

# **User's Manual**

**Wireless ARM9 4port Full function version with VPN**

**For internal reference only**

**Charlie 20031002**

**Note: This page should be remove before send to Customer**

1. This manual is modified base on 4-port wireless router, so some pictures are 4-port router, You may need to change them to fit your needs. **Note: Watch out COM port, and Printer port, if this product doesn't have them, you have to remove them.**

2. **Some functions are implemented on specific models only (the blue words)**

Charlie 20020807

4.add DHCP: gateway, Wireless: Pass-phrase Generator, Wizard: No ISP, MISC: Domain Filters, Ping Test, System Log: email alert, Syslog

Charlie 20020918

5. UI is totally re-modified (change a lot).

6. Add Primary/secondary DNS, Primary/secondary WINS,

Charlie 20020919

7. Add Primary setting: Virtual Computers, DHCP: Lease Time, Wireless: [802.1X Setting](#), System Time, VPN,

Charlie 20021007

8. Add 802.11G, Appendix B XP/2000 IPSEC configuration

9. Correct Chapter 5 Printer Setup

Charlie 20030526

10. Add RIPv1, RIPv2, SNMPv2, Log type, Email Alert – Username and Password, PPPOE –MTU, PPTP, L2TP Server, PPTP/L2TP pass through, URL Blocking,

20031002

Base on R1.9413vTIG

**Note: Although this Manual is base on [WQS4V7](#), but this version is not exactly for [WQS4V7](#), this is a full function version (for all [WQS4x7/ WQS4x8](#) series), so it has some features that Nobrand [WQS4V7](#) doesn't have. Please refer to your UI and remove those you don't need.**

## **Copyright**

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

## **Trademarks**

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

**FCC Interference Statement**

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

**CE Declaration of Conformity**

This equipment complies with the requirements relating to electromagnetic compatibility, EN 55022/A1 Class B, and EN 50082-1. This meets the essential protection requirements of the European Council Directive 89/336/EEC on the approximation of the laws of the member states relation to electromagnetic compatibility.

**Information to user.**

The users manual or instruction manual for an intentional or unintentional radiator shall caution the user that changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

## Table of Contents

Chapter 1	Introduction .....	7
	Functions and Features .....	7
	Packing List .....	9
Chapter 2	Hardware Installation .....	9
	2.1 <a href="#">Panel Layout (your product may need to be modified)</a> .....	9
	2.2 Procedure for Hardware Installation.....	12
Chapter 3	Network Settings and Software Installation.....	14
	3.1 Make Correct Network Settings of Your Computer.....	14
	3.2 <a href="#">Install the Software into Your Computers (Optional)</a> .....	14
Chapter 4	Configuring Wireless Broadband Router .....	18
	4.1 Start-up and Log in .....	18
	4.2 Status.....	19
	4.3 Wizard.....	20
	4.4 Basic Setting .....	22
	4.4.1 Primary Setup – WAN Type, Virtual Computers .....	23
	4.4.2 DHCP Server.....	28
	4.4.3 Wireless Setting, and <a href="#">802.1X setting</a> .....	30
	4.4.4 Change Password.....	32
	4.5 Forwarding Rules.....	33
	4.5.1 Virtual Server .....	34
	4.5.2 Special AP.....	35
	4.5.3 Miscellaneous Items.....	37
	4.6 Security Settings .....	38
	4.6.1 Packet Filter .....	39
	4.6.2 Domain Filter.....	44
	4.6.3 URL Blocking .....	46
	4.6.4 MAC Address Control .....	48
	4.6.5 VPN setting .....	50
	4.6.5 Miscellaneous Items.....	59
	4.7 Advanced Setting .....	61
	4.7.1 System Time.....	62
	4.7.2 System Log .....	63
	4.7.3 Dynamic DNS .....	65
	4.7.4 SNMP Setting .....	67
	4.7.5 Routing Table.....	69
	4.7.5 Schedule Rule .....	71

4.8 Toolbox .....	75
4.8.1 System Log .....	76
4.8.2 Firmware Upgrade .....	77
4.8.3 Backup Setting .....	78
4.8.4 Reset to default .....	78
4.8.5 Reboot .....	78
4.8.6 Miscellaneous Items.....	79
Chapter 5 <a href="#">Print Server</a> .....	80
5.1 Configuring on Windows 95/98 Platforms .....	80
5.2 Configuring on Windows NT Platforms .....	83
5.3 Configuring on Windows 2000 and XP Platforms.....	84
5.4 Configuring on Unix based Platforms .....	91
Appendix A <a href="#">TCP/IP Configuration for Windows 95/98</a> .....	92
A.1 Install TCP/IP Protocol into Your PC.....	92
A.2 Set TCP/IP Protocol for Working with NAT Router .....	93
Appendix B <a href="#">Win 2000/XP IPSEC Setting guide</a> .....	101
Local Security Policy Settings .....	103
VPN Settings - Tunnel 1 – IKE.....	129
VPN Settings - Tunnel 1 - Set IKE Proposal .....	130
VPN Settings - Tunnel 1 - Set IPSec Proposal .....	131
Appendix C <a href="#">Console Mode (optional)</a> .....	133

## Chapter 1 Introduction

Congratulations on your purchase of this outstanding Wireless 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

- **High speed for wireless LAN connection**  
Up to 54Mbps data rate by incorporating Orthogonal Frequency Division Multiplexing (OFDM).
- **Roaming**  
Provide seamless roaming within the IEEE 802.11b(11M) and IEEE 802.11g (54M) WLAN infrastructure.
- **IEEE 802.11b compatible (11M)**  
Allowing inter-operation among multiple vendors.
- **IEEE 802.11g compatible (54M)**  
Allowing inter-operation among multiple vendors.
- **Auto fallback**  
54M, 48M, 36M, 24M, 18M, 12M, 6M data rate with auto fallback in 802.11g mode.  
11M, 5.5M, 2M, 1M data rate with auto fallback in 802.11b mode
- **Broadband modem and NAT Router**  
Connects multiple computers to a broadband (cable or DSL) modem or an Ethernet router to surf the Internet.
- **Auto-sensing Ethernet Switch**  
Equipped with a 4-port auto-sensing Ethernet switch.
- **VPN supported**  
Supports multiple PPTP sessions and allows you to setup VPN server and VPN clients.
- **Printer sharing (Optional)**  
Embeds a print server to allow all of the networked computers to share one printer.  
Built-in both DB25 host to connect to DB25 printer and USB host to connect to USB printer for printer sharing
- **Firewall**  
All unwanted packets from outside intruders are blocked to protect your Intranet.
- **DHCP server supported**  
All of the networked computers can retrieve TCP/IP settings automatically from this product.
- **Web-based configuring**  
Configurable through any networked computer's web browser using Netscape or Internet Explorer.

- **Packet filter supported**

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

- **Universal Plug and Play (UPnP) supported**

**Universal Plug and Play (UPnP)** enable devices such as PCs, routers or other devices to be plugged into a network and automatically know about each other.

- **Virtual Server supported**

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

- **User-Definable Application Sensing Tunnel**

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

- **DMZ Host supported**

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

- **Domain Filter Supported**

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

- **URL Blocking Supported**

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

- **SNMP Supported**

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

- **Routing Table Supported**

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

- **System time Supported**

Allow you to synchronize system time with network time server.

- **Statistics of WAN Supported**

Enables you to monitor inbound and outbound packets



- **VPN Supported**  
Enables you to create virtual private tunnels to remote VPN gateways.
- **L2TP Server**  
L2TP Server enables user to build a virtual private network (VPN) connection from the remote user to the corporate LAN.
- **PPTP Server**  
PPTP Server enables user to build a virtual private network (VPN) connection from the remote user to the corporate LAN.
- **802.1X supported**  
When the 802.1X function is enable, the Wireless user must Authenticate to this router first to use the Network service.
- **Virtual Computers supported:** Virtual Computer enables you to use the original NAT feature, and allows you to setup the one-to-one mapping of multiple global IP address and local IP address.

## Packing List

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

## Chapter 2 Hardware Installation

### 2.1 Panel Layout (your product may need to be modified)

#### 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	Orange	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.
Wireless	Wireless activity	Green	Blinking	Sending or receiving data via wireless
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.

Port:

## **RESET**

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

1. Power off the device,
2. Press the reset button and hold,
3. Power on the device,
4. Keep the button pressed about 5 seconds,
5. Release the button,
6. Watch the M1 LED, they will flash 8 times and then M1 flash once per second.

### 2.1.2. Rear Panel



Figure 2-2 Rear Panel

Ports:

Port	Description
<b>5VDC</b>	Power inlet: DC 5V, 1.5A (minimum)
<b>WAN</b>	the port where you will connect your cable (or DSL) modem or Ethernet router.
<b>Port 1-4</b>	the ports where you will connect networked computers and other devices.
<b>USB</b>	USB Ports for USB printer.
<b>PRINTER</b>	Printer Port (Optional)
<b>COM</b>	Serial port (connect analog modem or console cable)(optional)

## 2.2 Procedure for Hardware Installation

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

You can place your Wireless Broadband Router on a desk or other flat surface, or you can mount it on a wall. For optimal performance, place your Wireless 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.
- b. Wireless LAN connection: locate this product at a proper position to gain the best transmit performance.

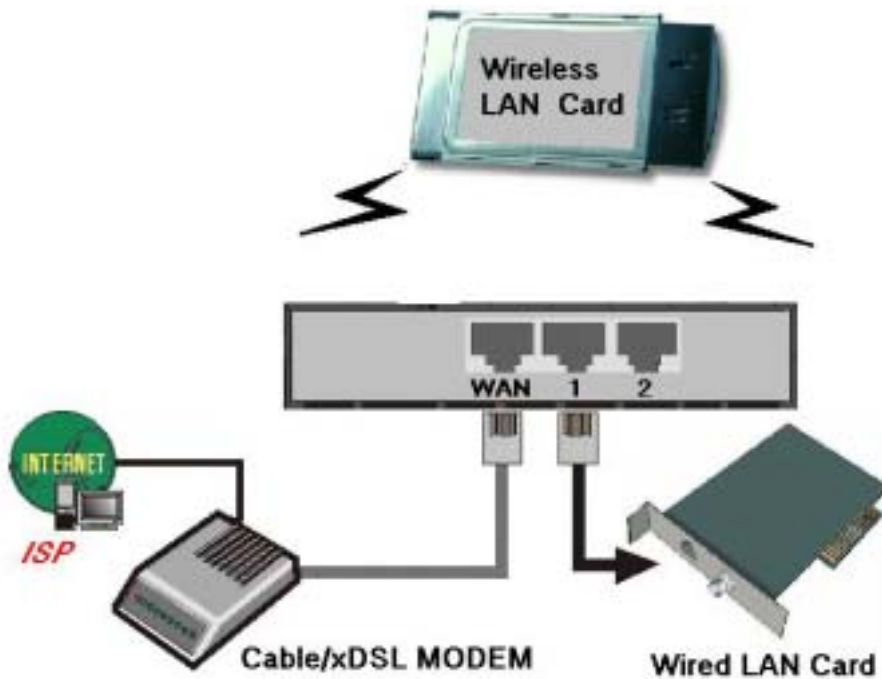


Figure 2-3 Setup of LAN and WAN connections for this product.

## 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 (Optional)

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

*Notice: Only Windows 95/98 need to install this Printer Driver. If you are using Windows 2000/XP, please refer to **Chapter 5 Printer** - 5.2 Configuring on Windows 2000 and XP Platforms.*

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



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



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





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



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



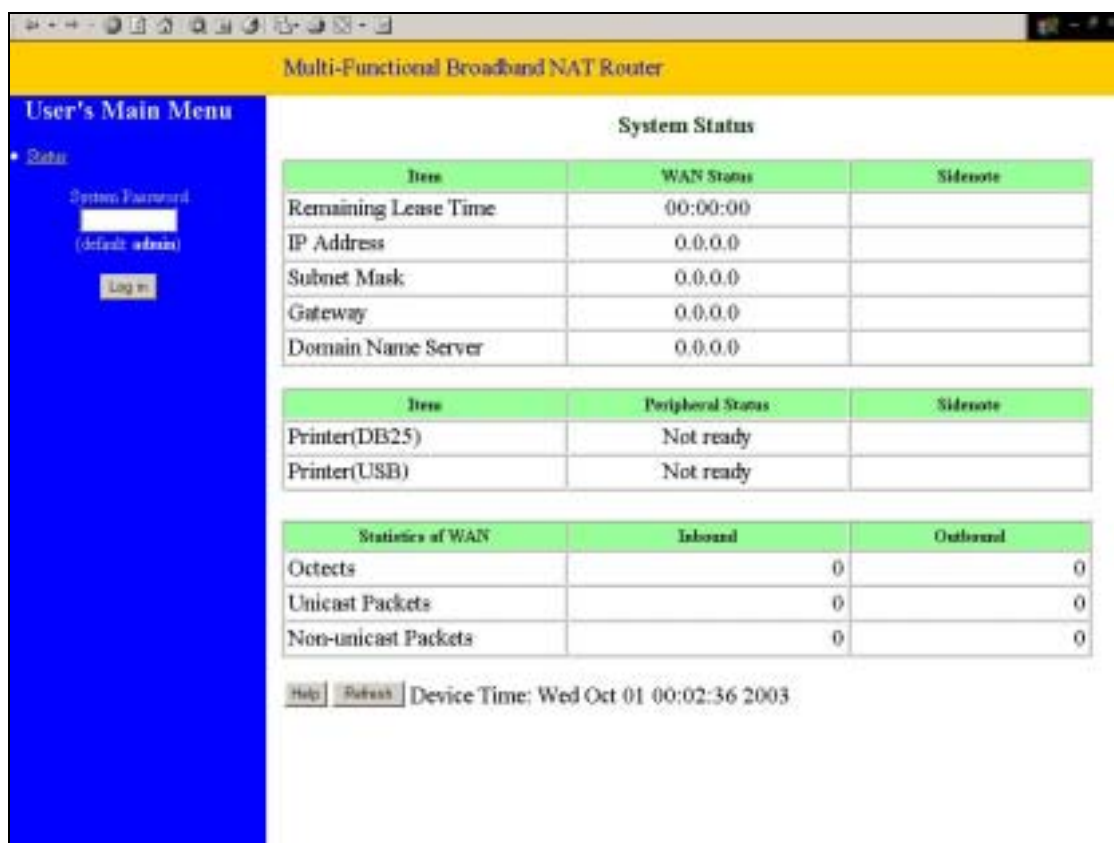
Step 6: After rebooting your computer, the software installation procedure is finished.

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

## Chapter 4 Configuring Wireless 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



The screenshot displays the web interface of a Multi-Functional Broadband NAT Router. The page is titled "Multi-Functional Broadband NAT Router" and features a blue sidebar on the left labeled "User's Main Menu" with a "Status" link. The main content area shows "System Status" with two tables. The first table lists WAN parameters: Remaining Lease Time (00:00:00), IP Address (0.0.0.0), Subnet Mask (0.0.0.0), Gateway (0.0.0.0), and Domain Name Server (0.0.0.0). The second table lists peripheral status: Printer(DB25) and Printer(USB), both marked as "Not ready". Below these is a "Statistics of WAN" table showing Inbound and Outbound traffic for Octets, Unicast Packets, and Non-unicast Packets, all at 0. At the bottom, there are "Help" and "Refresh" buttons, and the device time is displayed as "Wed Oct 01 00:02:36 2003".

Item	WAN Status	Sidenote
Remaining Lease Time	00:00:00	
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(DB25)	Not ready	
Printer(USB)	Not ready	

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

Help Refresh Device Time: Wed Oct 01 00:02:36 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

The screenshot displays the 'System Status' page of a Multi-Function Broadband NAT Router. The interface includes a blue sidebar with navigation options and a main content area with three tables and a footer.

**System Status**

Item	WAN Status	Sidenote
Remaining Lease Time	00:00:00	<input type="button" value="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	

**Peripheral Status**

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

**Statistics of WAN**

	Inbound	Outbound
Octets	0	0
Unicast Packets	0	0
Non-unicast Packets	0	0

View Log...

Device Time: Wed Oct 01 00:00:16 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.

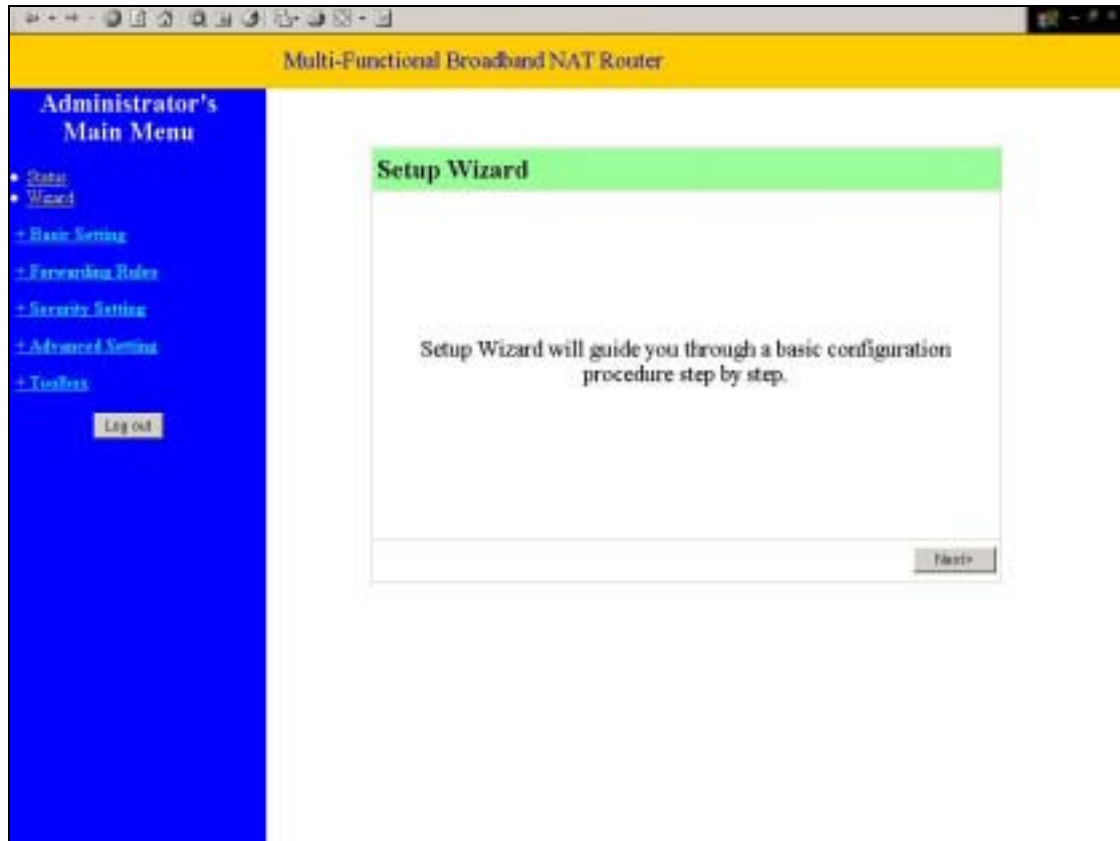
B. Modem Status.

C. Printer Status. There two printer types: Printer (DB25) and Printer (USB). The possible kinds of printer status include *“Ready”*, *“Not ready”*, *“Printing...”*, and *“Device error”*.

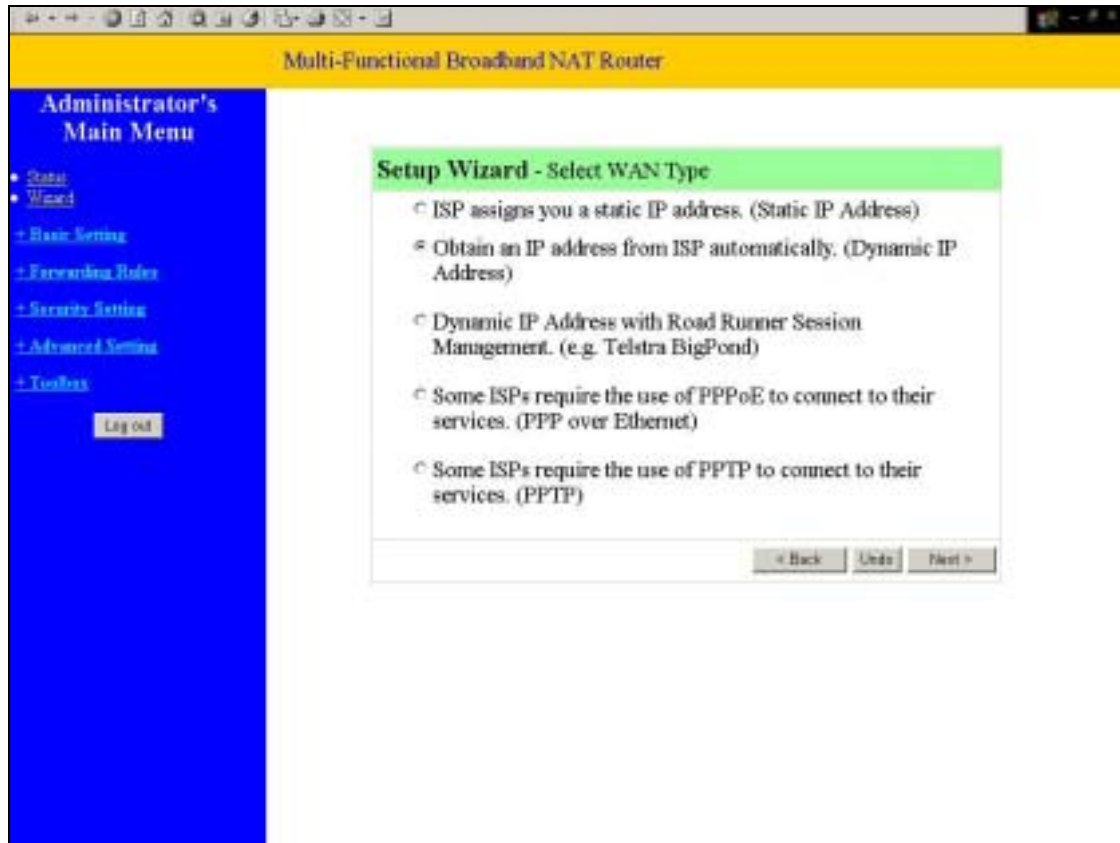
*When a job is printing, there may appear a **“Kill Job”** button on the Sidenote column. You can click this button to kill current printing job manually.*

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

### 4.3 Wizard

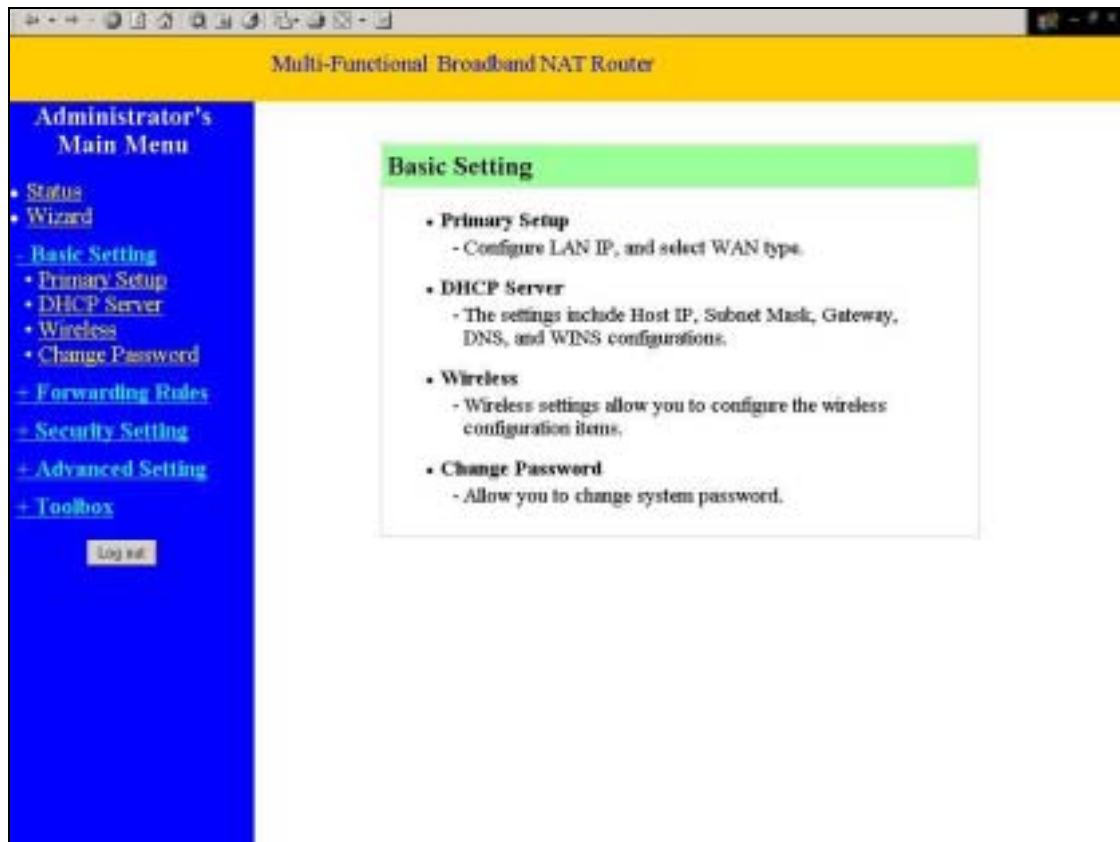


Setup Wizard will guide you through a basic configuration procedure step by step.  
Press "Next >"



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

## 4.4 Basic Setting



The screenshot displays the web interface of a Multi-Functional Broadband NAT Router. The browser window title is "Multi-Functional Broadband NAT Router". The page has a yellow header bar with the same text. On the left, there is a blue sidebar titled "Administrator's Main Menu" containing a list of navigation links: Status, Wizard, Basic Setting (highlighted), Primary Setup, DHCP Server, Wireless, Change Password, Forwarding Rules, Security Setting, Advanced Setting, and Toolbox. Below the menu is a "Log out" button. The main content area has a light green header for "Basic Setting" and lists four configuration categories:

- **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.

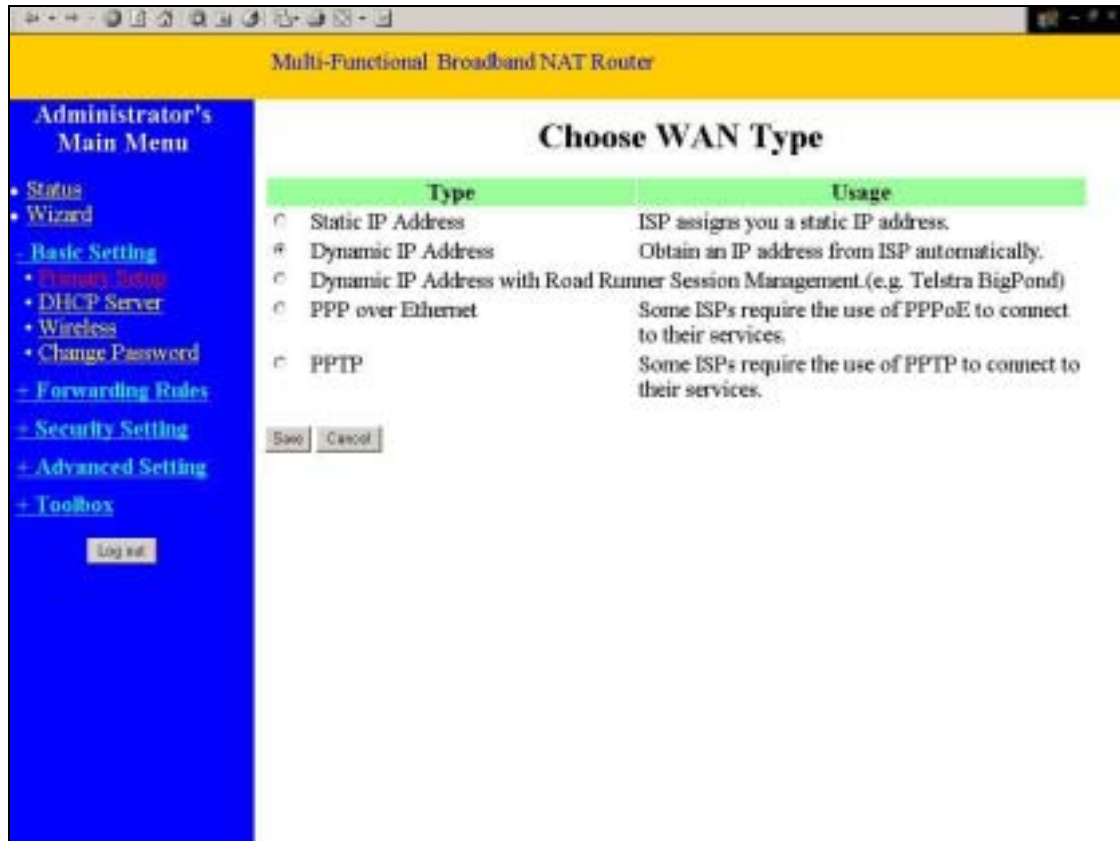
#### 4.4.1 Primary Setup – WAN Type, Virtual Computers

Multi-Functional Broadband NAT Router

### Primary Setup

Item	Setting
▶ LAN IP Address	192.168.1.23.254
▶ WAN Type	Dynamic IP Address <input type="button" value="Change"/>
▶ Host Name	<input type="text"/> (optional)
▶ WAN's MAC Address	FF-FF-FF-FF-FF-FF <input type="button" value="Clone MAC"/>
▶ Renew IP Forever	<input type="checkbox"/> Enable (Auto-reconnect)

Press “Change”



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

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

#### 4.4.1.1 Static IP Address

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

#### 4.4.1.2 Dynamic IP Address

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



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

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

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

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

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

- *Renew IP Forever*: this feature enable this product renew IP address automatically when the lease time is being expired even the system is in idle state.

#### **4.4.1.4 PPP over Ethernet**

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

#### **4.4.1.5 PPTP**

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

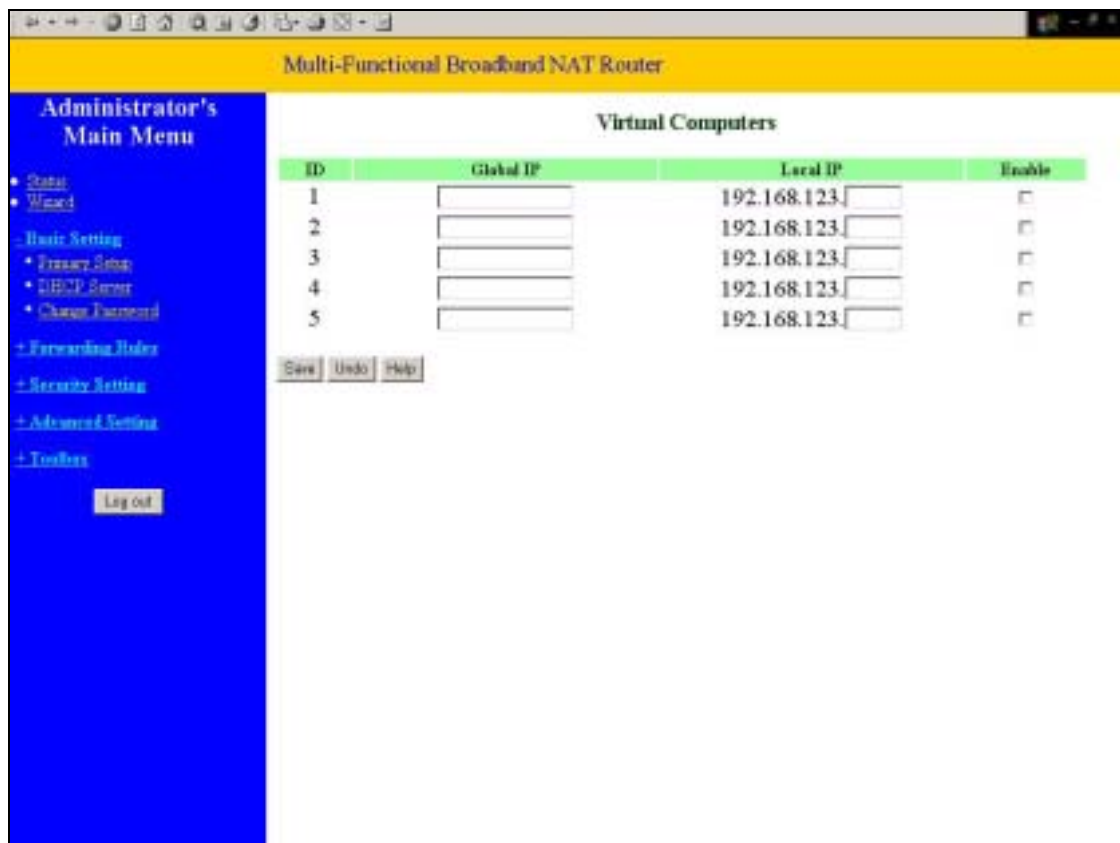
### Primary Setup

Item	Setting
▶ LAN IP Address	<input type="text" value="192.168.123.217"/>
▶ WAN Type	<b>PPTP</b> <input type="button" value="Change..."/>
▶ My IP Address	<input type="text" value="10.0.0.140"/>
▶ My Subnet Mask	<input type="text" value="255.255.255.0"/>
▶ Server IP Address	<input type="text" value="10.0.0.138"/>
▶ PPTP Account	<input type="text"/>
▶ PPTP Password	<input type="text"/>
▶ Connection ID	<input type="text" value="Input if ISP requires it"/> (optional)
▶ Maximum Idle Time	<input type="text" value="300"/> seconds <input type="checkbox"/> Auto-reconnect

#### 4.4.1.6 Dial-up Network

1. *Dial-up Telephone, Account and Password:* assigned by your ISP. For security, this field appears blank. If you don't want to change the password, leave it empty.
2. *Primary and Secondary DNS:* If they are configured as "0.0.0.0.", they will be automatically assigned upon connection.
3. *Maximum Idle Time:* the amount of time of inactivity before disconnecting your dial-up session.
4. *Baud Rate:* the communication speed between this product and your MODEM or ISDN TA.
5. *Extra Setting:* (initialization string) optional. Used to optimize the communication quality between the ISP and your MODEM or ISDN TA

#### 4.4.1.7 Virtual Computers



The screenshot displays the web interface of a Multi-Functional Broadband NAT Router. The top navigation bar is yellow and contains the text "Multi-Functional Broadband NAT Router". On the left, a blue sidebar titled "Administrator's Main Menu" lists various configuration options: Status, Wizard, Basic Setting (Primary Setup, DHCP Server, Change Password), Advanced Rules, Security Setting, Advanced Settings, and Tools. A "Log out" button is located at the bottom of the sidebar. The main content area is titled "Virtual Computers" and features a table with the following columns: ID, Global IP, Local IP, and Enable. The table contains five rows, each with an ID from 1 to 5. The "Global IP" column has empty input fields. The "Local IP" column shows the value "192.168.123." followed by an empty input field. The "Enable" column contains unchecked checkboxes. Below the table are three buttons: "Save", "Undo", and "Help".

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

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

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

## 4.4.2 DHCP Server

The screenshot shows the configuration interface for the DHCP Server on a Multi-Functional Broadband NAT Router. The interface is divided into a left sidebar and a main content area.

**Administrator's Main Menu**

- Status
- Wizard
- Basic Setting
  - Factory Setup
  - DHCP Server
  - Change Password
- Forwarding Rules
- Security Setting
- Advanced Settings
- Tools

[Log out](#)

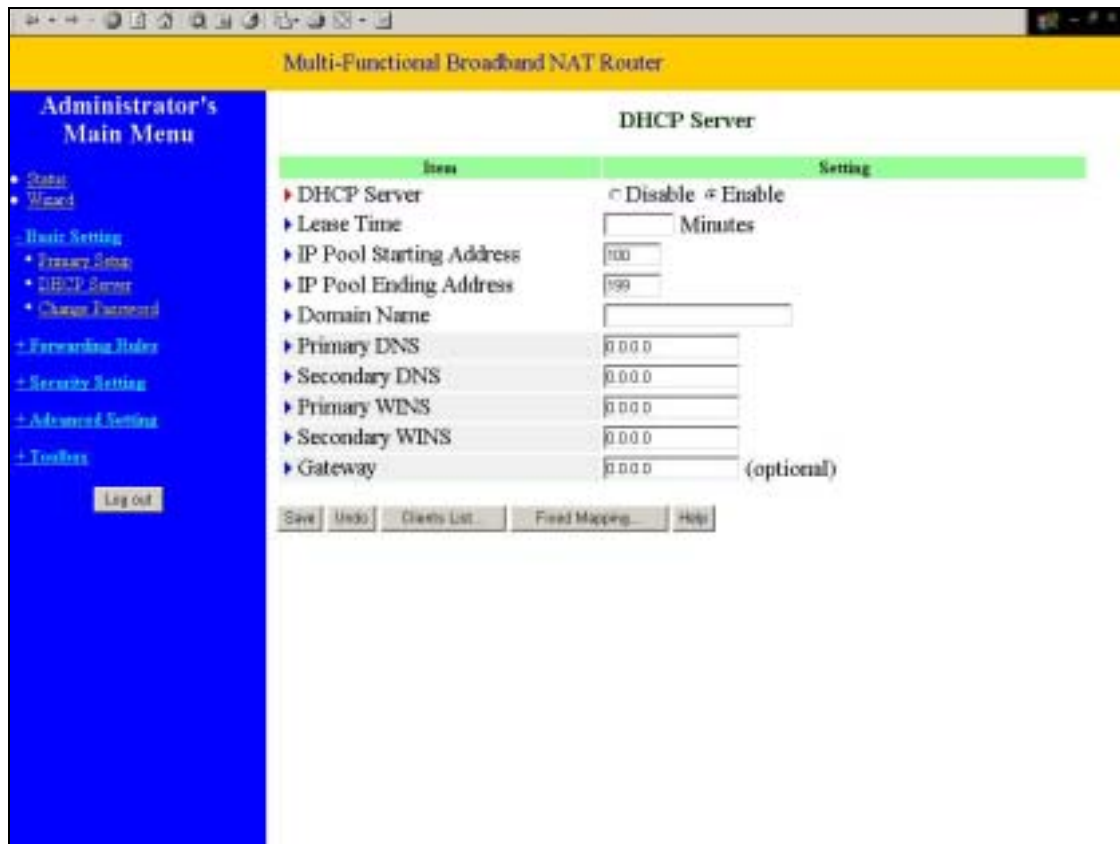
**Multi-Functional Broadband NAT Router**

**DHCP Server**

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

[Save](#) [Undo](#) [More>>](#) [Class List](#) [Fixed Mapping](#) [Help](#)

Press “More>>”

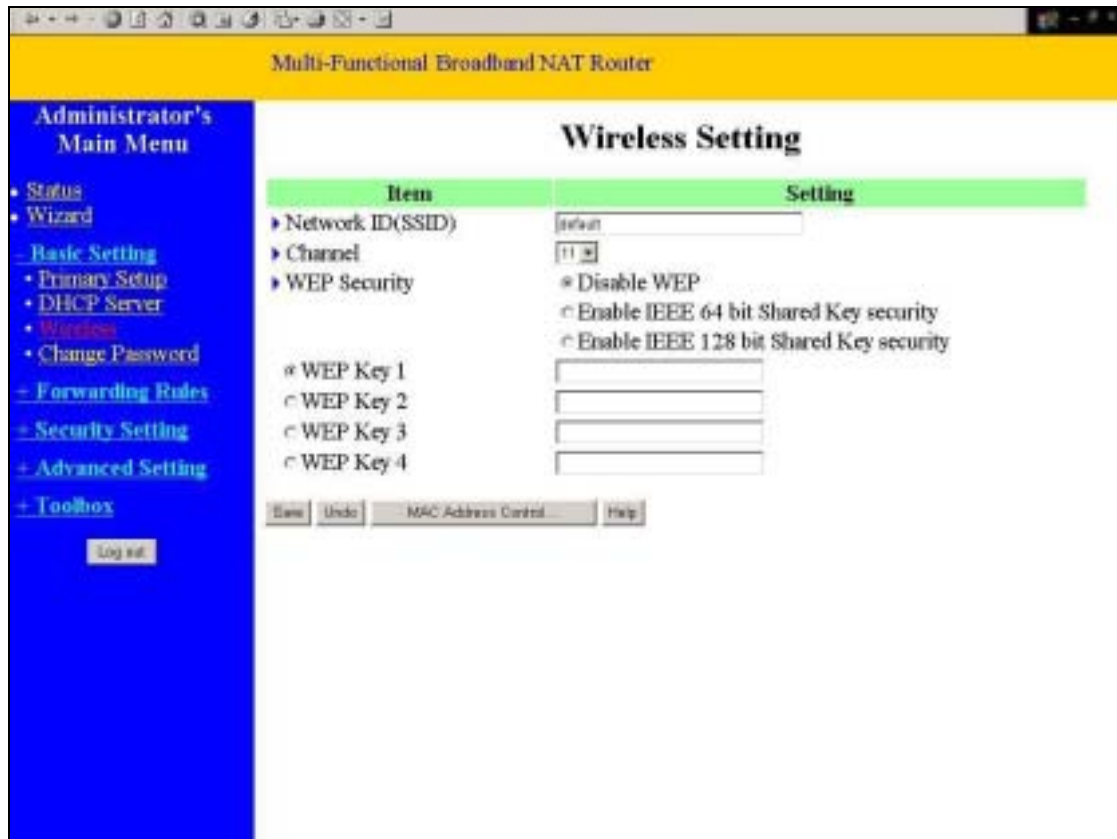


The settings of a TCP/IP environment include host IP, Subnet Mask, Gateway, and DNS configurations. It is not easy to manually configure all the computers and devices in your network. Fortunately, DHCP Server provides a rather simple approach to handle all these settings. This product supports the function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

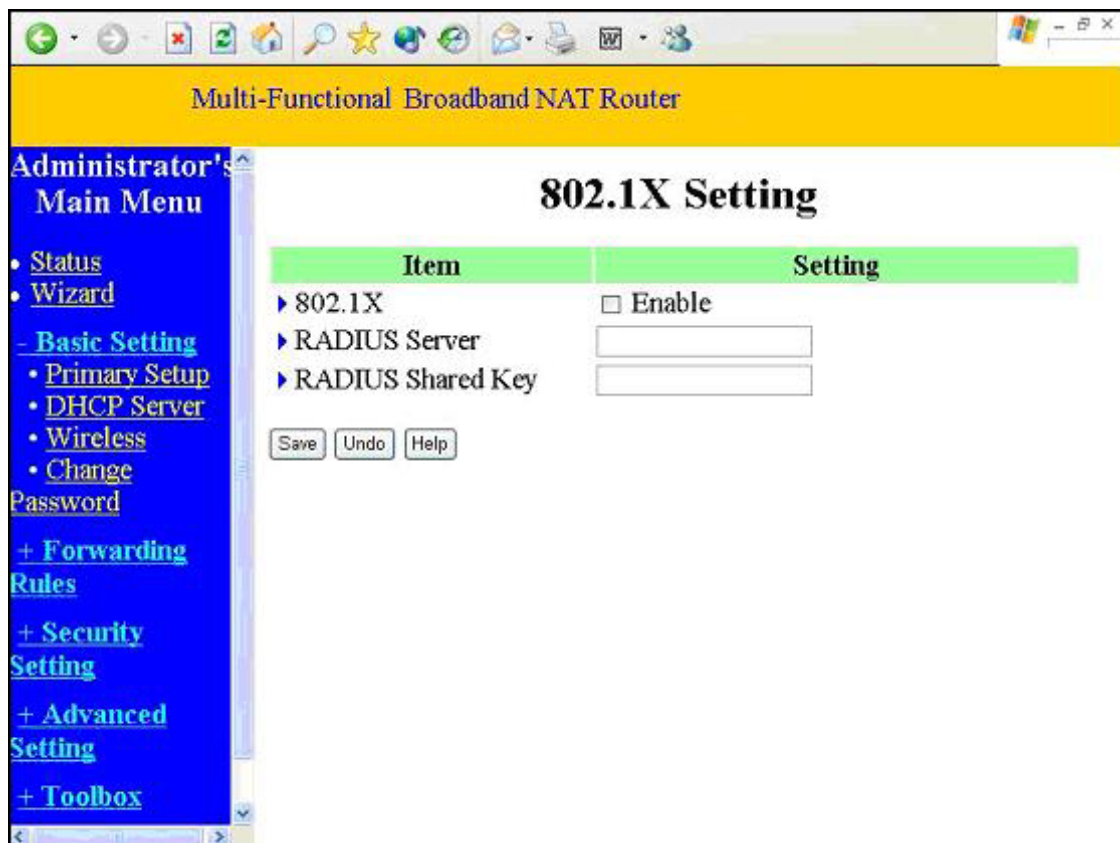
IP to your PC.

#### 4.4.3 Wireless Setting, and 802.1X setting



Wireless settings allow you to set the wireless configuration items.

1. **Network ID(SSID)**: Network ID is used for identifying the Wireless LAN (WLAN). Client stations can roam freely over this product and other Access Points that have the same Network ID. (The factory setting is “*default*”)
2. **Channel**: The radio channel number. The permissible channels depend on the Regulatory Domain. The factory setting is as follow: **channel 6** for North America; **channel 7** for European (ETSI); **channel 7** for Japan.
3. **WEP Security**: Select the data privacy algorithm you want. Enabling the security can protect your data while it is transferred from one station to another. The standardized IEEE 802.11 WEP (128 or 64-bit) is used here.
4. **WEP Key 1, 2, 3 & 4**: When you enable the 128 or 64 bit WEP key security, please select one WEP key to be used and input 26 or 10 hexadecimal (0, 1, 2...8, 9, A, B...F) digits.
5. **Pass-phrase Generator**: Since hexadecimal characters are not easily remembered, this device offers a conversion utility to convert a simple word or phrase into hex.
6. **802.1X Setting**



### 802.1X

CheckBox was used to switch the function of the 802.1X. When the 802.1X function is enable, the Wireless user must **authenticate** to this router first to use the Network service.

### RADIUS Server

IP address or the 802.1X server's domain-name.

### RADIUS Shared Key

Key value shared by the RADIUS server and this router. This key value is consistent with the key value in the RADIUS server.

#### 4.4.4 Change Password

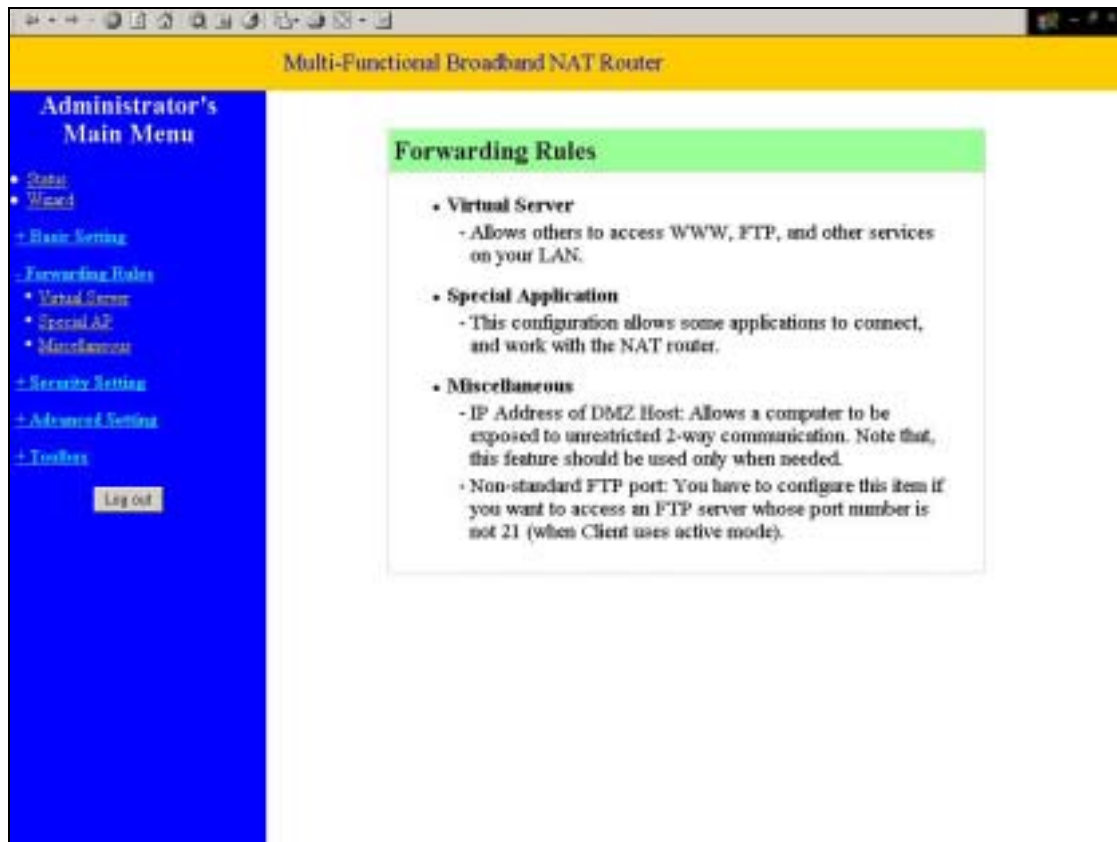
The screenshot shows the web interface of a Multi-Functional Broadband NAT Router. The page title is "Change Password". On the left is a blue sidebar menu with the following items: "Administrator's Main Menu", "Status", "Wizard", "Basic Setting" (with sub-items "Primary Setup", "DHCP Server", "Wireless", and "Change Password" in red), "Forwarding Rules", "Security Setting", "Advanced Setting", and "Toolbox". A "LOG OUT" button is at the bottom of the sidebar. The main content area has a table with two columns: "Item" and "Setting". The table contains three rows: "Old Password", "New Password", and "Reconfirm", each with an adjacent input field. Below the table are "Save" and "Undo" buttons.

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

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



## 4.5 Forwarding Rules



The screenshot displays the web interface of a Multi-Functional Broadband NAT Router. The page title is "Multi-Functional Broadband NAT Router". On the left, there is a blue sidebar titled "Administrator's Main Menu" with the following navigation options: [Status](#), [Wizard](#), [Basic Setting](#), [Forwarding Rules](#), [Virtual Server](#), [Special App](#), [Miscellaneous](#), [Security Setting](#), [Advanced Setting](#), and [Tools](#). A "Log Out" button is located at the bottom of the sidebar. The main content area is titled "Forwarding Rules" and contains the following information:

- **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

Multi-Function Broadband NAT Router

Administrator's Main Menu

- Status
- Wizard
- Basic Settings
- Forwarding Rules
- Virtual Server
- Special AP
- MicroGateway
- Security Setting
- Advanced Settings
- Tools

Log out

Virtual Server

ID	Service Ports	Server IP	Enable	Use Rules
1		192.168.123.	<input type="checkbox"/>	0
2		192.168.123.	<input type="checkbox"/>	0
3		192.168.123.	<input type="checkbox"/>	0
4		192.168.123.	<input type="checkbox"/>	0
5		192.168.123.	<input type="checkbox"/>	0
6		192.168.123.	<input type="checkbox"/>	0
7		192.168.123.	<input type="checkbox"/>	0
8		192.168.123.	<input type="checkbox"/>	0
9		192.168.123.	<input type="checkbox"/>	0
10		192.168.123.	<input type="checkbox"/>	0
11		192.168.123.	<input type="checkbox"/>	0
12		192.168.123.	<input type="checkbox"/>	0
13		192.168.123.	<input type="checkbox"/>	0
14		192.168.123.	<input type="checkbox"/>	0
15		192.168.123.	<input type="checkbox"/>	0
16		192.168.123.	<input type="checkbox"/>	0
17		192.168.123.	<input type="checkbox"/>	0
18		192.168.123.	<input type="checkbox"/>	0
19		192.168.123.	<input type="checkbox"/>	0
20		192.168.123.	<input type="checkbox"/>	0

Well known services:   
 Schedule rule:

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

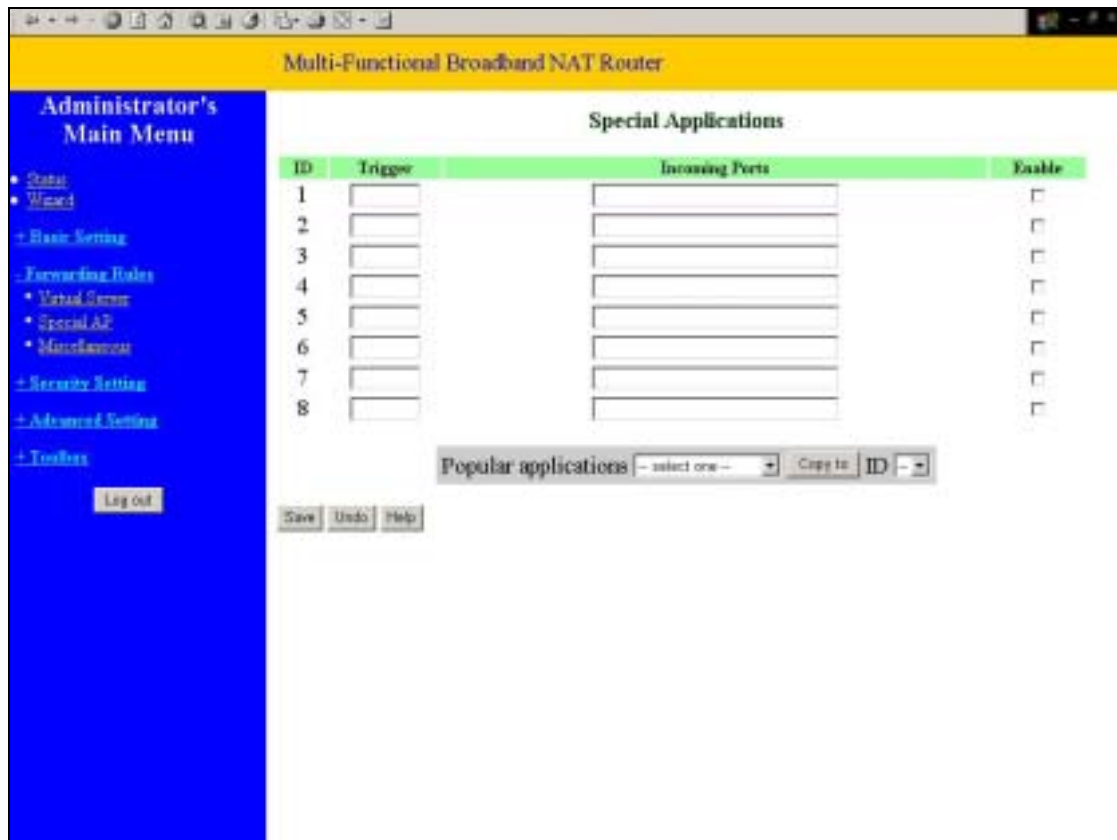
A virtual server is defined as a **Service Port**, and all requests to this port will be redirected to the computer specified by the **Server IP**. **Virtual Server** can work with **Scheduling Rules**, and give user more flexibility on Access control. For Detail, please refer to **Scheduling Rule**.

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

Service Port	Server IP	Enable
--------------	-----------	--------

21	192.168.123.1	V
80	192.168.123.2	V
1723	192.168.123.6	V

## 4.5.2 Special AP



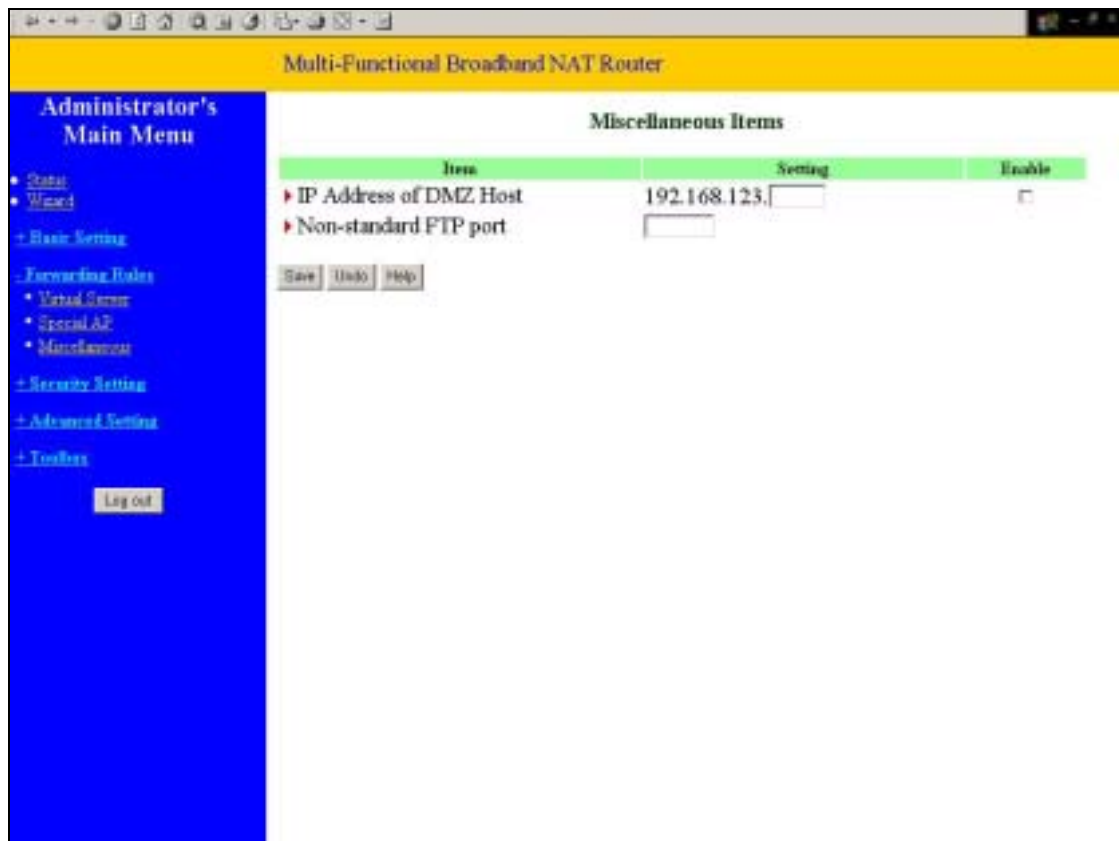
Some applications require multiple connections, like Internet games, Video conferencing, Internet telephony, etc. Because of the firewall function, these applications cannot work with a pure NAT router. The **Special Applications** feature allows some of these applications to work with this product.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

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

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

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

### 4.5.3 Miscellaneous Items



#### IP Address of DMZ Host

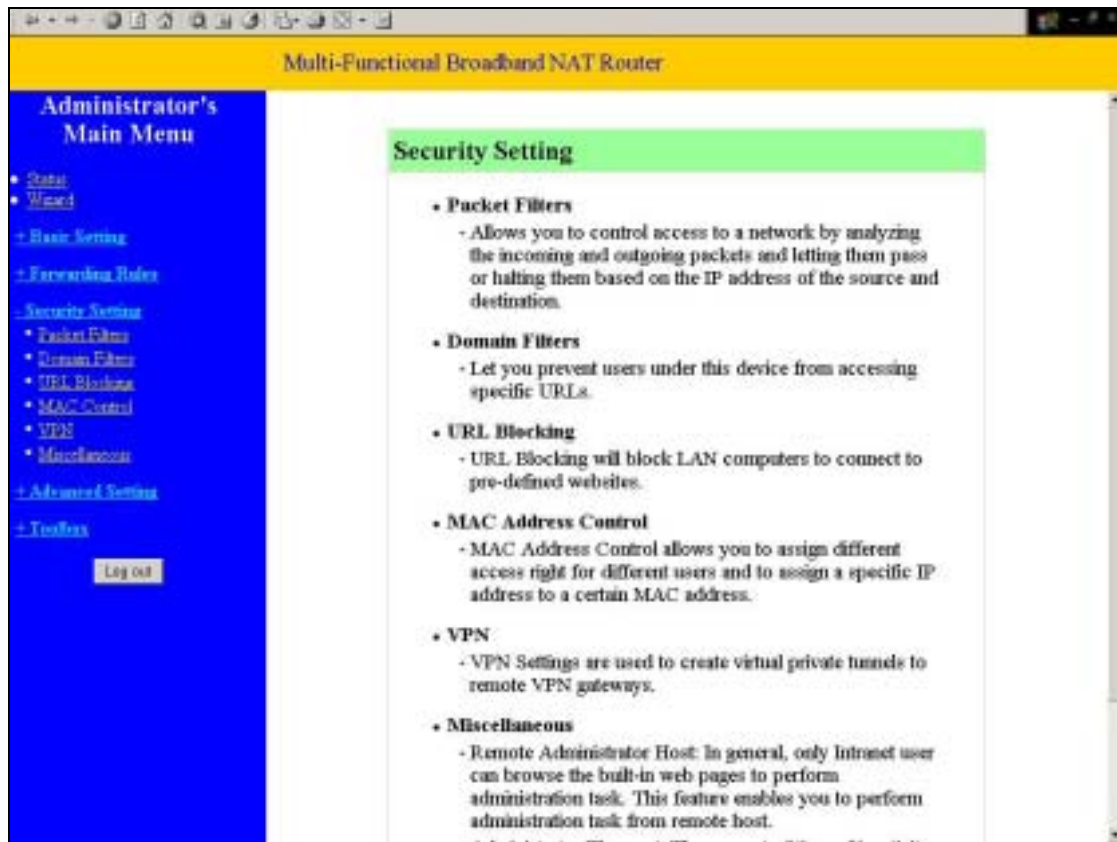
DMZ (DeMilitarized Zone) Host is a host without the protection of firewall. It allows a computer to be exposed to unrestricted 2-way communication for Internet games, Video conferencing, Internet telephony and other special applications.

*NOTE: This feature should be used only when needed.*

#### Non-standard FTP port

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

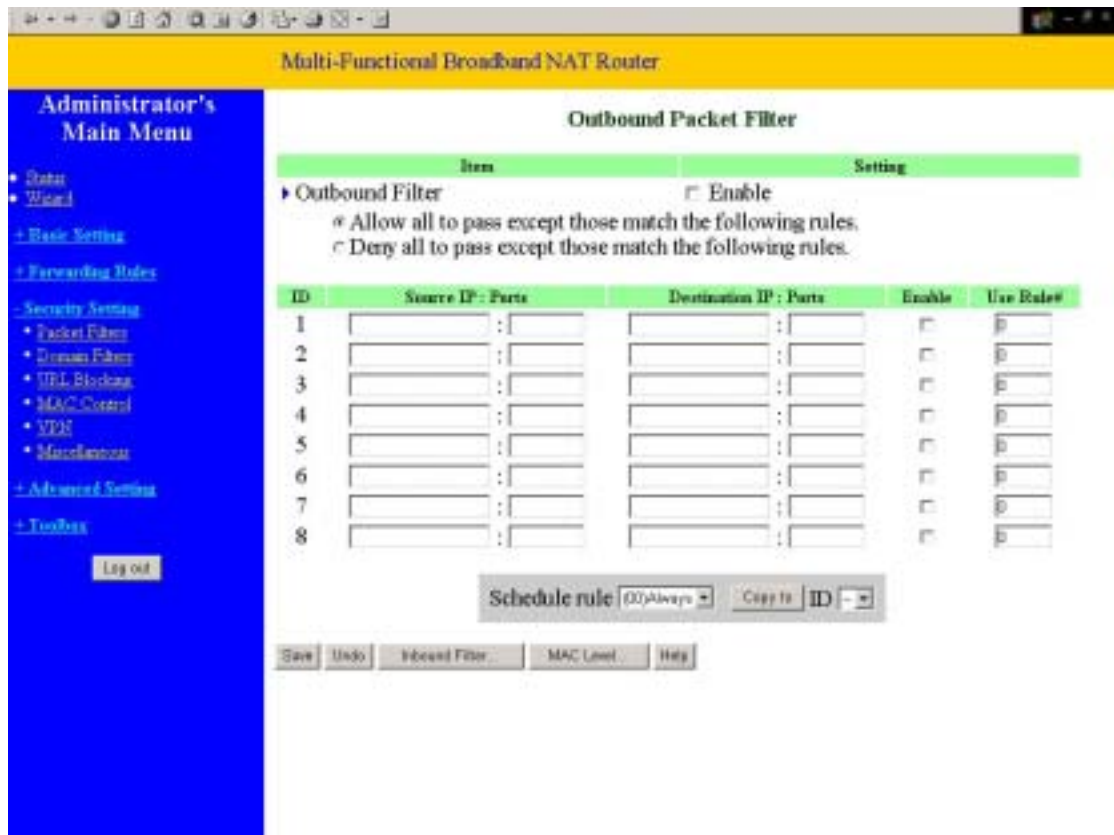
## 4.6 Security Settings



The screenshot displays the web interface of a Multi-Functional Broadband NAT Router. The page title is "Multi-Functional Broadband NAT Router". On the left, there is a blue sidebar titled "Administrator's Main Menu" with a "Log out" button. The main content area is titled "Security Setting" and lists several security features:

- Packet Filters**
  - Allows you to control access to a network by analyzing the incoming and outgoing packets and letting them pass or halting them based on the IP address of the source and destination.
- Domain Filters**
  - Let you prevent users under this device from accessing specific URLs.
- URL Blocking**
  - URL Blocking will block LAN computers to connect to pre-defined websites.
- MAC Address Control**
  - MAC Address Control allows you to assign different access right for different users and to assign a specific IP address to a certain MAC address.
- VPN**
  - VPN Settings are used to create virtual private tunnels to remote VPN gateways.
- Miscellaneous**
  - Remote Administrator Host: In general, only Intranet user can browse the built-in web pages to perform administration task. This feature enables you to perform administration task from remote host.

## 4.6.1 Packet Filter



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

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

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

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

For source or destination IP address, you can define a single IP address (4.3.2.1) or a range of IP

addresses (4.3.2.1-4.3.2.254). An empty implies all IP addresses.

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

Each rule can be enabled or disabled individually.

Inbound Filter:

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

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

**Example 1:**

ID	Source IP : Ports	Destination IP : Ports	Enable
1	1.2.3.100-1.2.3.149	: 25-110	<input checked="" type="checkbox"/>
2	1.2.3.10-1.2.3.20	:	<input checked="" type="checkbox"/>
3	:	:	<input type="checkbox"/>
4	:	:	<input type="checkbox"/>
5	:	:	<input type="checkbox"/>
6	:	:	<input type="checkbox"/>
7	:	:	<input type="checkbox"/>
8	:	:	<input type="checkbox"/>

(1.2.3.100-1.2.3.149) They are allow to send mail (port 25), receive mail (port 110),



and browse the Internet (port 80)

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

Others are all blocked.

### Example 2:

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

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

Others are all allowed.

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

Outbound Filter:

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

### Example 1:

Outbound Packet Filter					
Item		Setting			
▶ Outbound Filter		<input checked="" type="checkbox"/> Enable			
<input type="radio"/> Allow all to pass except those match the following rules.					
<input checked="" type="radio"/> Deny all to pass except those match the following rules.					
ID	Source IP:Ports		Destination IP:Ports		Enable
1	100-192.168.123.149			25-110	<input checked="" type="checkbox"/>
2	23.10-192.168.123.20				<input checked="" type="checkbox"/>
3					<input type="checkbox"/>
4					<input type="checkbox"/>
5					<input type="checkbox"/>
6					<input type="checkbox"/>
7					<input type="checkbox"/>
8					<input type="checkbox"/>
<input type="button" value="Save"/> <input type="button" value="Undo"/> <input type="button" value="Inbound Filter..."/> <input type="button" value="MAC Level..."/> <input type="button" value="Help"/>					

(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

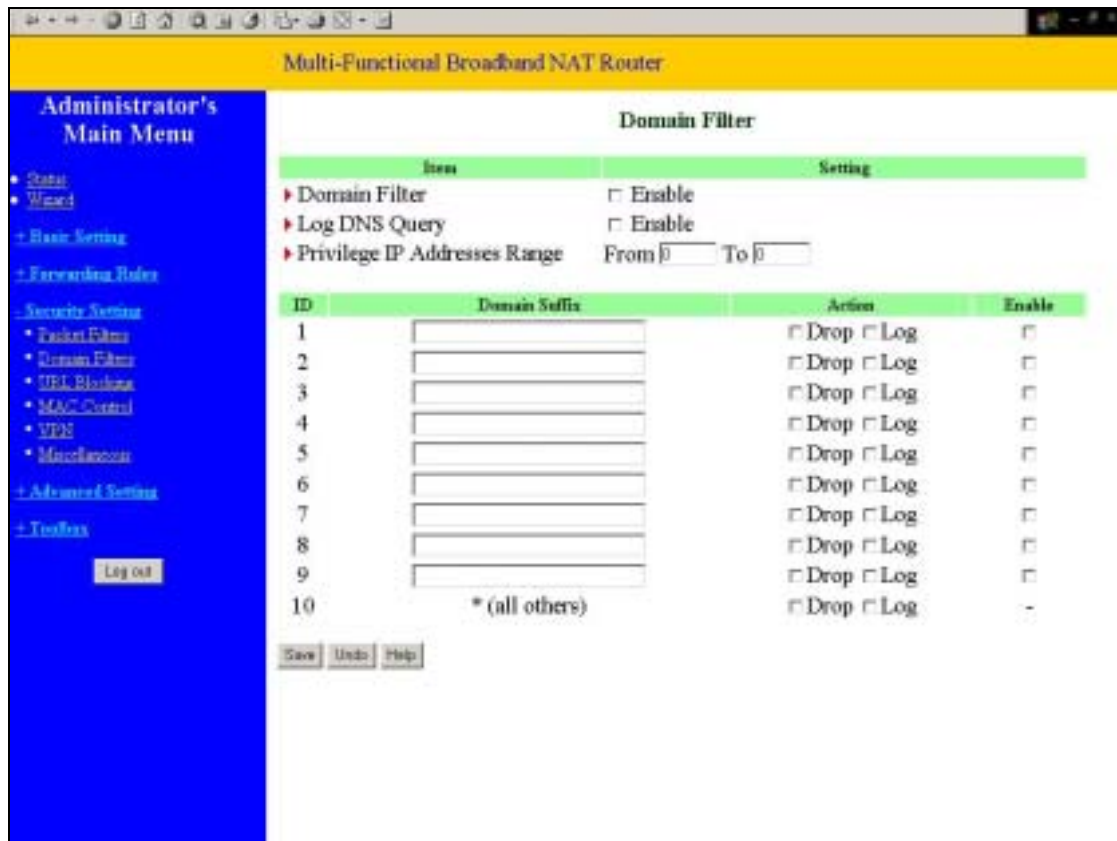
Item	Setting		
▶ Outbound Filter <span style="float: right;"><input checked="" type="checkbox"/> Enable</span>			
<input checked="" type="radio"/> Allow all to pass except those match the following rules. <input type="radio"/> Deny all to pass except those match the following rules.			
ID	Source IP:Ports	Destination IP:Ports	Enable
1	[100-192.168.123.119]	[ ] [21]	<input checked="" type="checkbox"/>
2	[100-192.168.100.119]	[ ] [119]	<input checked="" type="checkbox"/>
3	[ ] [ ]	[ ] [ ]	<input type="checkbox"/>
4	[ ] [ ]	[ ] [ ]	<input type="checkbox"/>
5	[ ] [ ]	[ ] [ ]	<input type="checkbox"/>
6	[ ] [ ]	[ ] [ ]	<input type="checkbox"/>
7	[ ] [ ]	[ ] [ ]	<input type="checkbox"/>
8	[ ] [ ]	[ ] [ ]	<input type="checkbox"/>

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

Others are allowed

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

## 4.6.2 Domain Filter



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

### Domain Filter Enable

*Check* if you want to enable Domain Filter.

### Log DNS Query

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

### Privilege IP Addresses Range

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

### Domain Suffix

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

### Action

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

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

### Enable

*Check* to enable each rule.

## Example:

Domain Filter			
Item	Setting		
▶ Domain Filter	<input checked="" type="checkbox"/> Enable		
▶ Log DNS Query	<input checked="" type="checkbox"/> Enable		
▶ Privilege IP Addresses Range	From <input type="text" value="1"/> To <input type="text" value="10"/>		

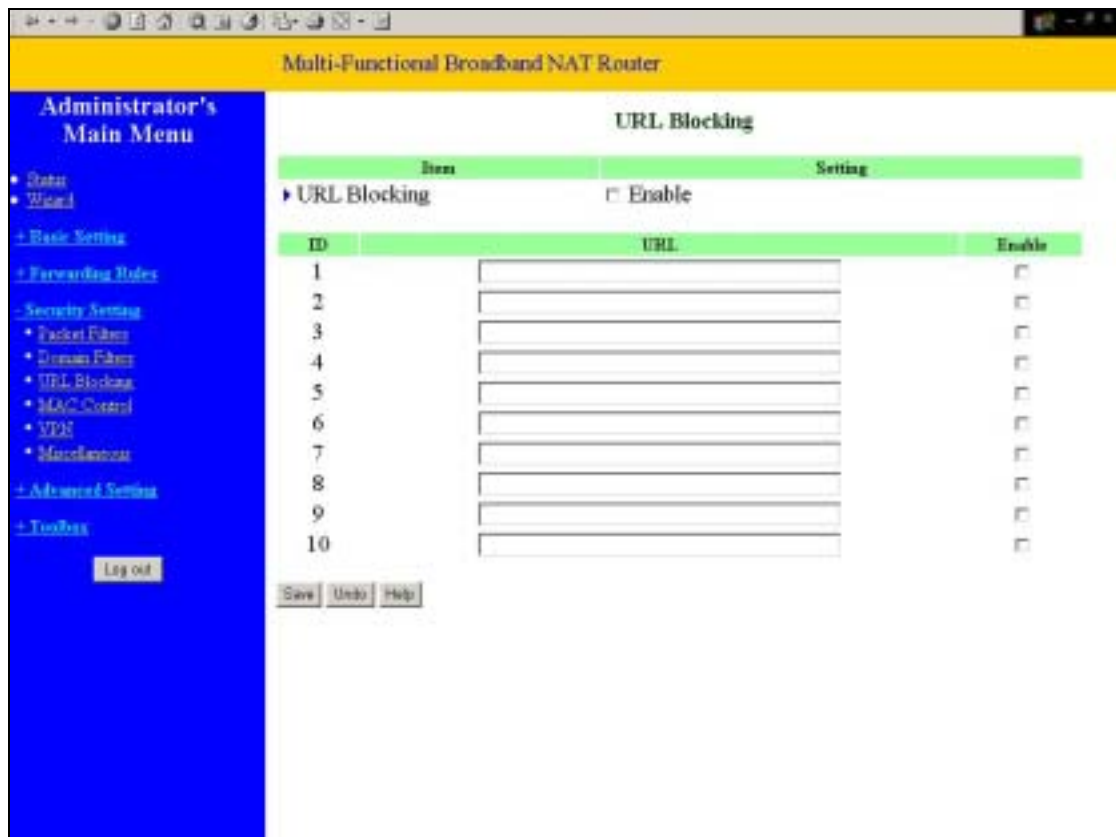
  

ID	Domain Suffix	Action	Enable
1	<input type="text" value="sex.com"/>	<input checked="" type="checkbox"/> Drop <input checked="" type="checkbox"/> Log	<input checked="" type="checkbox"/>
2	<input type="text" value="girl.com"/>	<input type="checkbox"/> Drop <input checked="" type="checkbox"/> Log	<input checked="" type="checkbox"/>
3	<input type="text" value="erotica.com"/>	<input checked="" type="checkbox"/> Drop <input type="checkbox"/> Log	<input checked="" type="checkbox"/>
4	<input type="text"/>	<input type="checkbox"/> Drop <input type="checkbox"/> Log	<input type="checkbox"/>
5	<input type="text"/>	<input type="checkbox"/> Drop <input type="checkbox"/> Log	<input type="checkbox"/>
6	<input type="text"/>	<input type="checkbox"/> Drop <input type="checkbox"/> Log	<input type="checkbox"/>
7	<input type="text"/>	<input type="checkbox"/> Drop <input type="checkbox"/> Log	<input type="checkbox"/>
8	<input type="text"/>	<input type="checkbox"/> Drop <input type="checkbox"/> Log	<input type="checkbox"/>
9	<input type="text"/>	<input type="checkbox"/> Drop <input type="checkbox"/> Log	<input type="checkbox"/>
10	* (all others)	<input type="checkbox"/> Drop <input type="checkbox"/> Log	-

In this example:

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

### 4.6.3 URL Blocking



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

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

#### **URL Blocking Enable**

*Checked* if you want to enable URL Blocking.

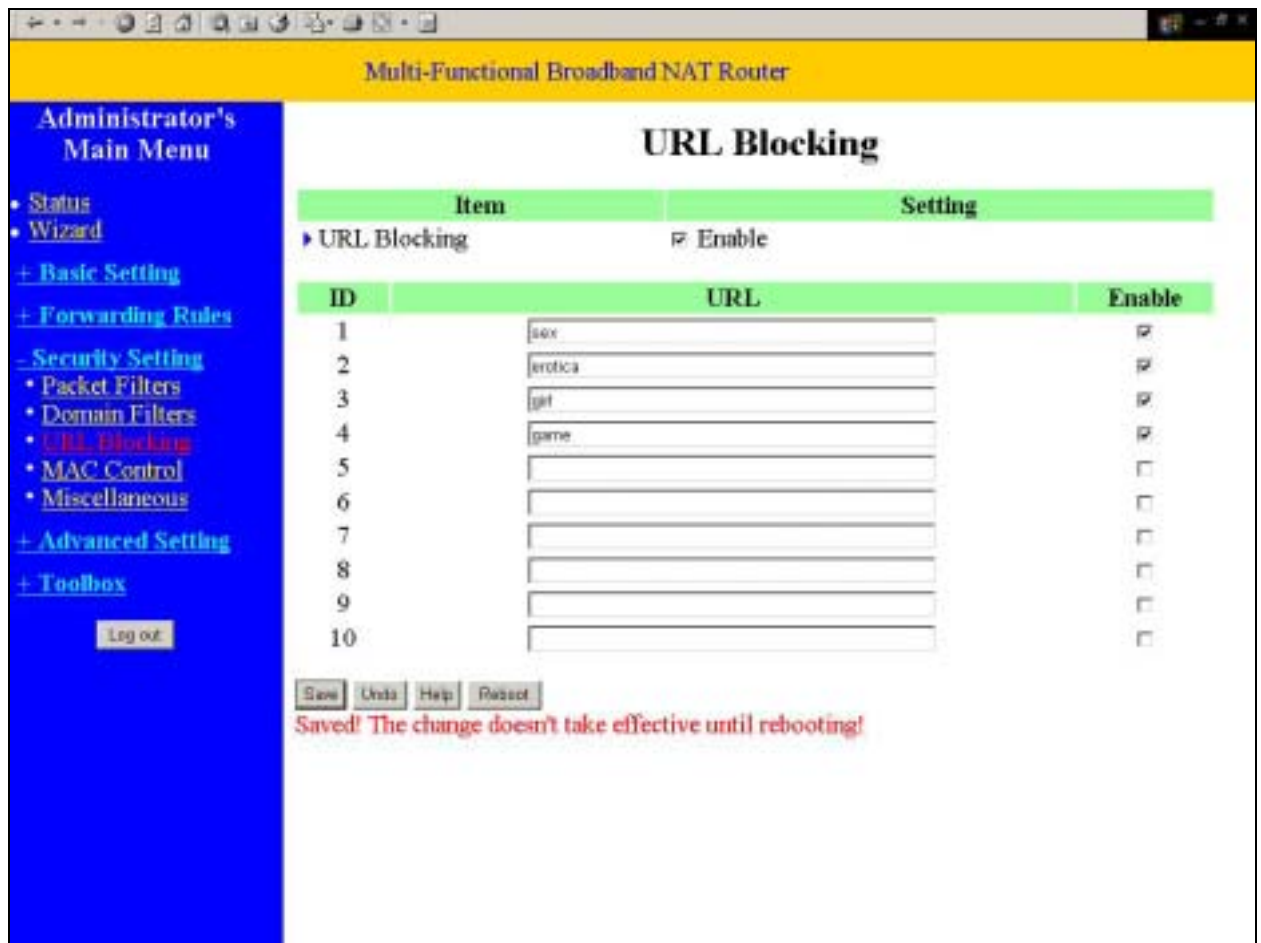
#### **URL**

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

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

#### **Enable**

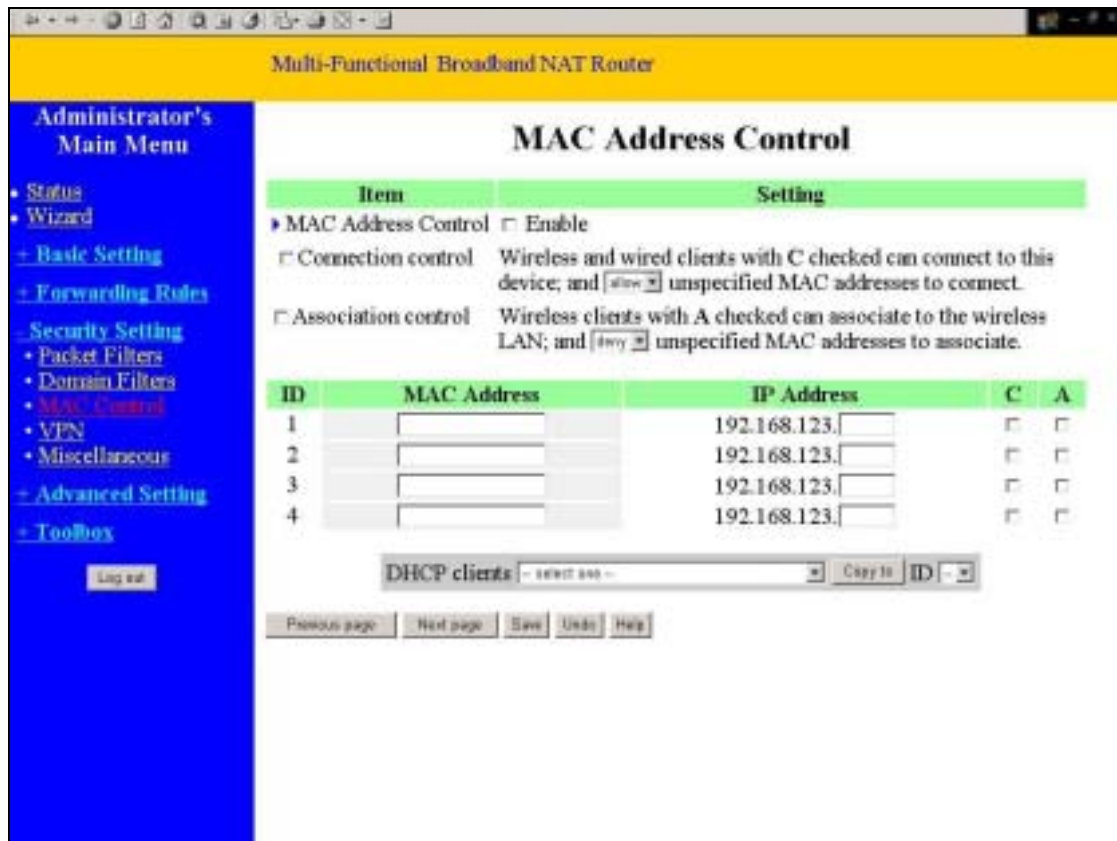
*Checked* to enable each rule.



In this example:

- 1.URL include “sex” will be blocked, and the action will be record in log-file.
- 2.URL include “erotica” will be blocked, but the action will be record in log-file
- 3.URL include “girl” will not be blocked, but the action will be record in log-file.
4. URL include “game” will be blocked, but the action will be record in log-file

## 4.6.4 MAC Address Control



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

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

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

**Association control** Check "Association control" to enable the controlling of which wireless client can associate to the wireless LAN. If a client is denied to associate to the wireless LAN, it means the client can't send or receive any data via this device. Choose "allow" or "deny" to



allow or deny the clients, whose MAC addresses are not in the "Control table", to associate to the wireless LAN.

### Control table

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

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

<b>MAC Address</b>	MAC address indicates a specific client.
<b>IP Address</b>	Expected IP address of the corresponding client. Keep it empty if you don't care its IP address.
<b>C</b>	When " <b>Connection control</b> " is checked, check "C" will allow the corresponding client to connect to this device.
<b>A</b>	When " <b>Association control</b> " is checked, check "A" will allow the corresponding client to associate to the wireless LAN.

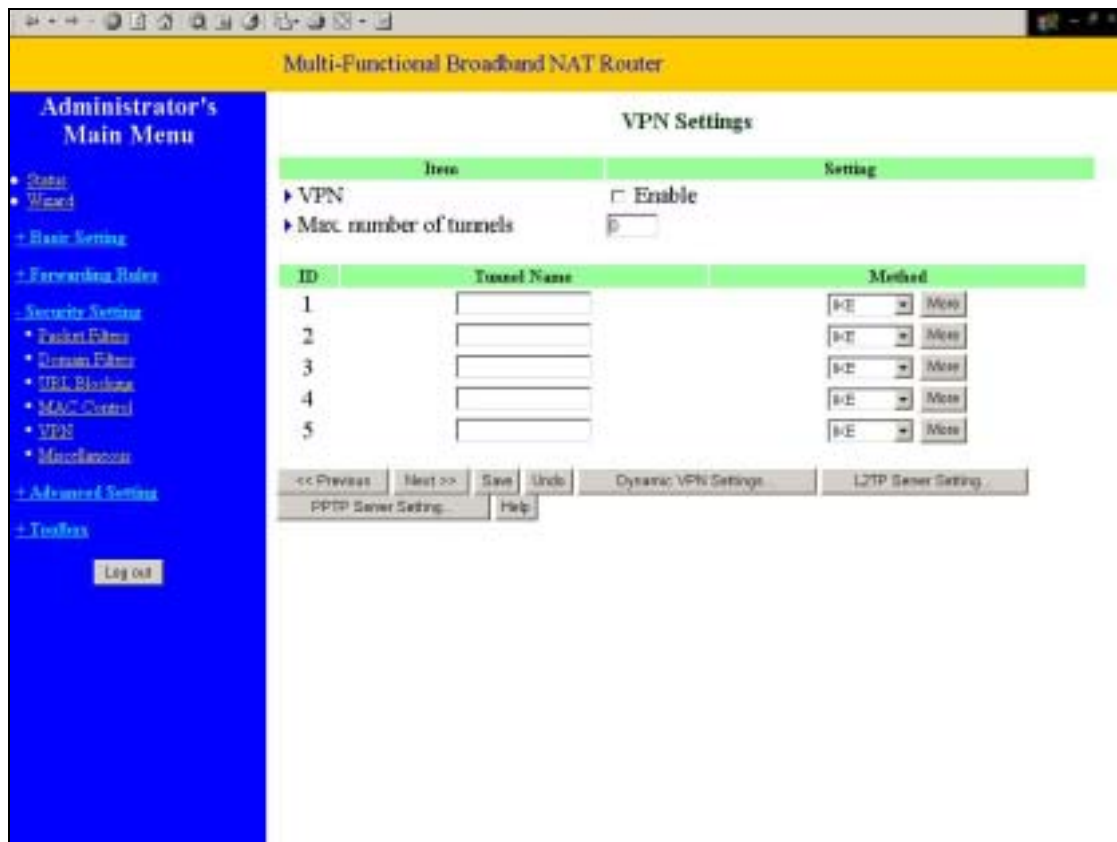
In this page, we provide the following Combobox and button to help you to input the MAC address.



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

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

## 4.6.5 VPN setting



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

- **VPN enable item**

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

- **Max. number of tunnels item**

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

- **Tunnel name**

Indicate which tunnel that is focused now.

- **Method**

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

## Function of Buttons

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

### 4.6.5.1 VPN Settings - IKE

The screenshot shows the configuration interface for a Multi-Functional Broadband NAT Router. The page title is "VPN Settings - Tunnel 1 - IKE". On the left is a blue sidebar with the "Administrator's Main Menu" containing links for Status, Wizard, Basic Settings, Expressions Rules, Security Settings (Packet Filter, Domain Filter, URL Blocking, MAC Control, VPN, Miscellaneous), Advanced Settings, and Tools. A "Log out" button is at the bottom of the sidebar. The main content area has a table with two columns: "Item" and "Setting".

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

At the bottom of the form are buttons for "Save", "Undo", "Back", and "Help", followed by a status indicator "No change!".

### •VPN Settings - IKE

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

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

#### - Basic setup:

##### Local subnet

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

##### Local netmask

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

**Remote subnet**

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

**Remote netmask**

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

**Remote gateway**

The IP address of remote VPN gateway.

**Pre-shared key**

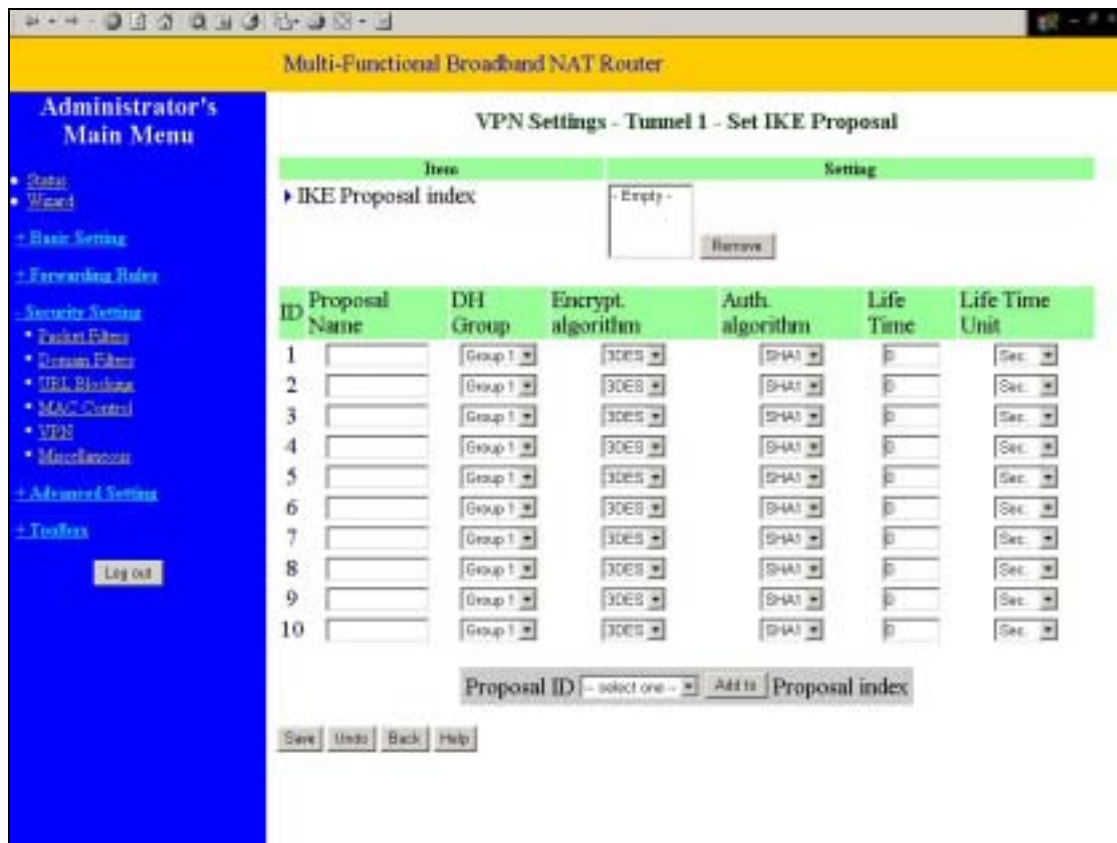
The first key that supports IKE mechanism of both VPN gateways for negotiating further security keys. The pre-shared key must be same for both end gateways.

**Function of Buttons**

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

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

**4.6.5.2 VPN Settings - Set IKE Proposal**



## •VPN Settings - Set IKE Proposal

### **IKE Proposal index**

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

### **Proposal name**

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

### • **DH group**

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

### **Encryption algorithm**

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

### **Authentication algorithm**

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

### **Life time**

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

### **Life time unit**

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

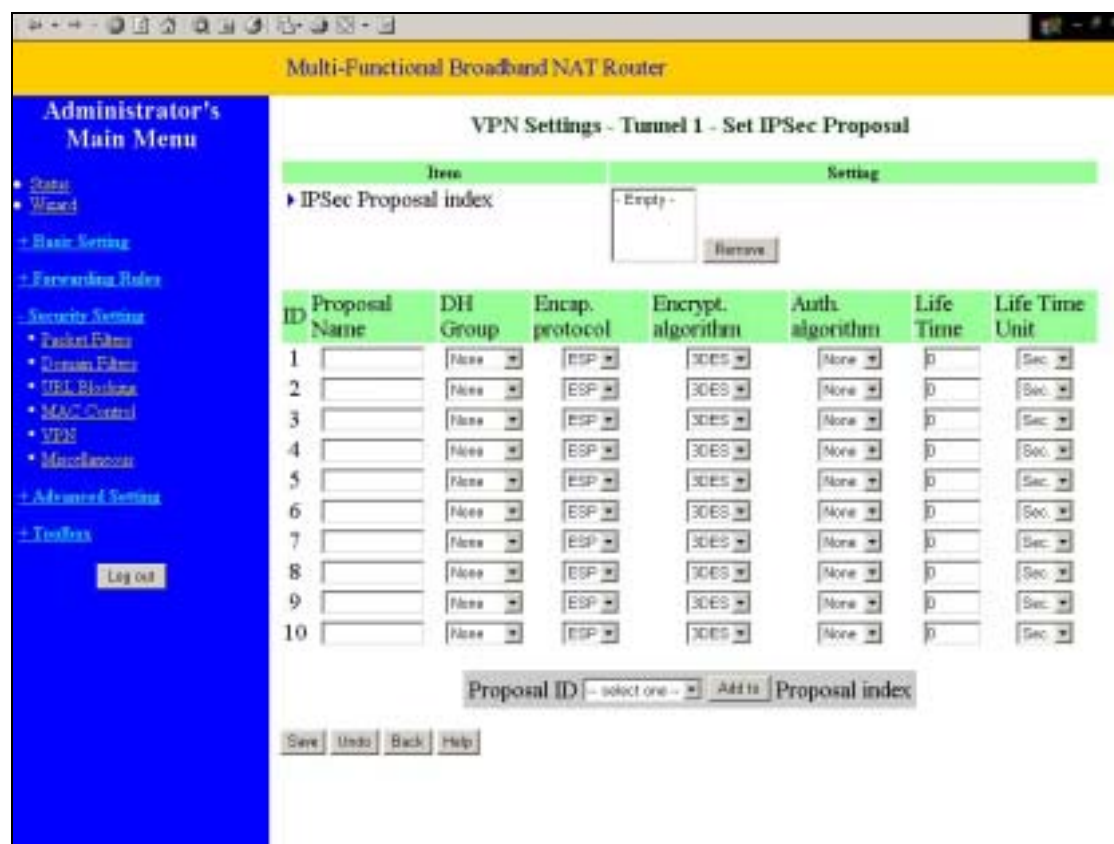
### **Proposal ID**

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

### **Function of Buttons**

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

### 4.6.5.3 VPN Settings -Set IPsec Proposal



### •VPN Settings -Set IPsec Proposal

#### IPsec Proposal index

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

#### Proposal name

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

#### • DH group

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

#### Encapsulation protocol

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

#### Encryption algorithm

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

### **Authentication algorithm**

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

### **Life time**

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

### **Life time unit**

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

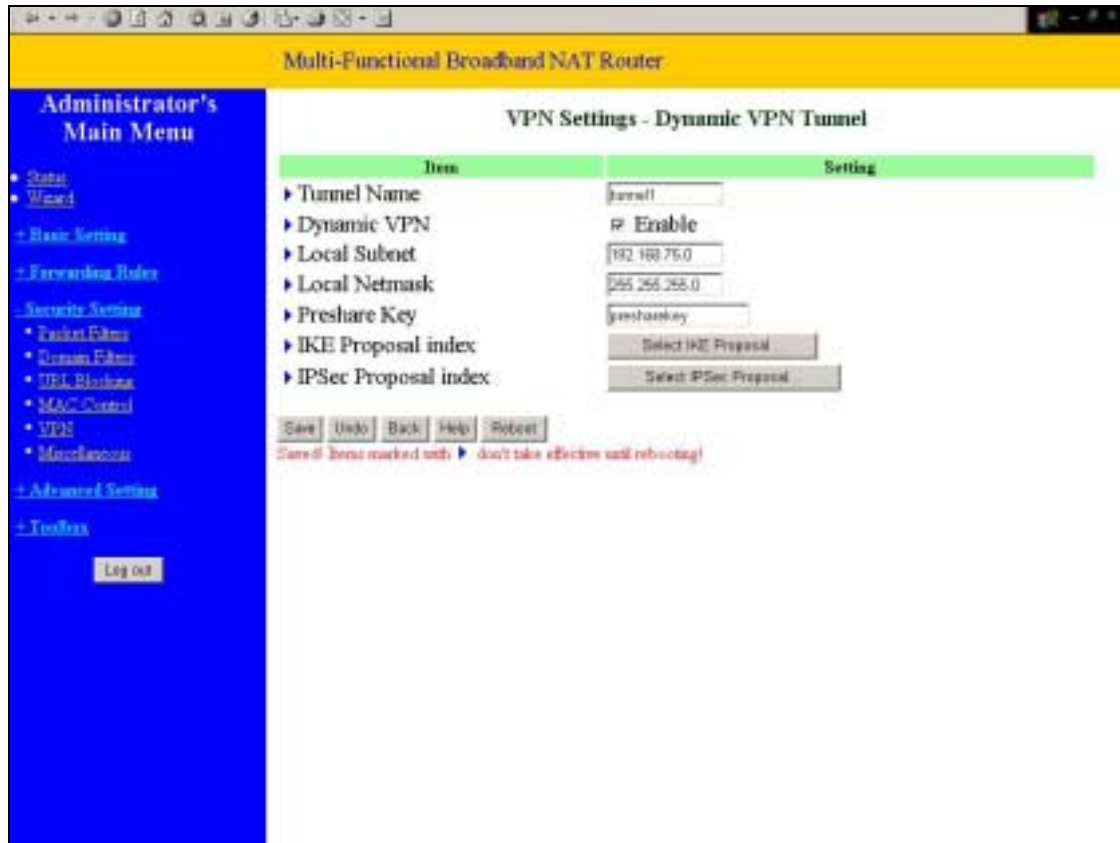
### **Proposal ID**

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

### **Function of Buttons**

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

#### **4.6.5.4 VPN Settings - Dynamic VPN Tunnel**



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.



#### 4.6.5.6 VPN Settings – L2TP Server

Multi-Functional Broadband NAT Router

Administrator's Main Menu

- Status
- Wizard
- Basic Setting
- Extension Rules
- Security Settings
  - Packet Filter
  - Domain Filter
  - URL Blocking
  - MAC Control
  - VPN
  - Miscellaneous
- Advanced Setting
- Tools

Log out

### VPN Settings - L2TP Server

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

ID	Tunnel Name	User Name	Password
1	<input type="text"/>	<input type="text"/>	<input type="text"/>
2	<input type="text"/>	<input type="text"/>	<input type="text"/>
3	<input type="text"/>	<input type="text"/>	<input type="text"/>
4	<input type="text"/>	<input type="text"/>	<input type="text"/>
5	<input type="text"/>	<input type="text"/>	<input type="text"/>

Back Save Undo Help

**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.

#### 4.6.5.7 VPN Settings – PPTP Server

The screenshot shows the configuration interface for a PPTP Server on a Multi-Functional Broadband NAT Router. The interface is divided into a left sidebar and a main content area.

**Administrator's Main Menu (Left Sidebar):**

- Status
- Wizard
- Basic Setting
- Extension Rules
- Security Settings
  - Packet Filter
  - Domain Filter
  - URL Blocking
  - MAC Control
  - VPN
  - Miscellaneous
- Advanced Setting
- Tools
- Log out

**VPN Settings - PPTP Server (Main Content Area):**

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

ID	Tunnel Name	User Name	Password
1	<input type="text"/>	<input type="text"/>	<input type="text"/>
2	<input type="text"/>	<input type="text"/>	<input type="text"/>
3	<input type="text"/>	<input type="text"/>	<input type="text"/>
4	<input type="text"/>	<input type="text"/>	<input type="text"/>
5	<input type="text"/>	<input type="text"/>	<input type="text"/>

Buttons: Back, Save, Undo, Help

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.

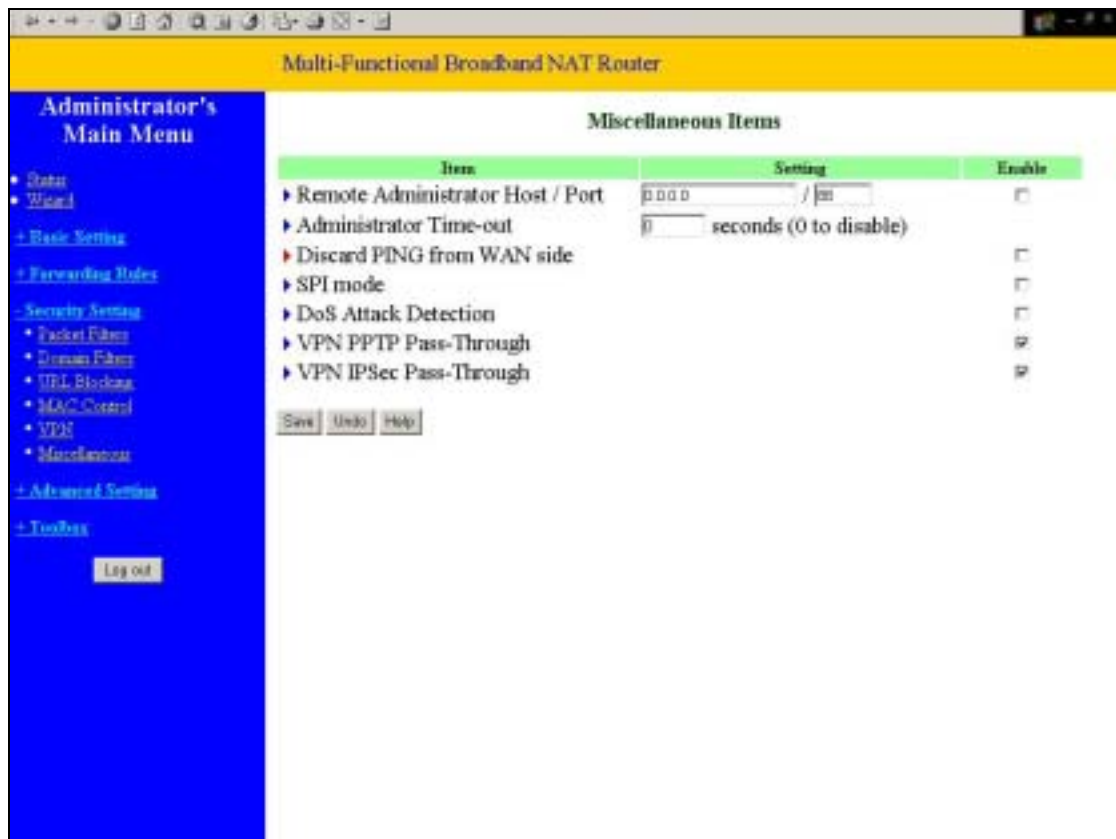
User can build up to five PPTP tunnels for PPTP clients. Each tunnel can accept more than one client. User is required to configure Virtual IP of PPTP Server, Authentication Protocol, PPTP Tunnel Name and User Account, Password.

**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.

## 4.6.5 Miscellaneous Items



### Remote Administrator Host/Port

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

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

### Administrator Time-out

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

### Discard PING from WAN side

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

### SPI Mode

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

**DoS Attack Detection**

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

**VPN PPTP/IPSec Pass-Through**

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