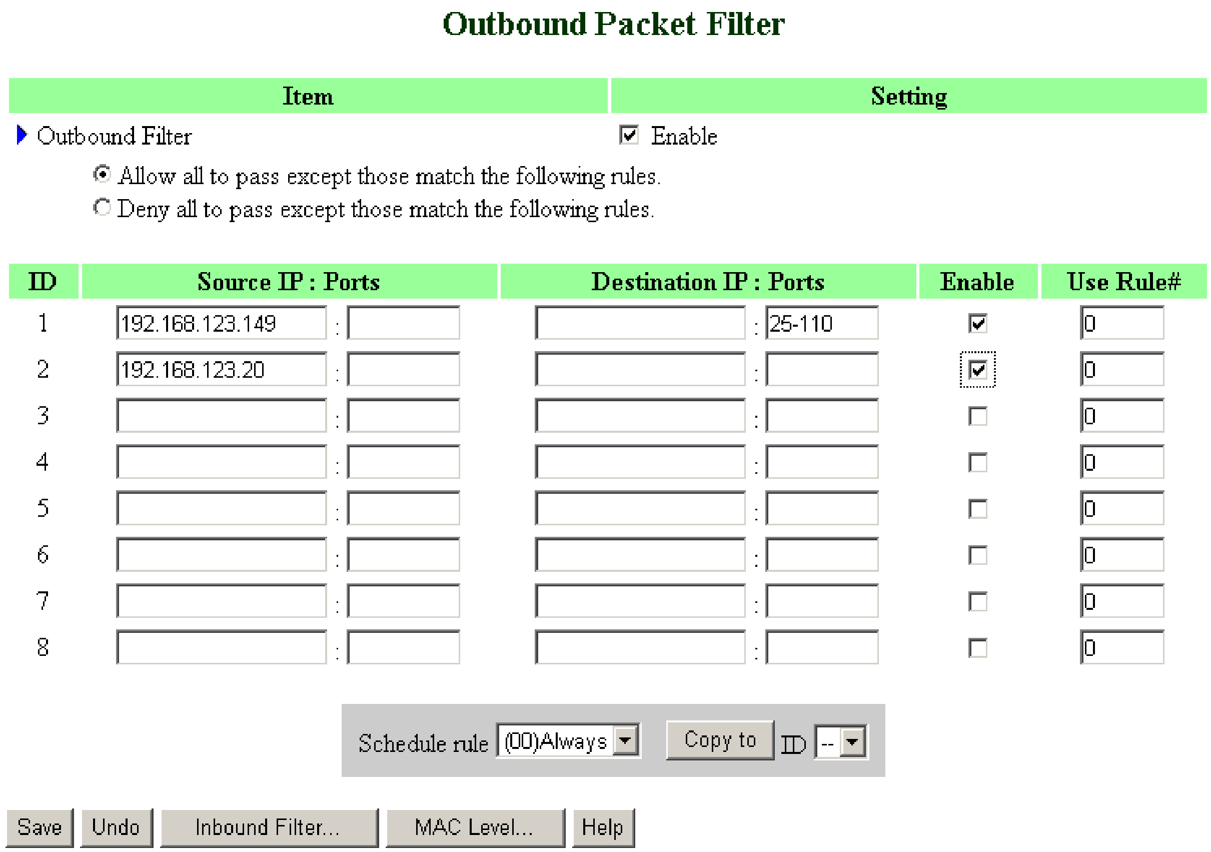
Others are all allowed.

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:



Outbound Packet Filter

Item	Setting
Outbound Filter	☑ Enable

● Allow all to pass except those match the following rules.
○ Deny all to pass except those match the following rules.

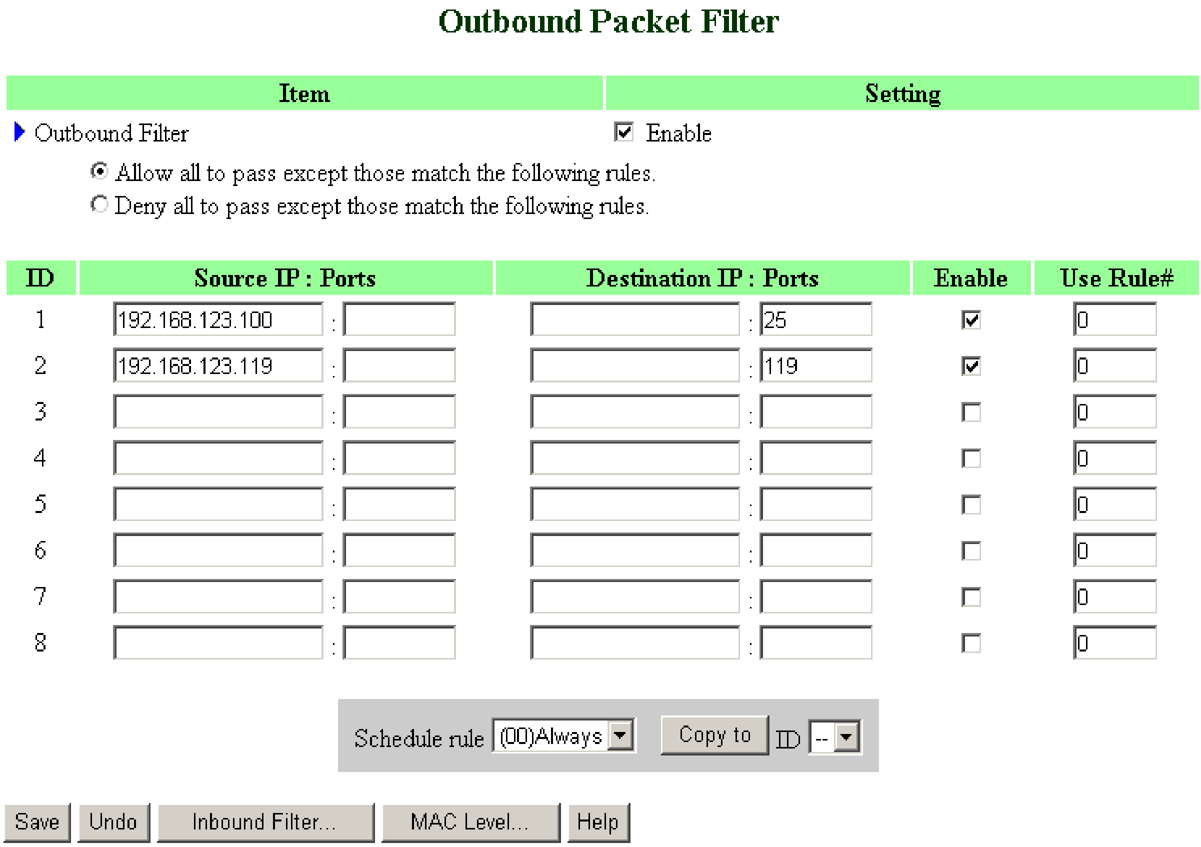
ID	Source IP : Ports		Destination IP : Ports		Enable	Use Rule#
1	192.168.123.149			25-110	☑	0
2	192.168.123.20				☑	0
3					□	0
4					□	0
5					□	0
6					□	0
7					□	0
8					□	0

Schedule rule (00)Always

(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:



Outbound Packet Filter

Item	Setting
Outbound Filter	☑ Enable

● Allow all to pass except those match the following rules.
○ Deny all to pass except those match the following rules.

ID	Source IP : Ports	Destination IP : Ports	Enable	Use Rule#
1	192.168.123.100 :	: 25	☑	0
2	192.168.123.119 :	: 119	☑	0
3	:	:	□	0
4	:	:	□	0
5	:	:	□	0
6	:	:	□	0
7	:	:	□	0
8	:	:	□	0

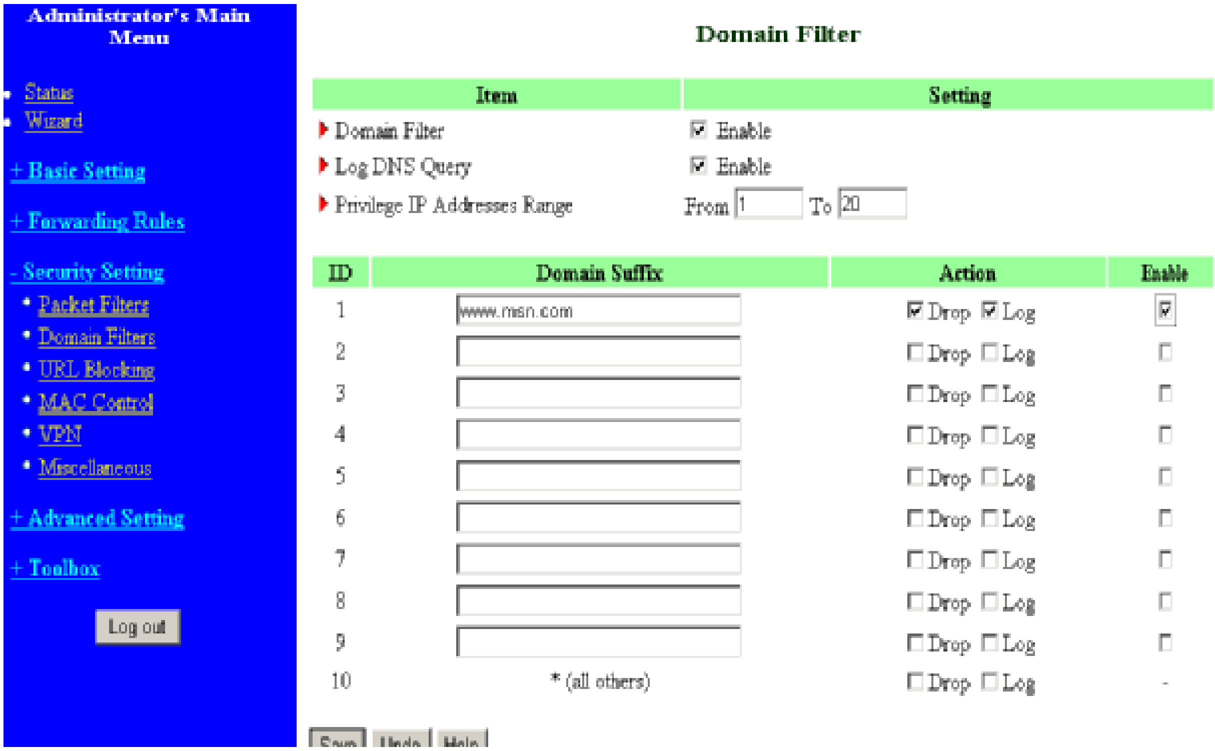
Schedule rule (00)Always ▾ Copy to ID -- ▾

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

Others are allowed

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

4.6.2 Domain Filter



Domain Filter

Item	Setting
Domain Filter	☑ Enable
Log DNS Query	☑ Enable
Privilege IP Addresses Range	From 1 To 20

ID	Domain Suffix	Action	Enable
1	www.msn.com	☑ Drop ☑ Log	☑
2		□ Drop □ Log	□
3		□ Drop □ Log	□
4		□ Drop □ Log	□
5		□ Drop □ Log	□
6		□ Drop □ Log	□
7		□ Drop □ Log	□
8		□ Drop □ Log	□
9		□ Drop □ Log	□
10	* (all others)	□ Drop □ Log	-

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

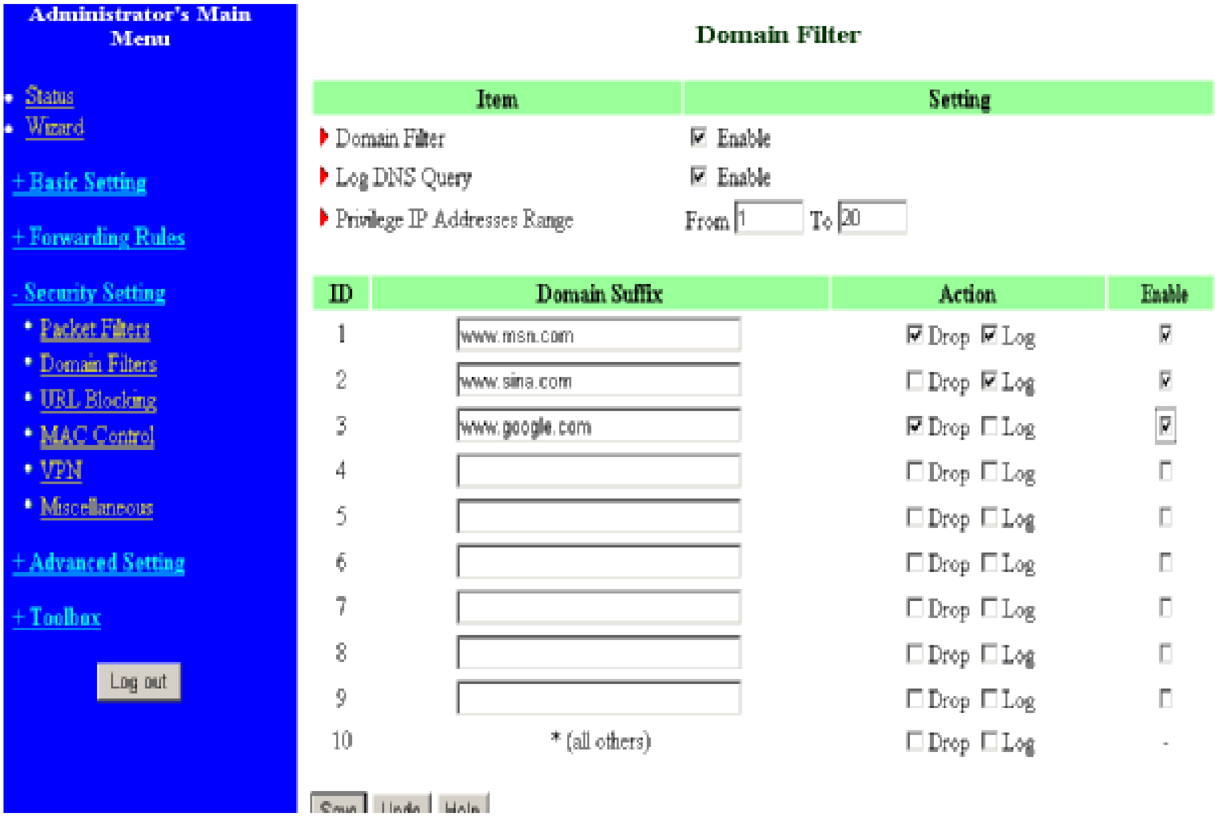
When someone is accessing the URL met the domain-suffix, what kind of action you want.

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

Enable

Check to enable each rule.

Example:



Domain Filter

Item	Setting
Domain Filter	☑ Enable
Log DNS Query	☑ Enable
Privilege IP Addresses Range	From 1 To 20

ID	Domain Suffix	Action	Enable
1	www.msn.com	☑ Drop ☑ Log	☑
2	www.sina.com	□ Drop ☑ Log	☑
3	www.google.com	☑ Drop □ Log	☑
4		□ Drop □ Log	□
5		□ Drop □ Log	□
6		□ Drop □ Log	□
7		□ Drop □ Log	□
8		□ Drop □ Log	□
9		□ Drop □ Log	□
10	* (all others)	□ Drop □ Log	-

In this example:

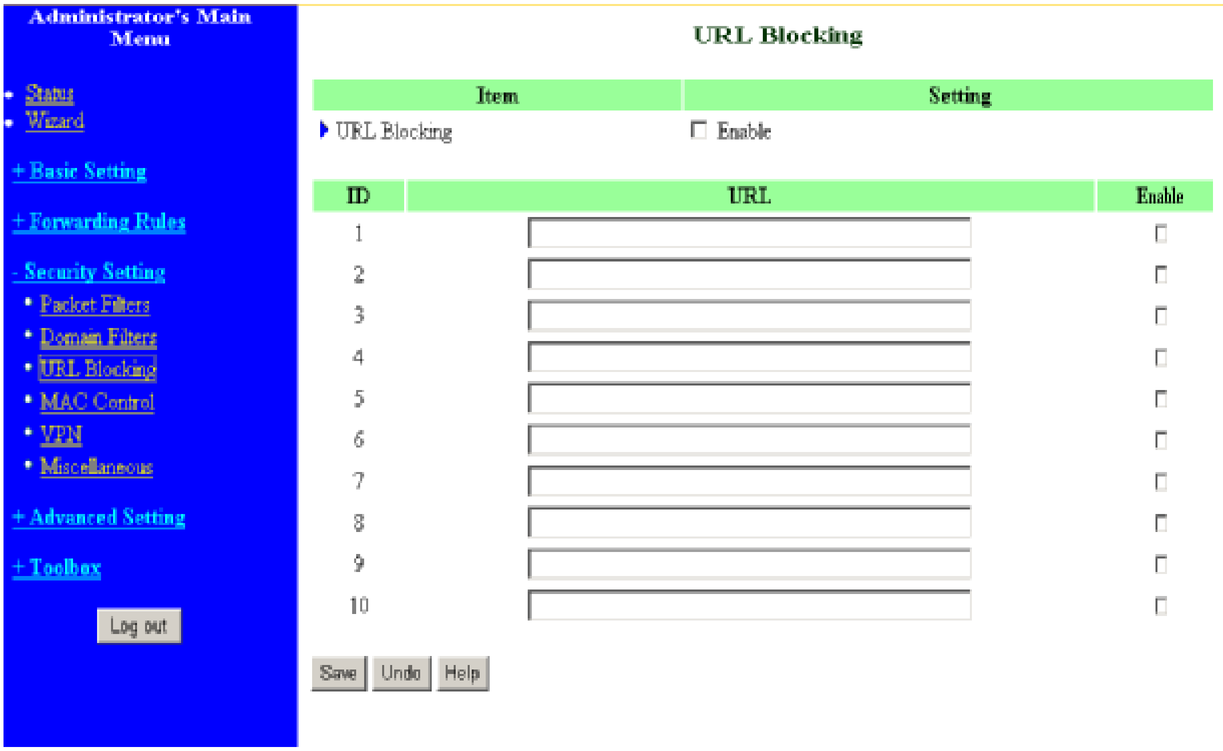
1. URL include "www.msn.com" will be blocked, and the action will be record in log-file.

2. URL include "www.sina.com" will not be blocked, but the action will be record in log-file.

3. URL include "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

Item	Setting
▸ URL Blocking	□ Enable

ID	URL	Enable
1		□
2		□
3		□
4		□
5		□
6		□
7		□
8		□
9		□
10		□

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.

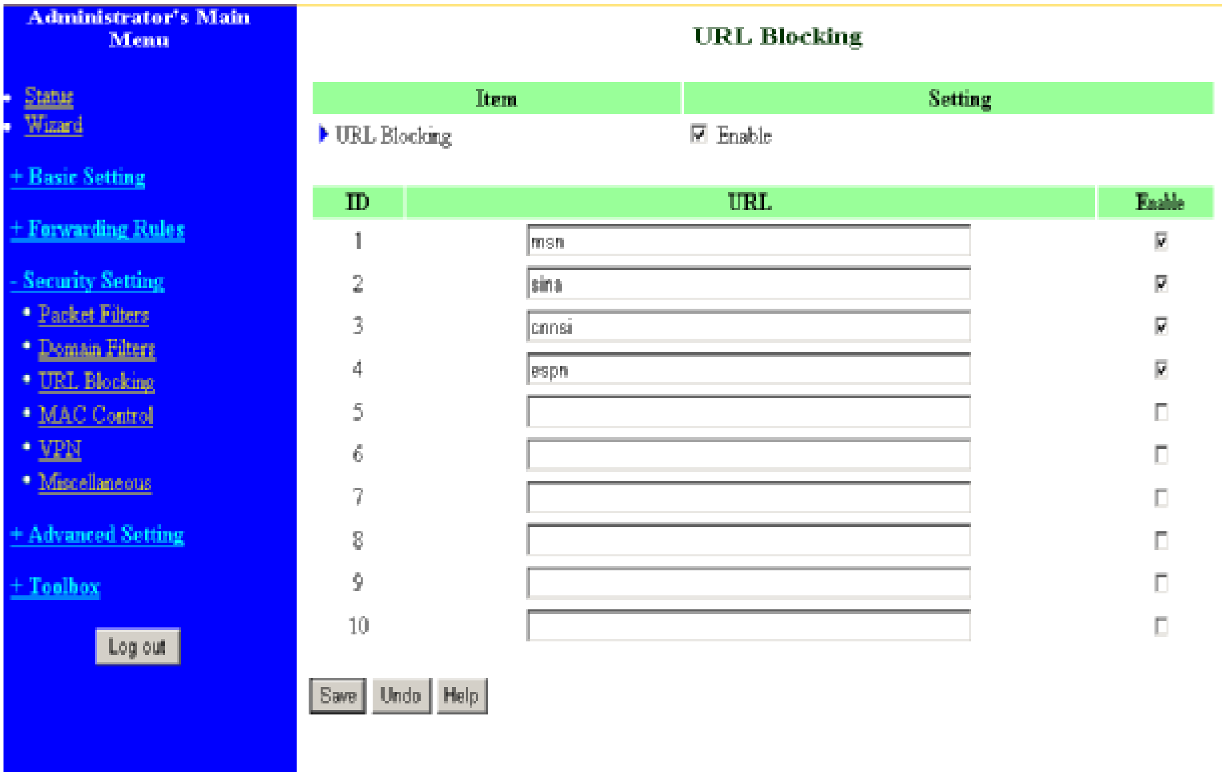
URL

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.



URL Blocking

Item	Setting
URL Blocking	☑ Enable

ID	URL	Enable
1	msn	☑
2	sina	☑
3	cnnsi	☑
4	espn	☑
5		□
6		□
7		□
8		□
9		□
10		□

In this example:

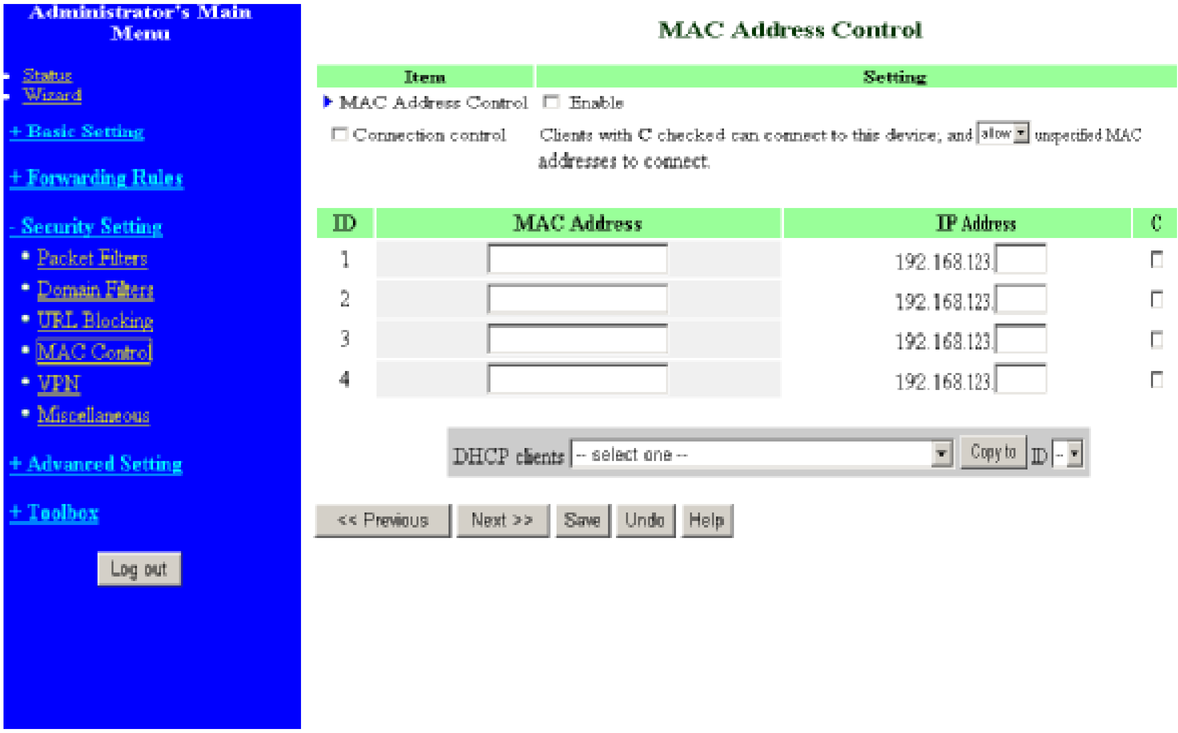
1.URL include “msn” will be blocked, and the action will be record in log-file.

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

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

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

4.6.4 MAC Address Control



MAC Address Control

Item	Setting
MAC Address Control	□ Enable
□ Connection control	Clients with C checked can connect to this device; and allow unspecified MAC addresses to connect.

ID	MAC Address	IP Address	C
1		192.168.123.	□
2		192.168.123.	□
3		192.168.123.	□
4		192.168.123.	□

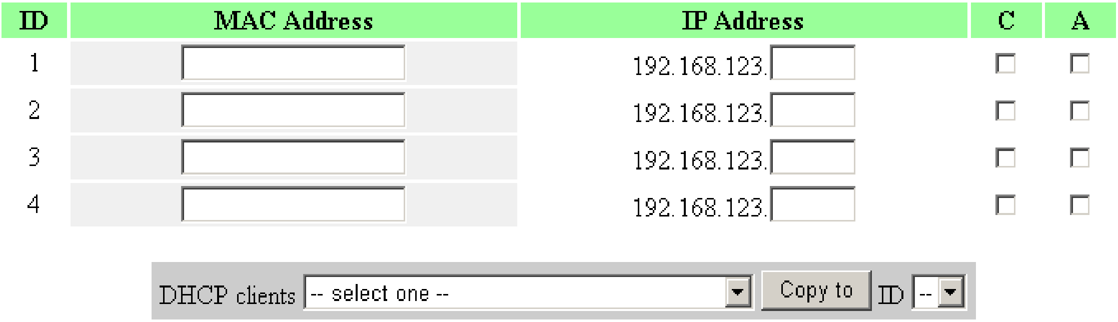
DHCP clients -- select one -- Copy to ID --

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

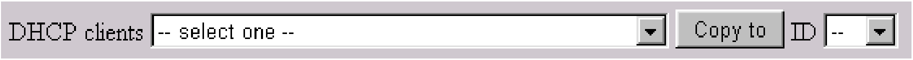


ID	MAC Address	IP Address	C	A
1		192.168.123.	□	□
2		192.168.123.	□	□
3		192.168.123.	□	□
4		192.168.123.	□	□

"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.

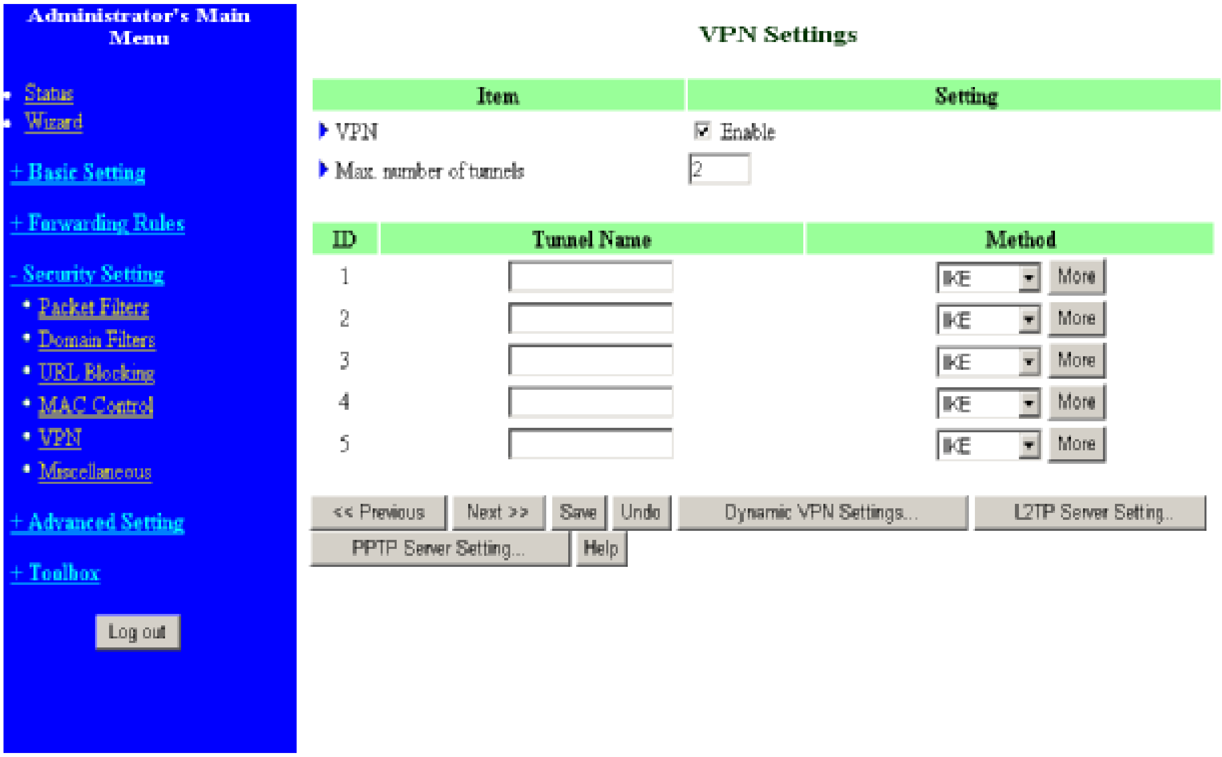
In this page, we provide the following Combo box and button to help you to input the MAC address.



You can select a specific client in the "DHCP clients" Combo box, 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" Combo box.

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

Item	Setting
VPN	☑ Enable
Max. number of tunnels	2

ID	Tunnel Name	Method
1		IKE More
2		IKE More
3		IKE More
4		IKE More
5		IKE More

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.

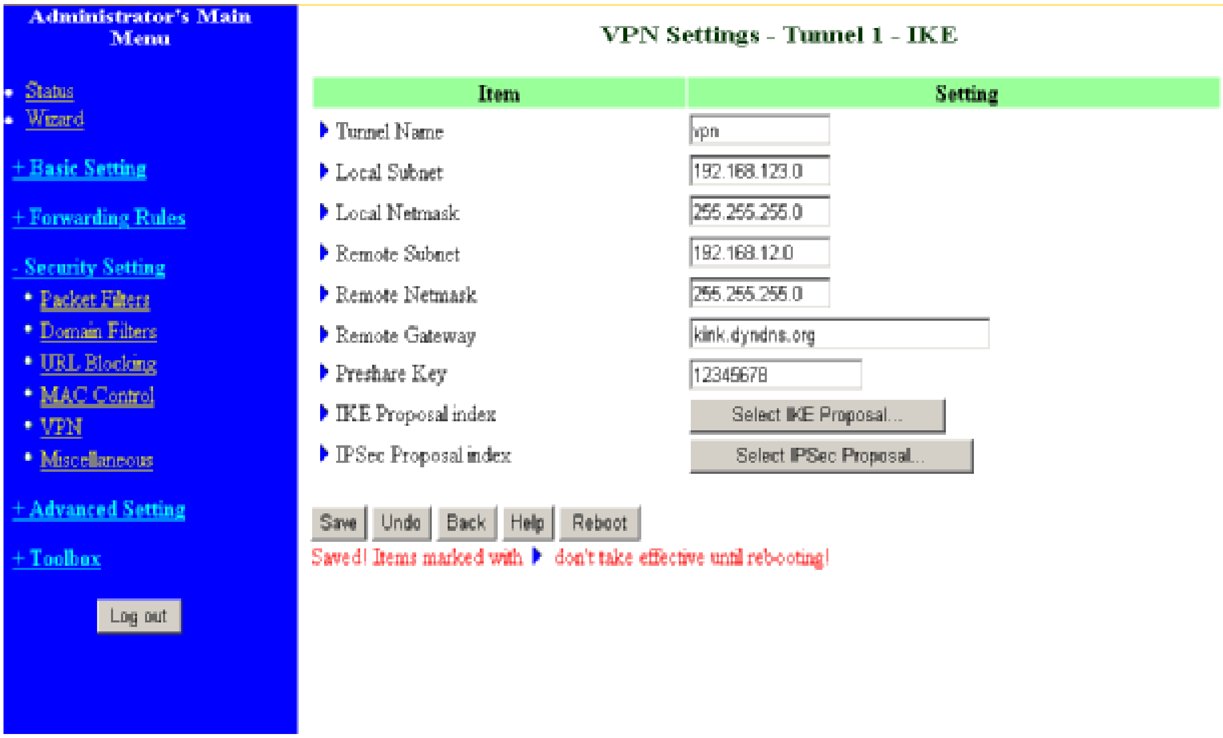
Method

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



VPN Settings - Tunnel 1 - IKE

Item	Setting
▶ Tunnel Name	vpn
▶ Local Subnet	192.168.123.0
▶ Local Netmask	255.255.255.0
▶ Remote Subnet	192.168.12.0
▶ Remote Netmask	255.255.255.0
▶ Remote Gateway	klink.dyndns.org
▶ Preshare Key	12345678
▶ IKE Proposal index	Select IKE Proposal...
▶ IPSec Proposal index	Select IPSec Proposal...

Saved! Items marked with ▶ don't take effective until rebooting!

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

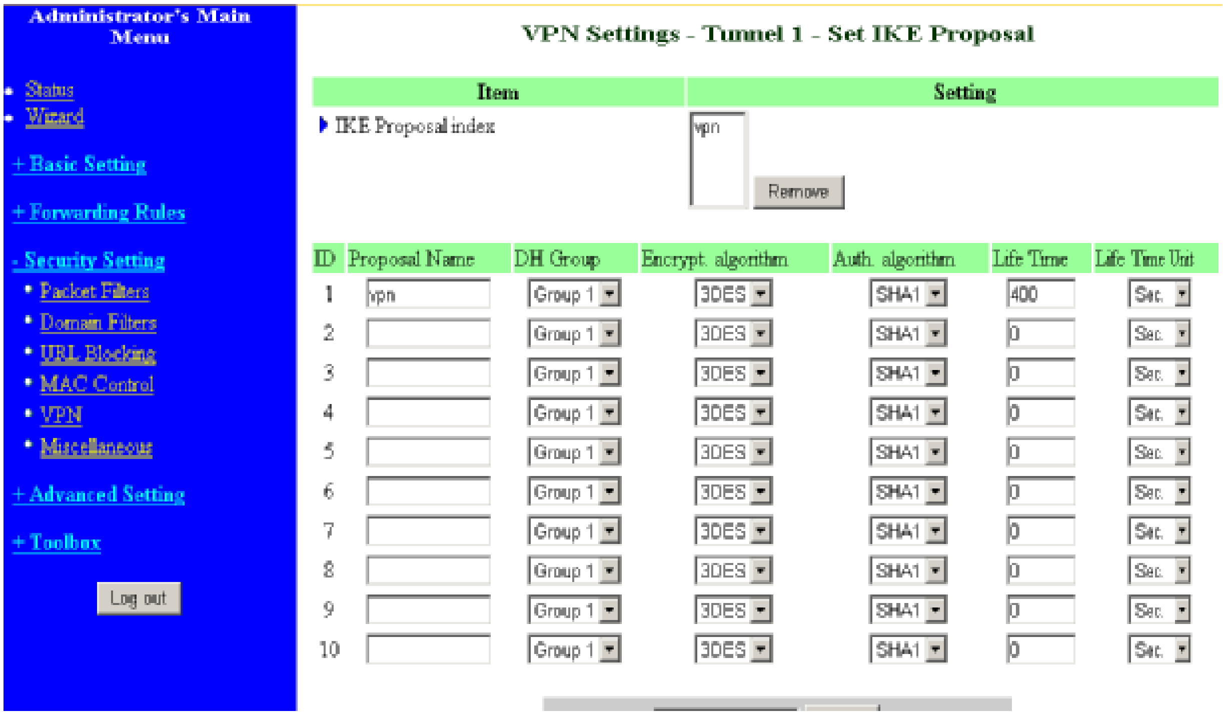
The first key that supports IKE mechanism of both VPN gateways for negotiating further security keys. The pre-shared key must be same for both end gateways.

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 proposalsand select from the set of IKE proposals for the dedicated tunnel.

VPN Settings - Set IKE Proposal



VPN Settings - Tunnel 1 - Set IKE Proposal

Item	Setting
IKE Proposal index	vpn

ID	Proposal Name	DH Group	Encrypt. algorithm	Auth. algorithm	Life Time	Life Time Unit
1	vpn	Group 1	3DES	SHA1	400	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 indexes

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.

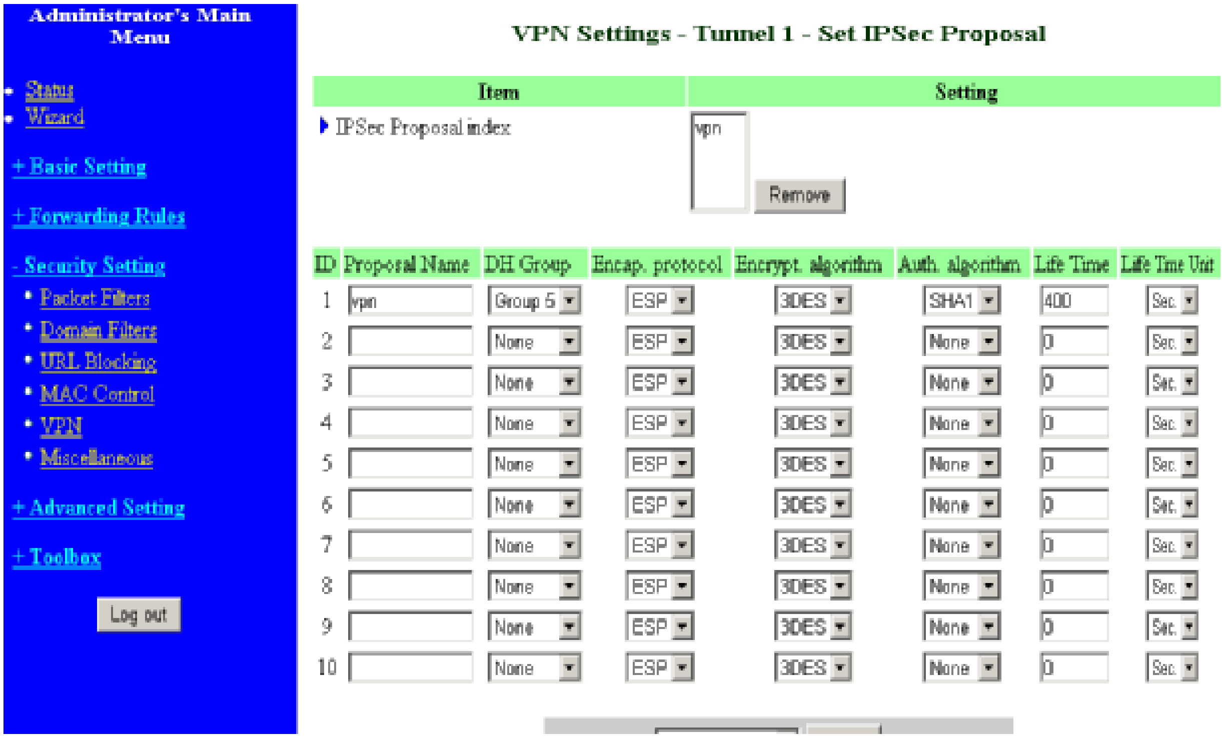
Proposal ID

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



VPN Settings - Tunnel 1 - Set IPSec Proposal

Item	Setting
IPSec Proposal index	vpn

ID	Proposal Name	DH Group	Encap. protocol	Encrypt. algorithm	Auth. algorithm	Life Time	Life Time Unit
1	vpn	Group 5	ESP	3DES	SHA1	400	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.

IPSec Proposal indexes

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.

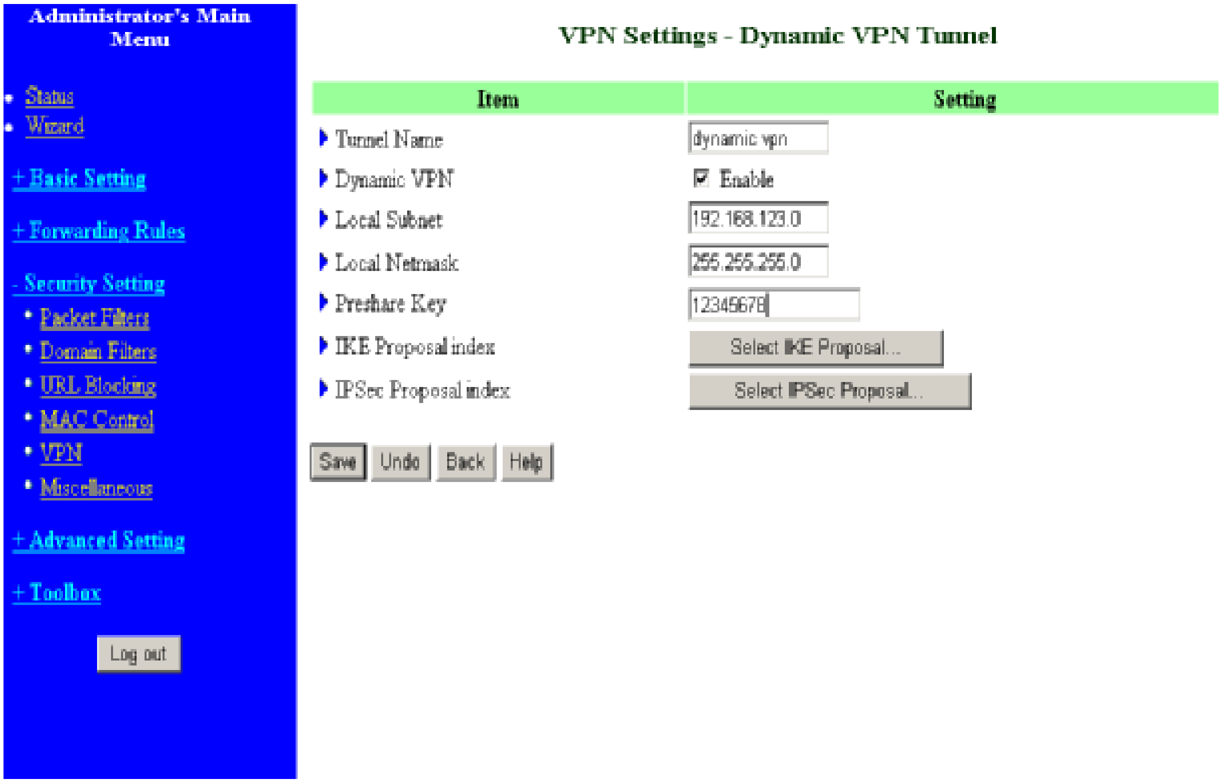
Proposal ID

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

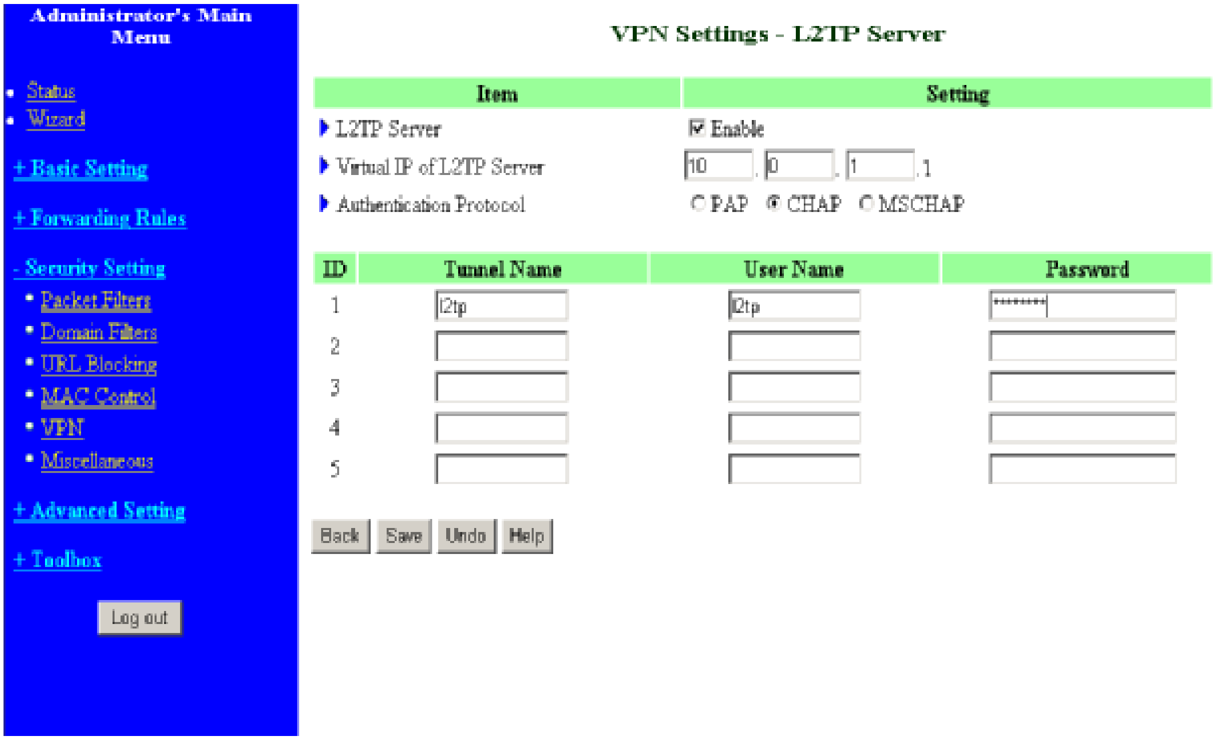


VPN Settings - Dynamic VPN Tunnel

Item	Setting
Tunnel Name	dynamic vpn
Dynamic VPN	☑ Enable
Local Subnet	192.168.123.0
Local Netmask	255.255.255.0
Preshare Key	12345678
IKE Proposal index	Select IKE Proposal...
IPSec Proposal index	Select IPSec Proposal...

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



VPN Settings - L2TP Server

Item	Setting
L2TP Server	☑ Enable
Virtual IP of L2TP Server	10 . 0 . 1 . 1
Authentication Protocol	○ PAP ● CHAP ○ MSCHAP

ID	Tunnel Name	User Name	Password
1	l2tp	l2tp	********
2			
3			
4			
5			

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.

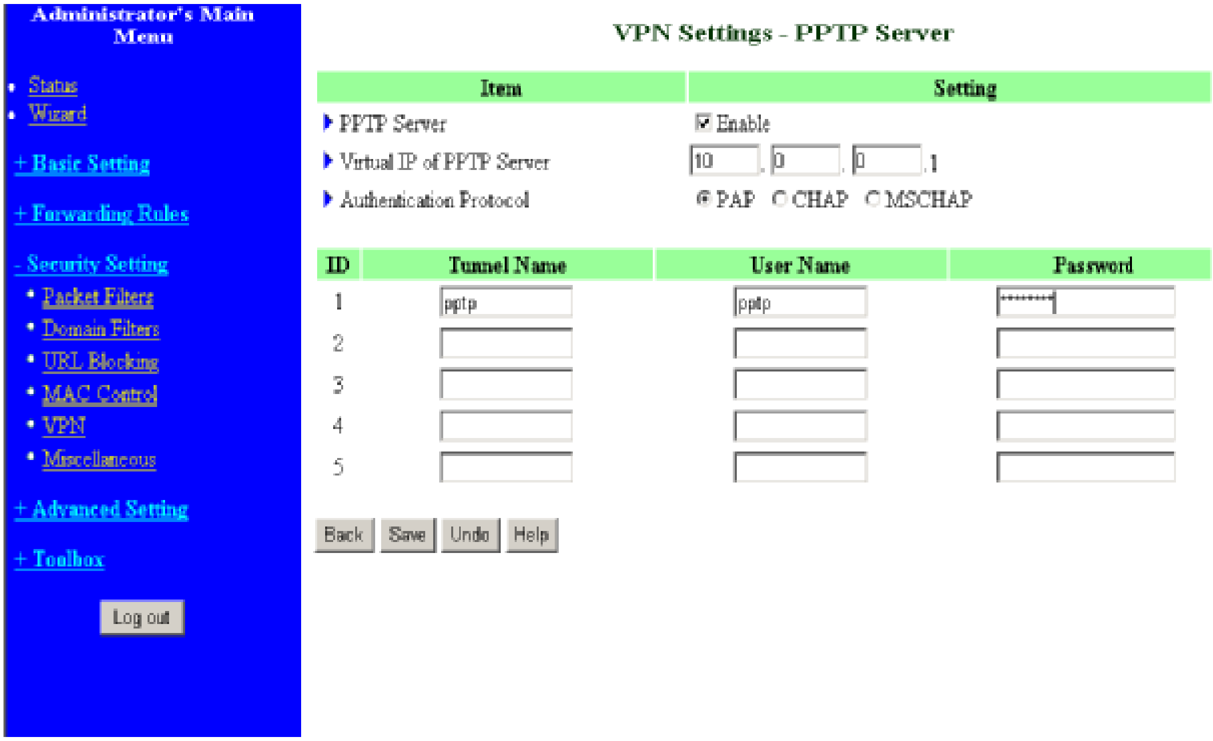
Virtual IP of L2TP Server: L2TP server's virtual IP. User must assign a virtual IP for L2TP Server.

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 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.



VPN Settings - PPTP Server

Item	Setting
PPTP Server	☑ Enable
Virtual IP of PPTP Server	10 . 0 . 0 .1
Authentication Protocol	● PAP ○ CHAP ○ MSCHAP

ID	Tunnel Name	User Name	Password
1	pptp	pptp	********
2			
3			
4			
5			

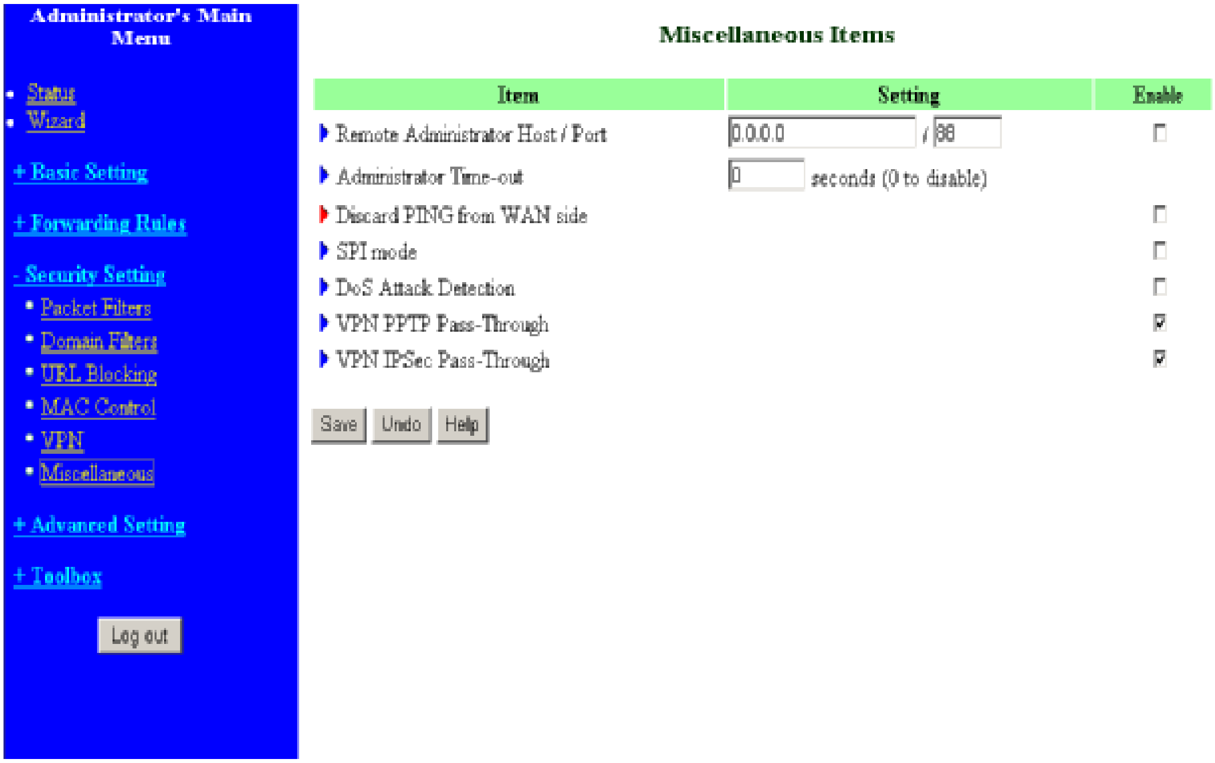
User can build up to five PPTP tunnels for PPTP clients. Each tunnel can accept more than one client. User is required to configure Virtual IP of PPTP Server, Authentication Protocol, PPTP Tunnel Name and User Account, Password.

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



Miscellaneous Items

Item	Setting	Enable
Remote Administrator Host / Port	0.0.0.0 / 88	□
Administrator Time-out	0 seconds (0 to disable)	
Discard PING from WAN side		□
SPI mode		□
DoS Attack Detection		□
VPN PPTP Pass-Through		☑
VPN IPSec Pass-Through		☑

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

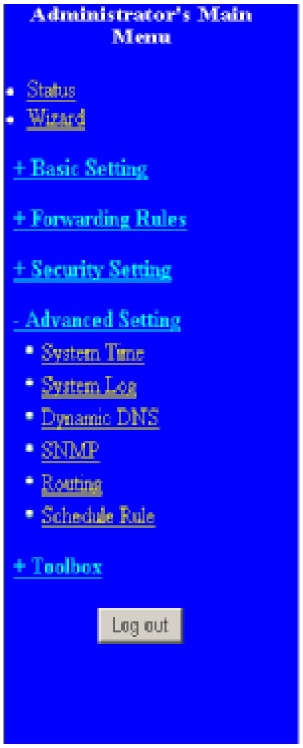
When this feature is enabled, the router will detect and log the DoS attack comes from the Internet.

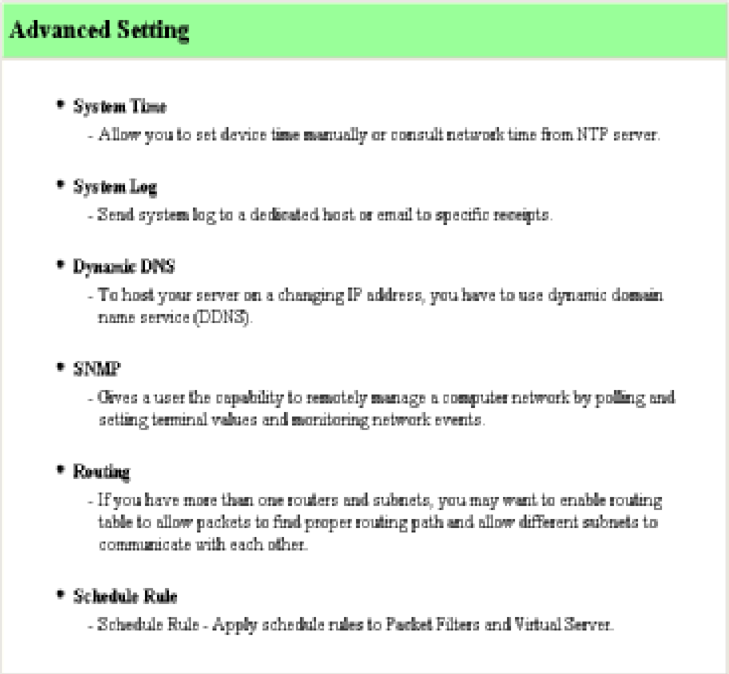
Currently, the router can detect the following DoS attack: SYN Attack, WinNuke, Port Scan, Ping of Death, and Land Attack etc.

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





Advanced Setting

- **System Time**

  - Allow you to set device time manually or consult network time from NTP server.

- **System Log**

  - Send system log to a dedicated host or email to specific receipts.

- **Dynamic DNS**

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

- **SNMP**

  - Gives a user the capability to remotely manage a computer network by polling and setting terminal values and monitoring network events.

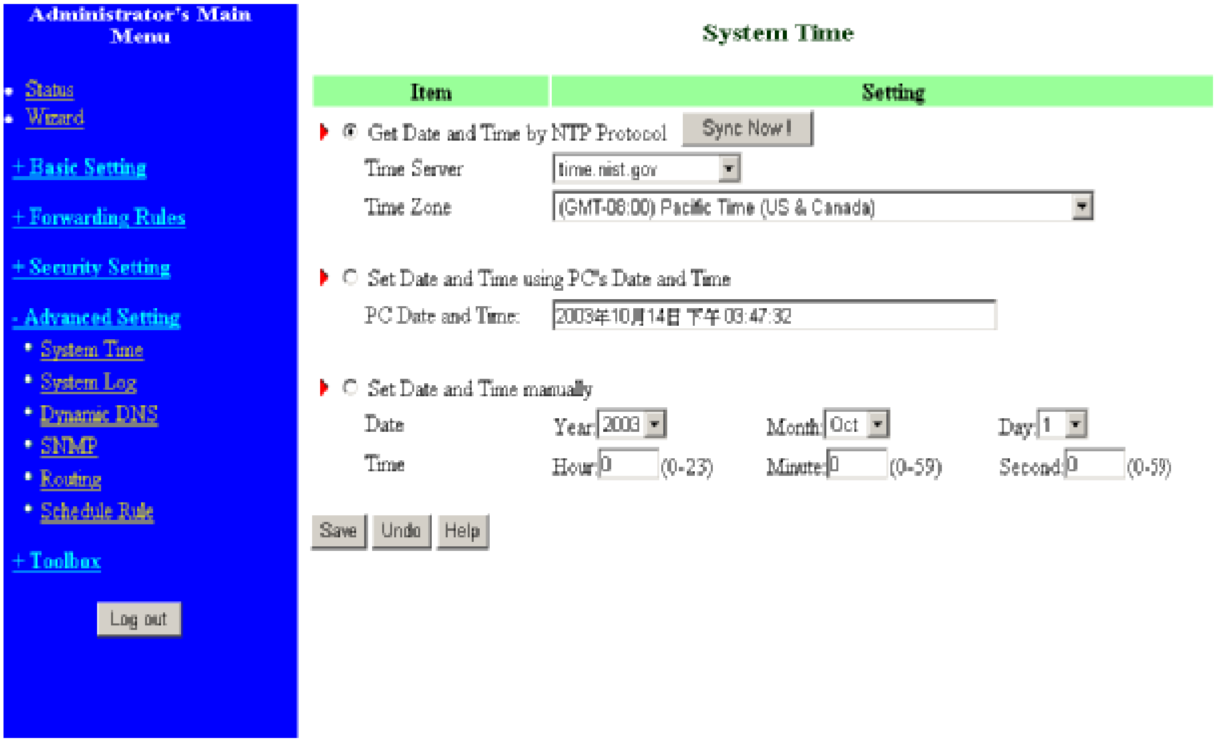
- **Routing**

  - If you have more than one routers and subnets, you may want to enable routing table to allow packets to find proper routing path and allow different subnets to communicate with each other.

- **Schedule Rule**

  - Schedule Rule - Apply schedule rules to Packet Filters and Virtual Server.

4.7.1 System Time



System Time

Item	Setting
● Get Date and Time by NTP Protocol	
Time Server	time.nist.gov
Time Zone	(GMT-08:00) Pacific Time (US & Canada)
○ Set Date and Time using PC's Date and Time	
PC Date and Time:	2003年10月14日 下午 03:47:32
○ Set Date and Time manually	
Date	Year: 2003 Month: Oct Day: 1
Time	Hour: 0 (0-23) Minute: 0 (0-59) Second: 0 (0-59)

Get Date and Time by NTP Protocol

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

Time Server

Select a NTP timeserver to consult UTC time

Time Zone

Select a time zone where this device locates.

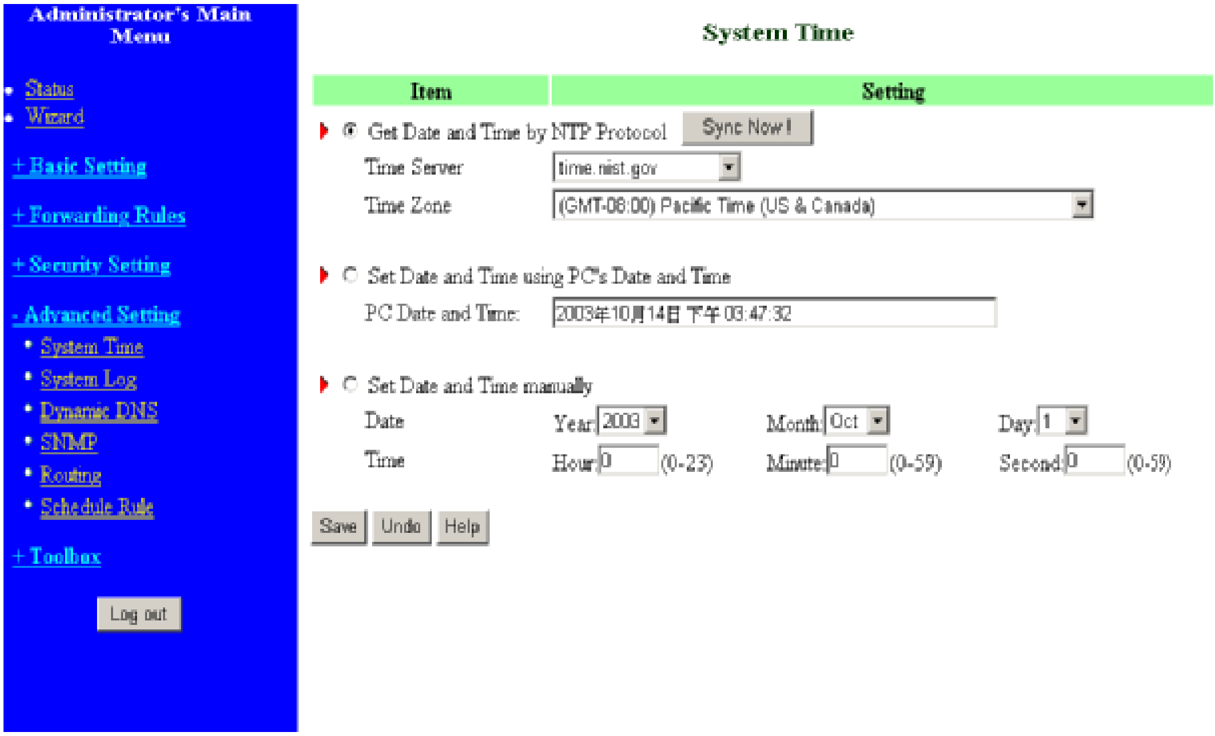
Set Date and Time manually

Selected if you want to Set Date and Time manually.

Function of Buttons

Sync Now: Synchronize system time with network timeserver

4.7.2 System Log



System Time

Item	Setting
● Get Date and Time by NTP Protocol	
Time Server	time.nist.gov
Time Zone	(GMT-08:00) Pacific Time (US & Canada)
○ Set Date and Time using PC's Date and Time	
PC Date and Time:	2003年10月14日 下午 03:47:32
○ Set Date and Time manually	
Date	Year: 2003 Month: Oct Day: 1
Time	Hour: 0 (0-23) Minute: 0 (0-59) Second: 0 (0-59)

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

Host IP of destination where syslogs will be sent.

Check **Enable** to enable this function.

E-mail Alert Enable

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

SMTP Server IP and Port

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

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

Send E-mail alert to

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

E-mail Subject

The subject of email alert. This setting is optional.

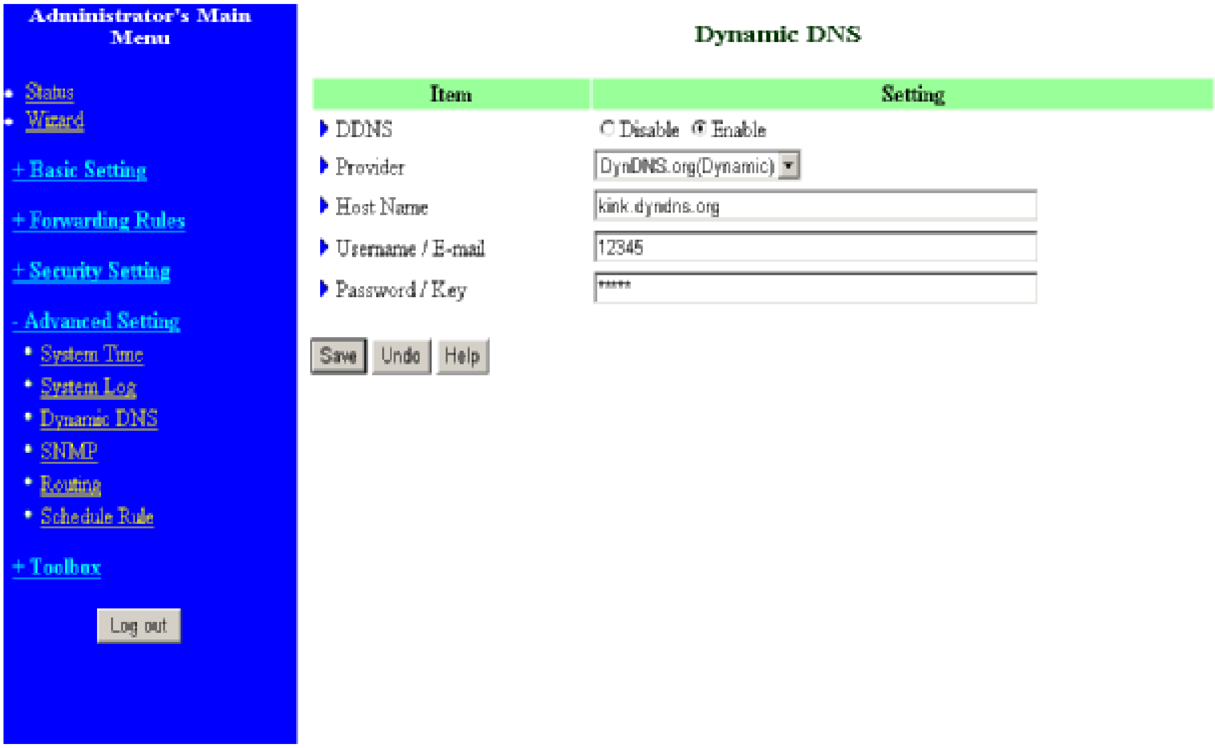
Username and Password

To fill some SMTP server's authentication requirement, you may need to input Username and Password that offered by your ISP.

Log type

Please select the activities that should be shown on log.

4.7.3 Dynamic DNS



Dynamic DNS

Item	Setting
DDNS	○ Disable ● Enable
Provider	DynDNS.org(Dynamic)
Host Name	kink.dyndns.org
Username / E-mail	12345
Password / Key	*****

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

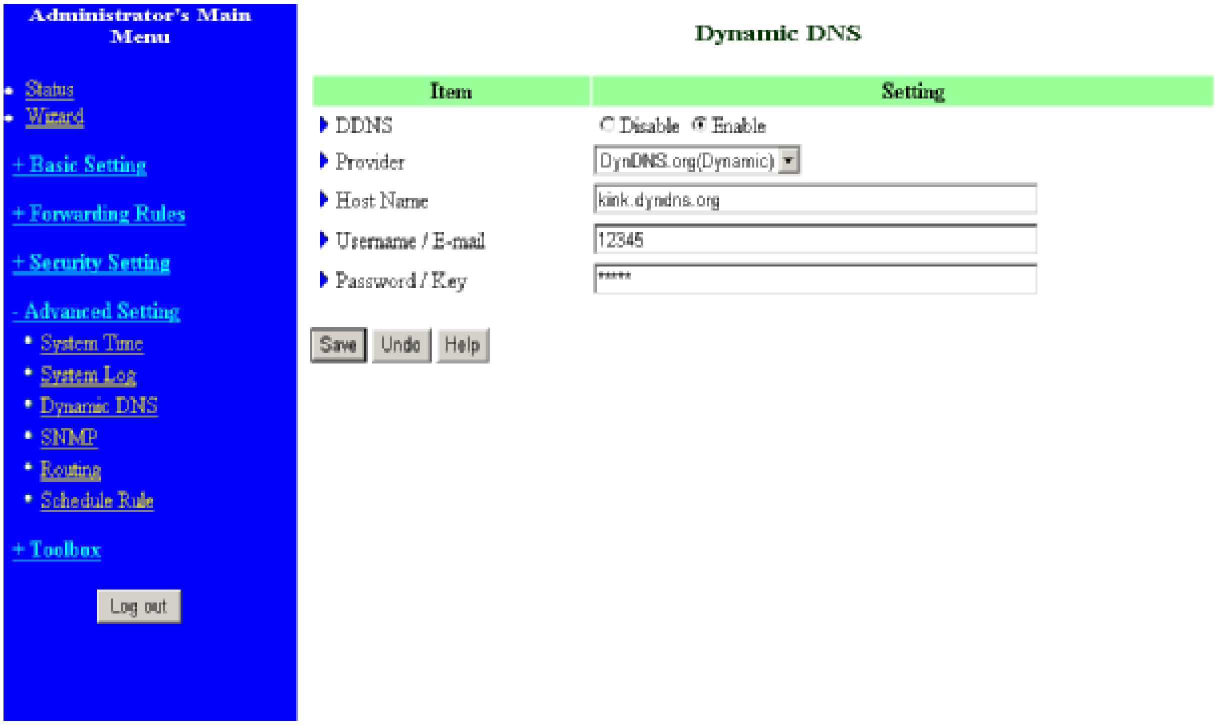
Host Name

Username/E-mail

Password/Key

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

Example:

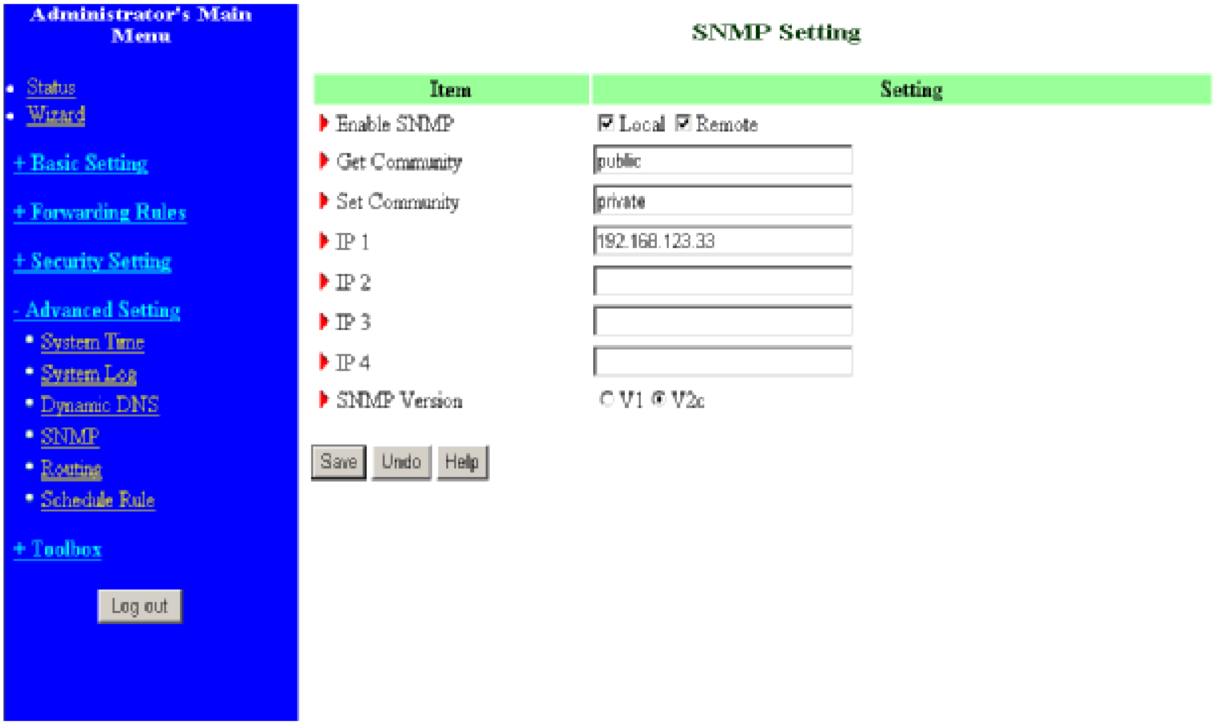


Dynamic DNS

Item	Setting
DDNS	○ Disable ● Enable
Provider	DynDNS.org(Dynamic)
Host Name	kink.dyndns.org
Username / E-mail	12345
Password / Key	*****

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

4.7.4 SNMP Setting



SNMP Setting

Item	Setting
Enable SNMP	☑ Local ☑ Remote
Get Community	public
Set Community	private
IP 1	192.168.123.33
IP 2	
IP 3	
IP 4	
SNMP Version	○ V1 ● V2c

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.

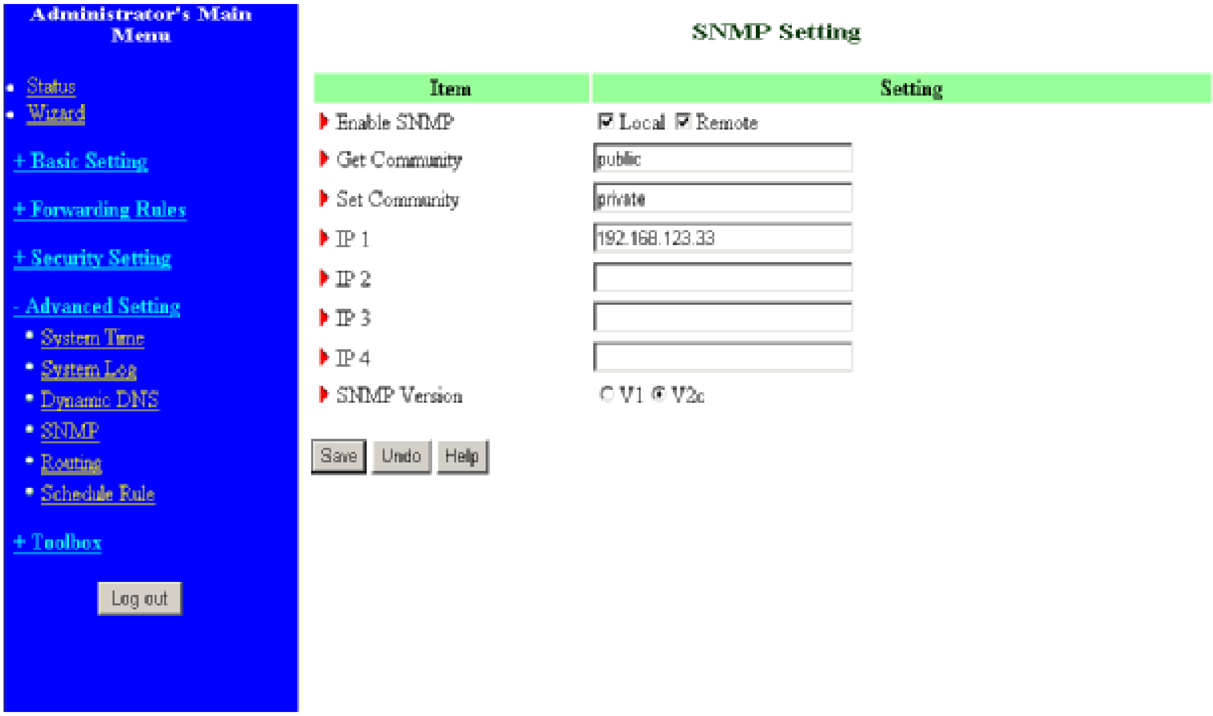
IP 1,IP 2,IP 3,IP 4

Input your SNMP Management PC’s IP here. User has to configure to where this device should send SNMP Trap message.

SNMP Version

Please select proper SNMP Version that your SNMP Management software supports

Example:



SNMP Setting

Item	Setting
Enable SNMP	☑ Local ☑ Remote
Get Community	public
Set Community	private
IP 1	192.168.123.33
IP 2	
IP 3	
IP 4	
SNMP Version	○ V1 ● V2c

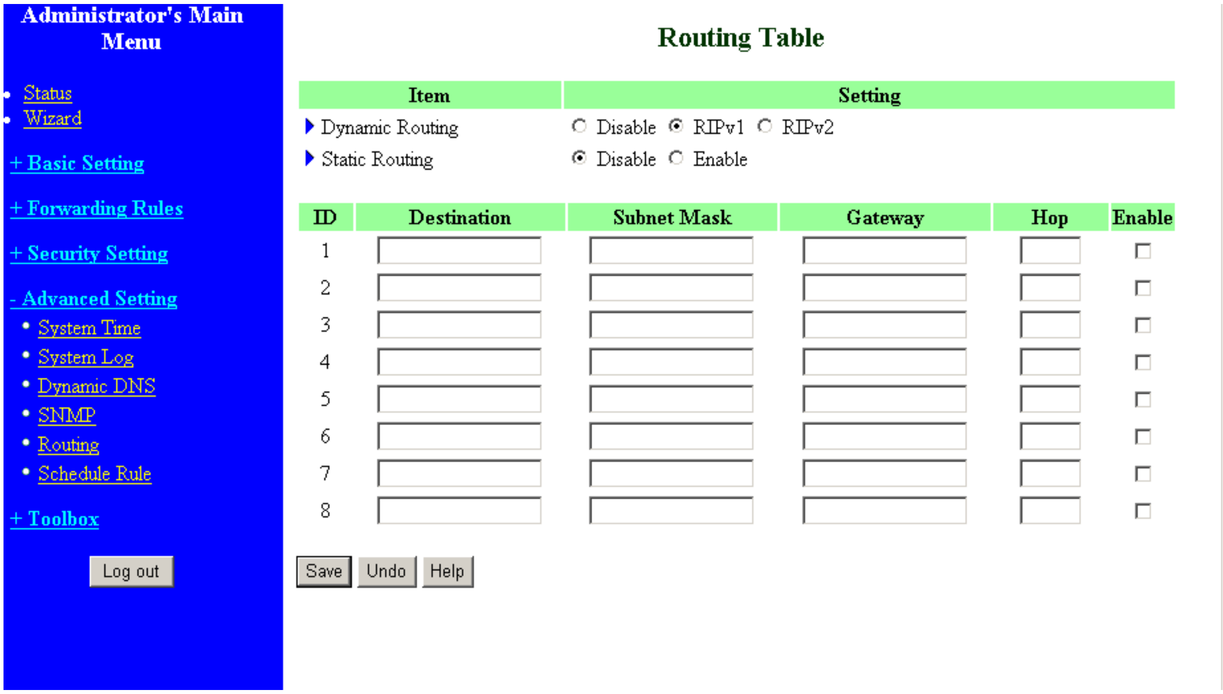
1. This device will response to SNMP client which's **get community** is set as "public"

2. This device will response to SNMP client which's **set community** is set as "private"

3. This device will response request from both LAN and WAN

4. This device will send SNMP Trap message to 192.168.123.33 (Use SNMP Version V2c)

4.7.5 Routing Table



Routing Table

Item	Setting
Dynamic Routing	○ Disable ● RIPv1 ○ RIPv2
Static Routing	● Disable ○ Enable

ID	Destination	Subnet Mask	Gateway	Hop	Enable
1					□
2					□
3					□
4					□
5					□
6					□
7					□
8					□

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.

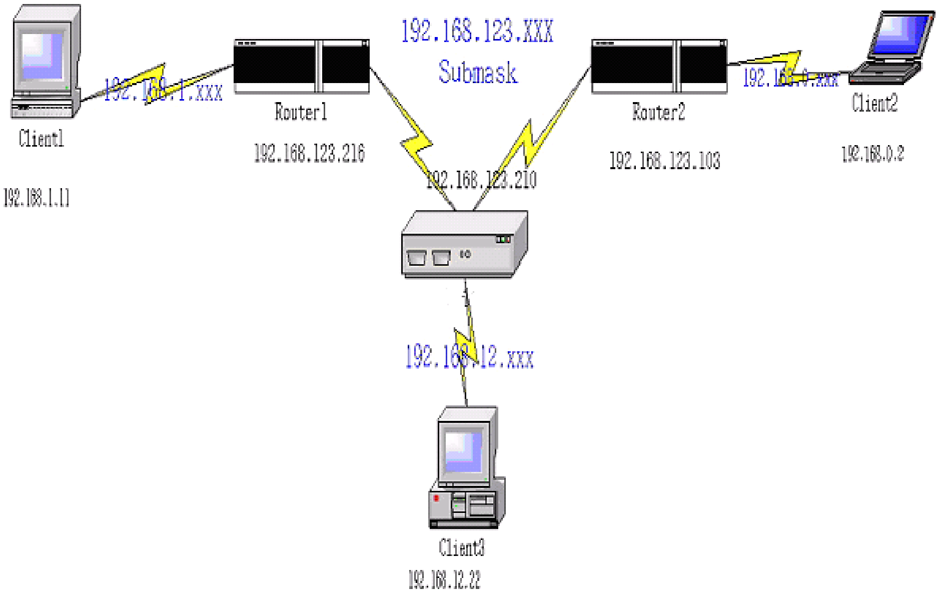
Routing Table settings are settings used to setup the functions of static and dynamic routing.

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, and gateway, hop for each routing rule, and then enable or disable the rule by checking or unchecking the Enable checkbox.

Example:



Configuration on NAT Router

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

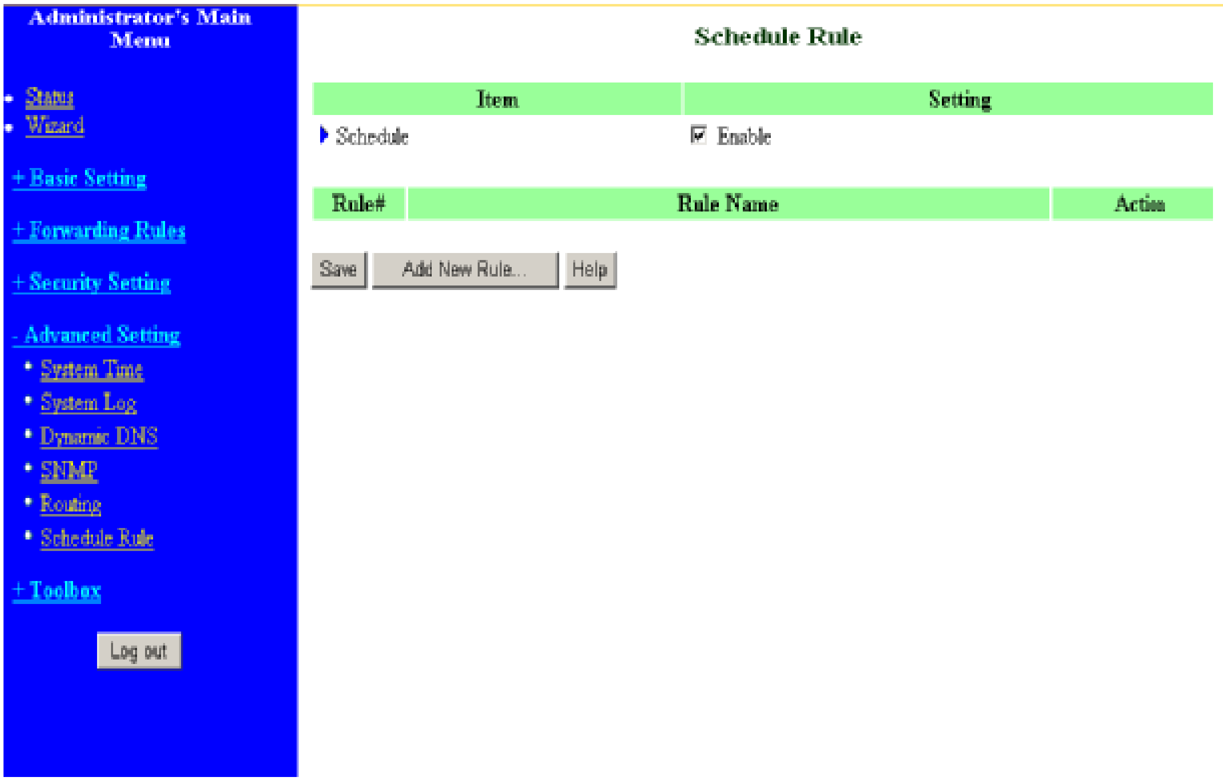
So if, for example, the client3 wanted to send an IP data gram to 192.168.0.2, it would use the above table to determine that it had to go via 192.168.123.103 (a gateway),

And if it sends Packets to 192.168.1.11 will go via 192.168.123.216

Each rule can be enabled or disabled individually.

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

4.7.6 Schedule Rule



Schedule Rule

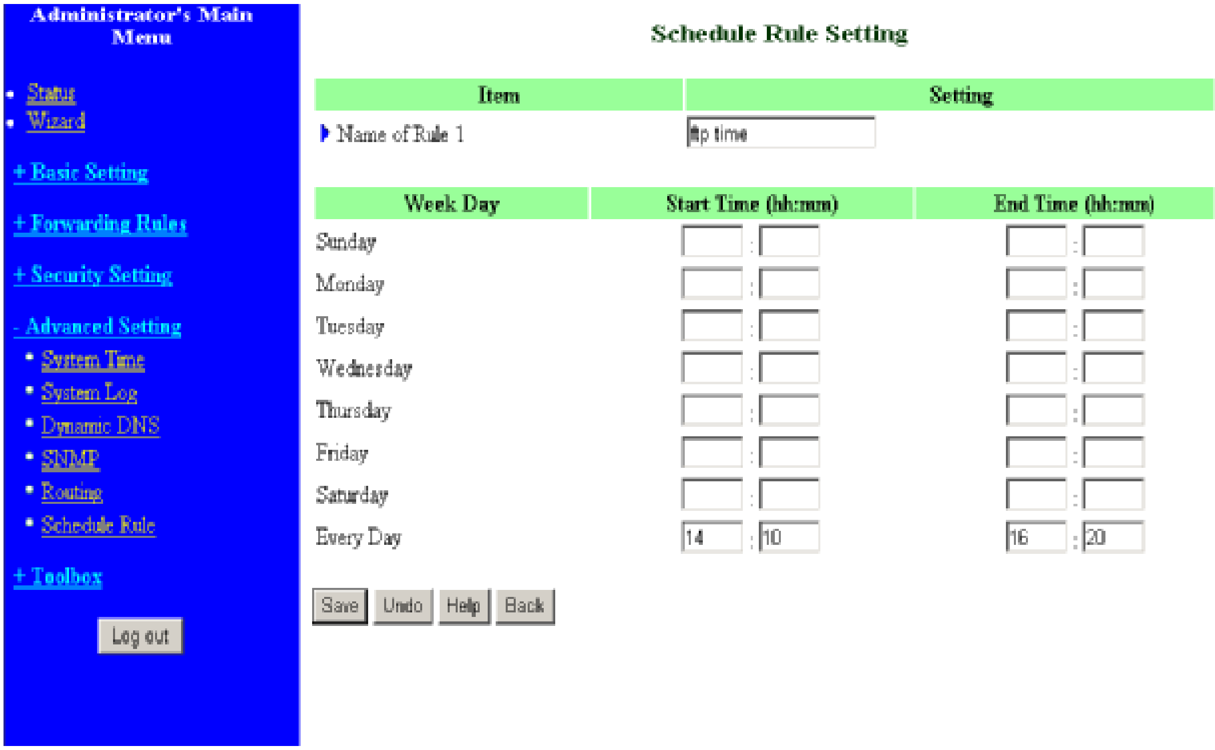
Item	Setting
Schedule	☑ Enable

Rule#	Rule Name	Action

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

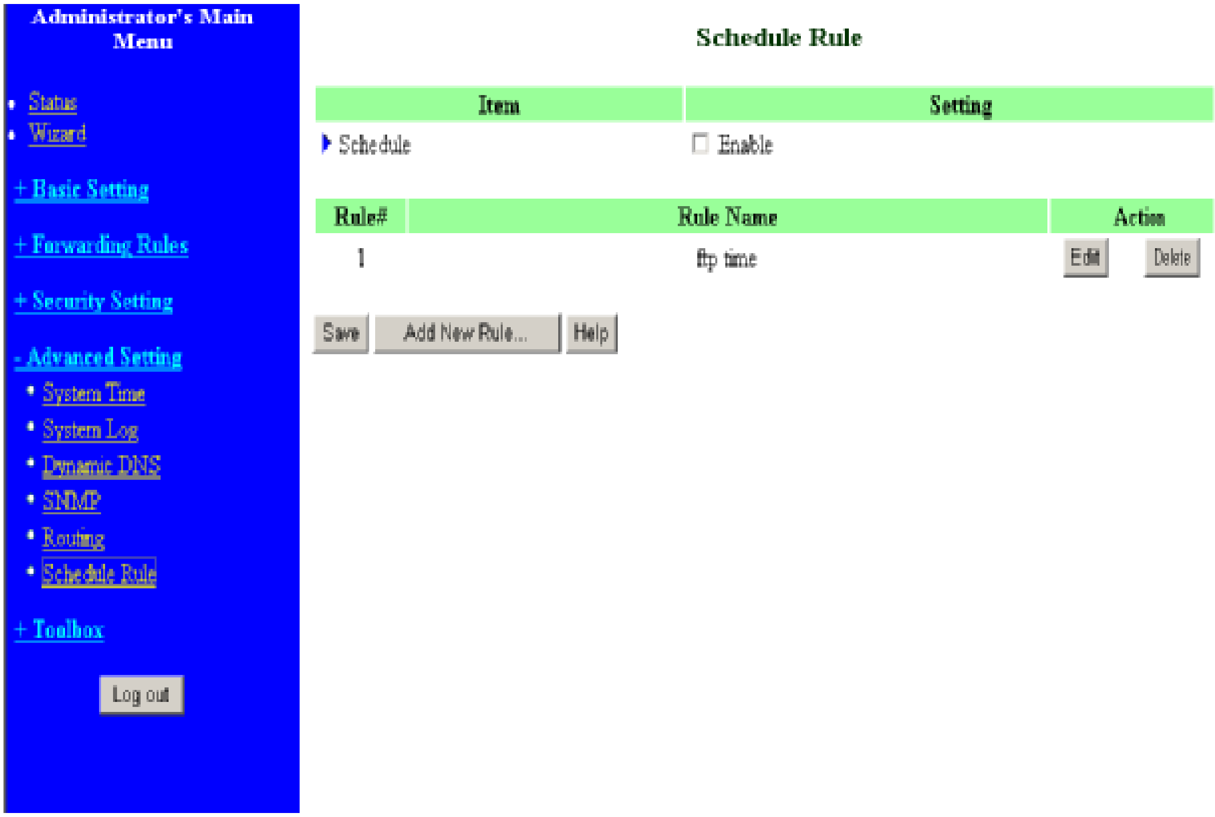


Schedule Rule Setting

Item	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

After configure Rule 1 à



Schedule Rule

Item	Setting
Schedule	□ Enable

Rule#	Rule Name	Action
1	ftp time	Edit Delete

Schedule Enable

Selected if you want to Enable the Scheduler.

Edit

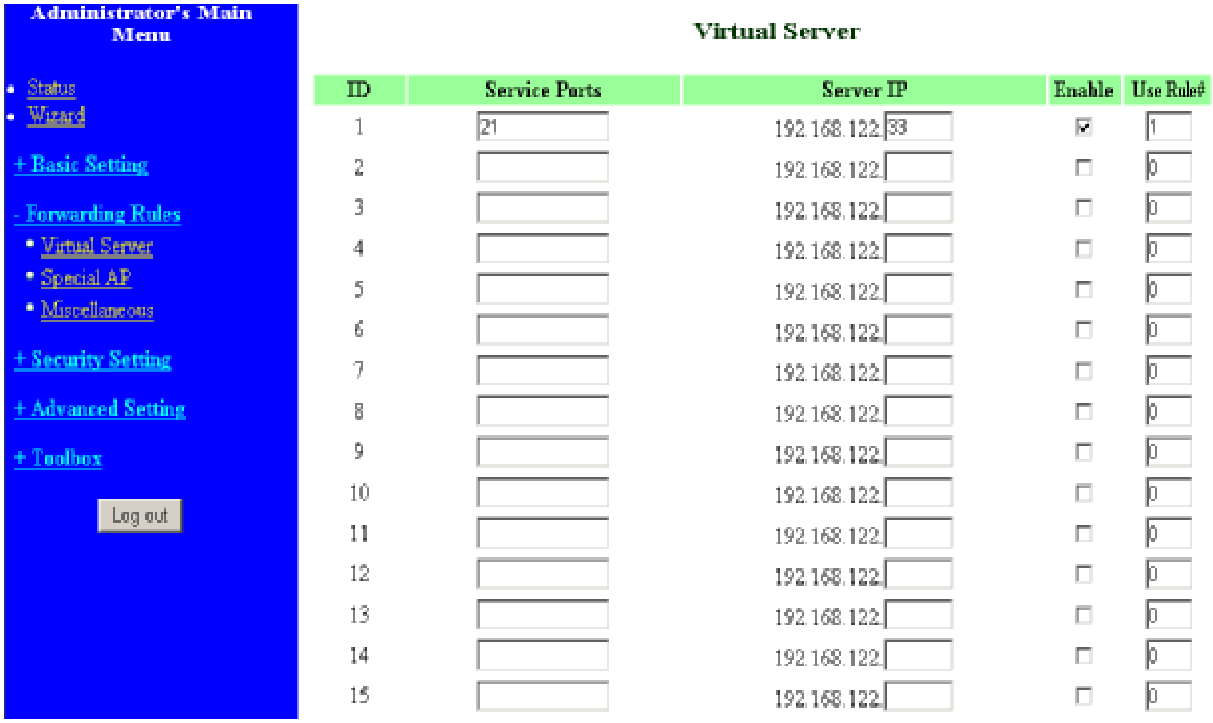
To edit the schedule rule.

Delete

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

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

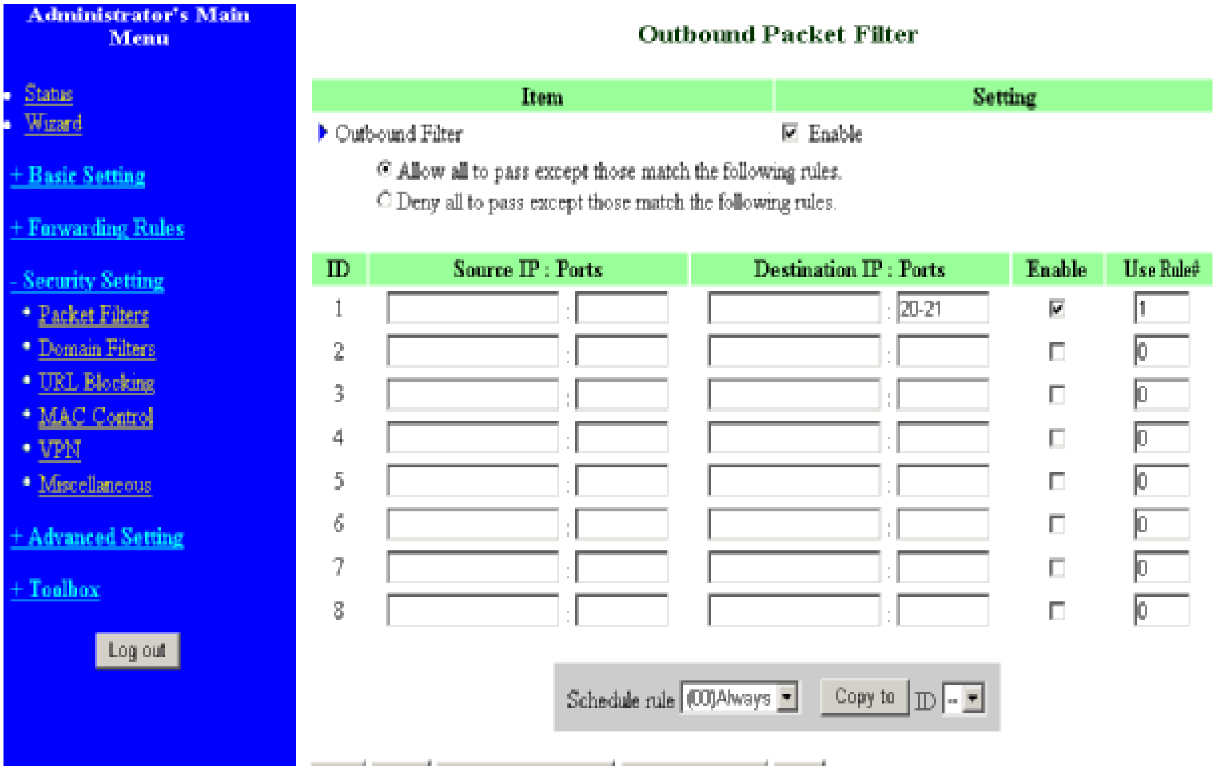
Exanple1: **Virtual Server** – Apply Rule#1 (ftp time: everyday 14:10 to 16:20)



Virtual Server

ID	Service Ports	Server IP	Enable	Use Rule#
1	21	192.168.122.33	☑	1
2		192.168.122.	□	0
3		192.168.122.	□	0
4		192.168.122.	□	0
5		192.168.122.	□	0
6		192.168.122.	□	0
7		192.168.122.	□	0
8		192.168.122.	□	0
9		192.168.122.	□	0
10		192.168.122.	□	0
11		192.168.122.	□	0
12		192.168.122.	□	0
13		192.168.122.	□	0
14		192.168.122.	□	0
15		192.168.122.	□	0

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



Outbound Packet Filter

Item	Setting
Outbound Filter	☑ Enable

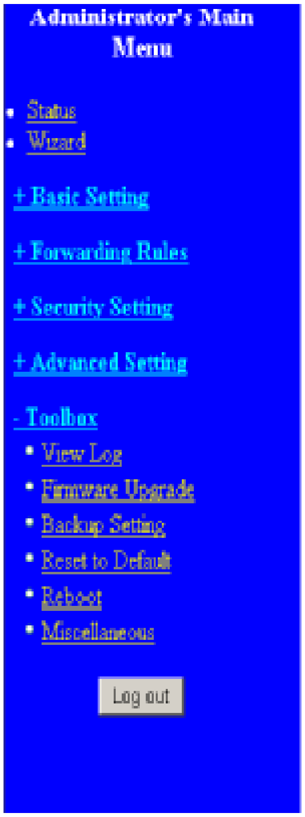
● Allow all to pass except those match the following rules.

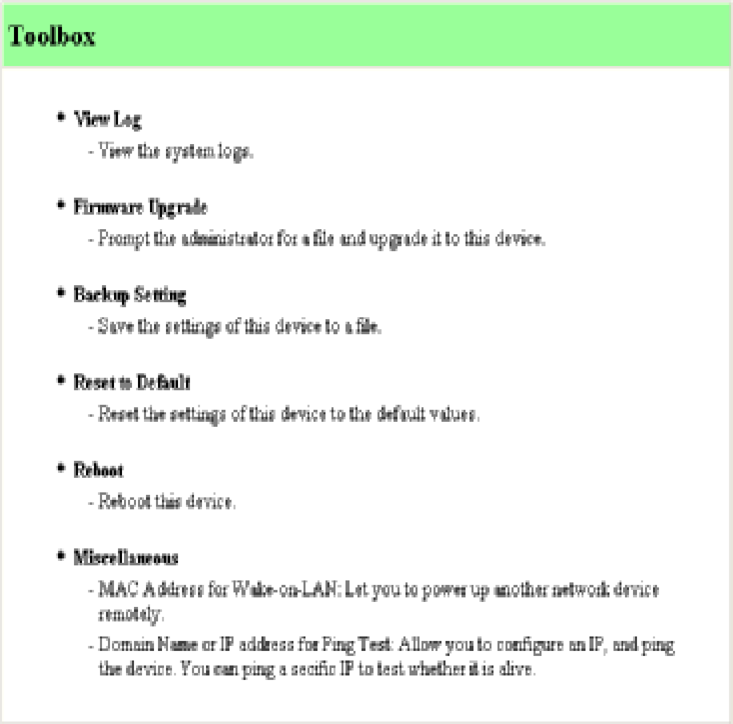
○ Deny all to pass except those match the following rules.

ID	Source IP : Ports		Destination IP : Ports		Enable	Use Rule#
1				20-21	☑	1
2					□	0
3					□	0
4					□	0
5					□	0
6					□	0
7					□	0
8					□	0

Schedule rule (00)Always Copy to ID --

4.8 Toolbox

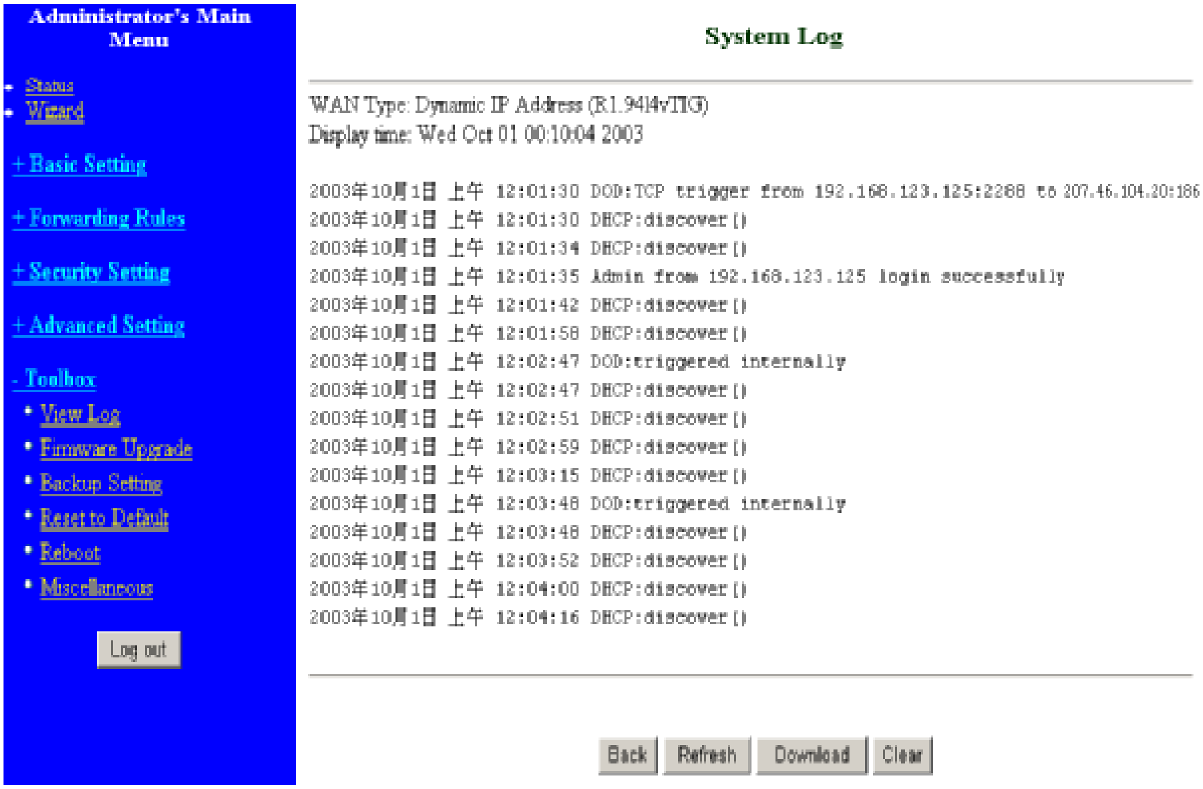




Toolbox

- **View Log**
  - View the system logs.
- **Firmware Upgrade**
  - Prompt the administrator for a file and upgrade it to this device.
- **Backup Setting**
  - Save the settings of this device to a file.
- **Reset to Default**
  - Reset the settings of this device to the default values.
- **Reboot**
  - Reboot this device.
- **Miscellaneous**
  - MAC Address for Wake-on-LAN: Let you to power up another network device remotely.
  - Domain Name or IP address for Ping Test: Allow you to configure an IP, and ping the device. You can ping a secific IP to test whether it is alive.

4.8.1 System Log



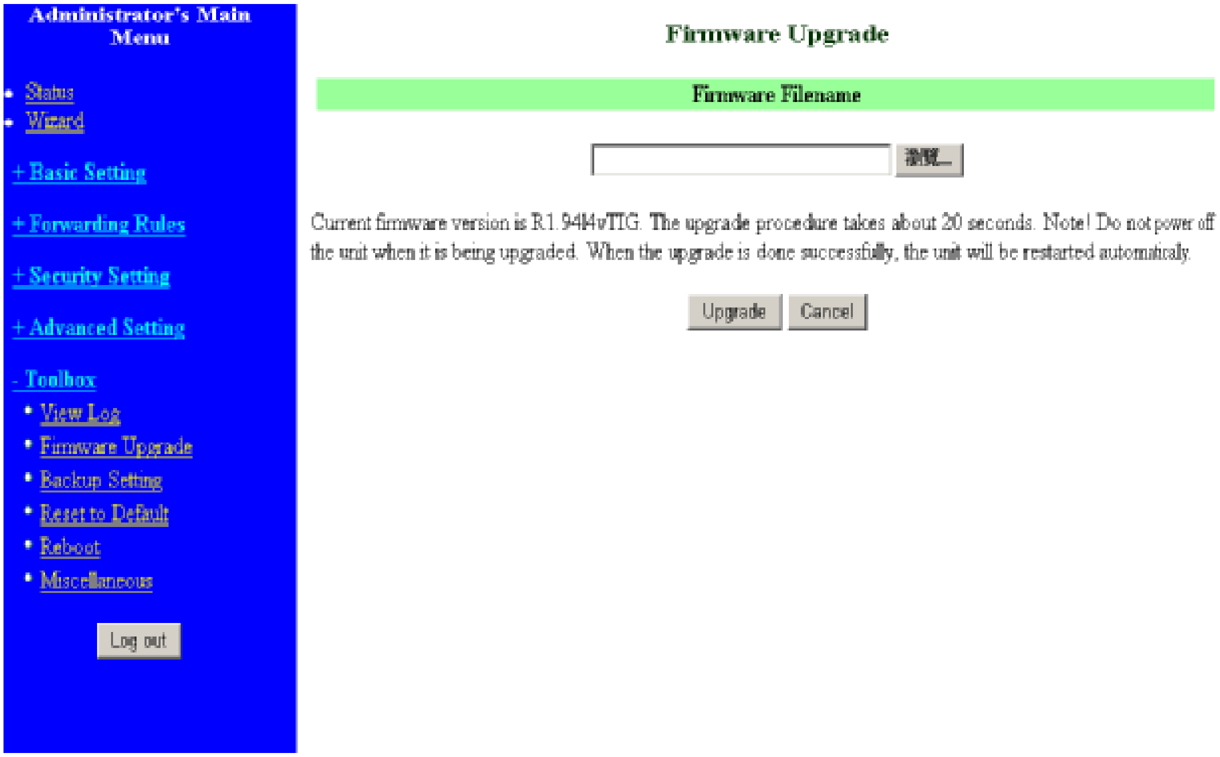
System Log

WAN Type: Dynamic IP Address (R1.94l4vTIG)
Display time: Wed Oct 01 00:10:04 2003

```
2003年10月1日 上午 12:01:30 DOD:TCP trigger from 192.168.123.125:2288 to 207.46.104.20:186
2003年10月1日 上午 12:01:30 DHCP:discover()
2003年10月1日 上午 12:01:34 DHCP:discover()
2003年10月1日 上午 12:01:35 Admin from 192.168.123.125 login successfully
2003年10月1日 上午 12:01:42 DHCP:discover()
2003年10月1日 上午 12:01:58 DHCP:discover()
2003年10月1日 上午 12:02:47 DOD:triggered internally
2003年10月1日 上午 12:02:47 DHCP:discover()
2003年10月1日 上午 12:02:51 DHCP:discover()
2003年10月1日 上午 12:02:59 DHCP:discover()
2003年10月1日 上午 12:03:15 DHCP:discover()
2003年10月1日 上午 12:03:48 DOD:triggered internally
2003年10月1日 上午 12:03:48 DHCP:discover()
2003年10月1日 上午 12:03:52 DHCP:discover()
2003年10月1日 上午 12:04:00 DHCP:discover()
2003年10月1日 上午 12:04:16 DHCP:discover()
```

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

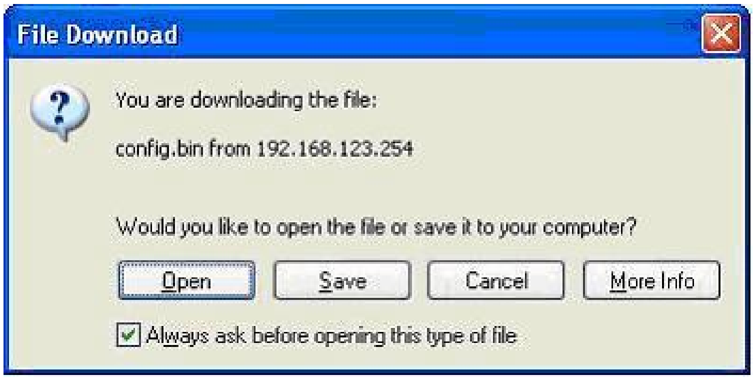
4.8.2 Firmware Upgrade



Current firmware version is R1.94h4vTIG. The upgrade procedure takes about 20 seconds. Note! Do not power off the unit when it is being upgraded. When the upgrade is done successfully, the unit will be restarted automatically.

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

4.8.3 Backup Setting


File Download

You are downloading the file:

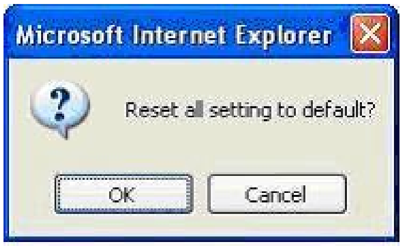
config.bin from 192.168.123.254

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

☑ Always ask before opening this type of file

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.

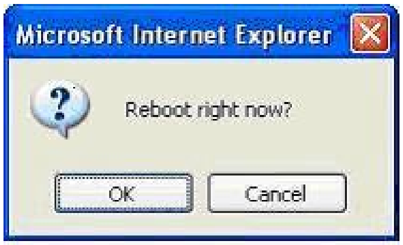
4.8.4 Reset to default


Microsoft Internet Explorer

Reset all setting to default?

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

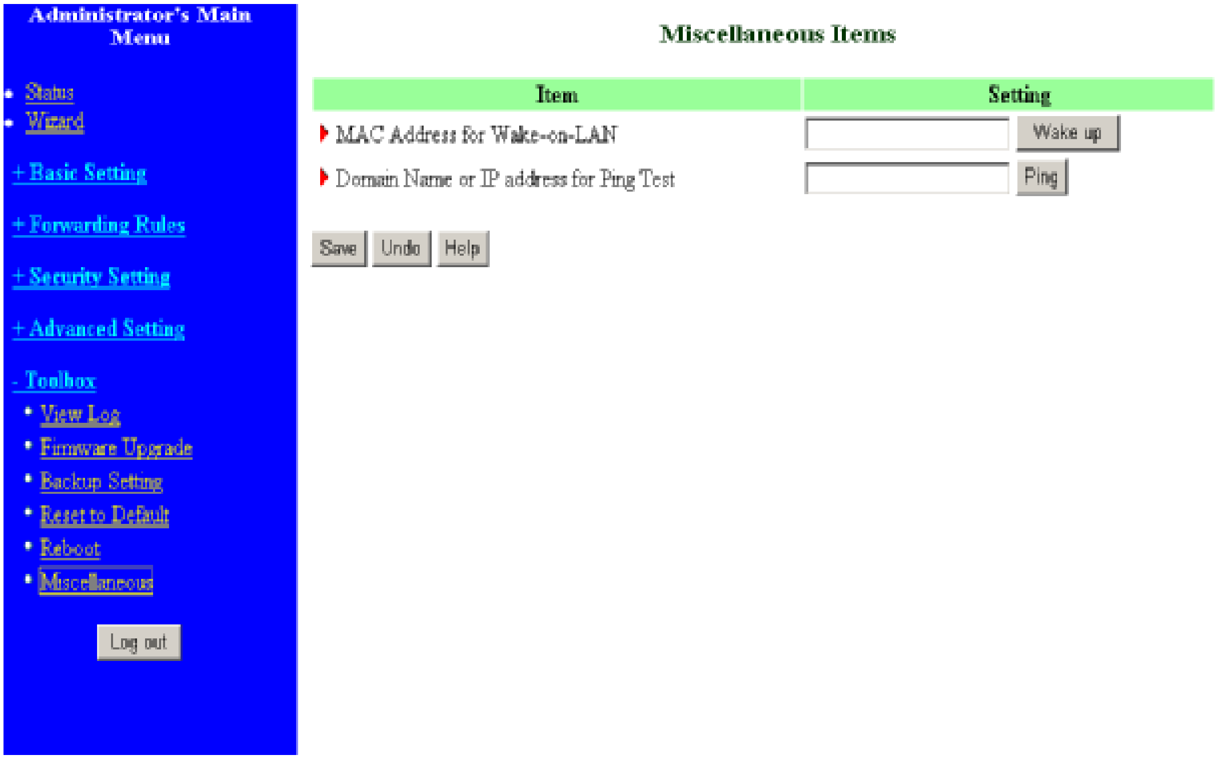
4.8.5 Reboot


Microsoft Internet Explorer

Reboot right now?

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

4.8.6 Miscellaneous Items



Miscellaneous Items

Item	Setting
MAC Address for Wake-on-LAN	Wake up
Domain Name or IP address for Ping Test	Ping

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

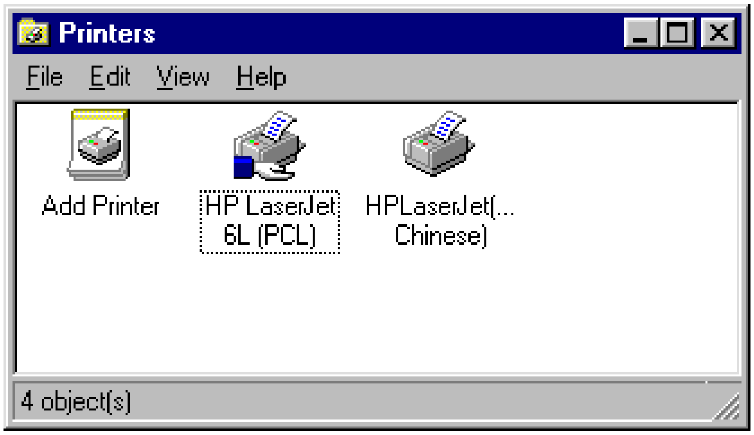
Allow you to configure an IP, and ping the device. You can ping a specific IP to test whether it is alive.

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.)

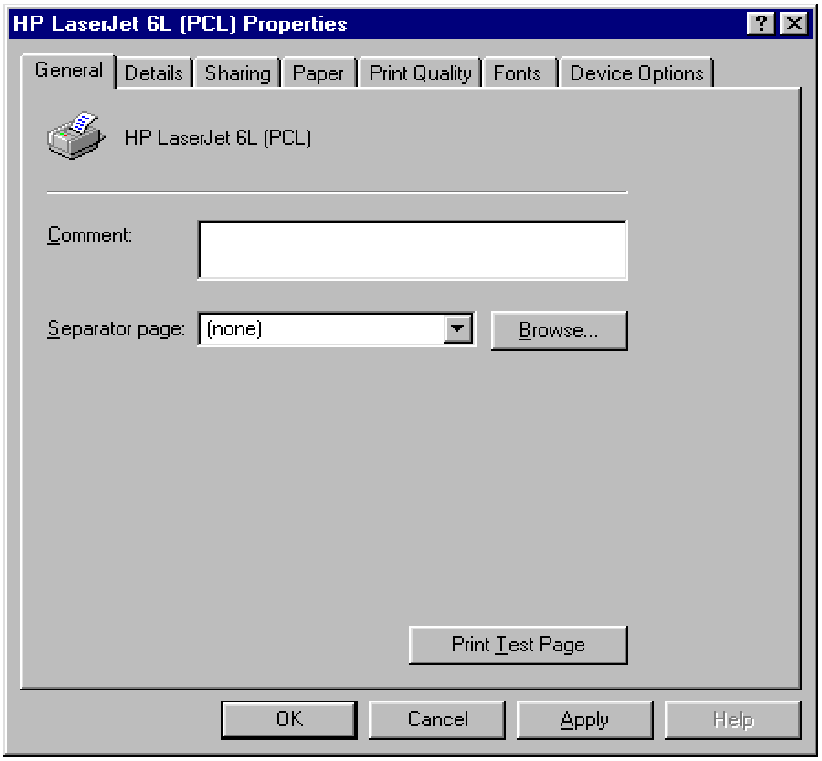
5.1 Configuring on Windows 95/98 Platforms

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, yon can configure the print server of this product:

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



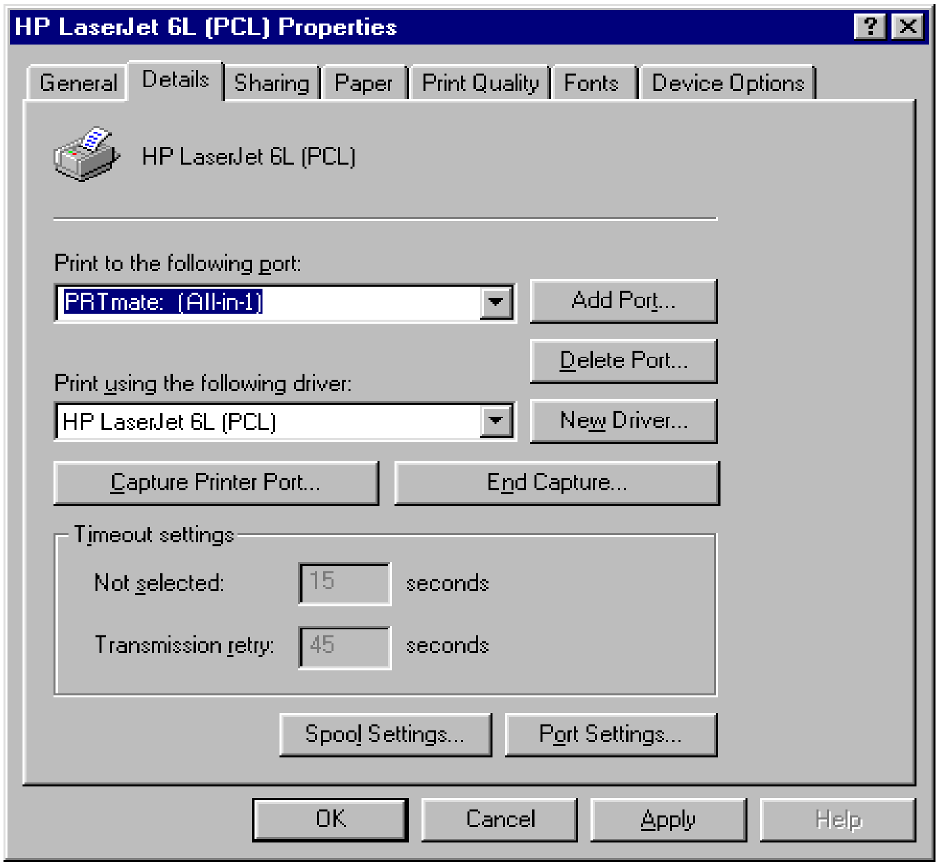
HP LaserJet 6L (PCL) Properties

HP LaserJet 6L (PCL)

Comment:

Separator page: (none)

2. Click the **Details** item:



HP LaserJet 6L (PCL)

Print to the following port: PRTmate: (All-in-1)

Print using the following driver: HP LaserJet 6L (PCL)

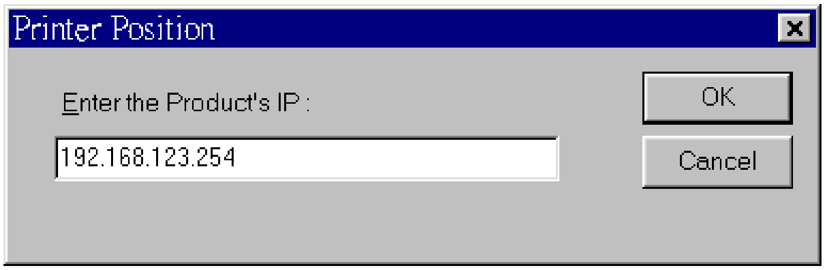
Timeout settings

Not selected: 15 seconds

Transmission retry: 45 seconds

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

4. Click on the button of **Port Settings**:



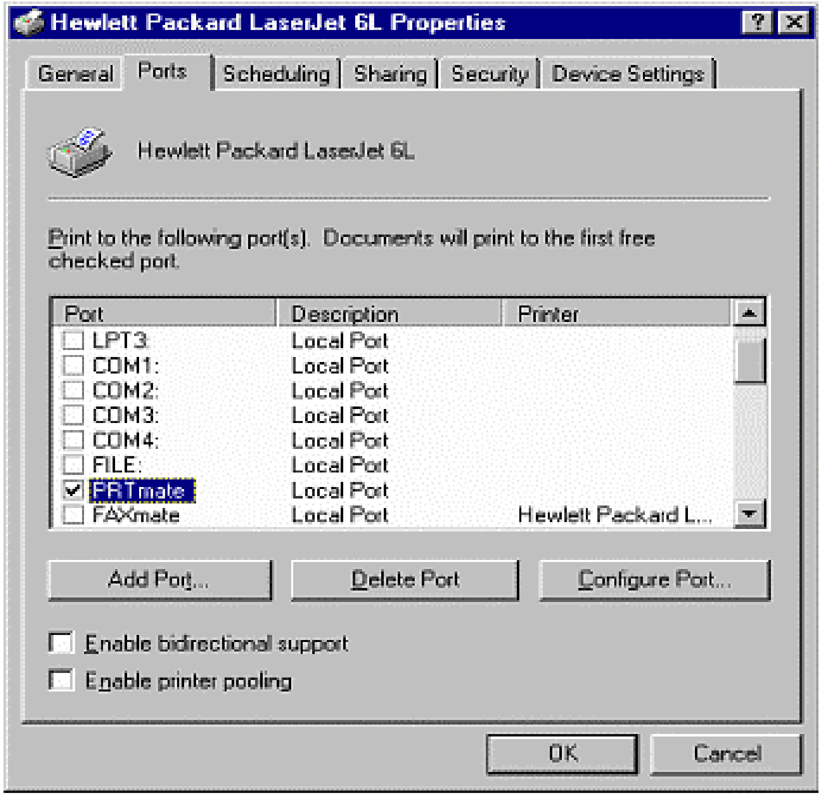
Enter the Product's IP : 192.168.123.254

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**:



Hewlett Packard LaserJet 6L

Print to the following port(s). Documents will print to the first free checked port.

Port	Description	Printer
□ LPT3:	Local Port	
□ COM1:	Local Port	
□ COM2:	Local Port	
□ COM3:	Local Port	
□ COM4:	Local Port	
□ FILE:	Local Port	
☑ PRTmate	Local Port	
□ FAXmate	Local Port	Hewlett Packard L...

□ Enable bidirectional support

□ Enable printer pooling

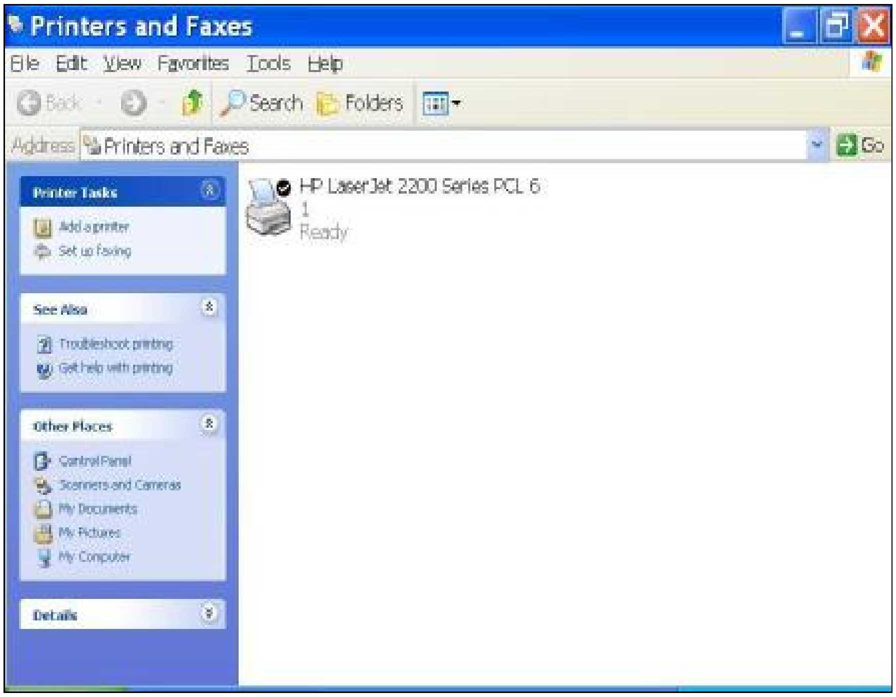
Compared to the procedure in last section, the selection of **Details** is equivalent to the selection of **Ports**, and **Port Settings** is equivalent to **Configure Port**.

5.3 Configuring on Windows 2000 and XP Platforms

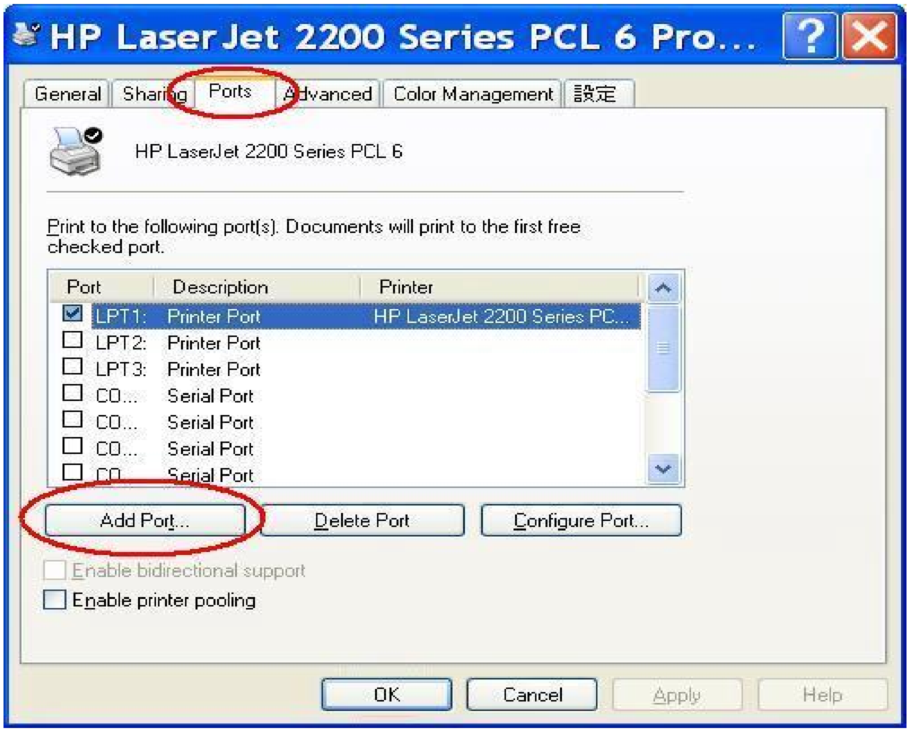
Windows 2000 and XP have built-in LPR client, users could utilize this feature to Print.

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

1.Open Printers and Faxes.



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


HP LaserJet 2200 Series PCL 6 Pro...
General
Sharing
Ports
Advanced
Color Management
設定
HP LaserJet 2200 Series PCL 6

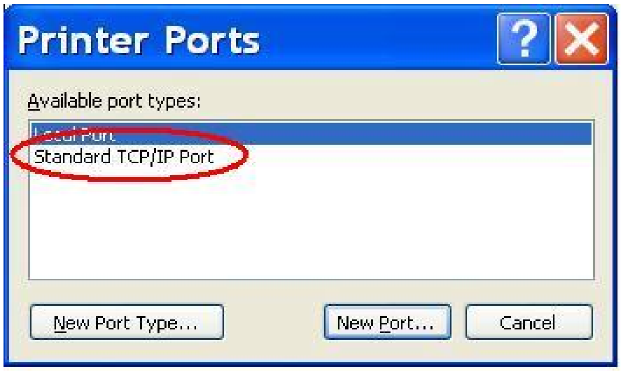
Print to the following port(s). Documents will print to the first free checked port.

Port	Description	Printer
☑ LPT1:	Printer Port	HP LaserJet 2200 Series PC...
□ LPT2:	Printer Port	
□ LPT3:	Printer Port	
□ CO...	Serial Port	
□ CO...	Serial Port	
□ CO...	Serial Port	
□ CO...	Serial Port	

□ Enable bidirectional support

□ Enable printer pooling

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

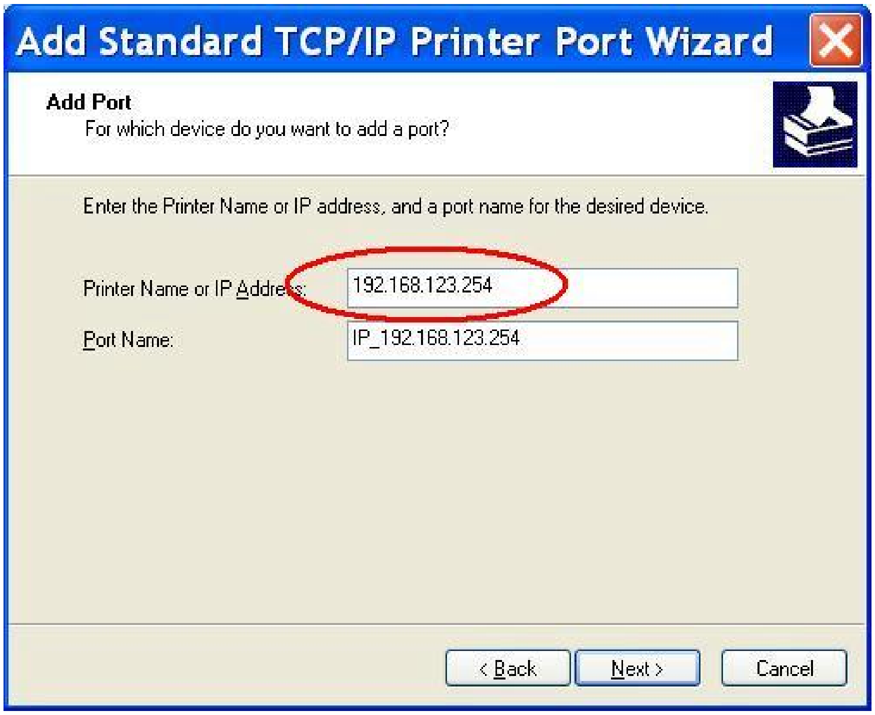


Available port types:

Local Port
Standard TCP/IP 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



Add Standard TCP/IP Printer Port Wizard

Add Port

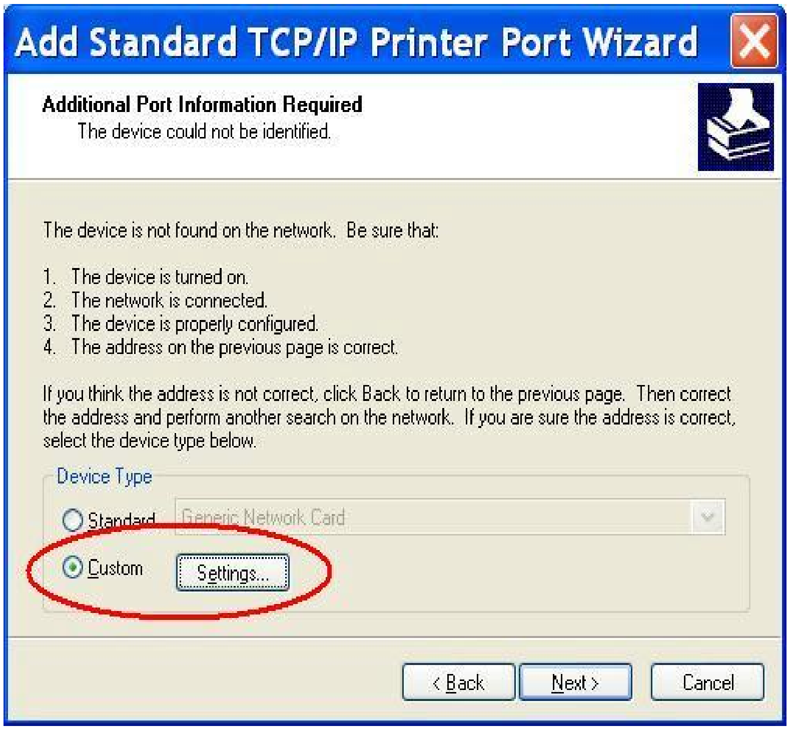
For which device do you want to add a port?

Enter the Printer Name or IP address, and a port name for the desired device.

Printer Name or IP Address: 192.168.123.254

Port Name: IP_192.168.123.254

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



Add Standard TCP/IP Printer Port Wizard

Additional Port Information Required

The device could not be identified.

The device is not found on the network. Be sure that:

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.

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.

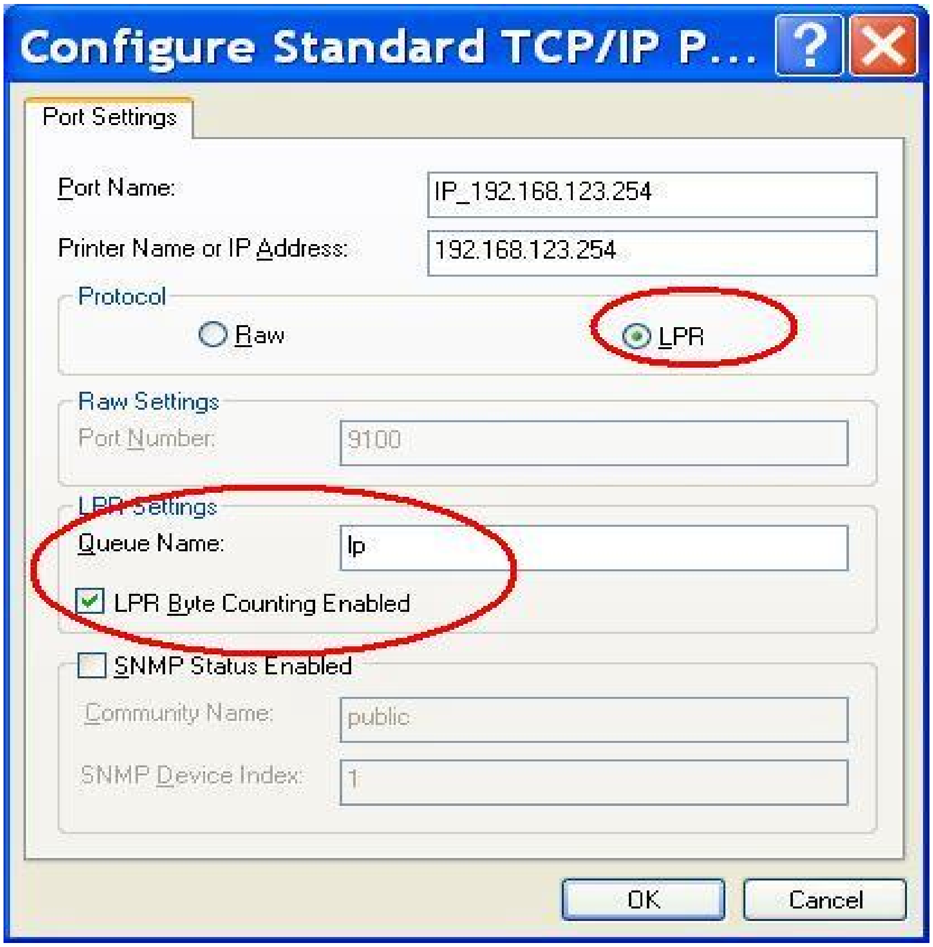
Device Type

○ Standard Generic Network Card

● Custom Settings...

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

And enable “LPR Byte Counting Enabled”.



Configure Standard TCP/IP P...

Port Settings

Port Name: IP_192.168.123.254

Printer Name or IP Address: 192.168.123.254

Protocol

○ Raw ● LPR

Raw Settings

Port Number: 9100

LPR Settings

Queue Name: lp

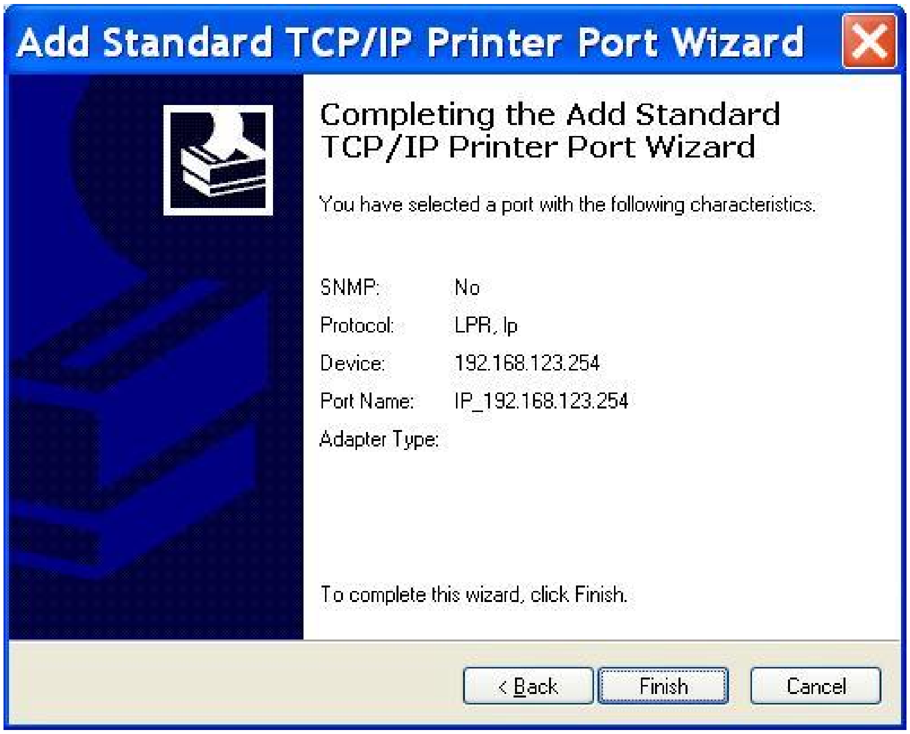
☑ LPR Byte Counting Enabled

□ SNMP Status Enabled

Community Name: public

SNMP Device Index: 1

7.Apply your settings

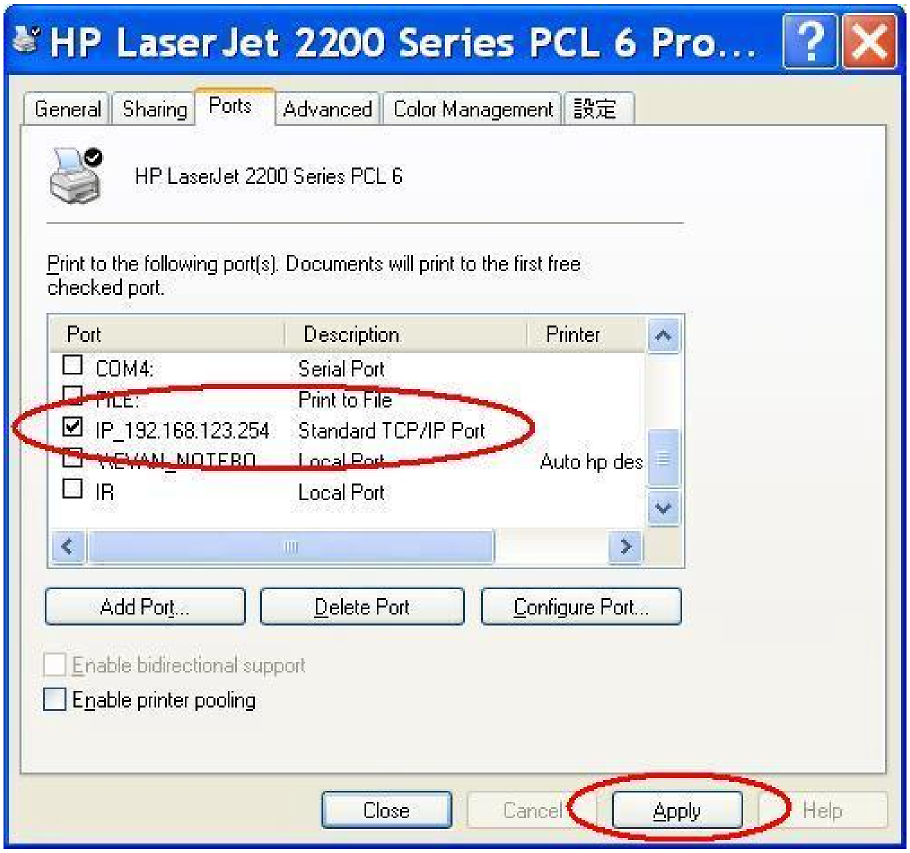

Add Standard TCP/IP Printer Port Wizard

Completing the Add Standard TCP/IP Printer Port Wizard

You have selected a port with the following characteristics.

SNMP: No
Protocol: LPR, lp
Device: 192.168.123.254
Port Name: IP_192.168.123.254
Adapter Type:

To complete this wizard, click Finish.


HP LaserJet 2200 Series PCL 6 Pro...

HP LaserJet 2200 Series PCL 6

Print to the following port(s). Documents will print to the first free checked port.

Port	Description	Printer
□ COM4:	Serial Port	
□ FILE:	Print to File	
☑ IP_192.168.123.254	Standard TCP/IP Port	
□ \\KEVAN_NOTEBO	Local Port	Auto hp des
□ IR	Local Port	

□ Enable bidirectional support

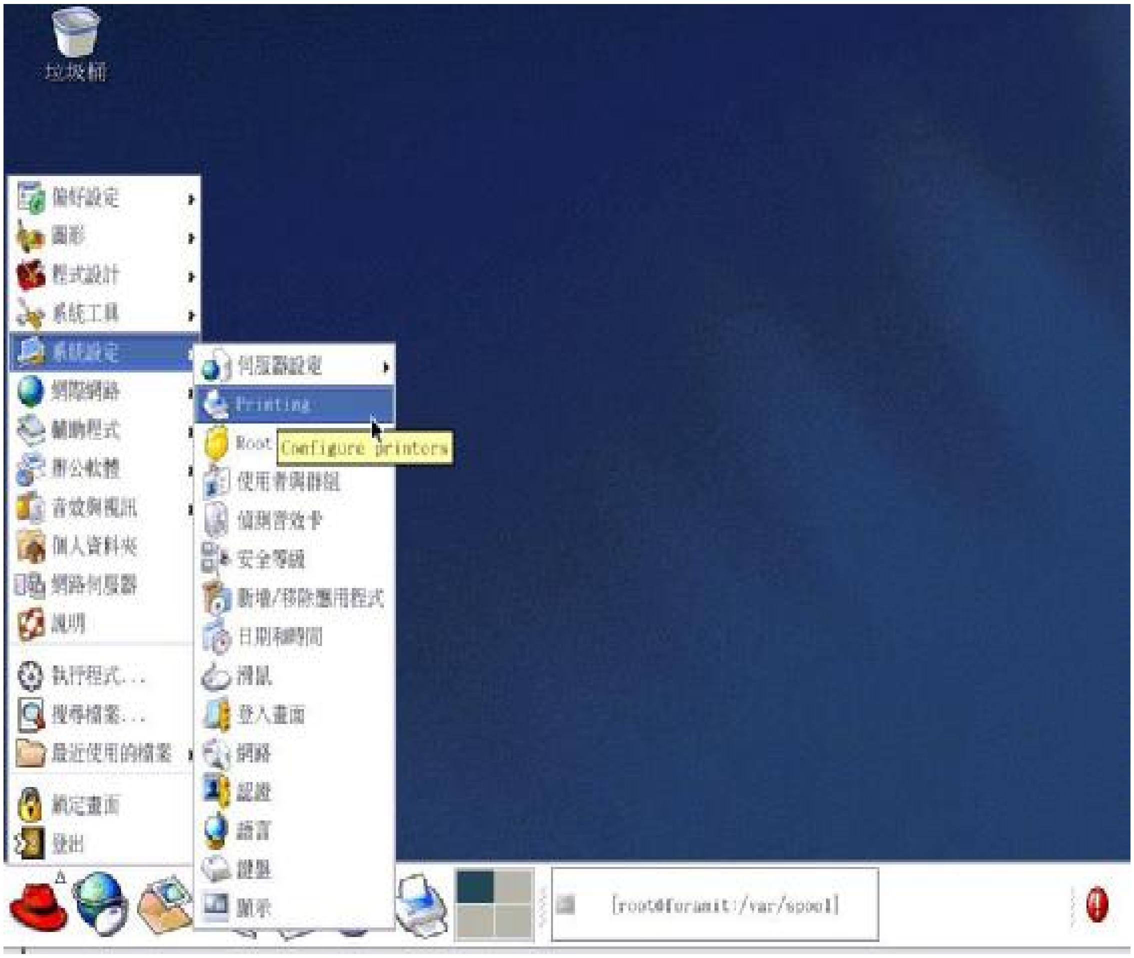
□ Enable printer pooling

5.4 Configuring on Unix-like based Platforms

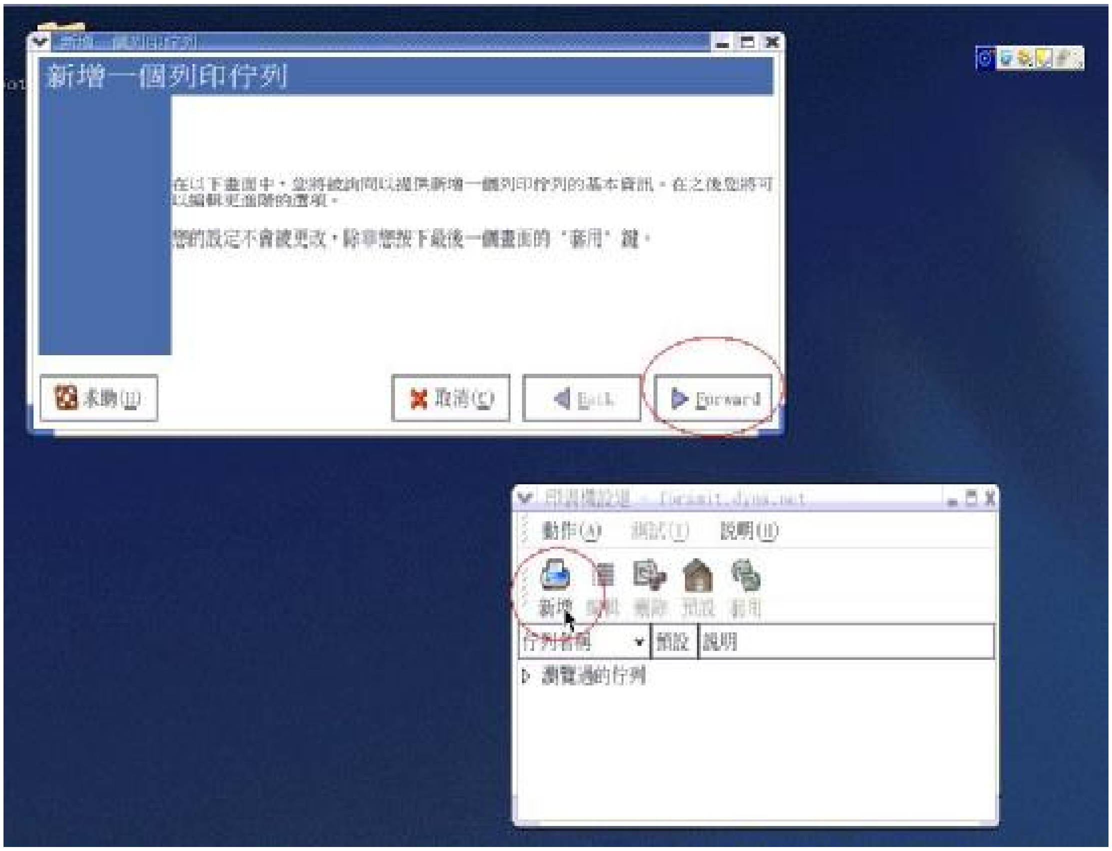
Please follow the traditional configuration procedure on Unix platforms to setup the print server of this product. The printer name is “lp.”

In X-Windows, for example, In Redhat Platforms,
Please follow the below steps to configure your printer on Red Hat 9.0.

1. Starts from the Red Hat---> System Setting---> Printing.



2. Click Add---> Forward.

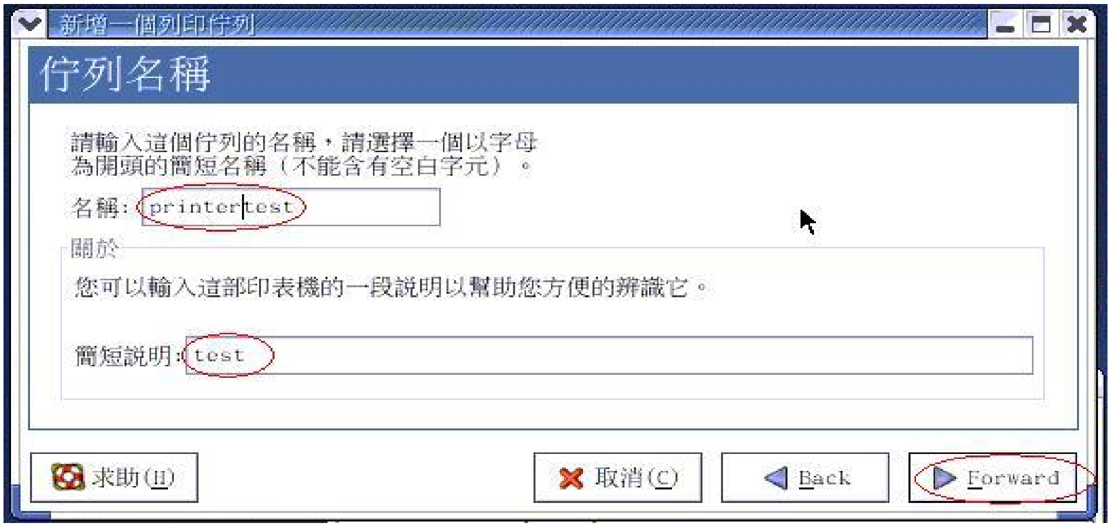


新增一個列印佇列

在以下畫面中，您將被詢問以提供新增一個列印佇列的基本資訊。在之後您將可以編輯更進階的選項。

您的設定不會被更改，除非您按下最後一個畫面的"套用"鍵。

3. Enter the Pinter Name, Comments then forward.



佇列名稱

請輸入這個佇列的名稱，請選擇一個以字母
為開頭的簡短名稱（不能含有空白字元）。

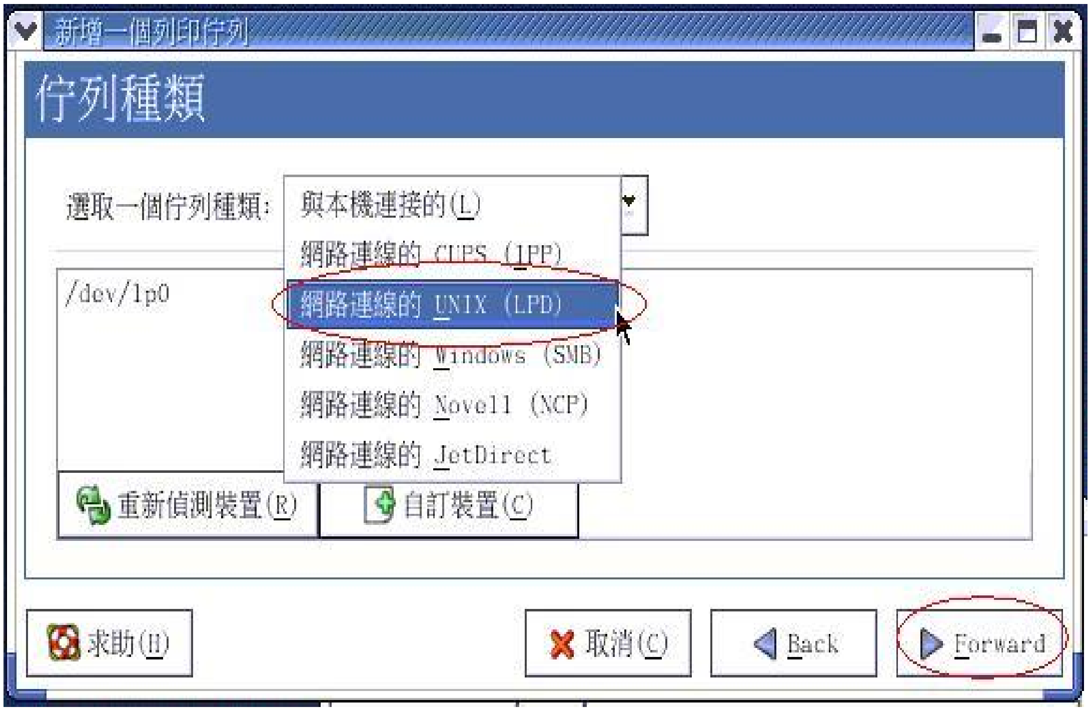
名稱：printertest

關於

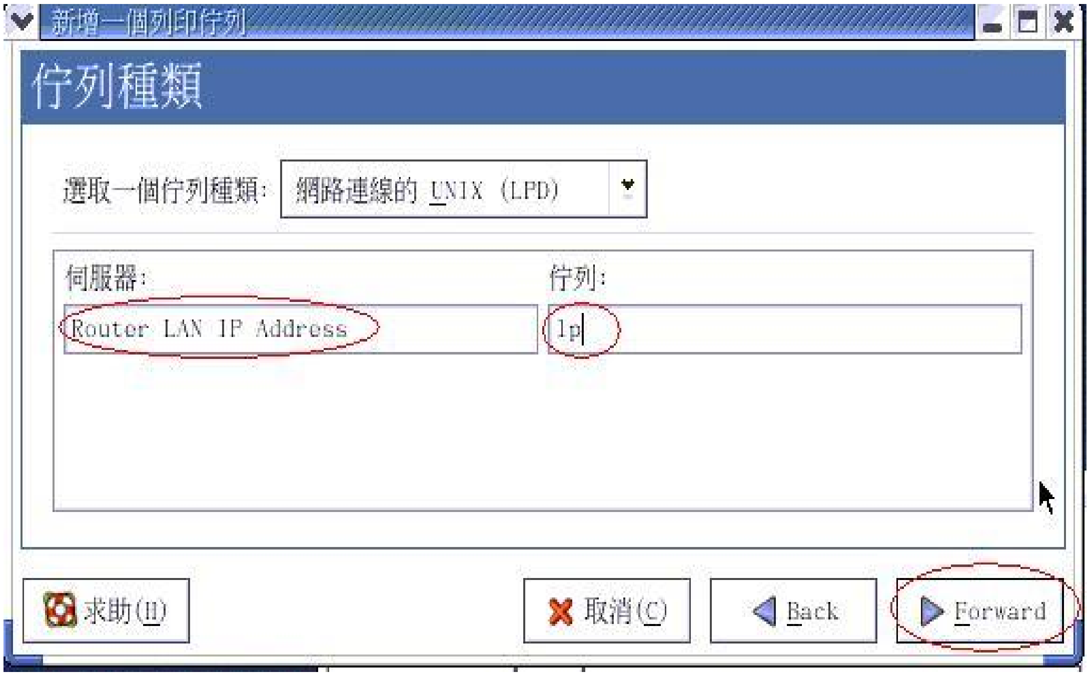
您可以輸入這部印表機的一段說明以幫助您方便的辨識它。

簡短說明：test

4. Select LPD protocol and then forward.



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

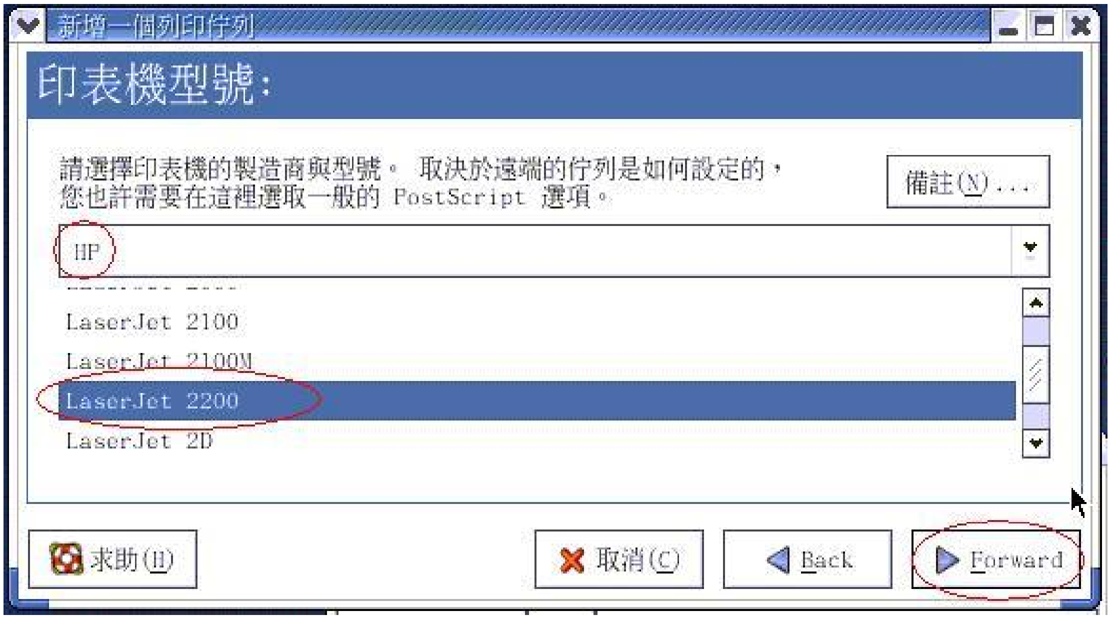


選取一個佇列種類: 網路連線的 UNIX (LPD)

伺服器: Router LAN IP Address

佇列: lp

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



新增一個列印佇列

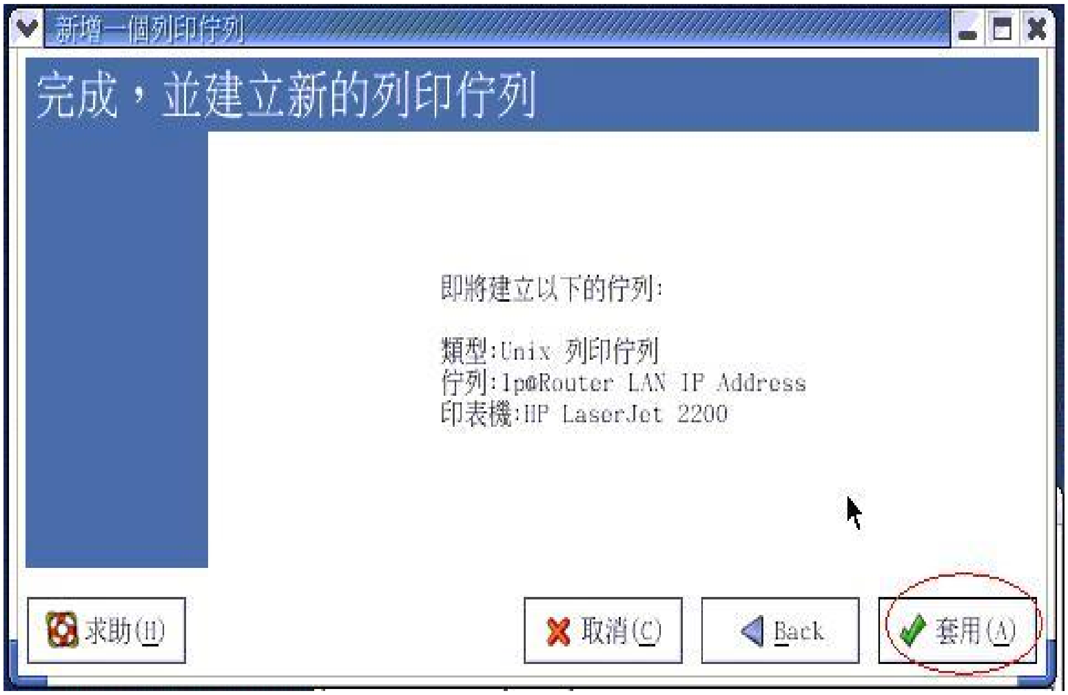
印表機型號:

請選擇印表機的製造商與型號。 取決於遠端的佇列是如何設定的，
您也許需要在這裡選取一般的 PostScript 選項。

HP

LaserJet 2100
LaserJet 2100M
LaserJet 2200
LaserJet 2D

7. Click Apply to finish setup.



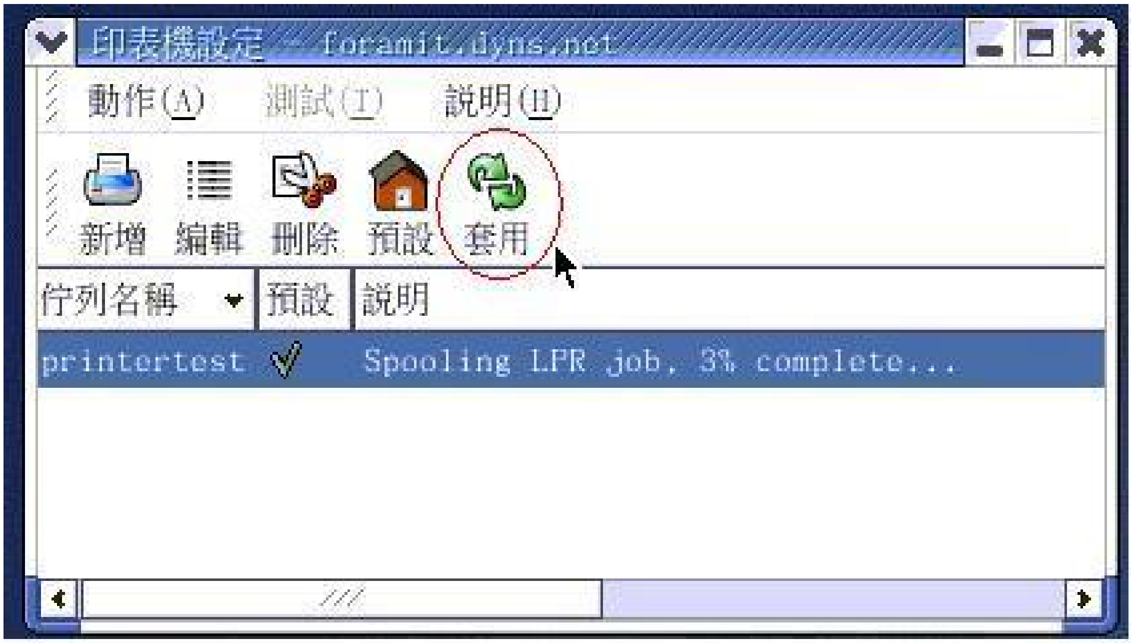
新增一個列印佇列

完成，並建立新的列印佇列

即將建立以下的佇列:

類型:Unix 列印佇列
佇列:lp@Router LAN IP Address
印表機:HP LaserJet 2200

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



佇列名稱	預設	說明
printertest	✓	Spooling LPR job, 3% complete...

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

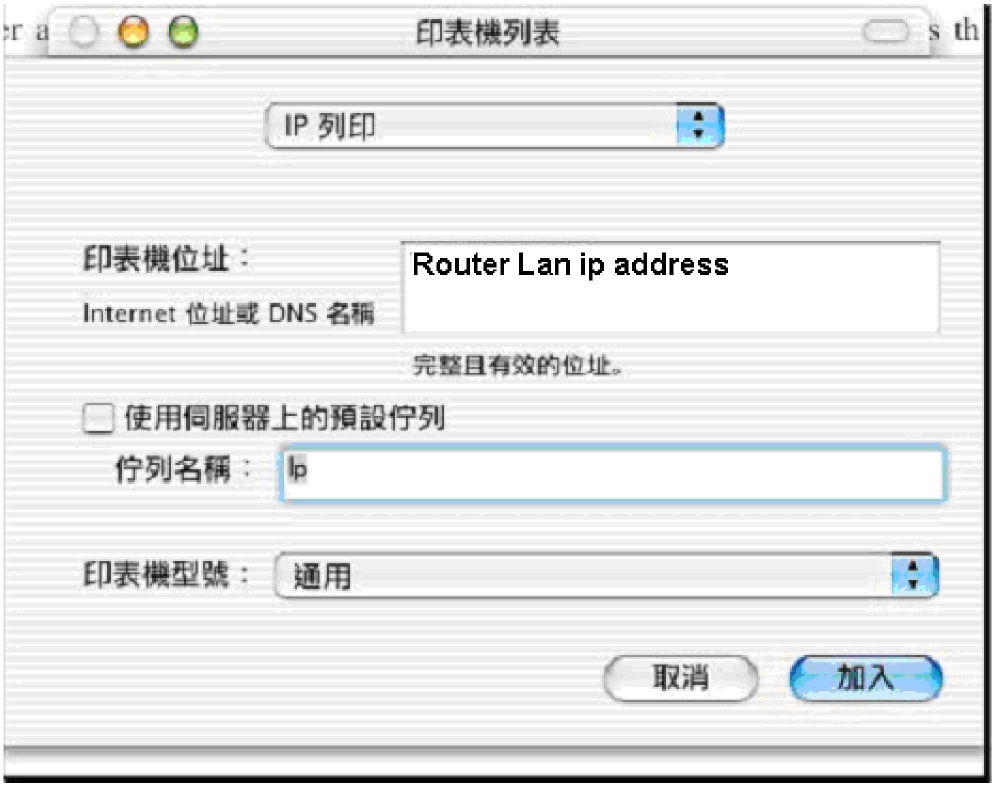
```
#mkdir /var/spool/lpd/lp
```

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



IP 列印

印表機位址：
Internet 位址或 DNS 名稱
Router Lan ip address

☐ 使用伺服器上的預設佇列

佇列名稱： lp

印表機型號： 通用

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

3.Disable “Default Queue of Server.” And fill in ‘ **lp** ‘ in Queue name item.

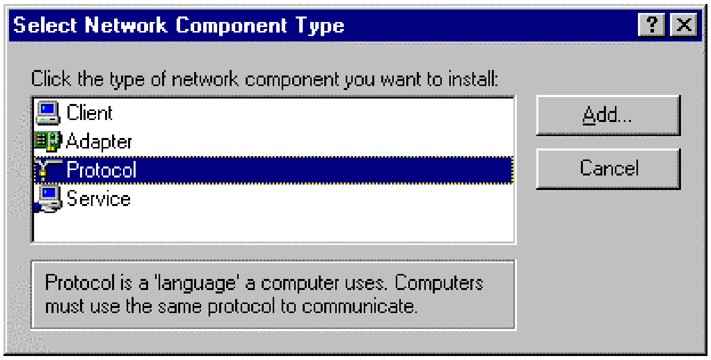
4.Printer type: Choose “General”.

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.

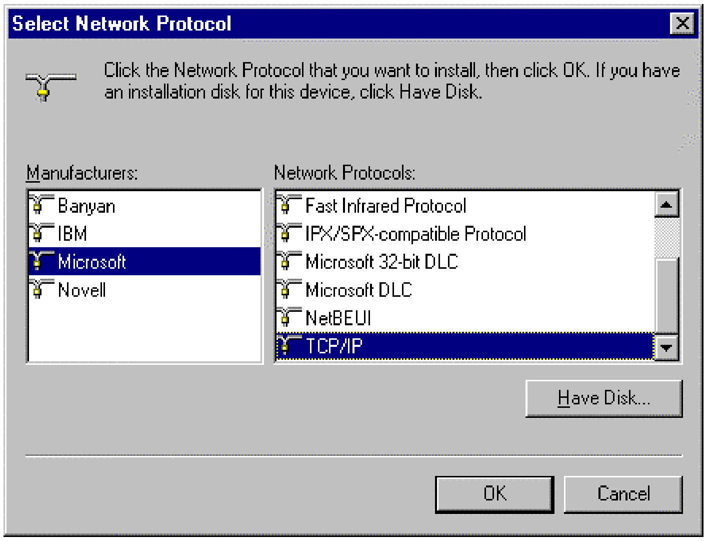
A.1 Install TCP/IP Protocol into Your PC

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.


Select Network Component Type
?
Click the type of network component you want to install:
Client
Adapter
Protocol
Service
Add...
Cancel

Protocol is a 'language' a computer uses. Computers must use the same protocol to communicate.

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



Select Network Protocol

Click the Network Protocol that you want to install, then click OK. If you have an installation disk for this device, click Have Disk.

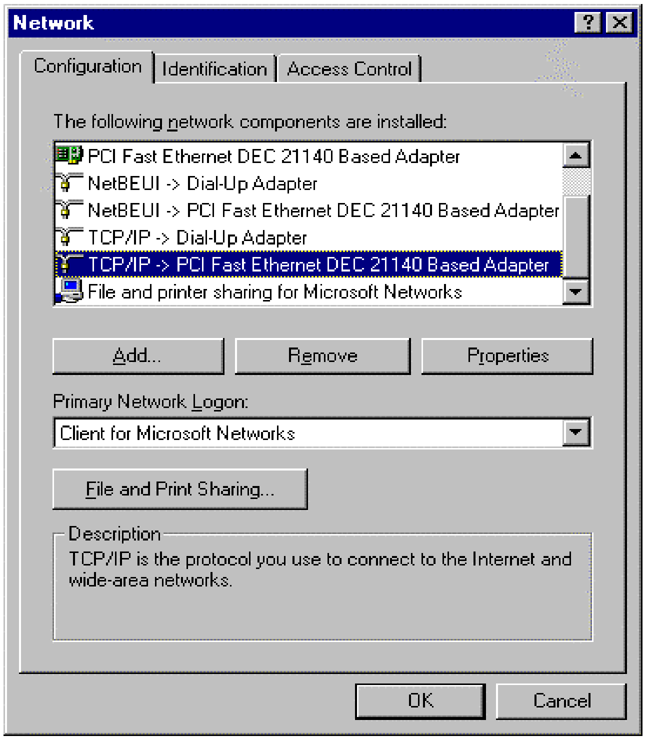
Manufacturers:
- Banyan
- IBM
- Microsoft
- Novell

Network Protocols:
- Fast Infrared Protocol
- IPX/SPX-compatible Protocol
- Microsoft 32-bit DLC
- Microsoft DLC
- NetBEUI
- TCP/IP

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.



The following network components are installed:

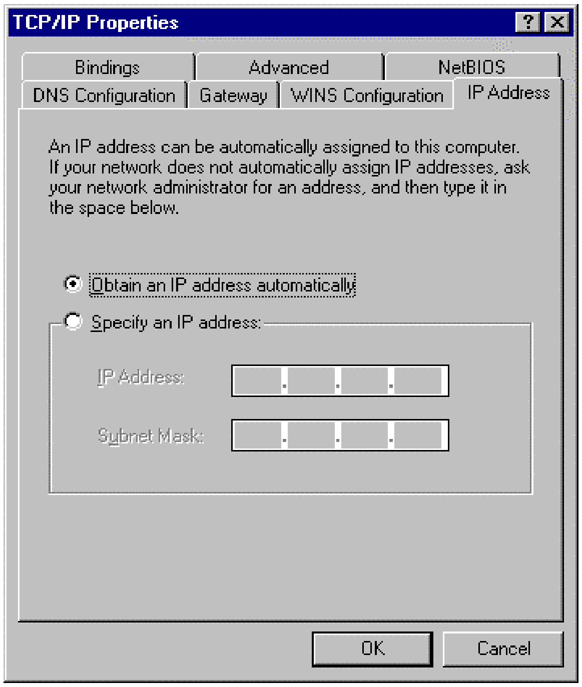
PCI Fast Ethernet DEC 21140 Based Adapter
NetBEUI -> Dial-Up Adapter
NetBEUI -> PCI Fast Ethernet DEC 21140 Based Adapter
TCP/IP -> Dial-Up Adapter
TCP/IP -> PCI Fast Ethernet DEC 21140 Based Adapter
File and printer sharing for Microsoft Networks

Primary Network Logon:
Client for Microsoft Networks

Description
TCP/IP is the protocol you use to connect to the Internet and wide-area networks.

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.

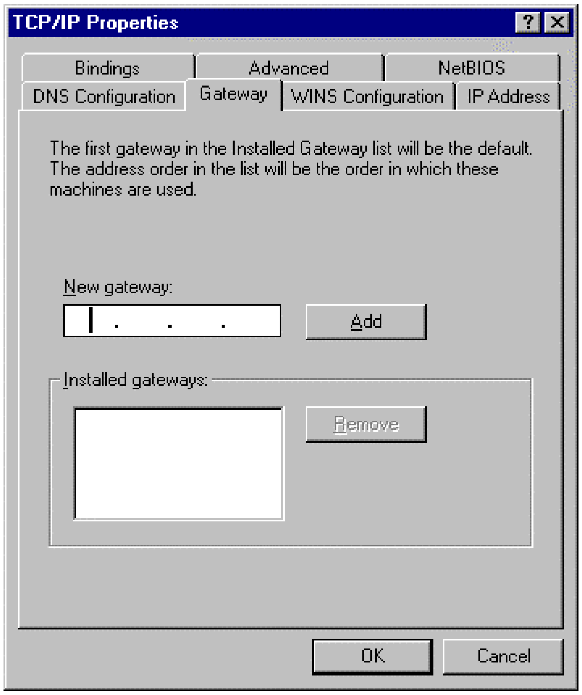


An IP address can be automatically assigned to this computer. If your network does not automatically assign IP addresses, ask your network administrator for an address, and then type it in the space below.

● Obtain an IP address automatically

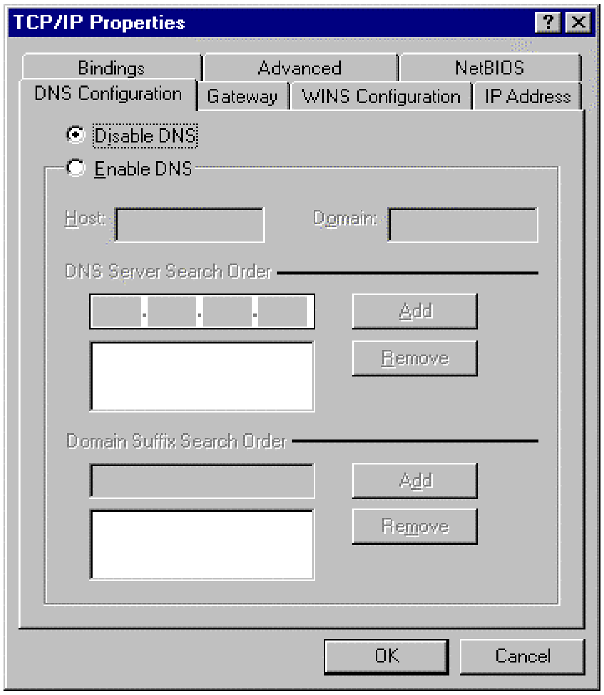
○ Specify an IP address:

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



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.

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

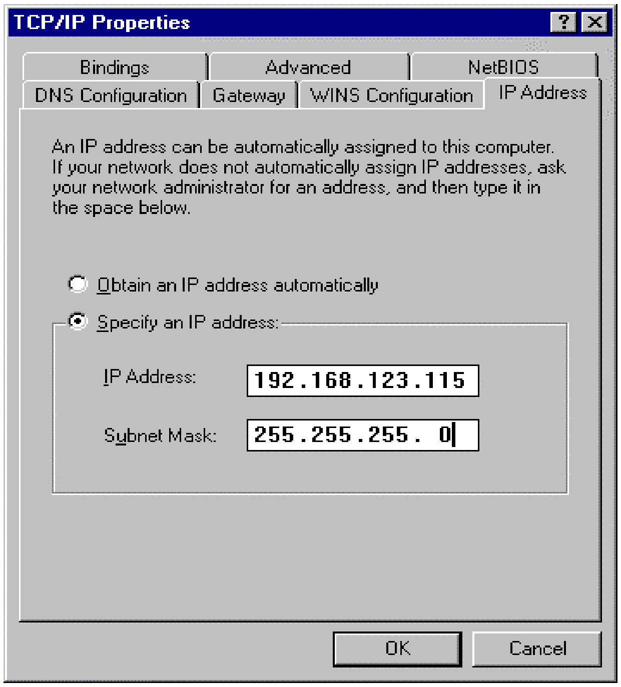


● Disable DNS

○ Enable DNS

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.



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.

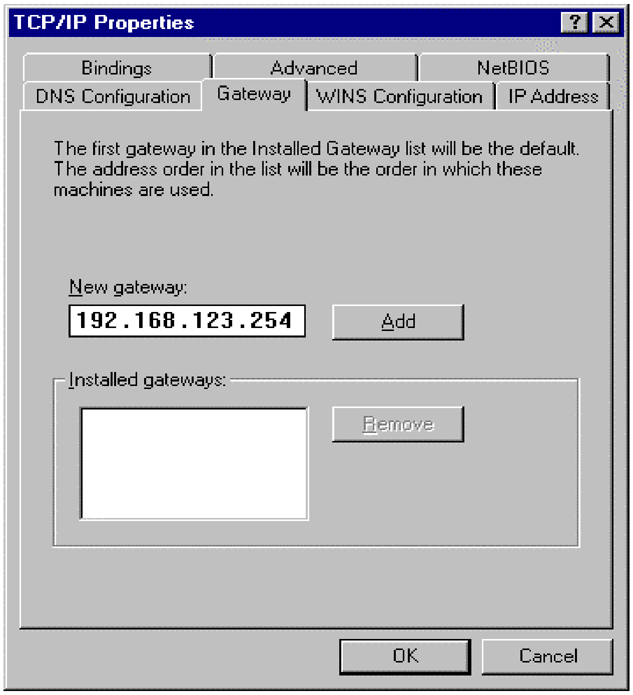
○ Obtain an IP address automatically

● Specify an IP address:

IP Address: 192.168.123.115

Subnet Mask: 255.255.255. 0

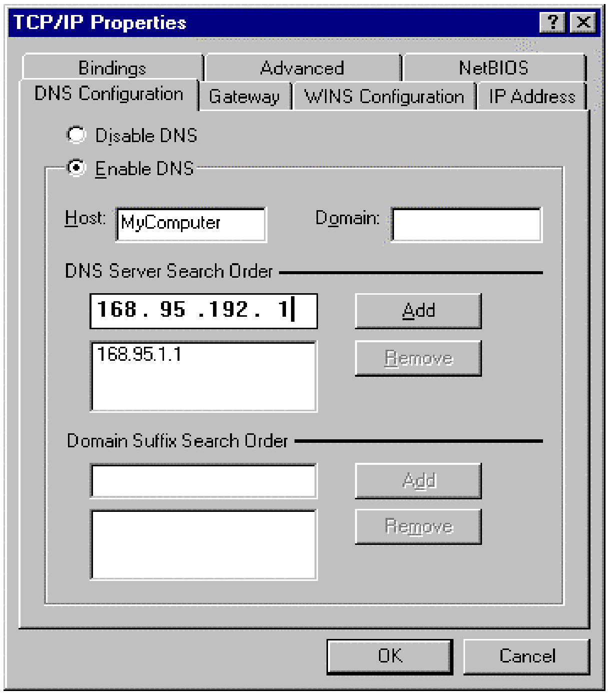
b. In the Gateway tab, add the IP address of this product (default IP is 192.168.123.254) in the New gateway field and click **Add** button.



The 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.

New gateway: 192.168.123.254

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.



○ Disable DNS

● Enable DNS

Host: MyComputer

Domain:

DNS Server Search Order

168 . 95 .192. 1

168.95.1.1

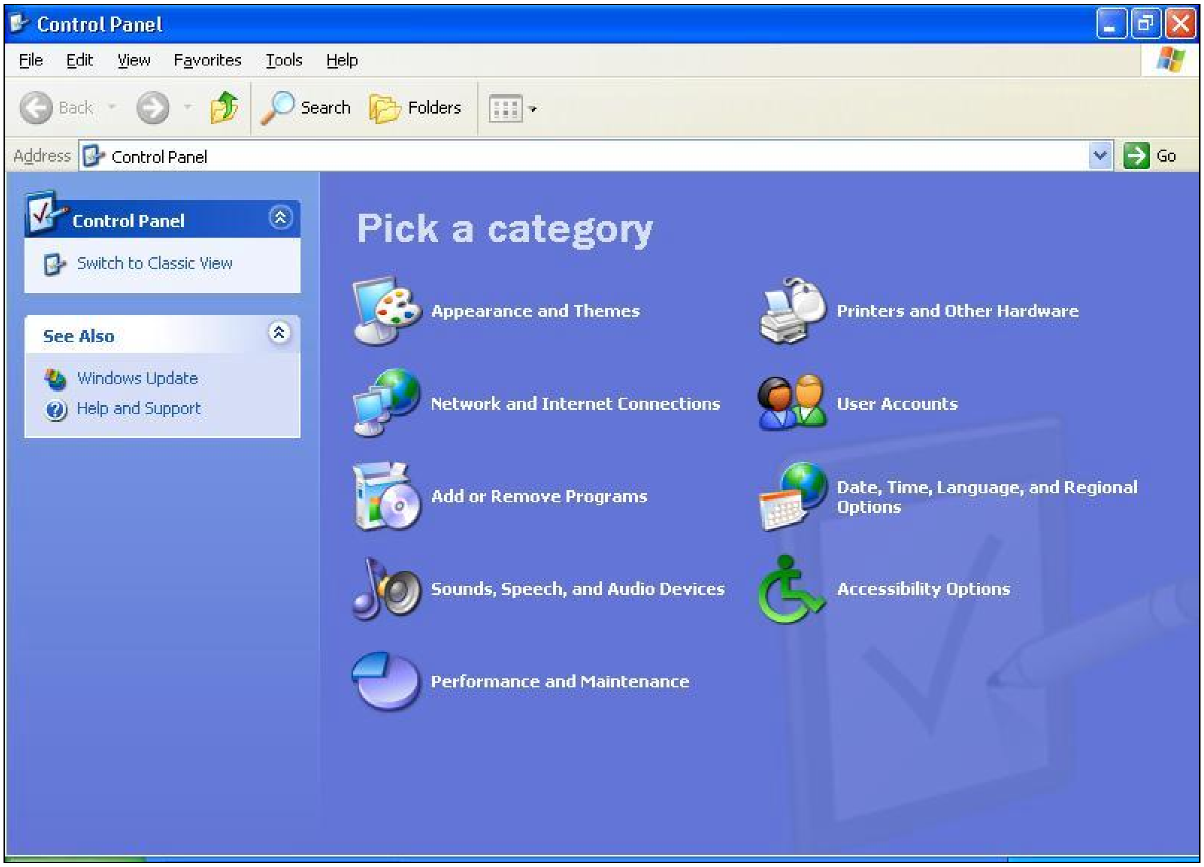
Appendix B Win 2000/XP IPSEC Setting guide

Example: Win XP/2000 à VPN Router

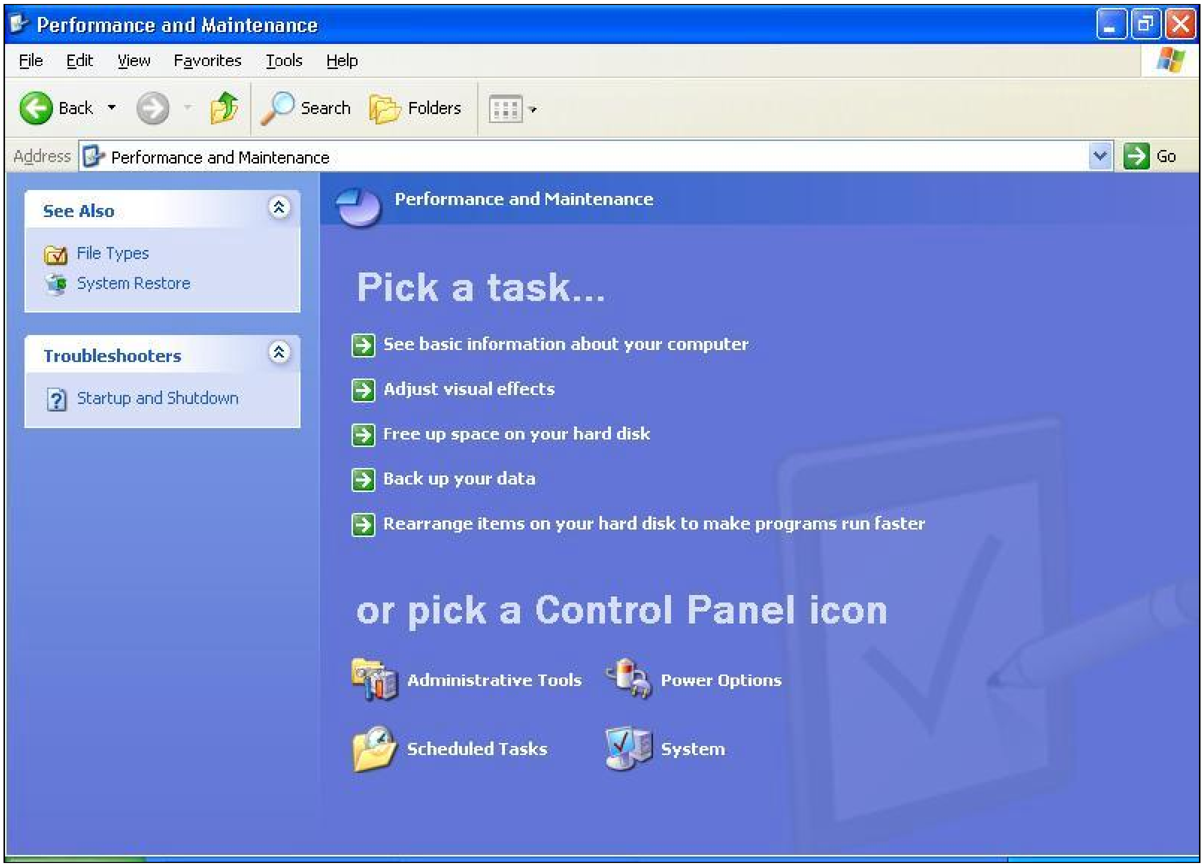
(Configuration on WIN 2000 is similar to XP)

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

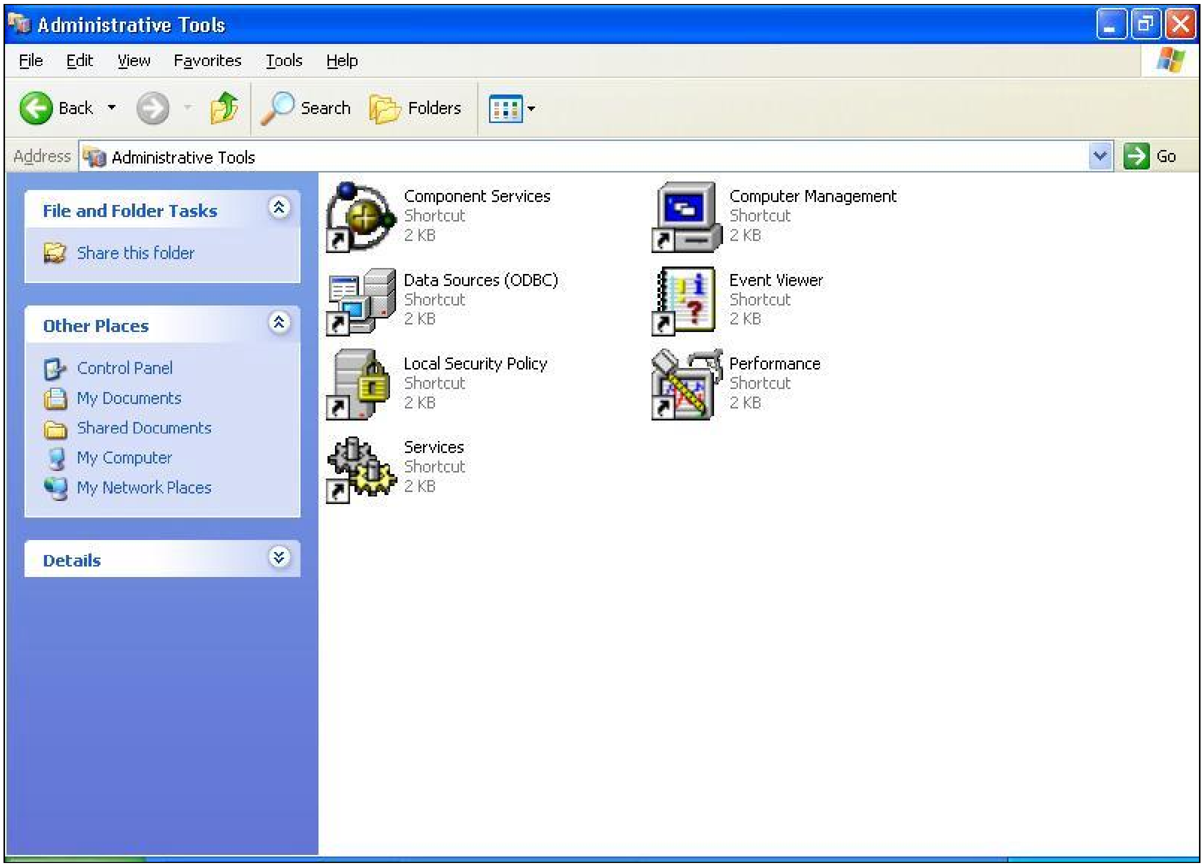
2. Or in Win XP, Click **[Control Pannel]**



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

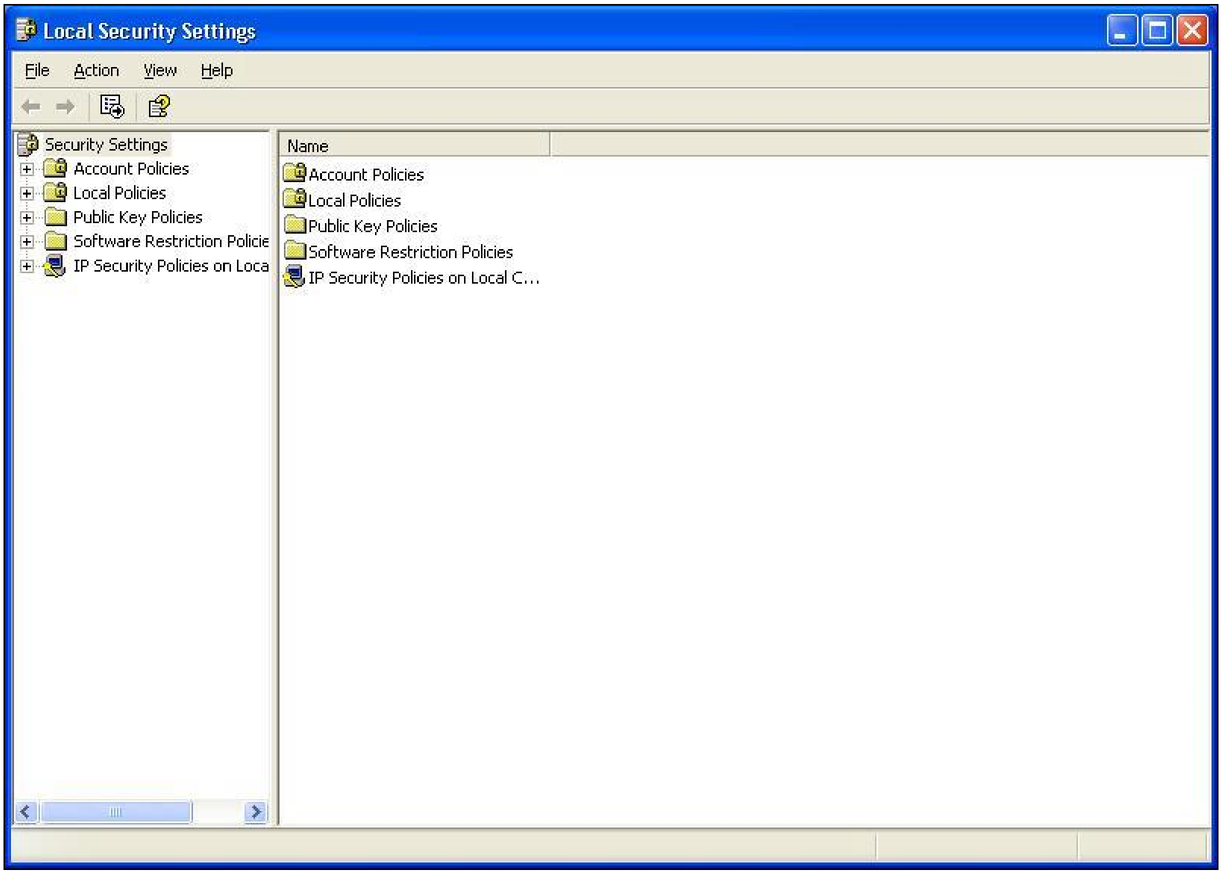

Performance and Maintenance
File
Edit
View
Favorites
Tools
Help
Back
Search
Folders
Address
Performance and Maintenance
Go
See Also
File Types
System Restore
Troubleshooters
Startup and Shutdown
Performance and Maintenance
Pick a task...
See basic information about your computer
Adjust visual effects
Free up space on your hard disk
Back up your data
Rearrange items on your hard disk to make programs run faster
or pick a Control Panel icon
Administrative Tools
Power Options
Scheduled Tasks
System

Double-click **[Administrative Tools]**



Local Security Policy Settings

Double-click **[Local Security Policy]**

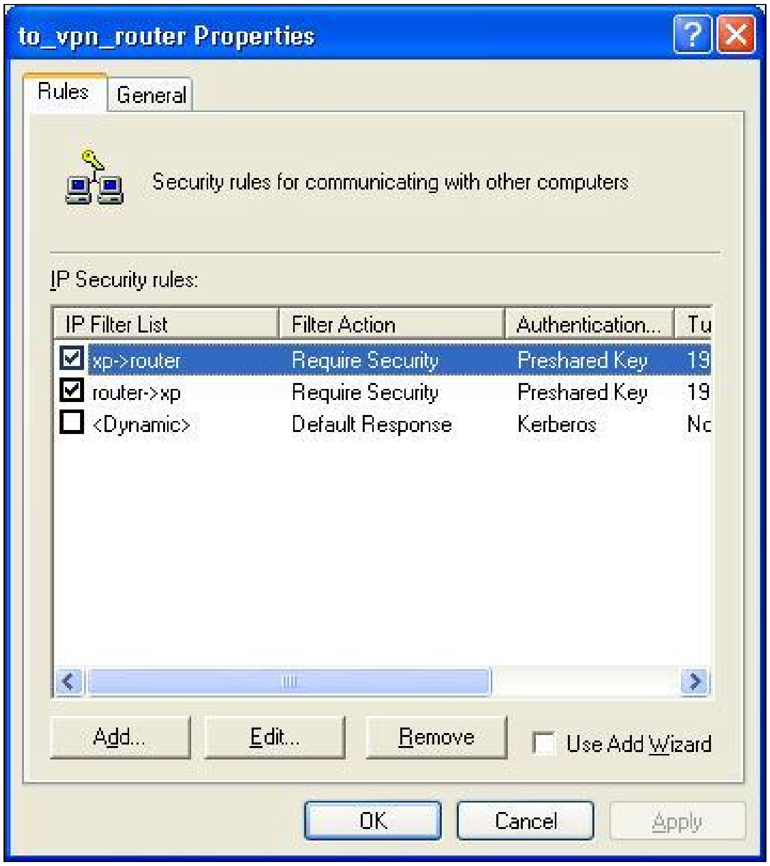


Right-click **[IP Security Policies on Local Computer]**, and click **[Create IP Security Policy]**.

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.

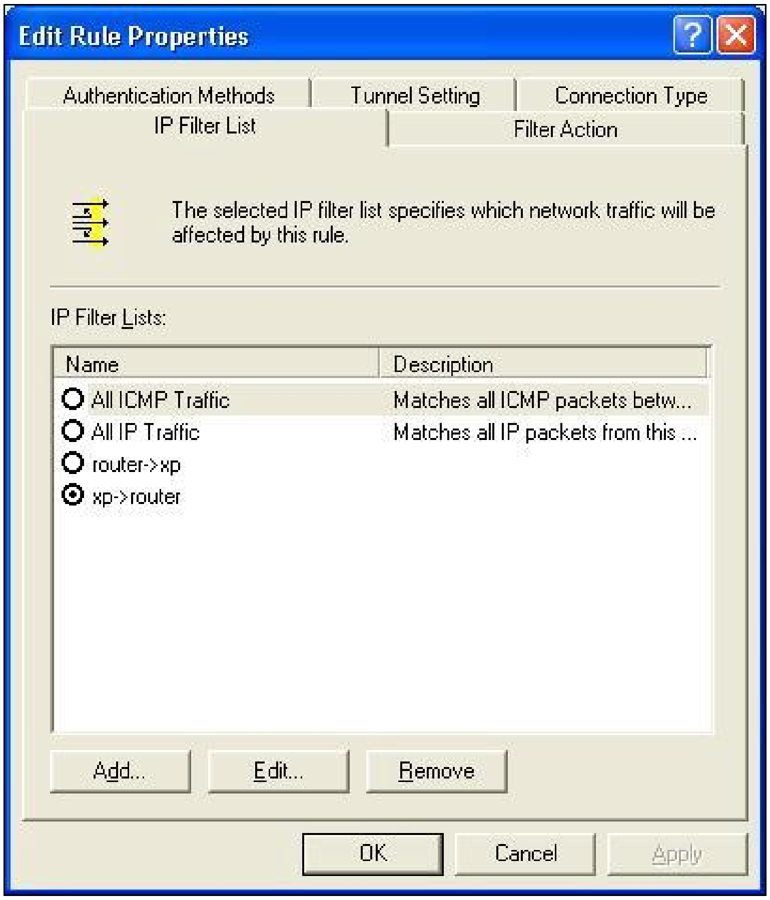


	IP Filter List	Filter Action	Authentication...	Tu
☑	xp->router	Require Security	Preshared Key	19
☑	router->xp	Require Security	Preshared Key	19
□	<Dynamic>	Default Response	Kerberos	Nc

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.

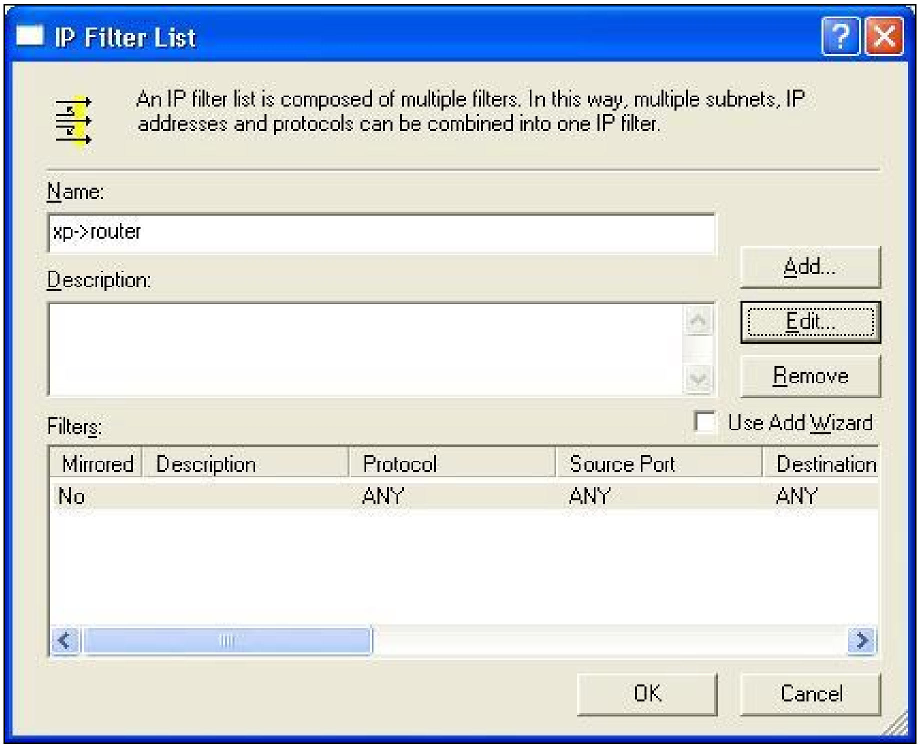


The selected IP filter list specifies which network traffic will be affected by this rule.

IP Filter Lists:

Name	Description
○ All ICMP Traffic	Matches all ICMP packets betw...
○ All IP Traffic	Matches all IP packets from this ...
○ router->xp	
◉ xp->router	

Click **[Add]** button



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: xp->router

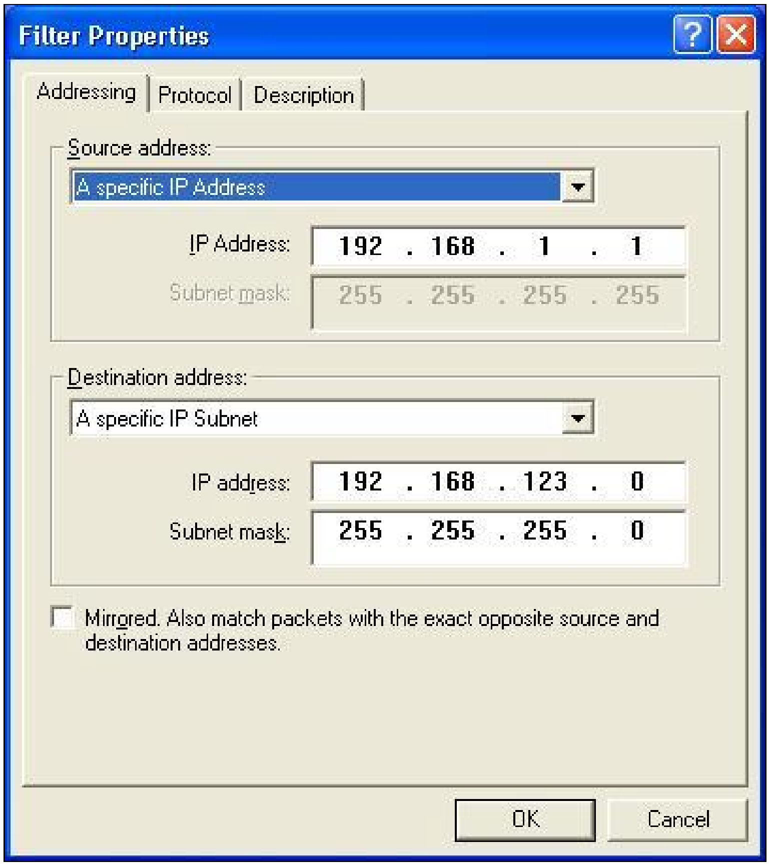
Description:

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

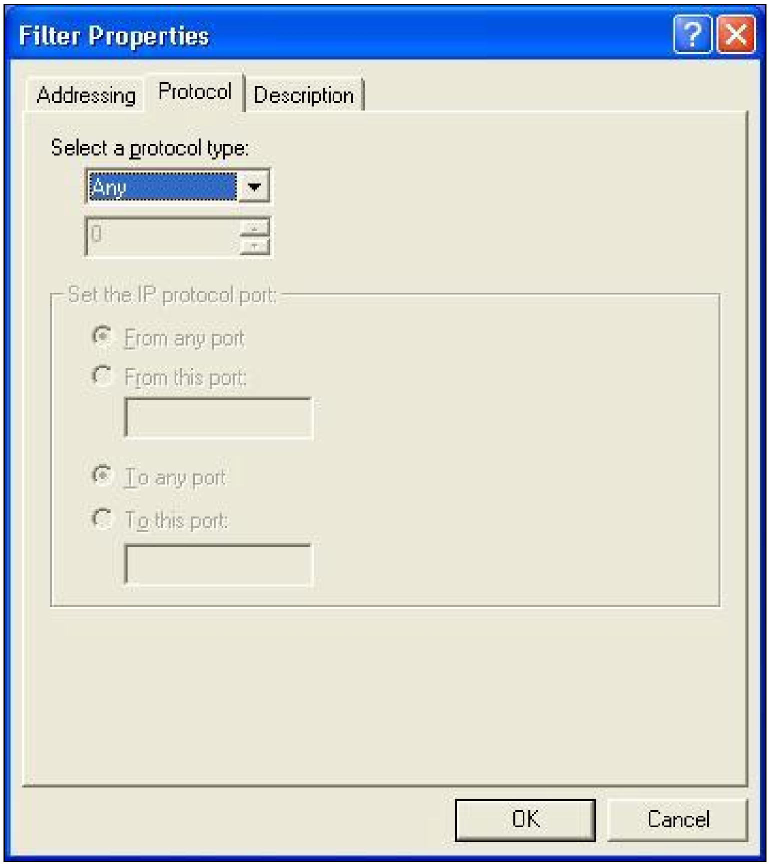
Subnet mask: 255 . 255 . 255 . 0

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

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.



Select a protocol type: Any

0

Set the IP protocol port:

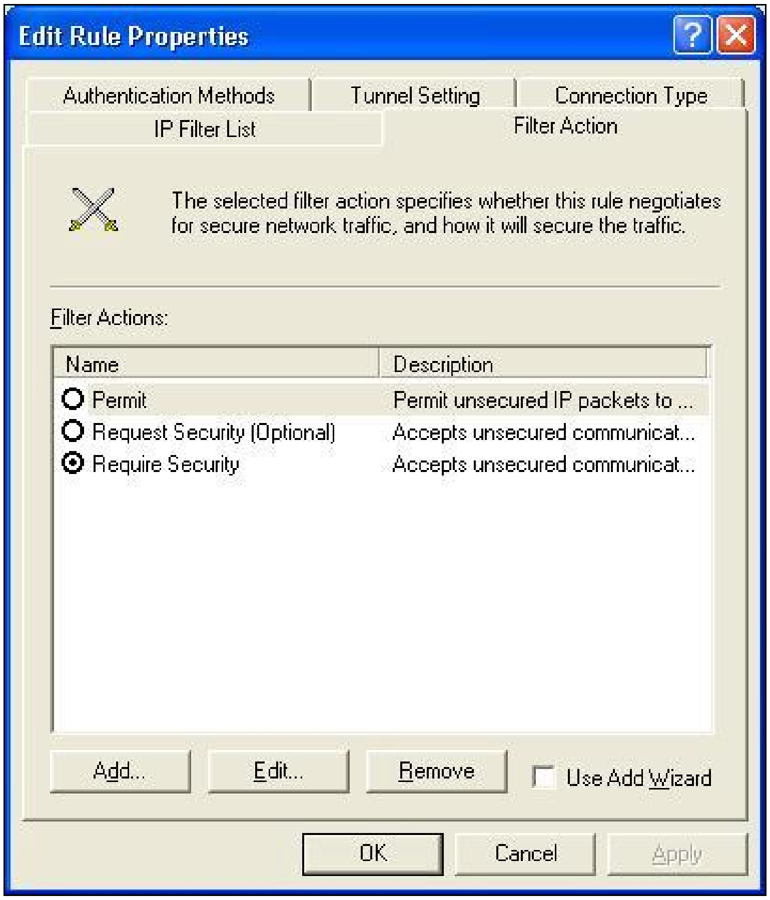
● From any port

○ From this port:

● To any port

○ To this port:

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

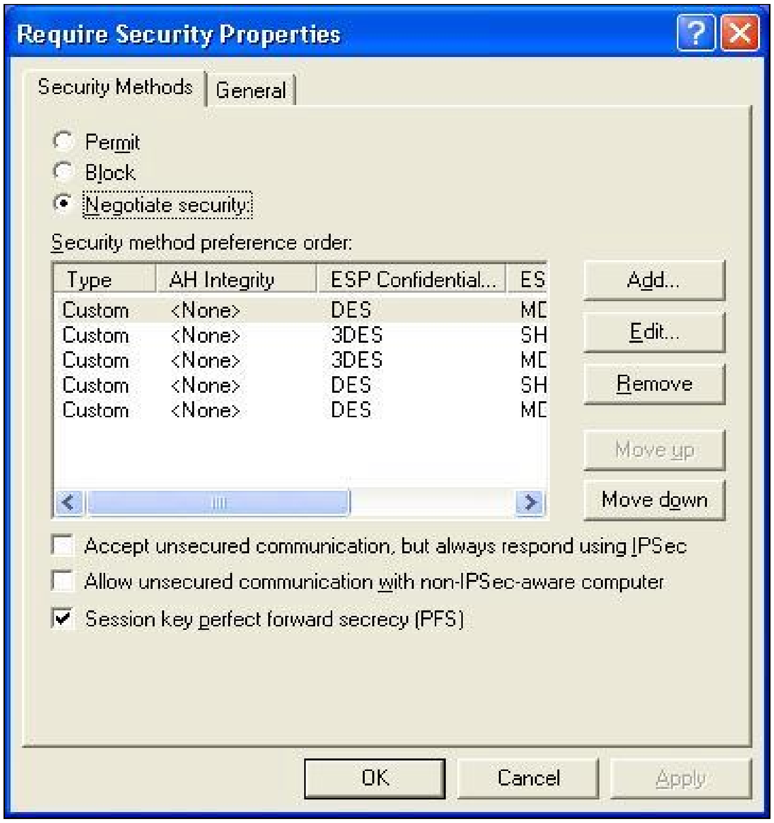


The selected filter action specifies whether this rule negotiates for secure network traffic, and how it will secure the traffic.

Filter Actions:

Name	Description
○ Permit	Permit unsecured IP packets to ...
○ Request Security (Optional)	Accepts unsecured communicat...
● Require Security	Accepts unsecured communicat...

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



Require Security Properties

Security Methods | General

○ Permit
○ Block
● Negotiate security:

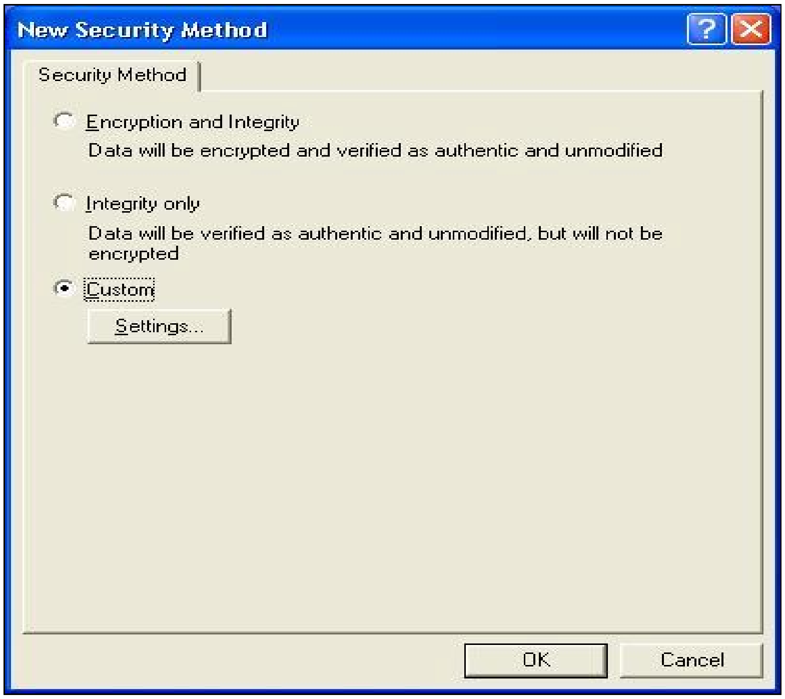
Security method preference order:

Type	AH Integrity	ESP Confidential...	ES
Custom	<None>	DES	MD
Custom	<None>	3DES	SH
Custom	<None>	3DES	MD
Custom	<None>	DES	SH
Custom	<None>	DES	MD

□ Accept unsecured communication, but always respond using IPSec
□ Allow unsecured communication with non-IPSec-aware computer
☑ Session key perfect forward secrecy (PFS)

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

Click **[Edit]** button.



New Security Method

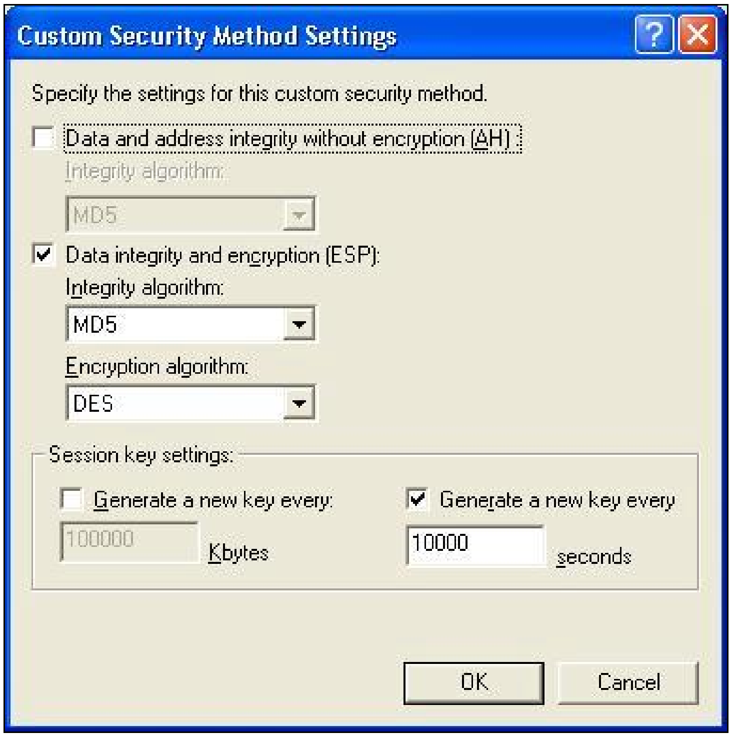
Security Method

○ Encryption and Integrity
Data will be encrypted and verified as authentic and unmodified

○ Integrity only
Data will be verified as authentic and unmodified, but will not be encrypted

● Custom

Select **[Custom]** button



Custom Security Method Settings

Specify the settings for this custom security method.

☐ Data and address integrity without encryption (AH) :

Integrity algorithm: MD5

☑ Data integrity and encryption (ESP):

Integrity algorithm: MD5

Encryption algorithm: DES

Session key settings:

☐ Generate a new key every: 100000 Kbytes

☑ Generate a new key every 10000 seconds

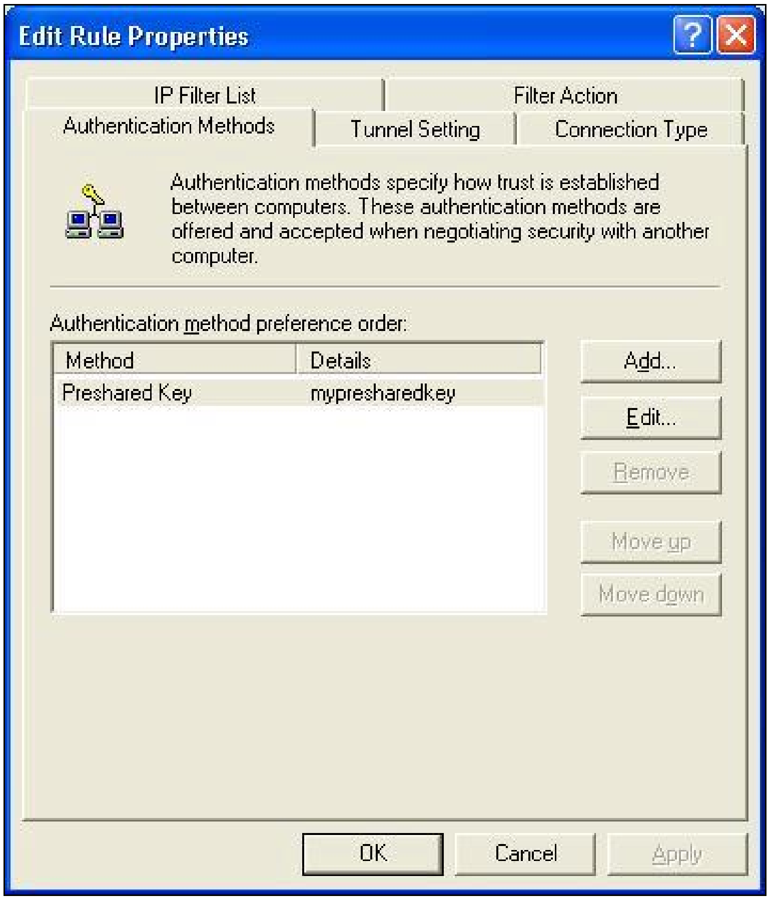
Select **[Data integrity and encryption (ESP)]**

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

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

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

Click **[OK]** button

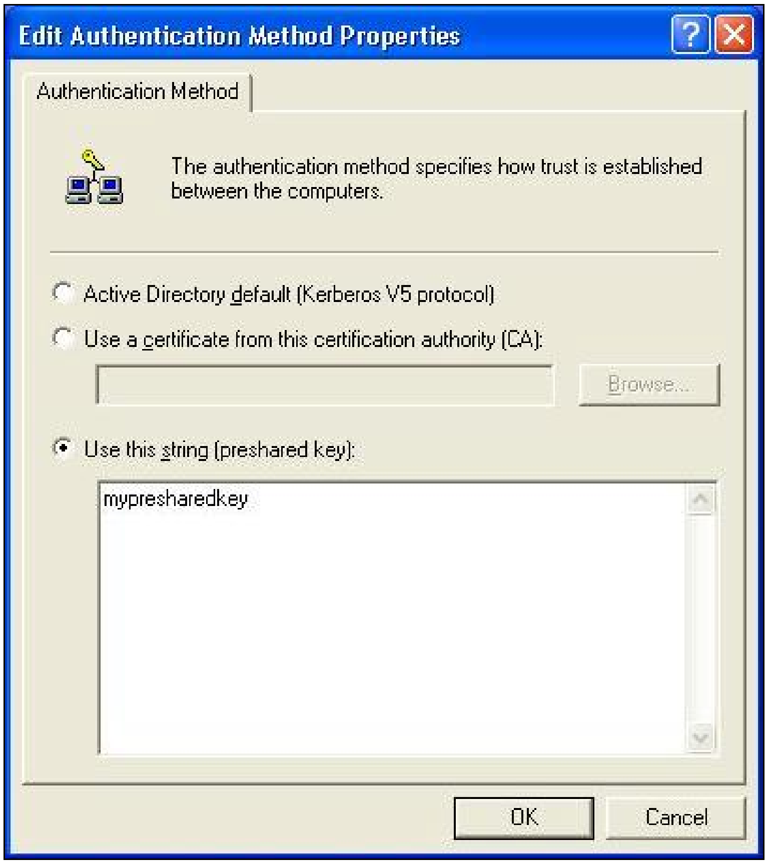


Authentication methods specify how trust is established between computers. These authentication methods are offered and accepted when negotiating security with another computer.

Authentication method preference order:

Method	Details
Preshared Key	mypresharedkey

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



The authentication method specifies how trust is established between the computers.

○ Active Directory default (Kerberos V5 protocol)

○ Use a certificate from this certification authority (CA):

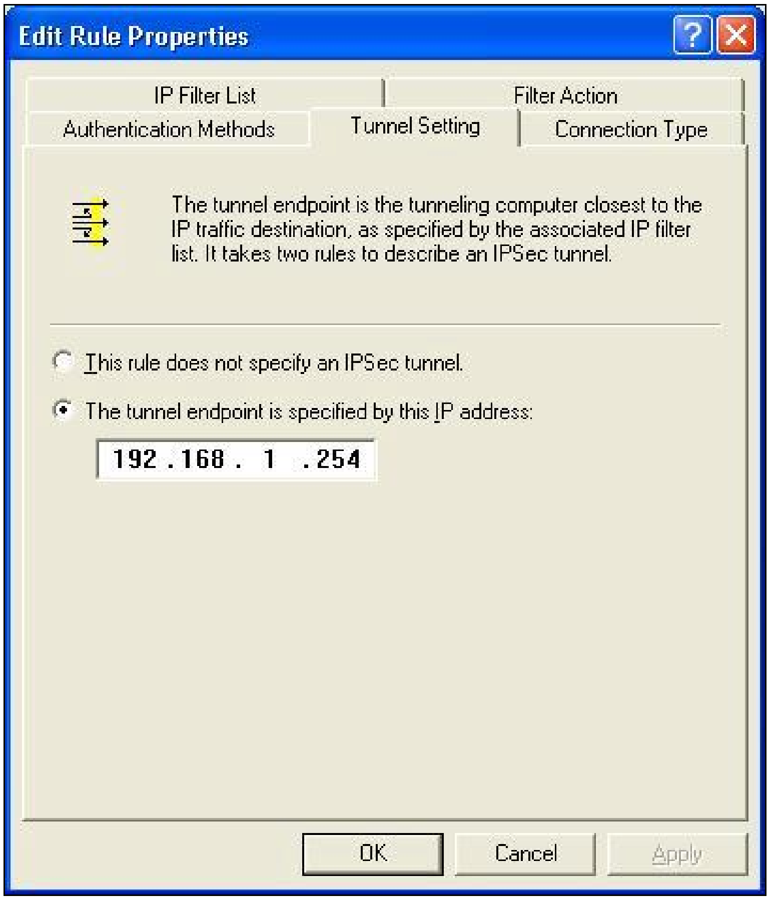
● Use this string (preshared key):

mypresharedkey

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]**



Edit Rule Properties

The tunnel endpoint is the tunneling computer closest to the IP traffic destination, as specified by the associated IP filter list. It takes two rules to describe an IPSec tunnel.

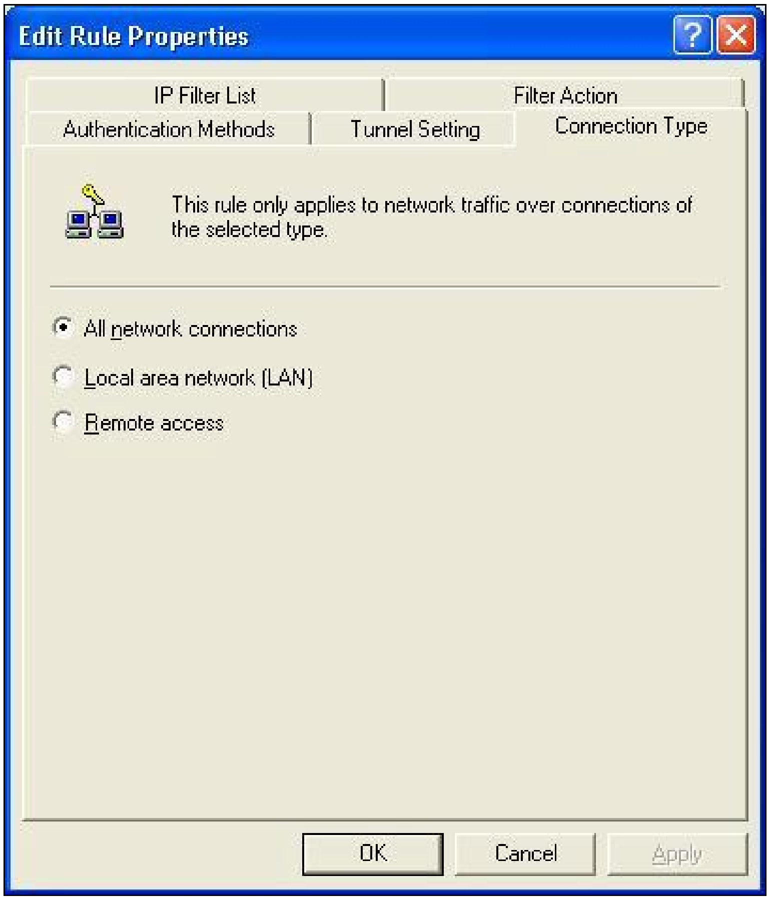
○ This rule does not specify an IPSec tunnel.

● The tunnel endpoint is specified by this IP address:

192 . 168 . 1 . 254

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

Select **[Connection Type]**



This rule only applies to network traffic over connections of the selected type.

● All network connections

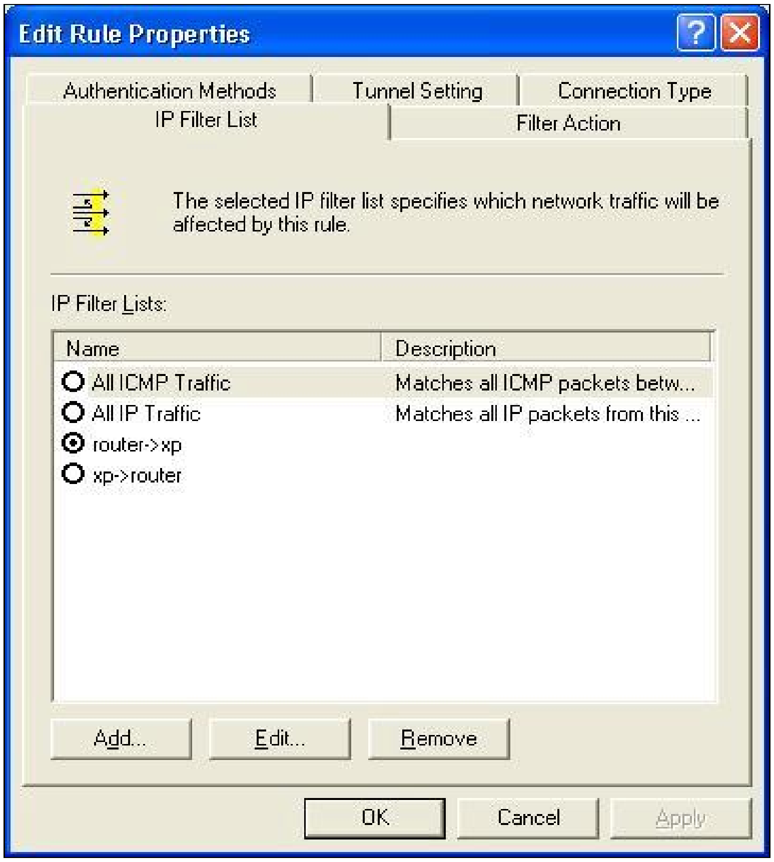
○ Local area network (LAN)

○ Remote access

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.

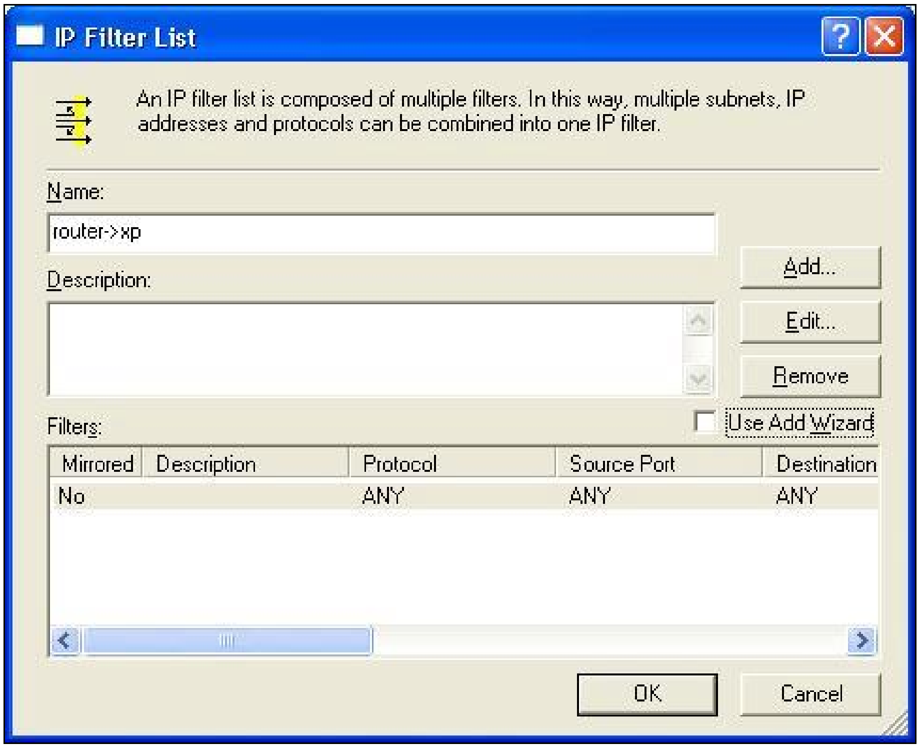


The selected IP filter list specifies which network traffic will be affected by this rule.

IP Filter Lists:

Name	Description
○ All ICMP Traffic	Matches all ICMP packets betw...
○ All IP Traffic	Matches all IP packets from this ...
● router->xp	
○ xp->router	

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.
Add...
Edit...
Remove
OK
Cancel

Name: router->xp

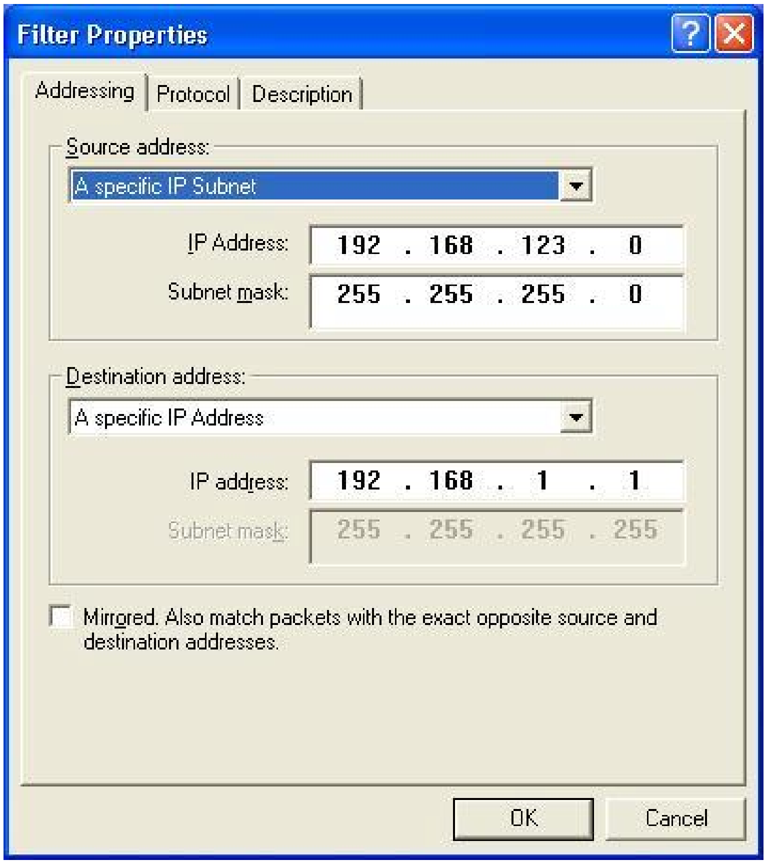
Description:

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.



Source address:

A specific IP Subnet

IP Address: 192 . 168 . 123 . 0

Subnet mask: 255 . 255 . 255 . 0

Destination address:

A specific IP Address

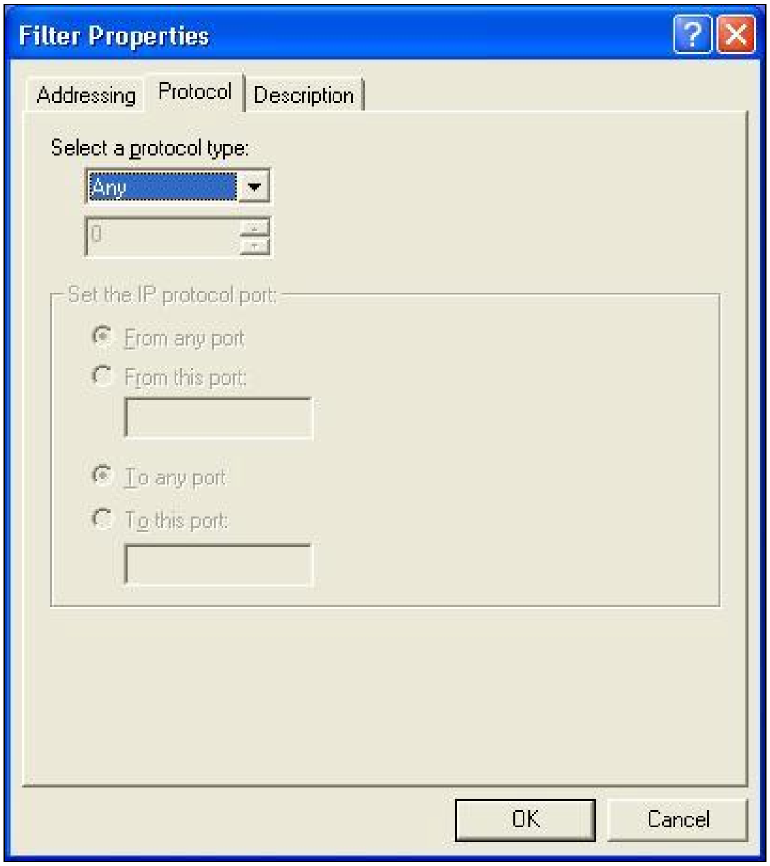
IP address: 192 . 168 . 1 . 1

Subnet mask: 255 . 255 . 255 . 255

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

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.



Select a protocol type: Any

0

Set the IP protocol port:

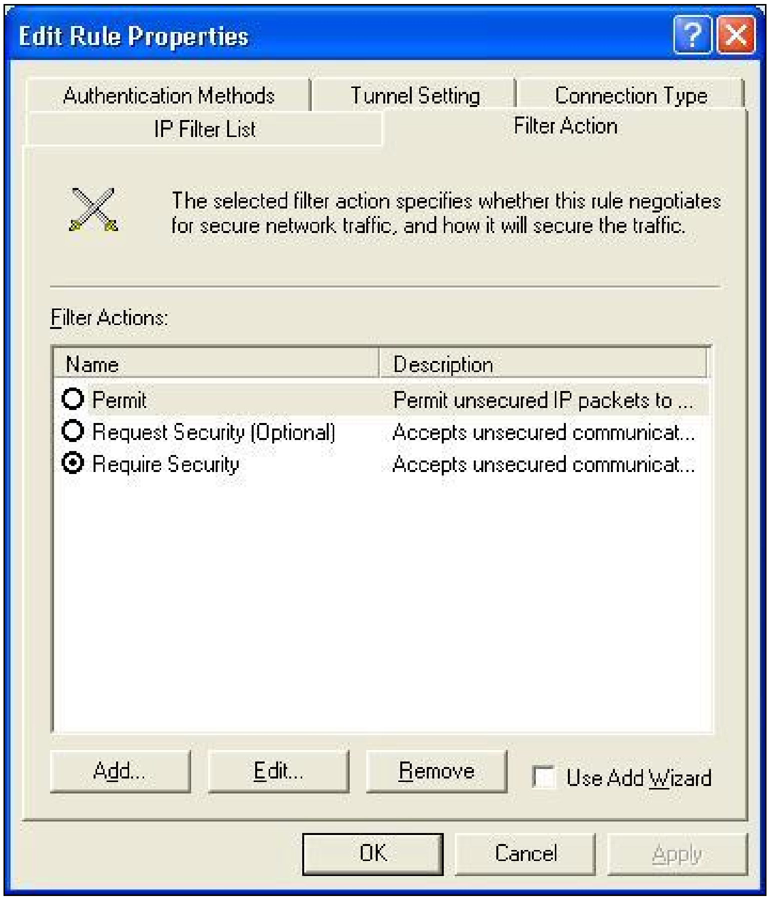
● From any port

○ From this port:

● To any port

○ To this port:

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



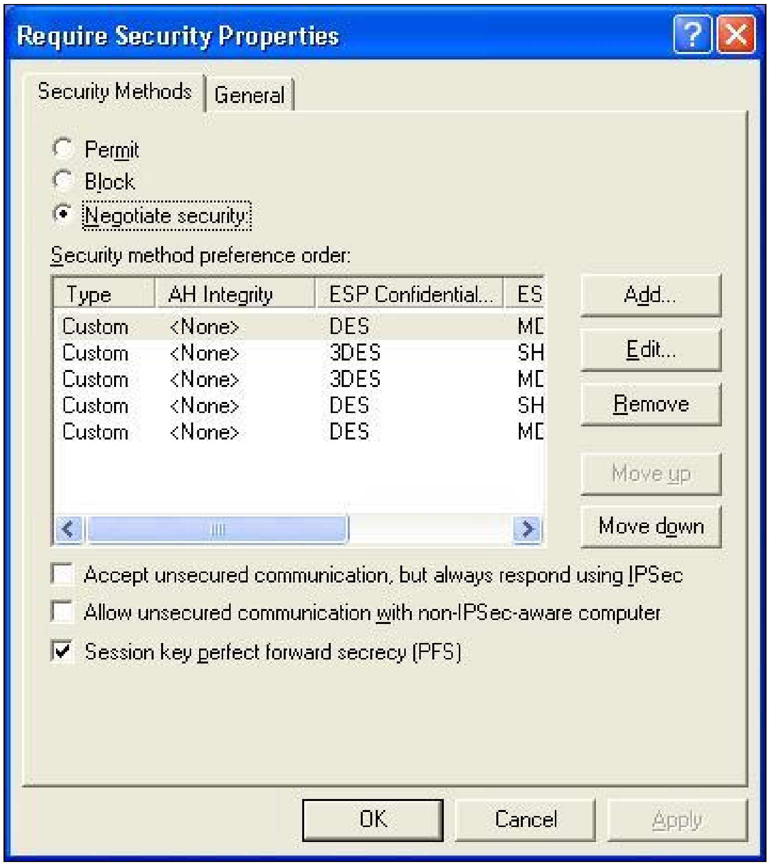
The selected filter action specifies whether this rule negotiates for secure network traffic, and how it will secure the traffic.

Filter Actions:

Name	Description
○ Permit	Permit unsecured IP packets to ...
○ Request Security (Optional)	Accepts unsecured communicat...
● Require Security	Accepts unsecured communicat...

□ Use Add Wizard

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



○ Permit
○ Block
● Negotiate security:

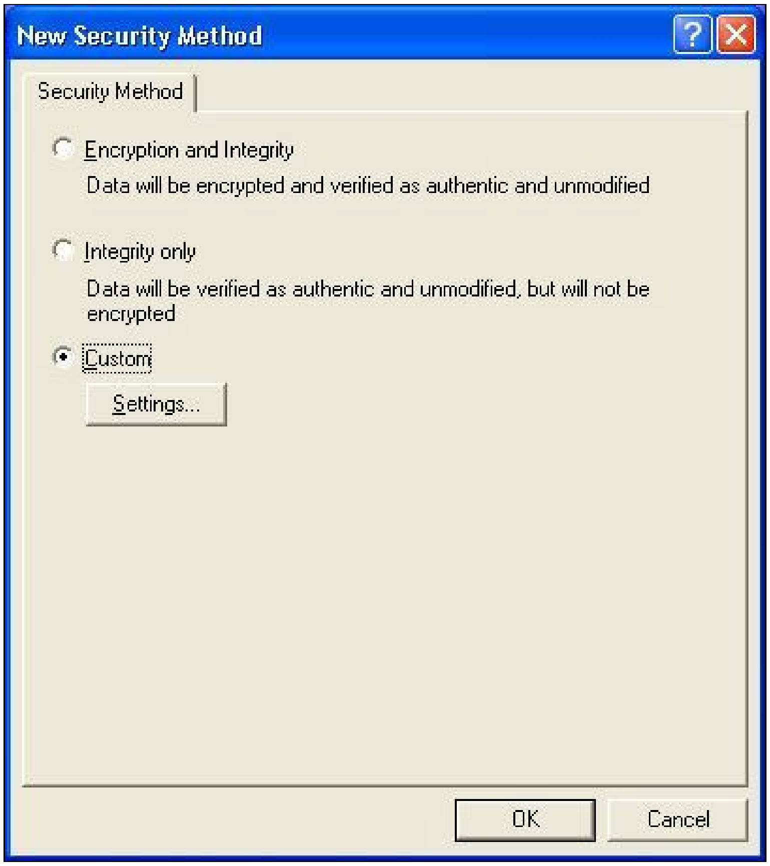
Security method preference order:

Type	AH Integrity	ESP Confidential...	ES
Custom	<None>	DES	MD
Custom	<None>	3DES	SH
Custom	<None>	3DES	MD
Custom	<None>	DES	SH
Custom	<None>	DES	MD

□ Accept unsecured communication, but always respond using IPSec
□ Allow unsecured communication with non-IPSec-aware computer
☑ Session key perfect forward secrecy (PFS)

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

Click **[Edit]** button.



New Security Method

Security Method

○ Encryption and Integrity

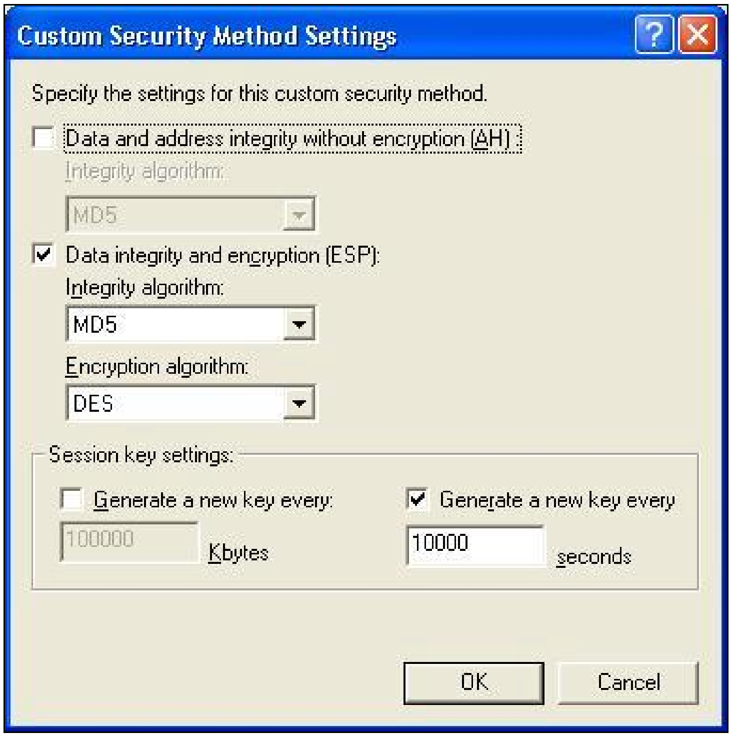
Data will be encrypted and verified as authentic and unmodified

○ Integrity only

Data will be verified as authentic and unmodified, but will not be encrypted

● Custom

Select **[Custom]** button



Custom Security Method Settings

Specify the settings for this custom security method.

☐ Data and address integrity without encryption (AH) :

Integrity algorithm: MD5

☑ Data integrity and encryption (ESP):

Integrity algorithm: MD5

Encryption algorithm: DES

Session key settings:

☐ Generate a new key every: 100000 Kbytes

☑ Generate a new key every 10000 seconds

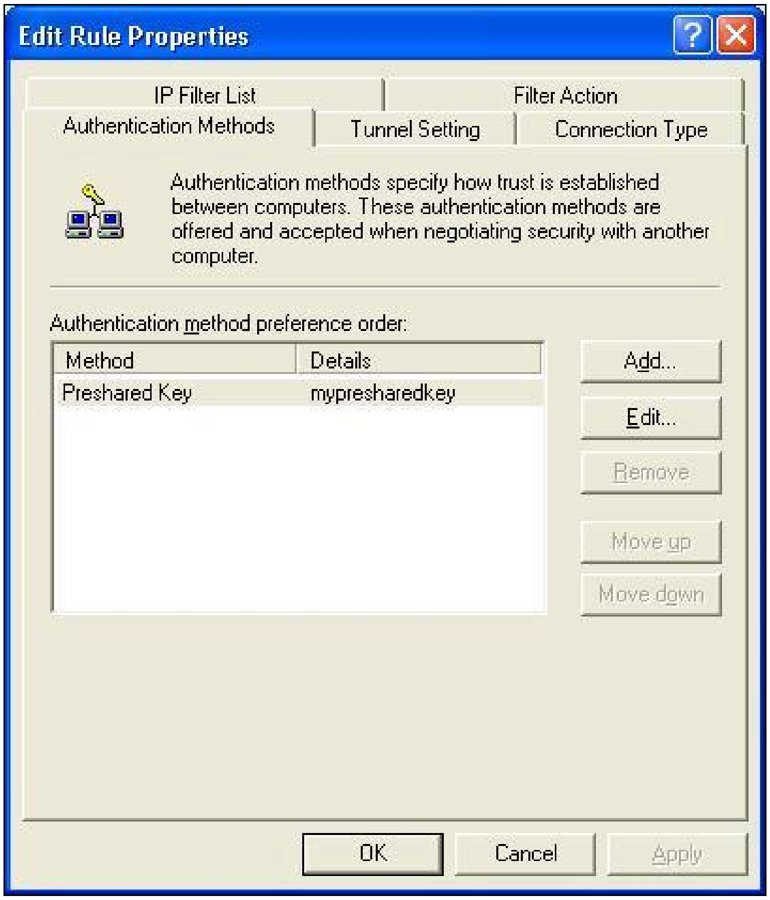
Select **[Data integrity and encryption (ESP)]**

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

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

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

Click **[OK]** button

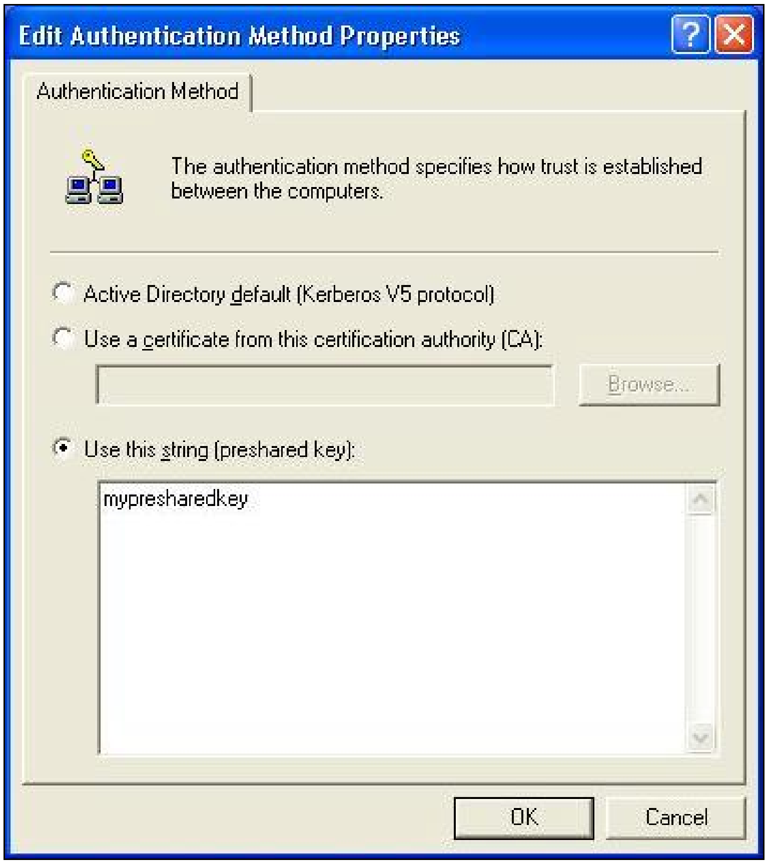


Authentication methods specify how trust is established between computers. These authentication methods are offered and accepted when negotiating security with another computer.

Authentication method preference order:

Method	Details
Preshared Key	mypresharedkey

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



Edit Authentication Method Properties

Authentication Method

The authentication method specifies how trust is established between the computers.

○ Active Directory default (Kerberos V5 protocol)

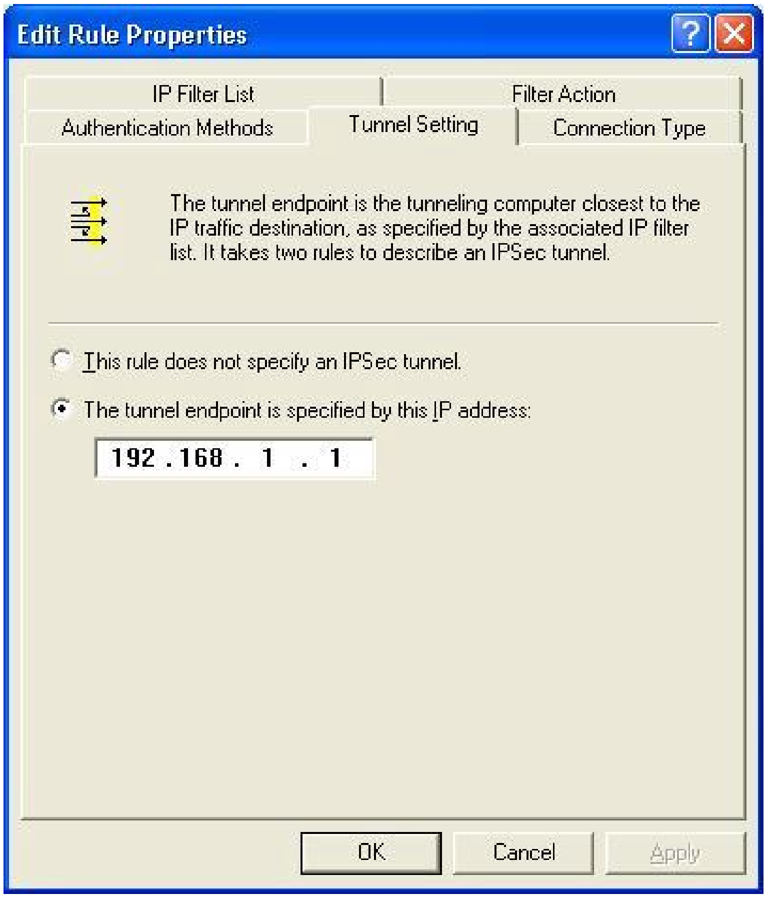
○ Use a certificate from this certification authority (CA):

● Use this string (preshared key):

mypresharedkey

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]**



Edit Rule Properties

The tunnel endpoint is the tunneling computer closest to the IP traffic destination, as specified by the associated IP filter list. It takes two rules to describe an IPSec tunnel.

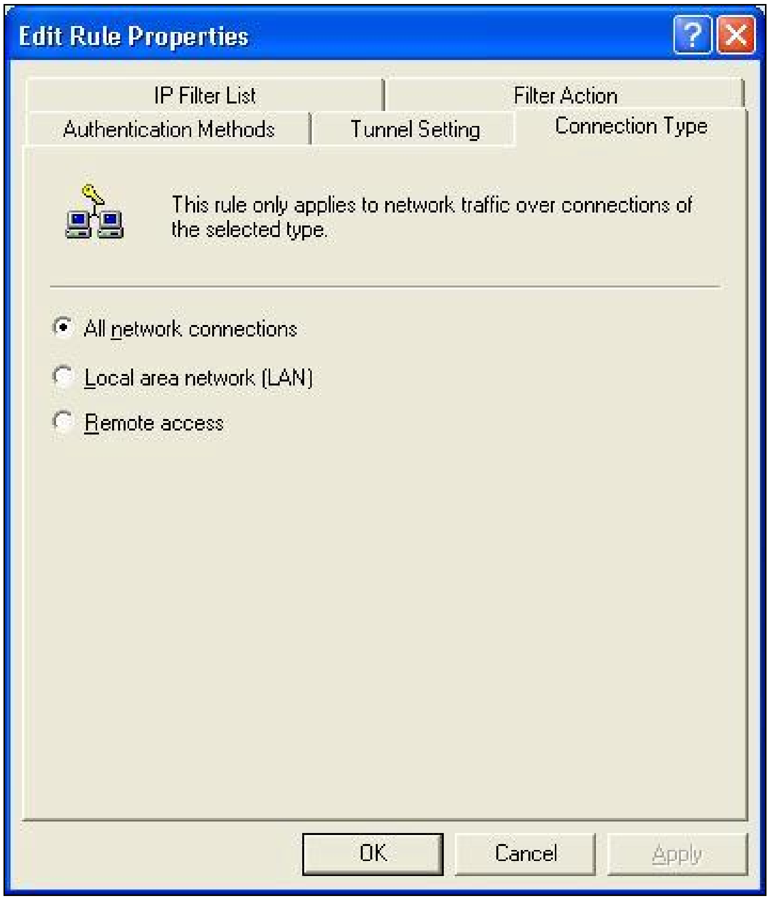
○ This rule does not specify an IPSec tunnel.

● The tunnel endpoint is specified by this IP address:

192 . 168 . 1 . 1

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

Select **[Connection Type]**



This rule only applies to network traffic over connections of the selected type.

● All network connections

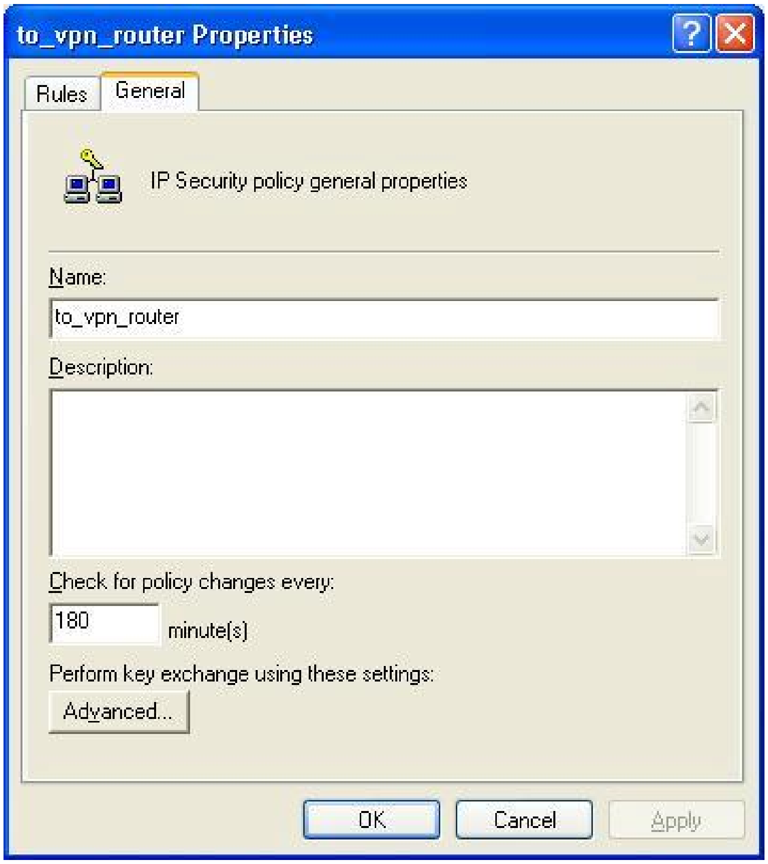
○ Local area network (LAN)

○ Remote access

Select **[All network connections]**

Configure IKE properties

Select **[General]**



to_vpn_router Properties

IP Security policy general properties

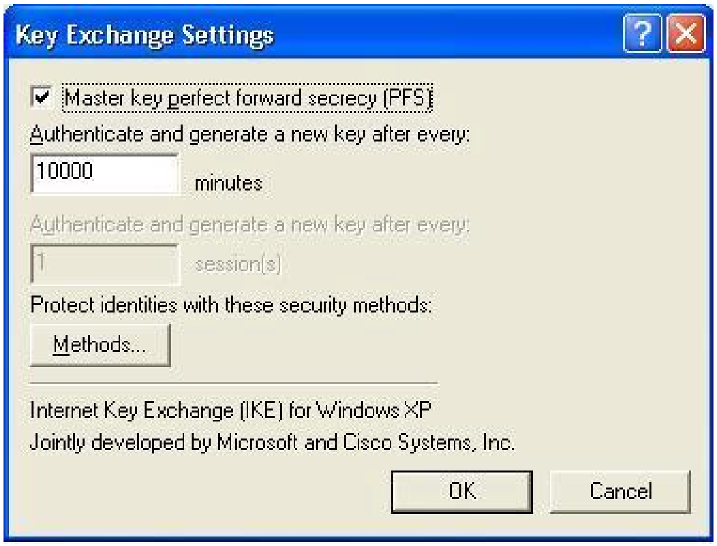
Name:
to_vpn_router

Description:

Check for policy changes every:
180 minute(s)

Perform key exchange using these settings:

Click **[Advanced…]**



☑ Master key perfect forward secrecy (PFS)

Authenticate and generate a new key after every:

10000 minutes

Authenticate and generate a new key after every:

1 session(s)

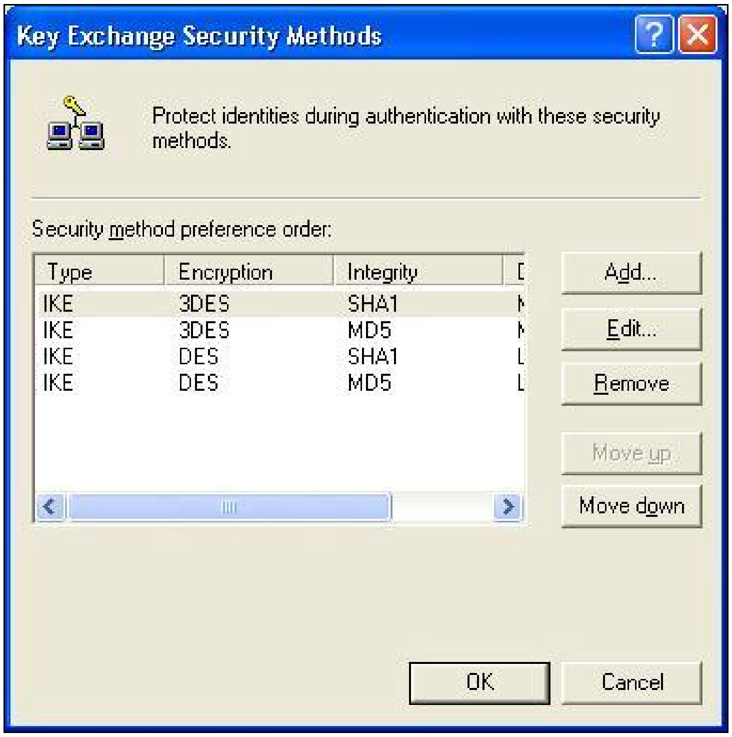
Protect identities with these security methods:

Internet Key Exchange (IKE) for Windows XP
Jointly developed by Microsoft and Cisco Systems, Inc.

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

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

Click **[Methods…]**

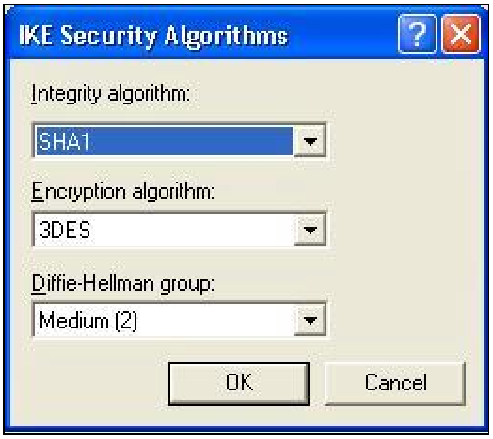


Protect identities during authentication with these security methods.

Security method preference order:

Type	Encryption	Integrity	D
IKE	3DES	SHA1	M
IKE	3DES	MD5	M
IKE	DES	SHA1	L
IKE	DES	MD5	L

Click **[Add]** button



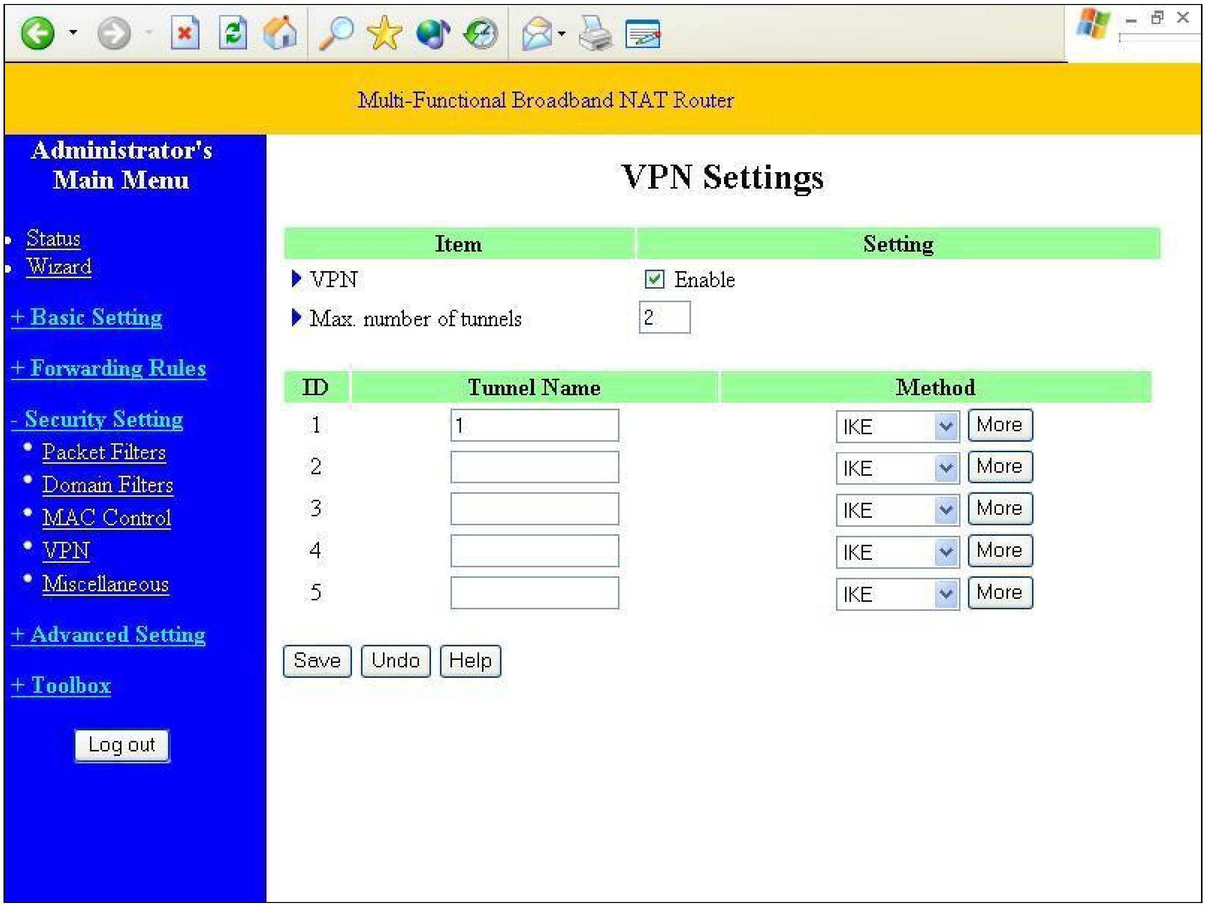
Configure "**Integrity algorithm**": **[SHA1]**

Configure "**Encryption algorithm**": **[3DES]**

Configure "**Diffie-Helman 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

Item	Setting
▸ VPN	☑ Enable
▸ Max. number of tunnels	2

ID	Tunnel Name	Method
1	1	IKE More
2		IKE More
3		IKE More
4		IKE More
5		IKE More

VPN Settings:

VPN: Enable

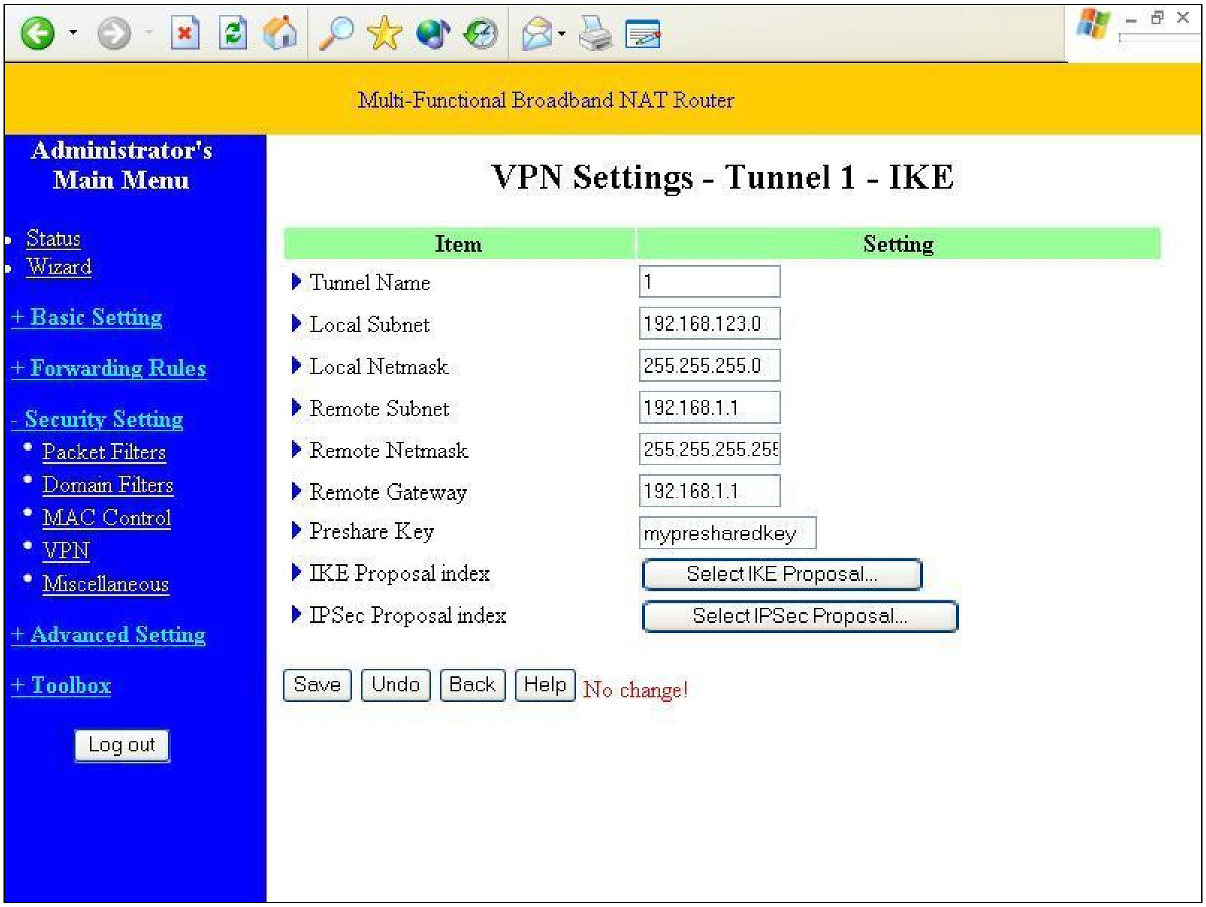
Max. Number of tunnels: 2

ID: 1

Tunnel Name: 1

Method: IKE

Press “**More**” **à**



VPN Settings - Tunnel 1 - IKE

Item	Setting
Tunnel Name	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	mypresharedkey
IKE Proposal index	Select IKE Proposal...
IPSec Proposal index	Select IPSec Proposal...

No change!

VPN Settings - Tunnel 1 – IKE

Tunnel: 1

Local Subnet: 192.168.123.0

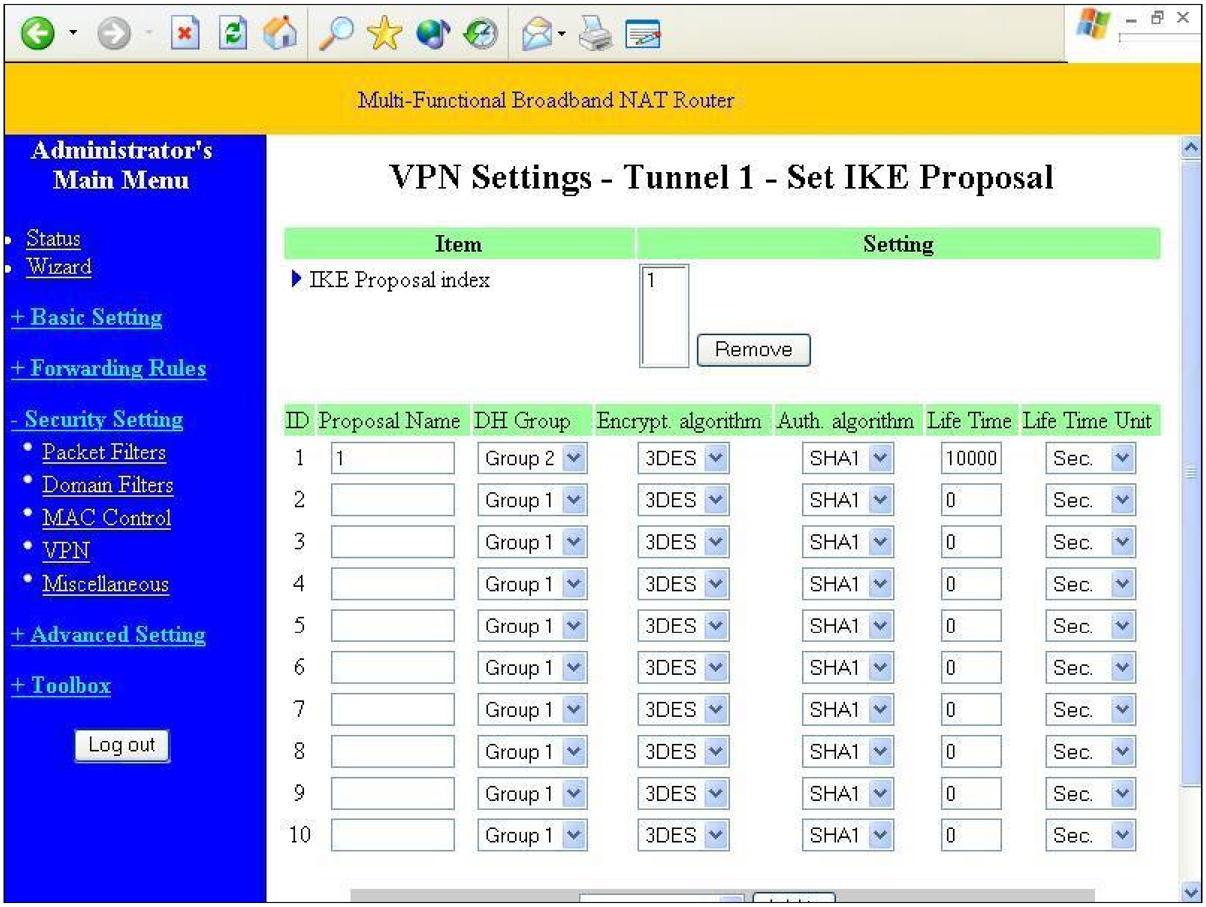
Local Netmask: 255.255.255.0

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

Item	Setting
IKE Proposal index	1

ID	Proposal Name	DH Group	Encrypt. algorithm	Auth. algorithm	Life Time	Life Time Unit
1	1	Group 2	3DES	SHA1	10000	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.

VPN Settings - Tunnel 1 - Set IKE Proposal

ID: 1

Proposal Name: 1

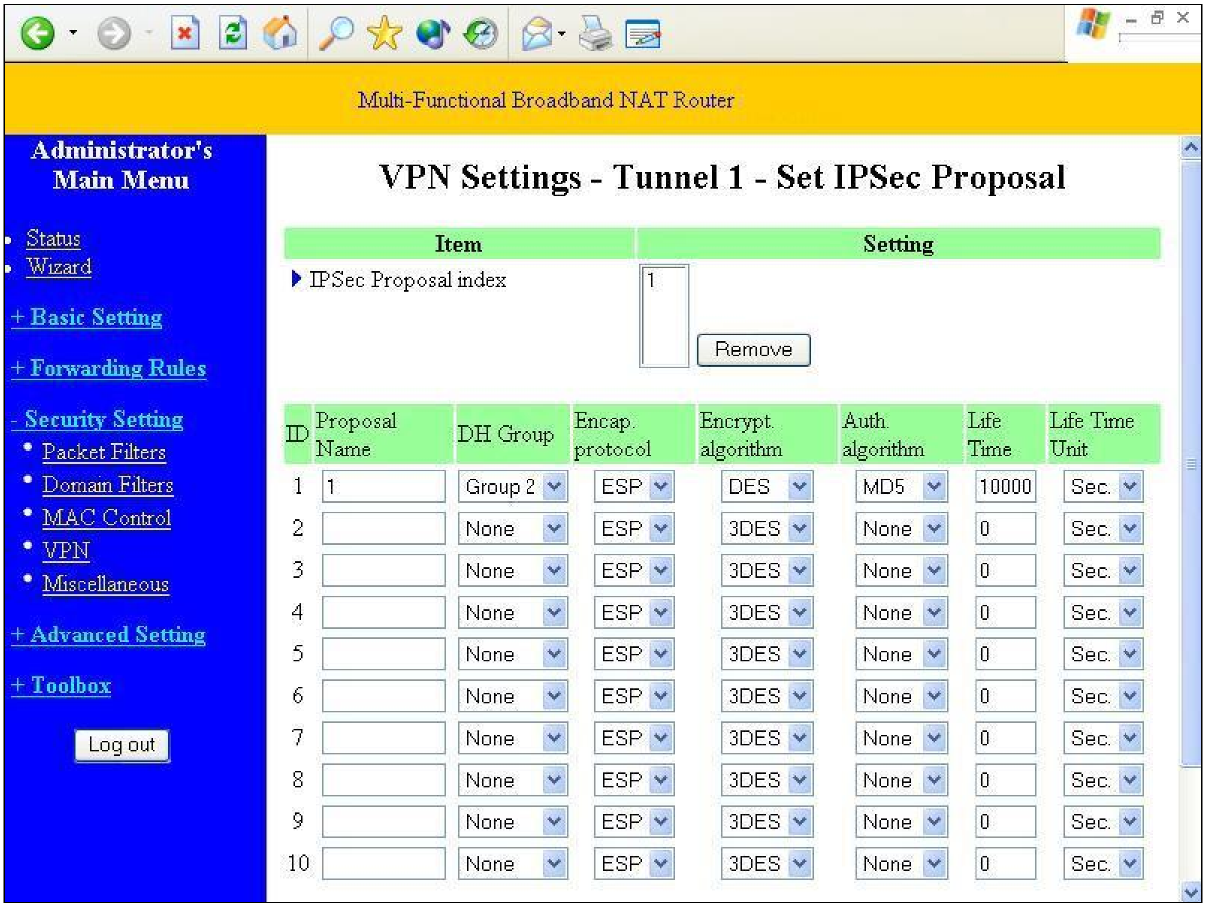
DH Group: Group2

Encrypt. Algorithm: 3DES

Auth. Algorithm: SHA1

Life Time: 10000

Life Time Unit: Sec.



VPN Settings - Tunnel 1 - Set IPSec Proposal

Item	Setting
IPSec Proposal index	1 Remove

ID	Proposal Name	DH Group	Encap. protocol	Encrypt. algorithm	Auth. algorithm	Life Time	Life Time Unit
1	1	Group 2	ESP	DES	MD5	10000	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.

VPN Settings - Tunnel 1 - Set IPSec Proposal

ID: 1

Proposal Name: proposal1

DH Group: Group2

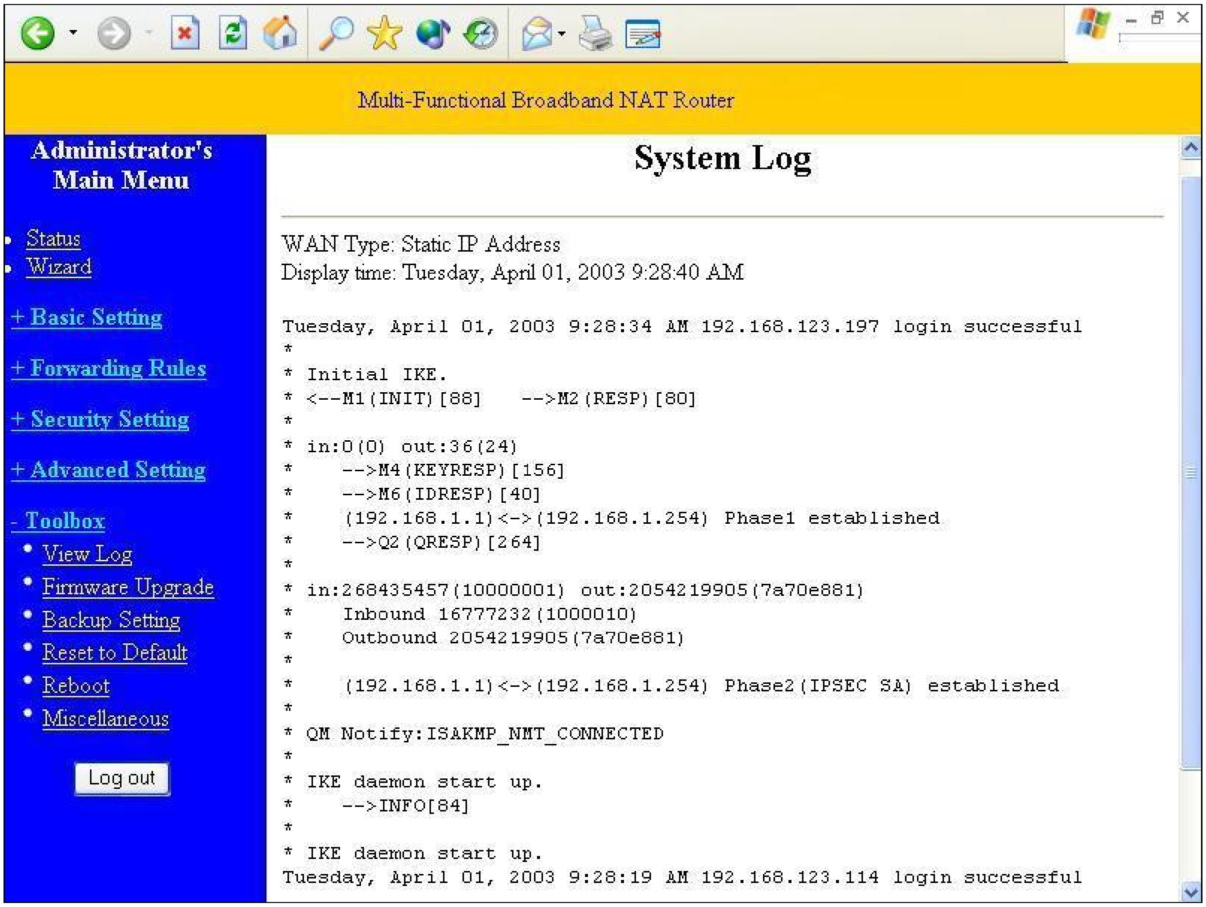
Encap. Protocol: ESP

Encrypt. Algorithm: DES

Auth. Algorithm: MD5

Life Time: 10000

Life Time Unit: Sec.



System Log

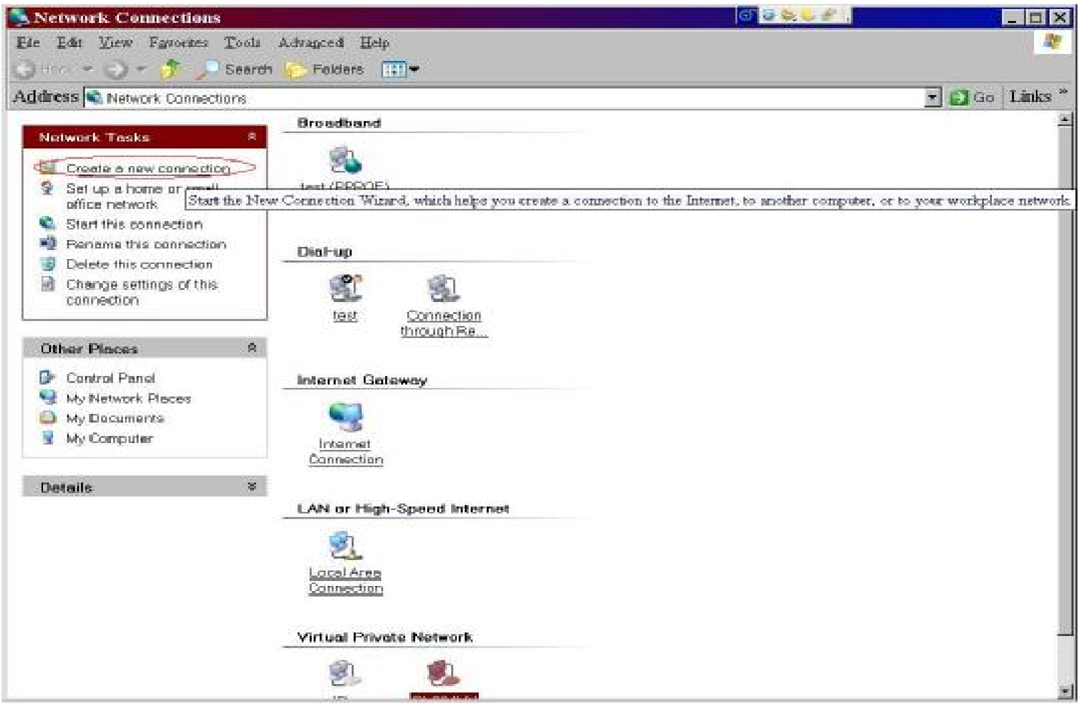
WAN Type: Static IP Address
Display time: Tuesday, April 01, 2003 9:28:40 AM

```
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.

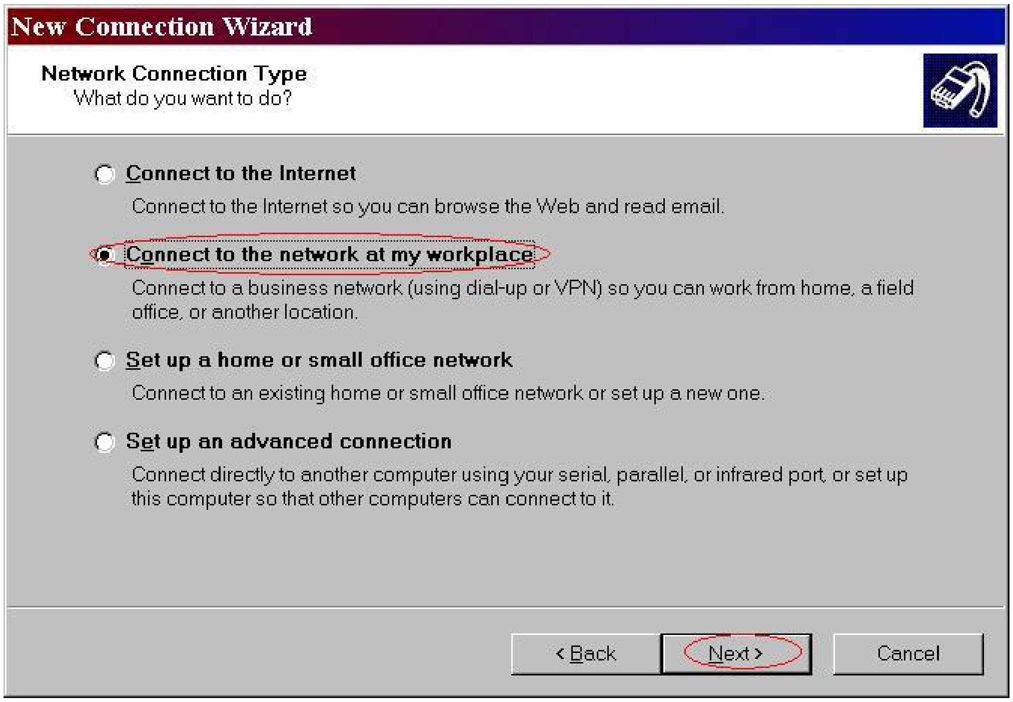
Appendix C PPTP and L2TP Configurations

1. First, please go to the Network connection



Start the New Connection Wizard, which helps you create a connection to the Internet, to another computer, or to your workplace network.

2. Connect to network at my workplace



Network Connection Type

What do you want to do?

○ Connect to the Internet

Connect to the Internet so you can browse the Web and read email.

● Connect to the network at my workplace

Connect to a business network (using dial-up or VPN) so you can work from home, a field office, or another location.

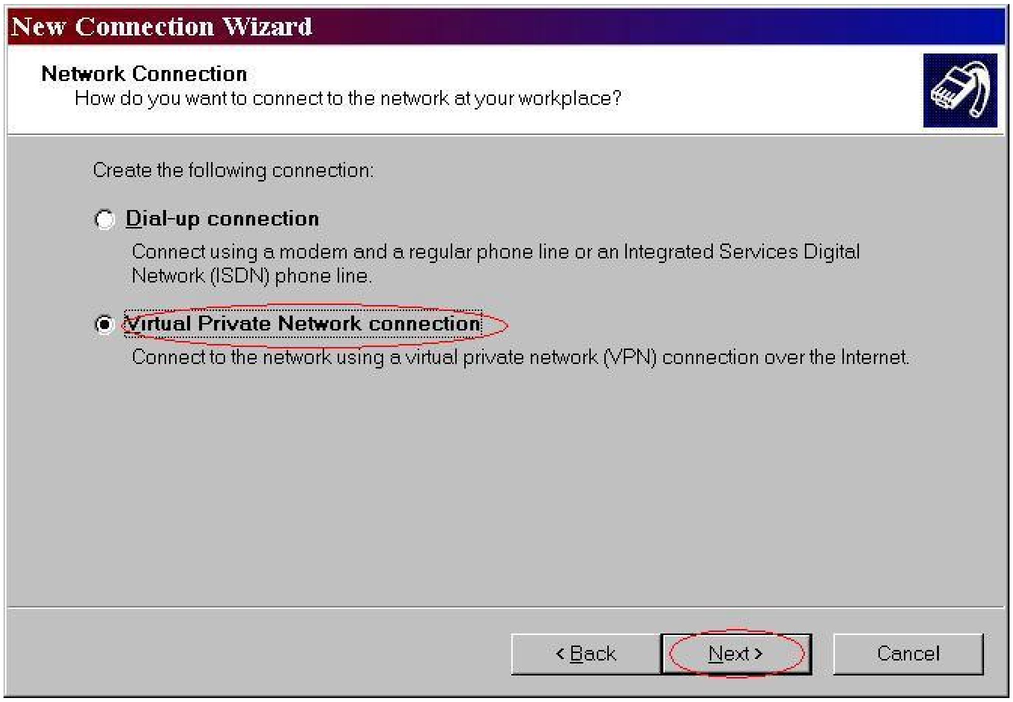
○ Set up a home or small office network

Connect to an existing home or small office network or set up a new one.

○ Set up an advanced connection

Connect directly to another computer using your serial, parallel, or infrared port, or set up this computer so that other computers can connect to it.

3. Choose Virtual Private Network



New Connection Wizard

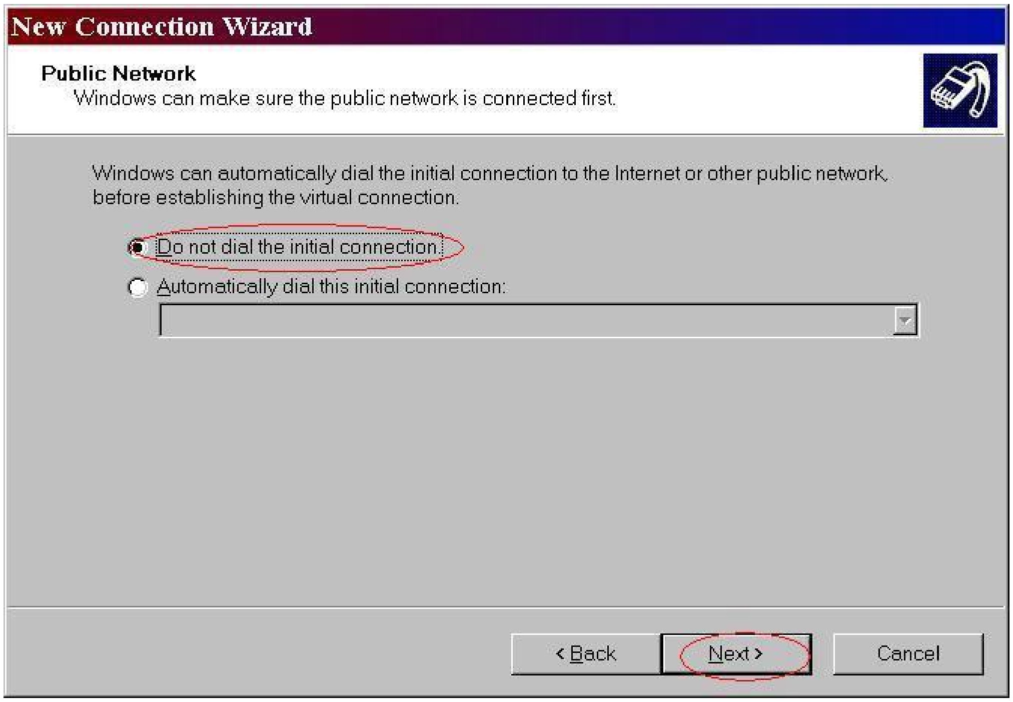
Network Connection
How do you want to connect to the network at your workplace?

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.

4. Do not dial to initial connection



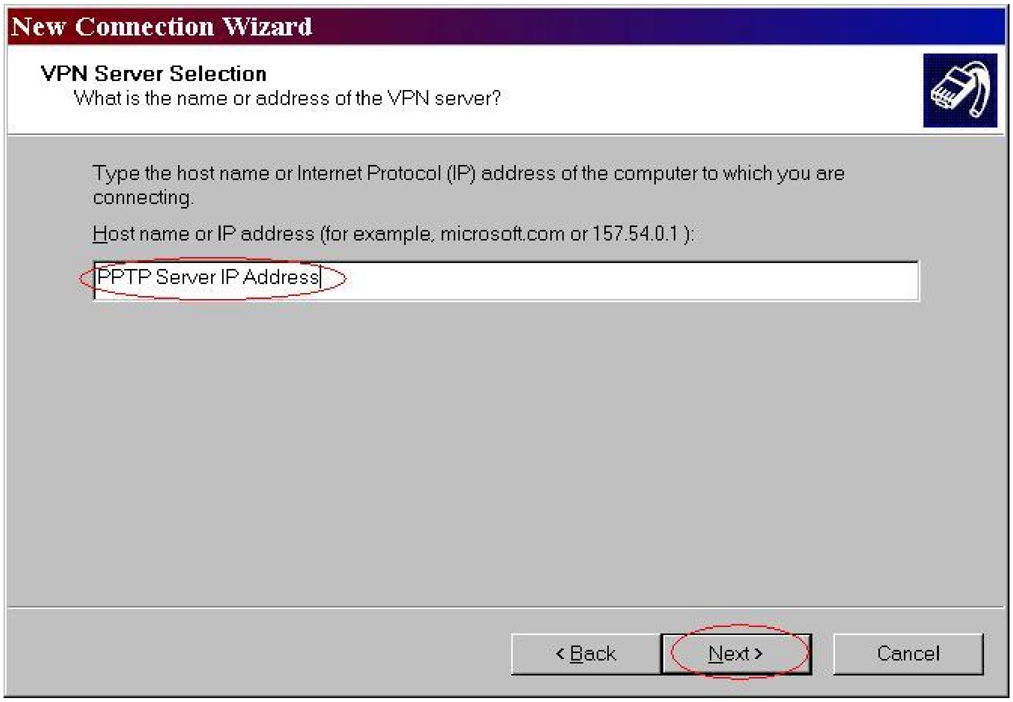
New Connection Wizard

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:

5. Input the router wan ip address



New Connection Wizard

VPN Server Selection

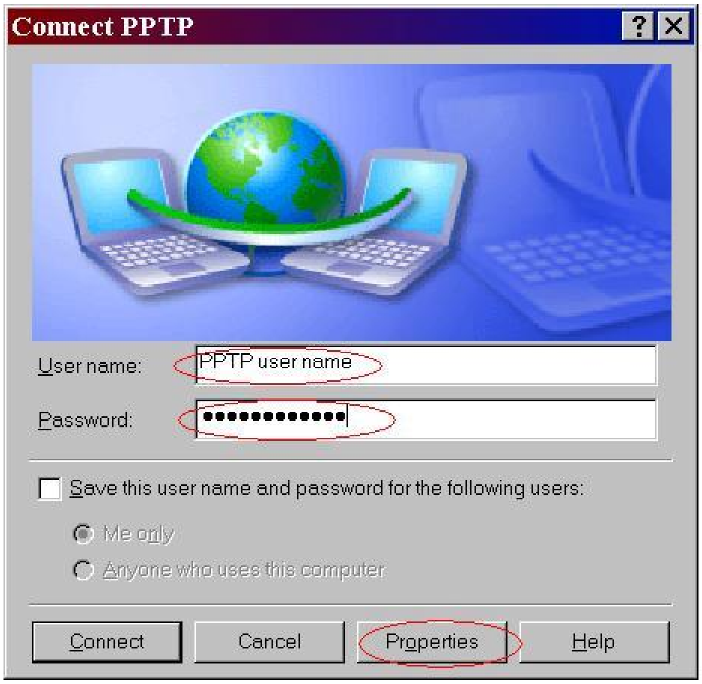
What is the name or address of the VPN server?

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

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



Connect PPTP

User name: PPTP user name

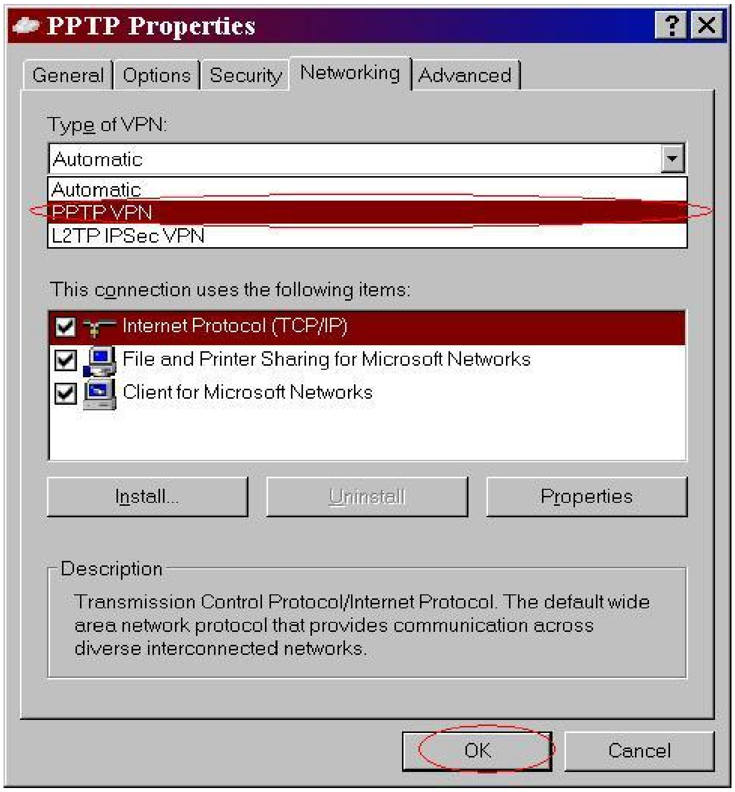
Password: •••••••••••••

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

● Me only

○ Anyone who uses this computer

7. Select the type of VPN



Type of VPN:

Automatic

- Automatic
- PPTP VPN
- L2TP IPSec VPN

This connection uses the following items:

☑ Internet Protocol (TCP/IP)

☑ File and Printer Sharing for Microsoft Networks

☑ Client for Microsoft Networks

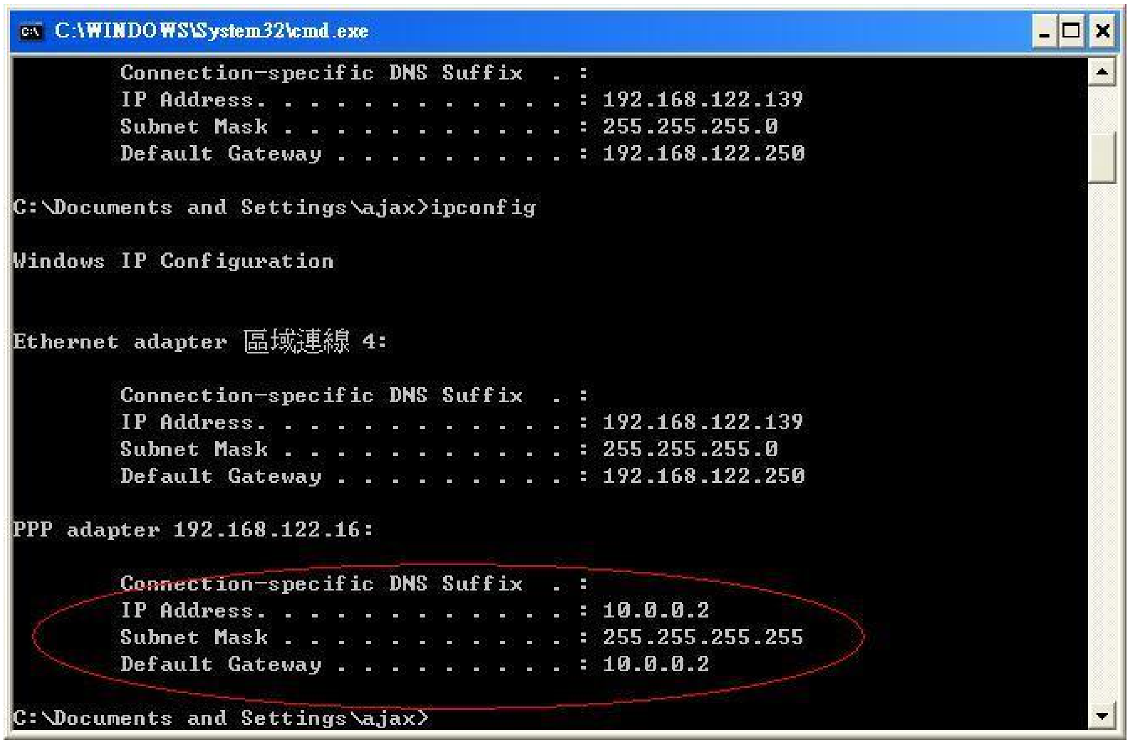
Description

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

However, you should add the Authentication Protocol in advanced (Custom setting) of Security option, like below t o support pap, chap, and 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>
```

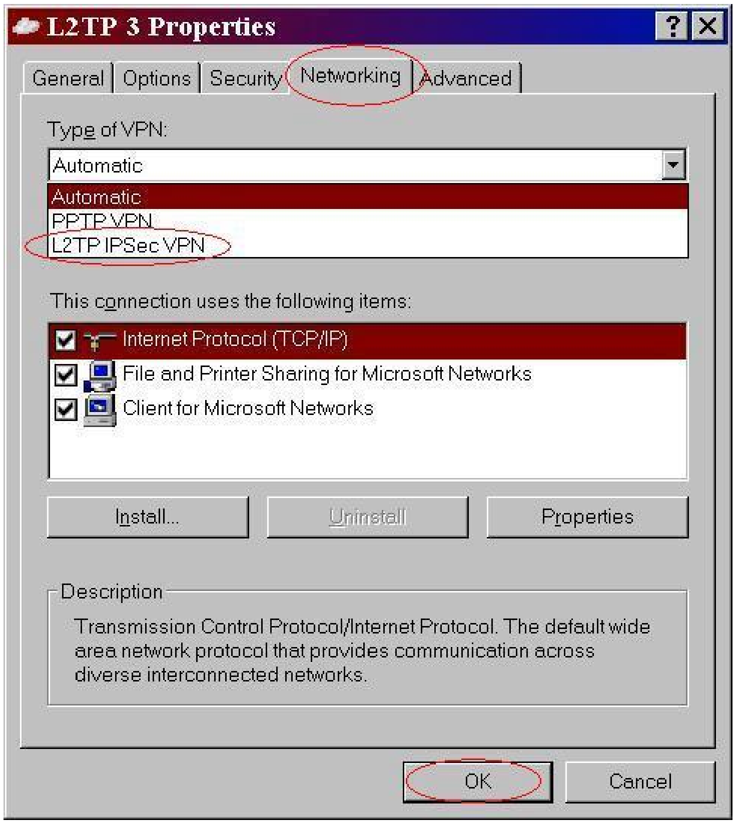
L2TP

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

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:



Type of VPN: Automatic

Automatic
PPTP VPN
L2TP IPSec VPN

This connection uses the following items:

☑ Internet Protocol (TCP/IP)

☑ File and Printer Sharing for Microsoft Networks

☑ Client for Microsoft Networks

Description

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

Then the steps refer to pptp settings.

Appendix D FAQ and Troubleshooting

Reset to factory Default

There are 3 methods to reset to default.

1. **Restore with console mode**

Please notice that this method requires a **null modem cable** and terminal program (e.g. HyperTerminal for MS Windows). First, configure the setting of your terminal program as 19200 N-8-1. And then, power off and on the router. When "AT" prompt is appeared, press, "ENTER" once to show the console mode commands. Just type "RR" command to restore the factory setting. Please refer to User Manual for the details.

2. **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 M1 and or M2 LED (or Status LED) start flashing, then move away the hand. If LED flashes about 8 times, the RESTORE process is completed. However, if LED flashes 2 times, repeat.

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

First, hold the RESET button about 5 seconds (M1 will start flashing about 5 times), move away the hand. The RESTORE process is completed.