LevelOne

FBR-1411TX

1W,4L High Performance
Broadband Router w/VPN/DMZ port

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

Table of Contents

Chapter 1 Introduction Table of Contents

Congratulations on your purchase of this outstanding LevelOne FBR-1411TX Broadband Router. LevelOne FBR-1411TX is specifically designed for Small Office and Home Office needs. It provides a complete SOHO solution for Internet surfing and office resources sharing, and it is easy to configure and operate for even non-technical users. Instructions for installing and configuring this product can be found in this manual. Before you install and use this product, please read this manual carefully for fully exploiting the functions of this product.

1.1 Functions and Features

- **Broadband Modem and NAT Router**
  This device allows you to connect multiple computers to a broadband (cable or DSL) modem or an Ethernet router to surf the Internet.
- **Auto-sensing Ethernet Switch**
  This device is equipped with a 4-port auto-sensing Ethernet switch.
- **Multiple Connection Approaches to ISP**
  This device supports multiple connection approaches to ISP, for example, static IP address, dynamic IP address, PPPoE connection and PPTP connection…etc.
- **Firewall**
  All unwanted packets from outside intruders are blocked to protect your Intranet.
- **DHCP server supported**
  All of the networked computers can retrieve TCP/IP settings automatically from this product.
- **Web-based configuring**
  Device can be configured through any networked computer's web browser by using Netscape or Internet Explorer.
- **Packet filter supported**
  Packet Filter allows you to control access to a network by analyzing the incoming and outgoing TCP/UDP packets and letting them pass or halting them based on the IP address or port 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**
  This device 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**

  Domain Filter prevents users under this device from accessing specific domains.

- **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. Besides, dynamic routing information protocol RIP v1/2 is also supported.

- **VPN Supported (initiator-responder and pass-through)**

  This device supports IPSec initiator and responder. It can initiate a tunnel with a remote VPN gateway or host; it also can accept a tunnel creation request from a remote VPN gateway or host. The device can also be configured to pass all VPN packets this device through LAN and WAN interfaces.

- **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.

- **DDNS supported**

  This device supports dynamic domain name service (DDNS) to host your server on a changing IP address. So that anyone wishing to reach your host only needs to know the name of it.

- **Firmware Upgrade, Configuration Backup and Alert by Email supported**

  This device supports firmware upgrade to upgrade the system firmware with new one. It also supports configuration backup and restore, so that user can save various system configuration profiles and restore it when he needs. Besides, some urgent message that needs manager to know can be delivered by email approach.

- **Hardware DMZ - Demilitarized Zone supported**

  This feature allow user to configure 10 Global IP for DMZ Hosts while other Hosts on LAN can still share WAN IP. With this feature, user can enjoy both benefits of the conveniences from DMZ Zone and the Security from other Filter settings. This feature also separates DMZ Hosts from LAN Network; so LAN network is much safer than ever.

1.2 Packing List

- Broadband router unit
- Manual CD
- Power adapter

Chapter 2 Hardware Installation [Table of Contents]

2.1 Panel Layout

2.1.1. Front Panel

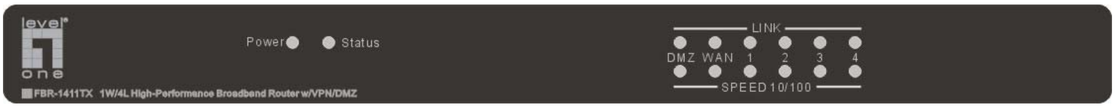

level one
Power
Status
LINK
DMZ
WAN
1
2
3
4
SPEED 10/100
FBR-1411TX 1W/4L High-Performance Broadband Router w/VPN/DMZ

Figure 2-1 FBR-1411TX Front Panels.

LED:

LED	Function	Color	Status	Description
Status	System status indicators	Orange	Blinking	Status is flashed once per second to indicate system is alive.
DMZ	DMZ port activity	Green	On	The WAN port is linked.
			Blinking	The WAN port is sending or receiving data.
WAN	WAN port activity	Green	On	The WAN port is linked.
			Blinking	The WAN port is sending or receiving data.
Link/Act. 1~4	Link status	Green	On	An active station is connected to the corresponding LAN port.
			Blinking	The corresponding LAN port is sending or receiving data.
SPEED 10/100	10Mbps/ 100Mbps	Green	On	On indicates 100Mbps speed.

Port:

RESET	Press RESET button for about 7 seconds to reset system settings to factory defaults.

2.1.2. Rear Panel

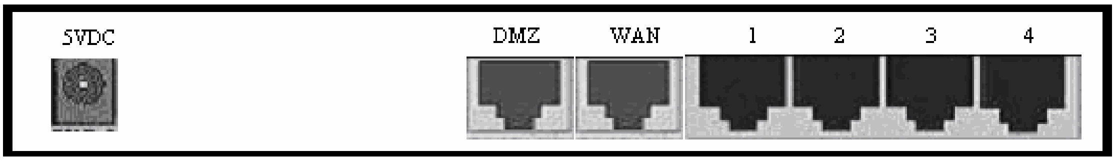


Figure 2-2 Rear Panel.

Ports:

Port	Description
5VDC	Power inlet: DC 5V, 1.5A (minimum)
DMZ	The port where you will connect networked servers and other devices.
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.

2.2 Installation Requirements

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

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

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

2.3 Procedure for Hardware Installation

1. **Setup LAN connection:** Connect an Ethernet cable from your computer's Ethernet port to one of the LAN ports of this product.
2. **Setup WAN connection:** Prepare an Ethernet cable for connecting this product to your cable/xDSL modem or Ethernet backbone.
3. **Power on:** Connecting the power cord to power inlet, this product will automatically enter the

self-test phase. When it is in the self-test phase, the indicator M1 will be lighted OFF for about 15 seconds. Finally, the M1 will be continuously flashed once per second to indicate that this product is in normal operation.

Chapter 3 Network Settings Table of Contents

To use LevelOne FBR-1411TX correctly, you have to properly configure the network settings of your computers.

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?*

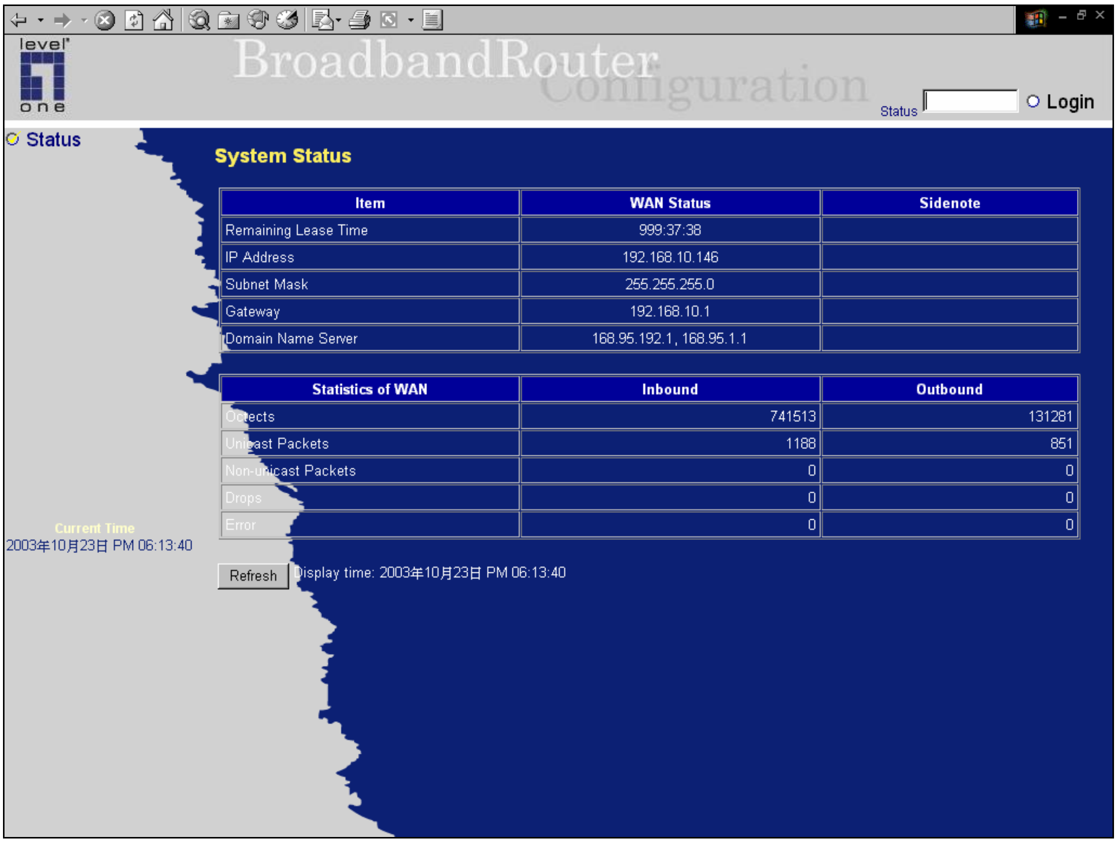
   Tip: If the IP address of this product is 192.168.123.254, the IP address of your computer must be 192.168.123.X and default gateway must be 192.168.123.254.

Chapter 4 Configuring NAT Router Table of Contents

LevelOne FBR-1411TX provides Web based configuration scheme. That is, to configure the router device 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.

There are seven sections to describe the configuring NAT router. They are Login, Status, Wizard, Basic Setting, Forwarding Rules, Security Setting, Advanced Setting, and Toolbox, respectively.

4.1 Start-up and Log in Chapter Home



System Status

Item	WAN Status	Sidenote
Remaining Lease Time	999:37:38	
IP Address	192.168.10.146	
Subnet Mask	255.255.255.0	
Gateway	192.168.10.1	
Domain Name Server	168.95.192.1, 168.95.1.1	

Statistics of WAN	Inbound	Outbound
Octects	741513	131281
Unicast Packets	1188	851
Non-unicast Packets	0	0
Drops	0	0
Error	0	0

Current Time
2003年10月23日 PM 06:13:40

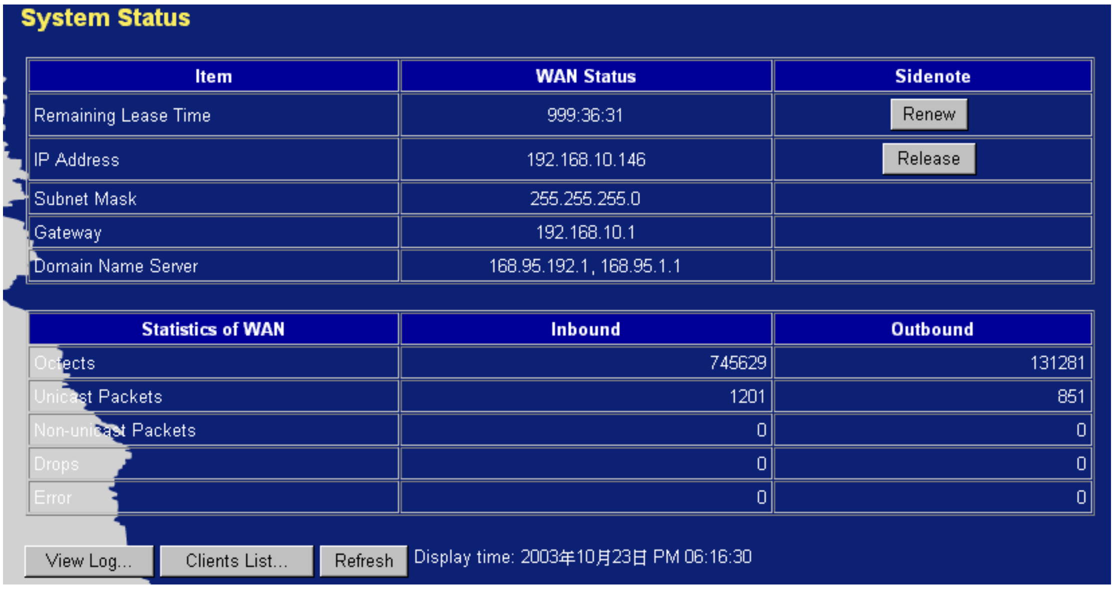
Display time: 2003年10月23日 PM 06:13:40

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 Chapter Home



System Status

Item	WAN Status	Sidenote
Remaining Lease Time	999:36:31	Renew
IP Address	192.168.10.146	Release
Subnet Mask	255.255.255.0	
Gateway	192.168.10.1	
Domain Name Server	168.95.192.1 , 168.95.1.1	

Statistics of WAN	Inbound	Outbound
Octects	745629	131281
Unicast Packets	1201	851
Non-unicast Packets	0	0
Drops	0	0
Error	0	0

Display time: 2003年10月23日 PM 06:16:30

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

A. WAN Port Status.

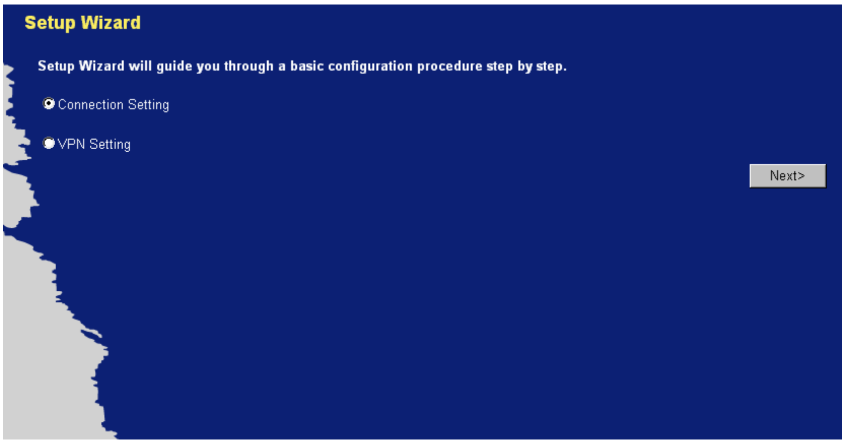
If the WAN port is not assigned a static IP, there may appear a “**Renew**” or “**Release**” button on the *Side note* column. You can click this button to renew or release IP manually.

B. Statistics of WAN.

If the WAN port of router device is connected to the Internet, the statistics of all packets passed the WAN interface will be shown on the Statistics of WAN, including the total counts of delivered data in bytes, unicast packets, non-unicast packets, dropped packets and error packets for inbound and outbound of WAN port.

4.3 Wizard Chapter Home

4.3.1 Setup Wizard – Select WAN Type



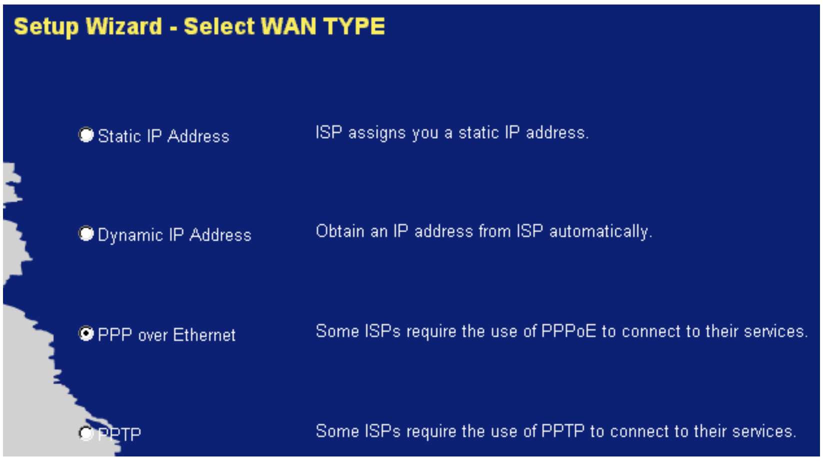
Setup Wizard

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

● Connection Setting

○ VPN Setting

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



Setup Wizard - Select WAN TYPE

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

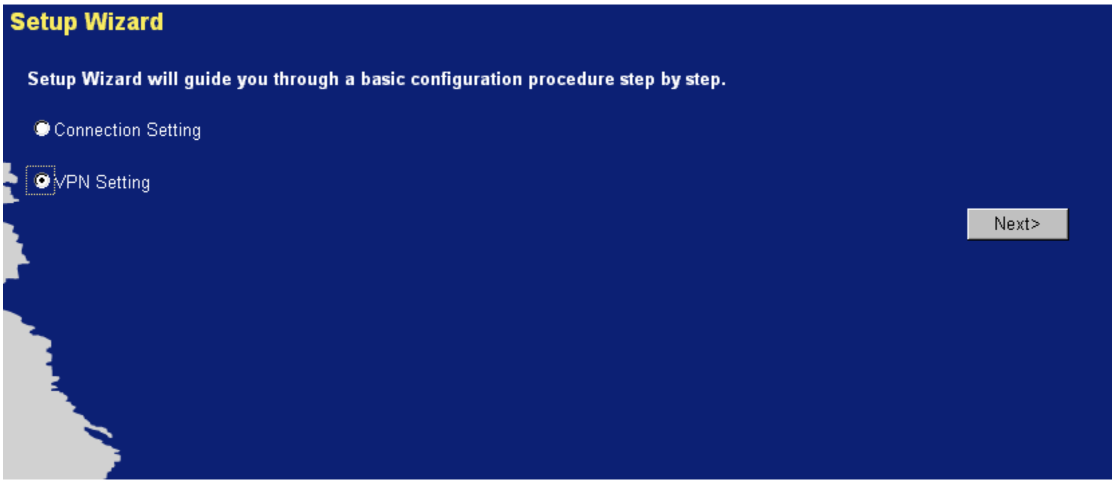
○ Dynamic IP Address Obtain an IP address from ISP automatically.

● 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.

Setup Wizard - Select WAN Type: For detail settings, please refer to Section 4.4 primary setup.

4.3.2 Setup Wizard – VPN Setting



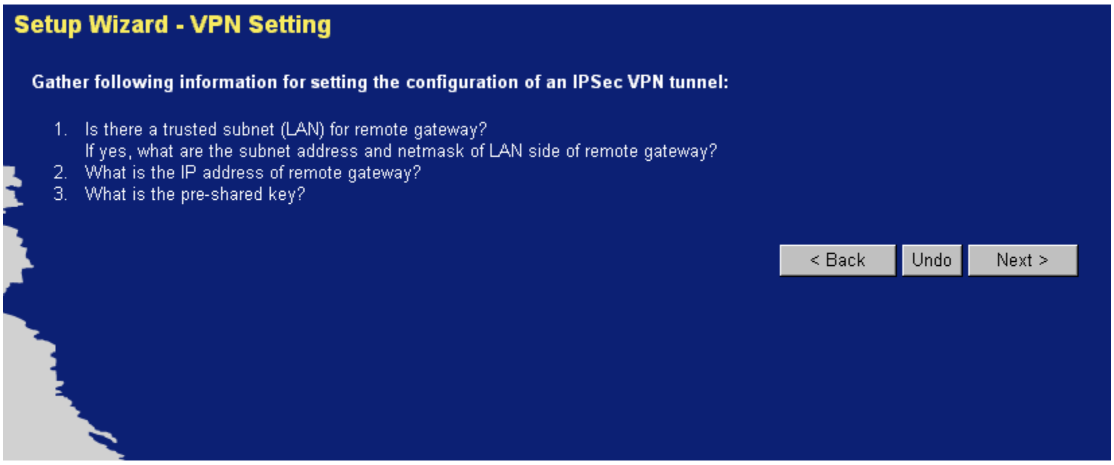
Setup Wizard

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

○ Connection Setting

● VPN Setting

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


Setup Wizard - VPN Setting

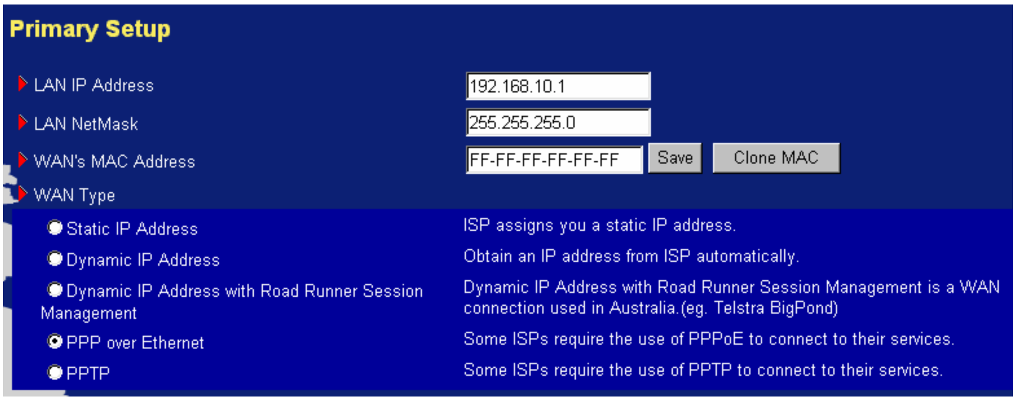
Gather following information for setting the configuration of an IPSec VPN tunnel:

1. Is there a trusted subnet (LAN) for remote gateway?
   If yes, what are the subnet address and netmask of LAN side of remote gateway?
2. What is the IP address of remote gateway?
3. What is the pre-shared key?

Setup Wizard – VPN Setting: For detail settings, please refer to Section 4.15 VPN-IPSEC.

4.4 Basic Setting Chapter Home

4.4.1 Primary Setup – LAN's IP, WAN's MAC Address, WAN Type, Virtual Computers


Primary Setup

LAN IP Address: 192.168.10.1

LAN NetMask: 255.255.255.0

WAN's MAC Address: FF-FF-FF-FF-FF-FF

WAN Type

○ 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	Dynamic IP Address with Road Runner Session Management is a WAN connection used in Australia.(eg. 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 configuration enables 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***: It is 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's MAC Address***: It is the MAC address of WAN interface of this device and can be set by user manually. Usually, the device is attached with one unique MAC address when it leaves the factory.

3. **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.

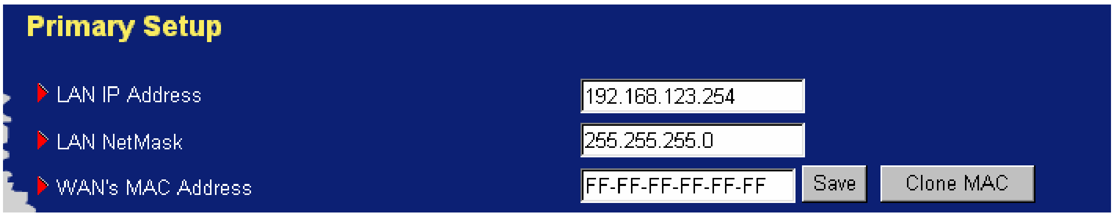
   B. Dynamic IP Address: Obtain an IP address from ISP automatically.

   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 LAN's IP Address



Primary Setup

LAN IP Address: 192.168.123.254

LAN NetMask: 255.255.255.0

WAN's MAC Address: FF-FF-FF-FF-FF-FF

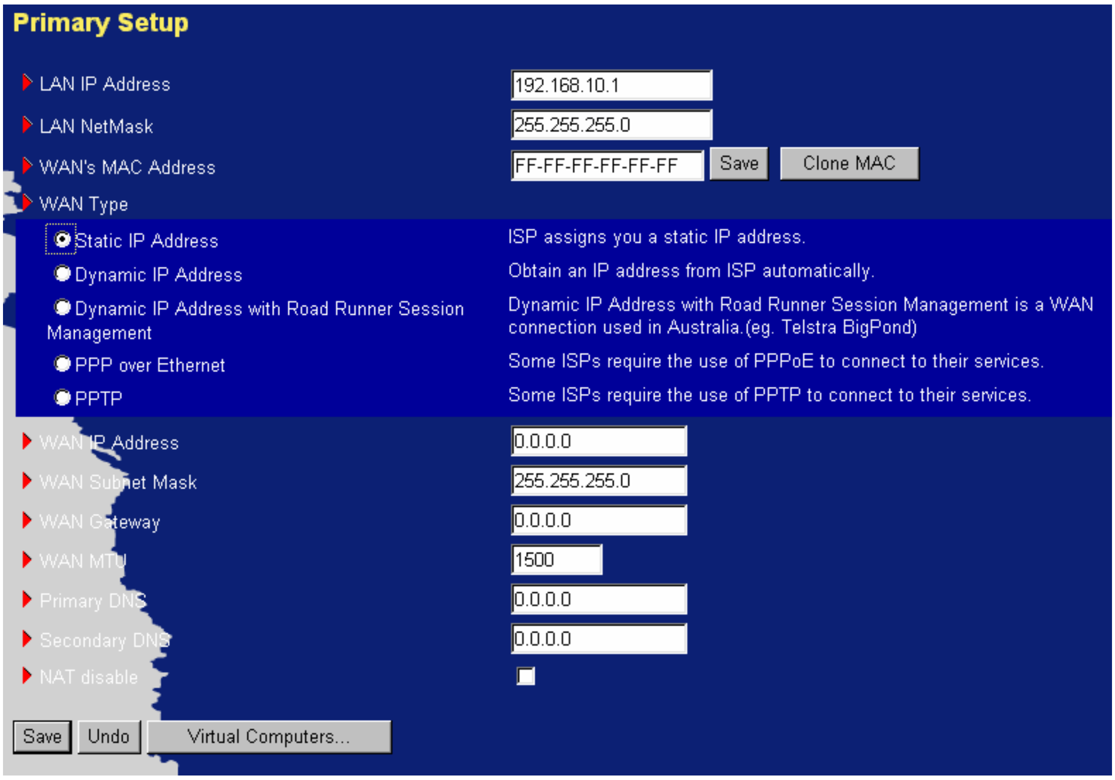
Set the local IP address of this device if necessary, the default *IP address* of this product is 192.168.123.254.

4.4.1.2 WAN's MAC Address

Set the MAC address of WAN interface of this device if necessary, the factory one is default and unique. Certainly, user can set it by himself. Besides, user also can clone the MAC address of LAN host that is browsing the web page for the one of WAN interface of router device by clicking on the Clone MAC button.

4.4.1.3 WAN Type

4.4.1.3.1 Static IP Address



Primary Setup

LAN IP Address: 192.168.10.1

LAN NetMask: 255.255.255.0

WAN's MAC Address: FF-FF-FF-FF-FF-FF

WAN Type

● 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 — Dynamic IP Address with Road Runner Session Management is a WAN connection used in Australia.(eg. 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.

WAN IP Address: 0.0.0.0

WAN Subnet Mask: 255.255.255.0

WAN Gateway: 0.0.0.0

WAN MTU: 1500

Primary DNS: 0.0.0.0

Secondary DNS: 0.0.0.0

NAT disable: □

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

2. ***WAN MTU*****:** User can set the MTU value of the connection to ISP. The default value for static WAN type is 1500.

4.4.1.3.2 Dynamic IP Address

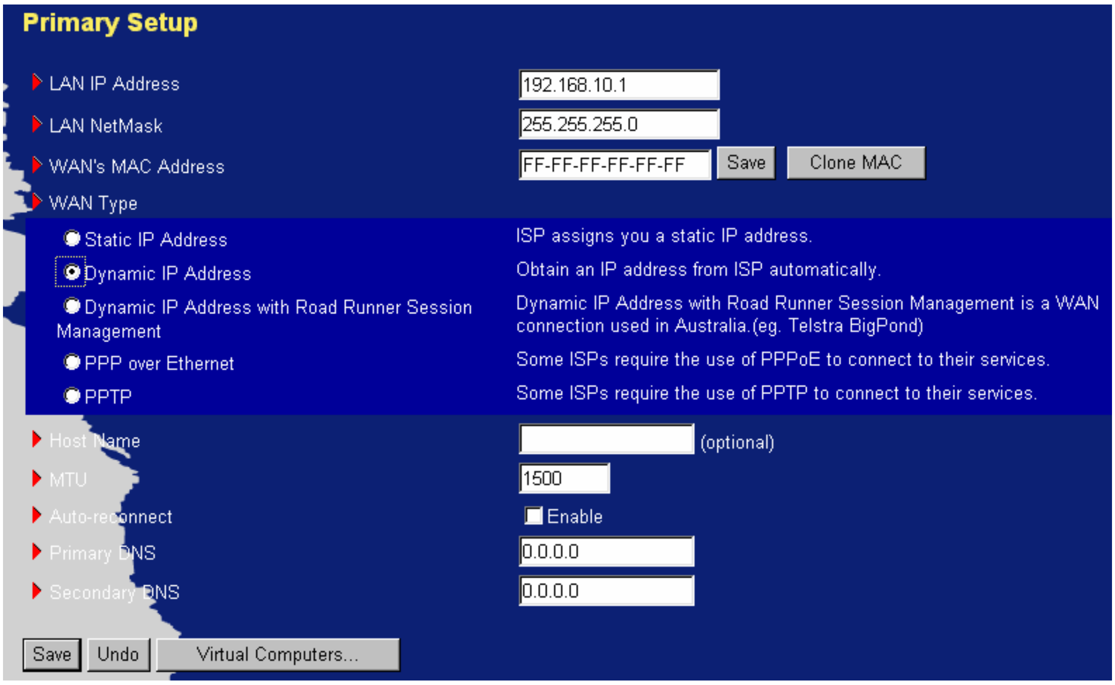
1. ***Host Name*****:** Optional and required by some ISPs.

2. ***MTU*****:** User can set the MTU value of the connection to ISP. The default value for dynamic WAN

type is 1500.

3. ***Auto-reconnect*****:** Keep alive of the connection to ISP.

4. ***Primary*** **and** ***Secondary DNS*****:** Enter the proper setting provided by your ISP.



Primary Setup

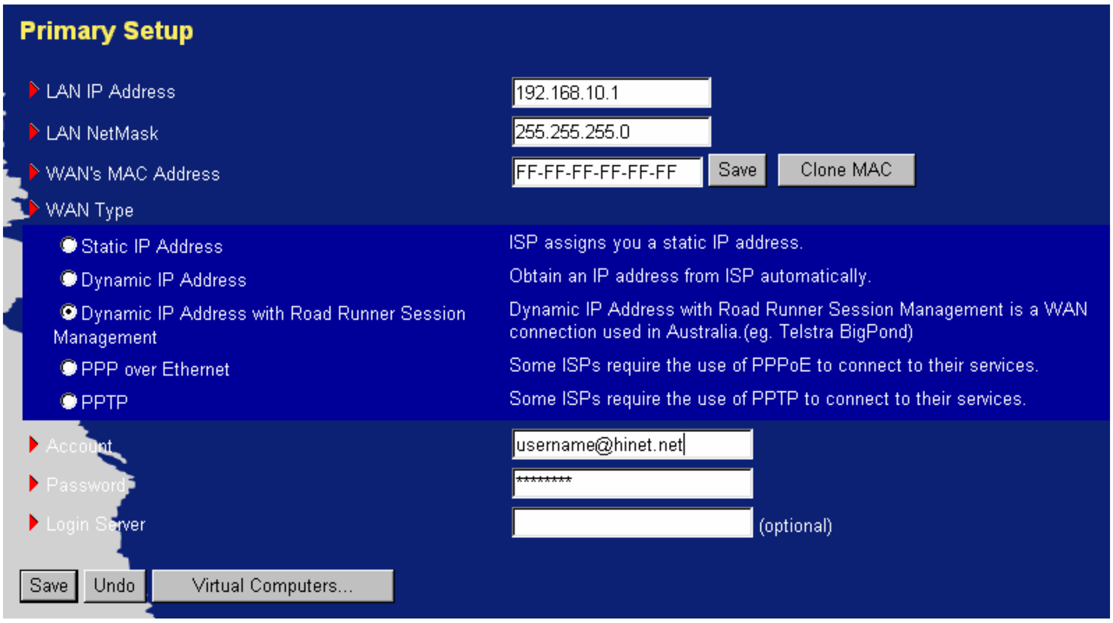
- LAN IP Address: 192.168.10.1
- LAN NetMask: 255.255.255.0
- WAN's MAC Address: FF-FF-FF-FF-FF-FF [Save] [Clone MAC]
- WAN Type
  - ○ Static IP Address — ISP assigns you a static IP address.
  - ● Dynamic IP Address — Obtain an IP address from ISP automatically.
  - ○ Dynamic IP Address with Road Runner Session Management — Dynamic IP Address with Road Runner Session Management is a WAN connection used in Australia.(eg. 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.
- Host Name: (optional)
- MTU: 1500
- Auto-reconnect: □ Enable
- Primary DNS: 0.0.0.0
- Secondary DNS: 0.0.0.0

4.4.1.3.3 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!

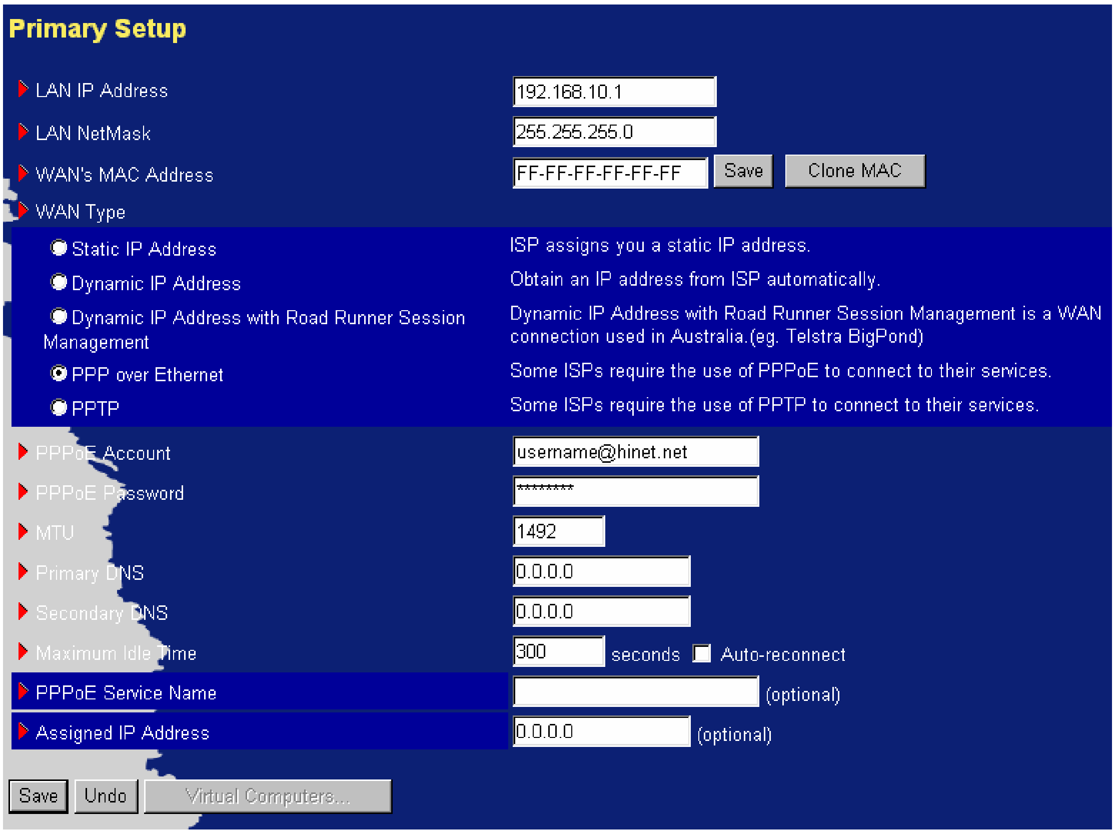
3. Login Server: optional. Required by some ISPs, e.g. @Home.



Primary Setup

- LAN IP Address: 192.168.10.1
- LAN NetMask: 255.255.255.0
- WAN's MAC Address: FF-FF-FF-FF-FF-FF [Save] [Clone MAC]
- WAN Type
  - ○ 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 — Dynamic IP Address with Road Runner Session Management is a WAN connection used in Australia.(eg. 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.
- Account: username@hinet.net
- Password: ********
- Login Server: (optional)

4.4.1.3.4 PPP over Ethernet

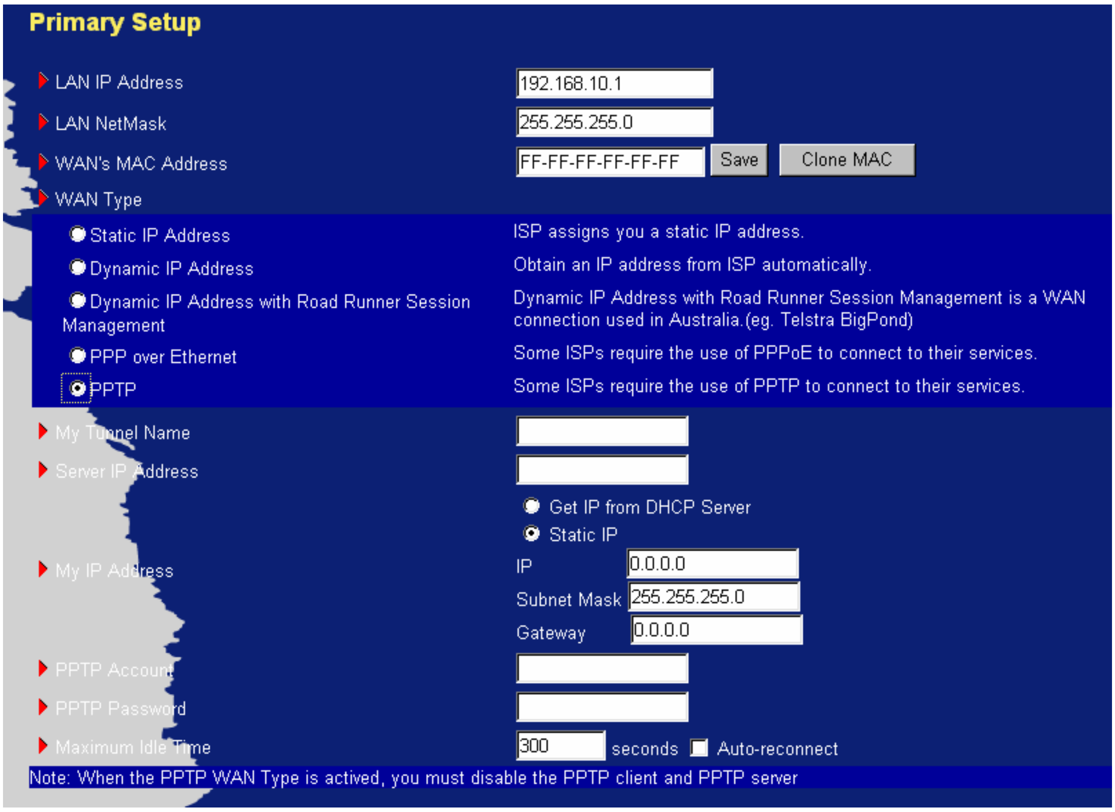


Primary Setup

LAN IP Address	192.168.10.1
LAN NetMask	255.255.255.0
WAN's MAC Address	FF-FF-FF-FF-FF-FF Save Clone MAC
WAN Type	
○ 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	Dynamic IP Address with Road Runner Session Management is a WAN connection used in Australia.(eg. 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.
PPPoE Account	username@hinet.net
PPPoE Password	********
MTU	1492
Primary DNS	0.0.0.0
Secondary DNS	0.0.0.0
Maximum Idle Time	300 seconds □ Auto-reconnect
PPPoE Service Name	(optional)
Assigned IP Address	0.0.0.0 (optional)

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.
5. Service name: optional. Required by some ISPs, e.g. @Home.

4.4.1.3.5 PPTP



Primary Setup

LAN IP Address: 192.168.10.1

LAN NetMask: 255.255.255.0

WAN's MAC Address: FF-FF-FF-FF-FF-FF

WAN Type

○ 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 — Dynamic IP Address with Road Runner Session Management is a WAN connection used in Australia.(eg. 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.

My Tunnel Name:

Server IP Address:

My IP Address: ○ Get IP from DHCP Server ● Static IP

IP: 0.0.0.0

Subnet Mask: 255.255.255.0

Gateway: 0.0.0.0

PPTP Account:

PPTP Password:

Maximum Idle Time: 300 seconds □ Auto-reconnect

Note: When the PPTP WAN Type is actived, you must disable the PPTP client and PPTP server

There are two kinds of types in this connection.

One is that gets ip from isp (DHCP server),the other is that setup the ip manually.

1. My tunnel name: (optional).ex: router

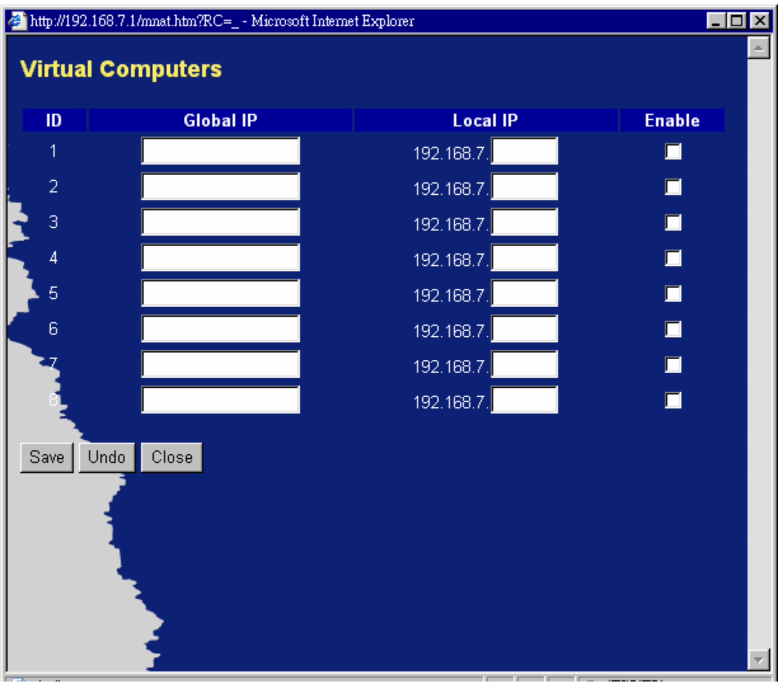
2. Server IP Address: the IP address of the PPTP server.

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

4. 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.

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.

4.4.1.4 Virtual Computers


http://192.168.7.1/mnat.htm?RC=_ - Microsoft Internet Explorer

Virtual Computers

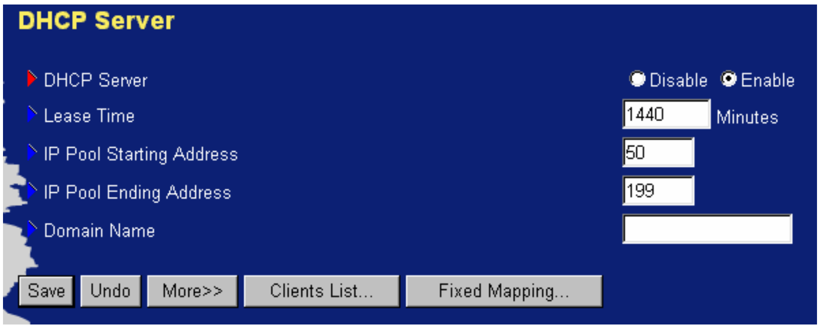
ID	Global IP	Local IP	Enable
1		192.168.7.	☐
2		192.168.7.	☐
3		192.168.7.	☐
4		192.168.7.	☐
5		192.168.7.	☐
6		192.168.7.	☐
7		192.168.7.	☐
8		192.168.7.	☐

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. The function can be activated only when the WAN type is static and dynamic.

- ***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 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:


DHCP Server

DHCP Server ○ Disable ● Enable

Lease Time 1440 Minutes

IP Pool Starting Address 50

IP Pool Ending Address 199

Domain Name

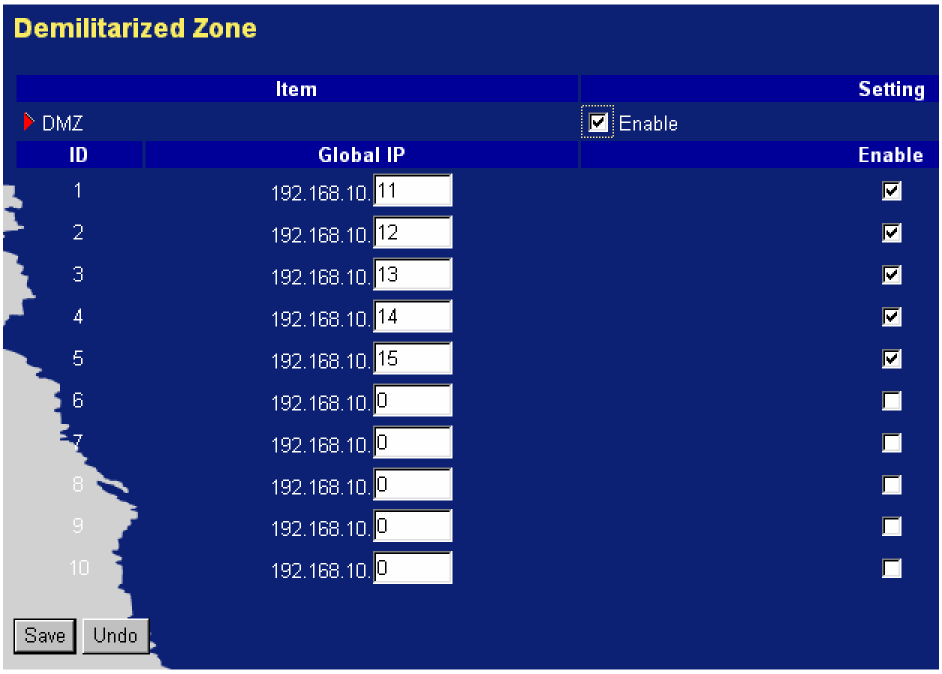
1. ***DHCP Server***: Choose "*Disable*" or "*Enable.*"
2. ***Lease Time:*** this feature allows you to configure IP's lease time (DHCP client).
3. ***IP pool starting Address/ IP pool ending Address***: Whenever there is a request, the DHCP

server will automatically allocate an unused IP address from the *IP address pool* to the requesting computer. You must specify the starting and ending address of the IP address pool.

4. ***Domain Name***: Optional, this information will be passed to the client.
5. ***Primary DNS/Secondary DNS***: This feature allows you to assign DNS Servers for configuring all the computers and devices in your network.
6. ***Primary WINS/Secondary WINS***: This feature allows you to assign WINS Servers for configuring all the computers and devices in your network.

4.4.3 Hardware DMZ - Demilitarized Zone

This Demilitarized Zone page will show only when Hardware DMZ port is supported.



Demilitarized Zone

Item	Setting
DMZ	☑ Enable

ID	Global IP	Enable
1	192.168.10.11	☑
2	192.168.10.12	☑
3	192.168.10.13	☑
4	192.168.10.14	☑
5	192.168.10.15	☑
6	192.168.10.0	□
7	192.168.10.0	□
8	192.168.10.0	□
9	192.168.10.0	□
10	192.168.10.0	□

Hardware DMZ - Demilitarized Zone – This feature allow user to configure 10 Global IP for DMZ Hosts while other Hosts on LAN can still share the WAN IP. With this feature, user can enjoy both benefits of the conveniences from DMZ Zone and the Security from other Filter settings. This feature also separates DMZ Hosts from LAN Network; so LAN network is much more save than ever.

To enable **Hardware DMZ - Demilitarized Zone** click the check box next to **Enable** in the **DMZ** field.

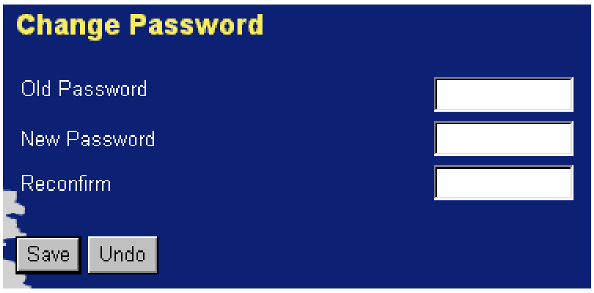
Global IP: Global IP and WAN IP should be in the same subnet.

Example shown as above figure.

In this Example, WAN IP is192.168.10.10

DMZ Hosts are192.168.10.11~192.168.10.15

4.4.4 Change Administrator's Password



Change Password

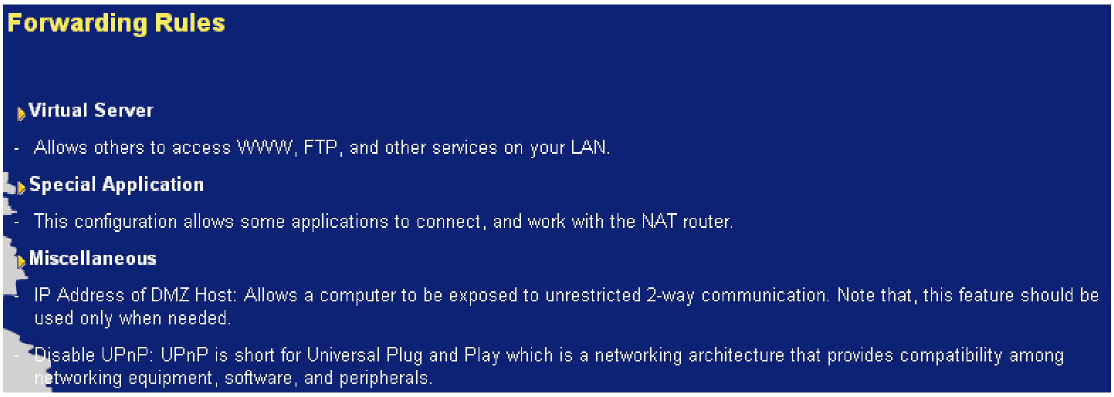
Old Password

New Password

Reconfirm

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

4.5 Forwarding Rules Chapter Home



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

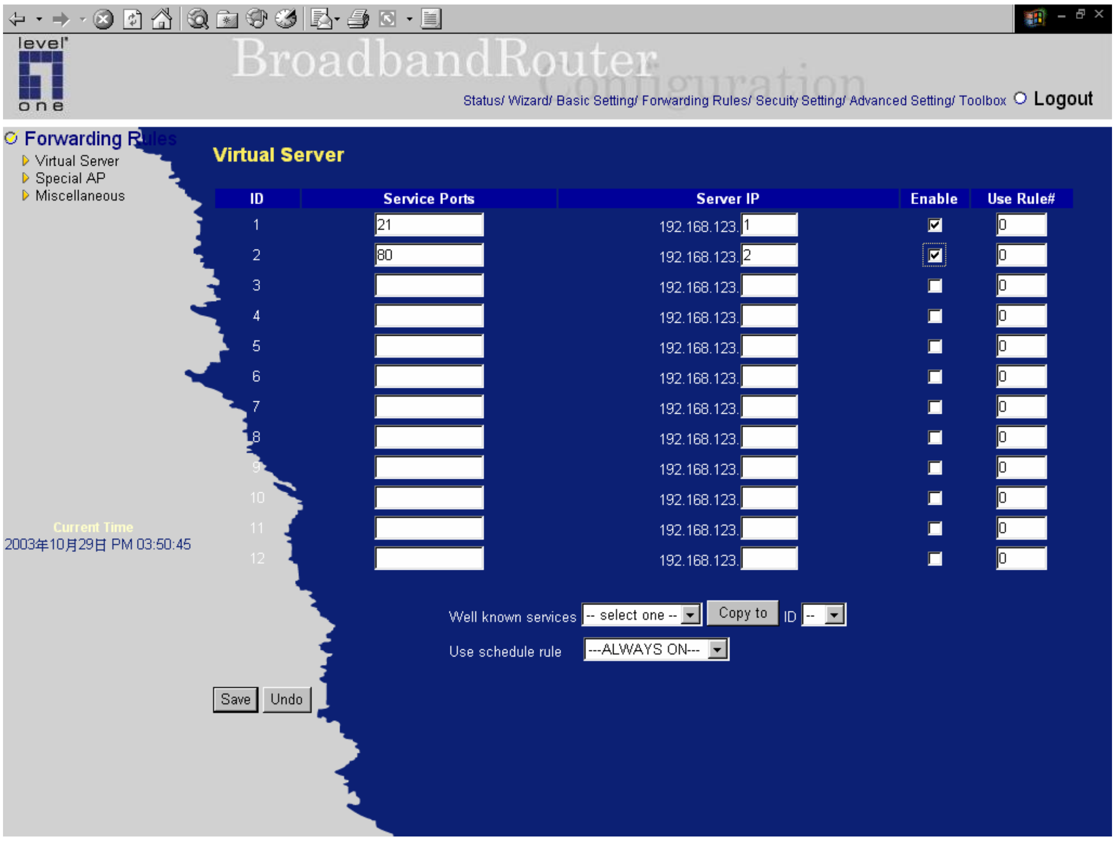
- IP Address of DMZ Host: Allows a computer to be exposed to unrestricted 2-way communication. Note that, this feature should be used only when needed.
- Disable UPnP: UPnP is short for Universal Plug and Play which is a networking architecture that provides compatibility among networking equipment, software, and peripherals.

4.5.1 Virtual Server

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

A virtual server is defined as a ***Service Port****,* and all requests to this port will be redirected to the computer specified by the ***Server IP***.

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


level one
BroadbandRouter Configuration
Status/ Wizard/ Basic Setting/ Forwarding Rules/ Secuity Setting/ Advanced Setting/ Toolbox
Logout
Forwarding Rules
Virtual Server
Special AP
Miscellaneous
Current Time
2003年10月29日 PM 03:50:45

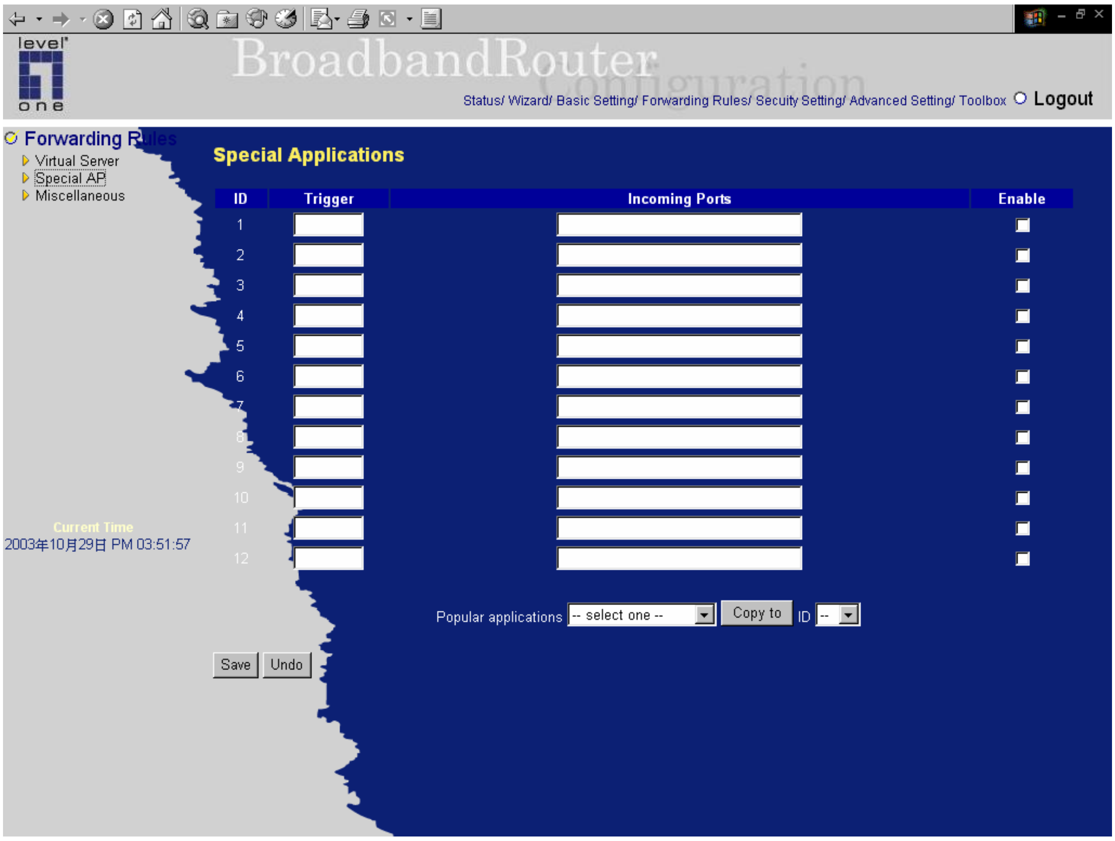
Virtual Server

ID	Service Ports	Server IP	Enable	Use Rule#
1	21	192.168.123.1	☑	0
2	80	192.168.123.2	☑	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

Well known services -- select one -- Copy to ID --

Use schedule rule ---ALWAYS ON---

4.5.2 Special AP


level one
BroadbandRouter Configuration
Status/ Wizard/ Basic Setting/ Forwarding Rules/ Secuity Setting/ Advanced Setting/ Toolbox
Logout
Forwarding Rules
Virtual Server
Special AP
Miscellaneous
Current Time
2003年10月29日 PM 03:51:57

Special Applications

ID	Trigger	Incoming Ports	Enable
1			☐
2			☐
3			☐
4			☐
5			☐
6			☐
7			☐
8			☐
9			☐
10			☐
11			☐
12			☐

Popular applications -- select one -- Copy to ID --

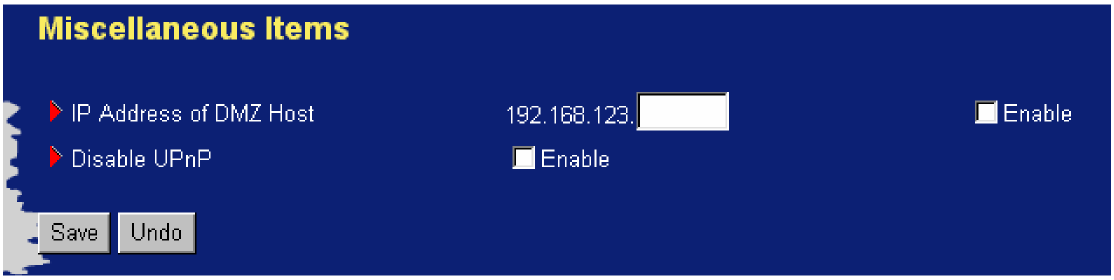
Some applications require multiple connections, like Internet games, Video conferencing, Internet telephony, etc. Because of the firewall function, these applications cannot work with a pure NAT router. The **Special Applications** feature allows some of these applications to work with this product.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

IP Address of DMZ Host 192.168.123.[ ] □ Enable

Disable UPnP □ Enable

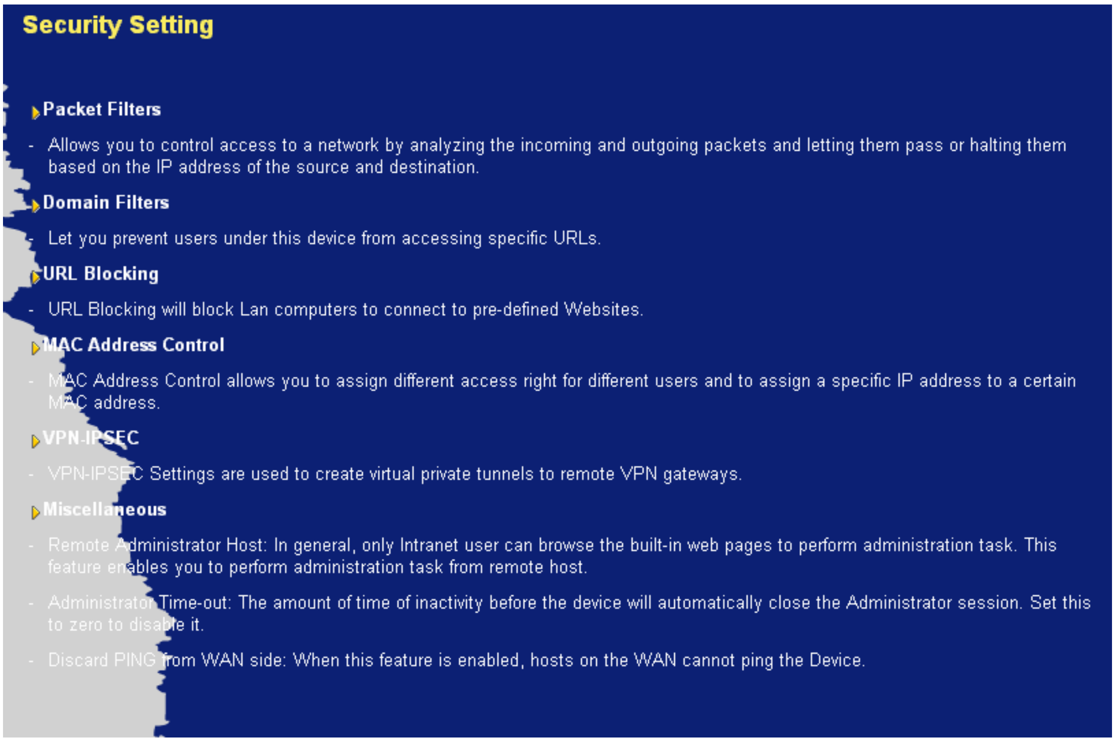
IP Address of DMZ Host

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.

This function is to simulate a hardware DMZ port and can be viewed as the software DMZ. But it only supports one DMZ host but hardware DMZ can supports multiple DMZ hosts.

NOTE: This feature should be used only when needed.

4.6 Security Settings Chapter Home



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 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.

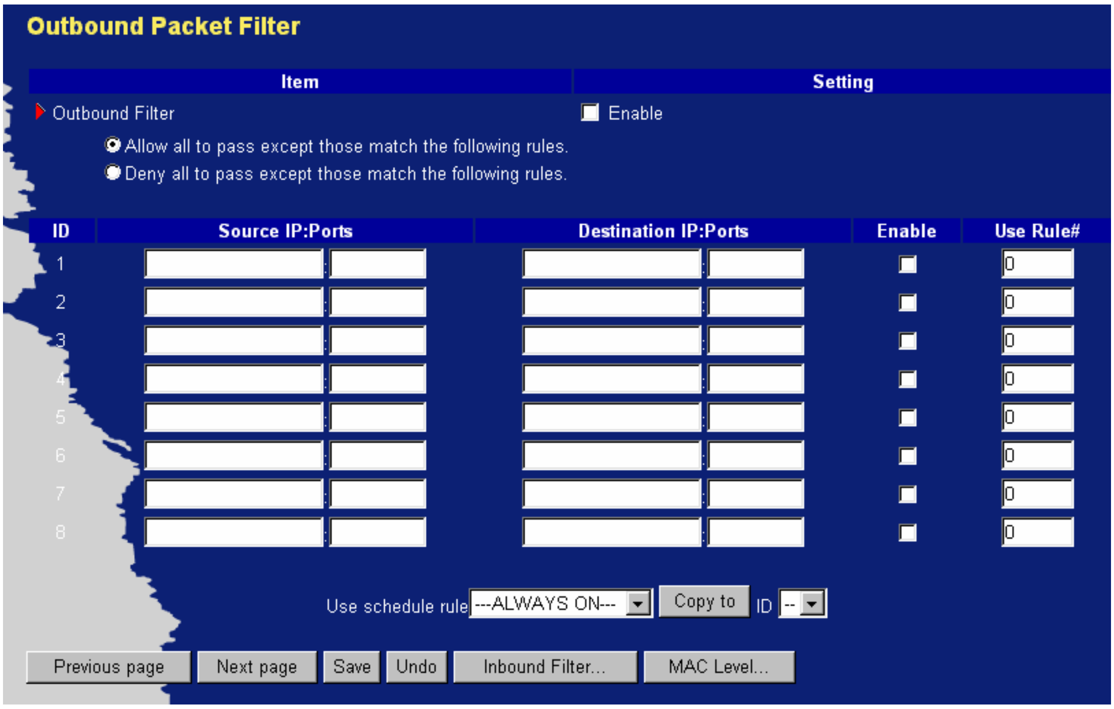
VPN-IPSEC

- VPN-IPSEC 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

Use schedule rule ---ALWAYS ON--- Copy to ID --

Previous page | Next page | Save | Undo | Inbound Filter... | MAC Level...

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

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

For source or destination IP address, you can define a single IP address (4.3.2.1) or a range of IP addresses (4.3.2.1/24). 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, or U2000-2999. No prefix indicates both TCP and UDP are defined. An empty implies all port addresses.

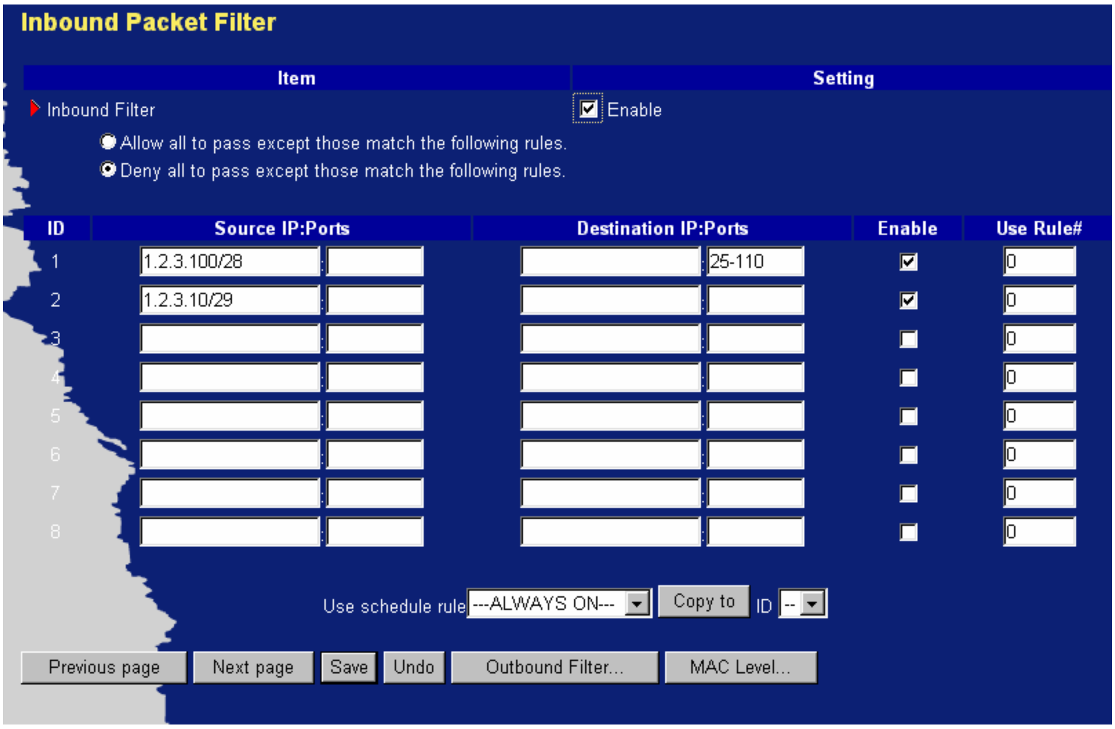
Each rule can be enabled or disabled individually.

Inbound Filter:

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

Example 1:

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.



Inbound Packet Filter

Item	Setting
Inbound Filter	☑ Enable

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

ID	Source IP:Ports		Destination IP:Ports		Enable	Use Rule#
1	1.2.3.100/28			25-110	☑	0
2	1.2.3.10/29				☑	0
3					□	0
4					□	0
5					□	0
6					□	0
7					□	0
8					□	0

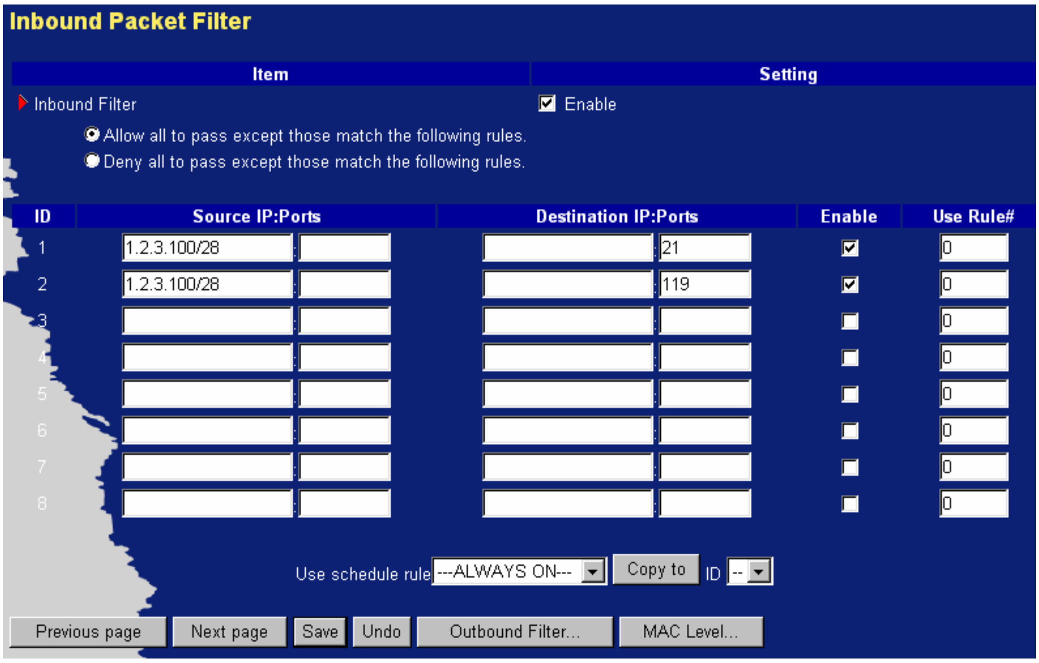
Use schedule rule ---ALWAYS ON--- Copy to ID --

(1.2.3.100/28): It stands for a subnet of IP address ranging from 1.2.3.96 to 1.2.3.111 and 1.2.3.100 is an element in the range set. The value of 28 stands for the netmask of subnet and 4 (=32-28) least significant bits in the last byte of IP address are unmask bits. Hosts within the subnet are allowed to send mail (port 25), receive mail (port 110), and browse the Internet (port 80).

(1.2.3.10/29): It stands for a subnet of IP address ranging from 1.2.3.8 to 1.2.3.15 and 1.2.3.10 is an element in the range set. The value of 29 stands for the netmask of subnet and 3 (=32-29) least significant bits in the last byte of IP address are unmask bits. Hosts within the subnet can do everything (block nothing).

And others are all blocked.

Example **2:**



Inbound Packet Filter

Item	Setting
Inbound Filter	☑ Enable

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

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

ID	Source IP:Ports		Destination IP:Ports		Enable	Use Rule#
1	1.2.3.100/28			21	☑	0
2	1.2.3.100/28			119	☑	0
3					☐	0
4					☐	0
5					☐	0
6					☐	0
7					☐	0
8					☐	0

Use schedule rule ---ALWAYS ON--- ID --

(1.2.3.100/28): It stands for a subnet of IP address ranging from 1.2.3.96 to 1.2.3.111 and they can do everything except read net news (port 119) and transfer files via FTP (port 21).

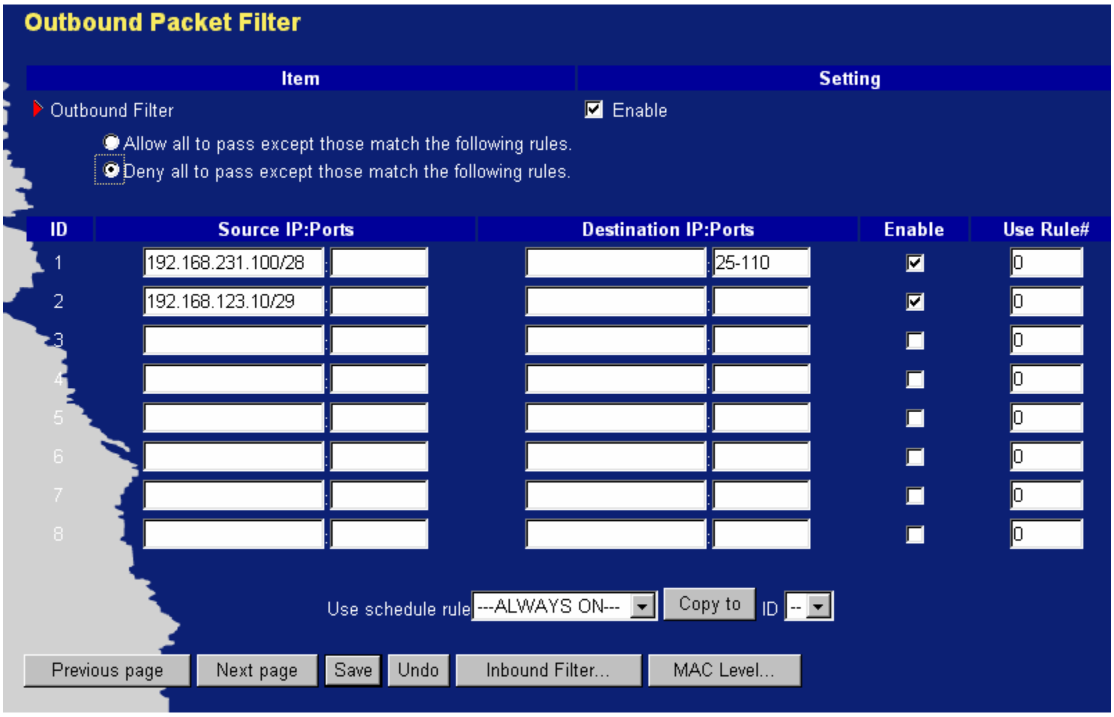
Others are all allowed.

After **Inbound Packet Filter** setting is configured, click on 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	192.168.231.100/28			25-110	☑	0
2	192.168.123.10/29				☑	0
3					□	0
4					□	0
5					□	0
6					□	0
7					□	0
8					□	0

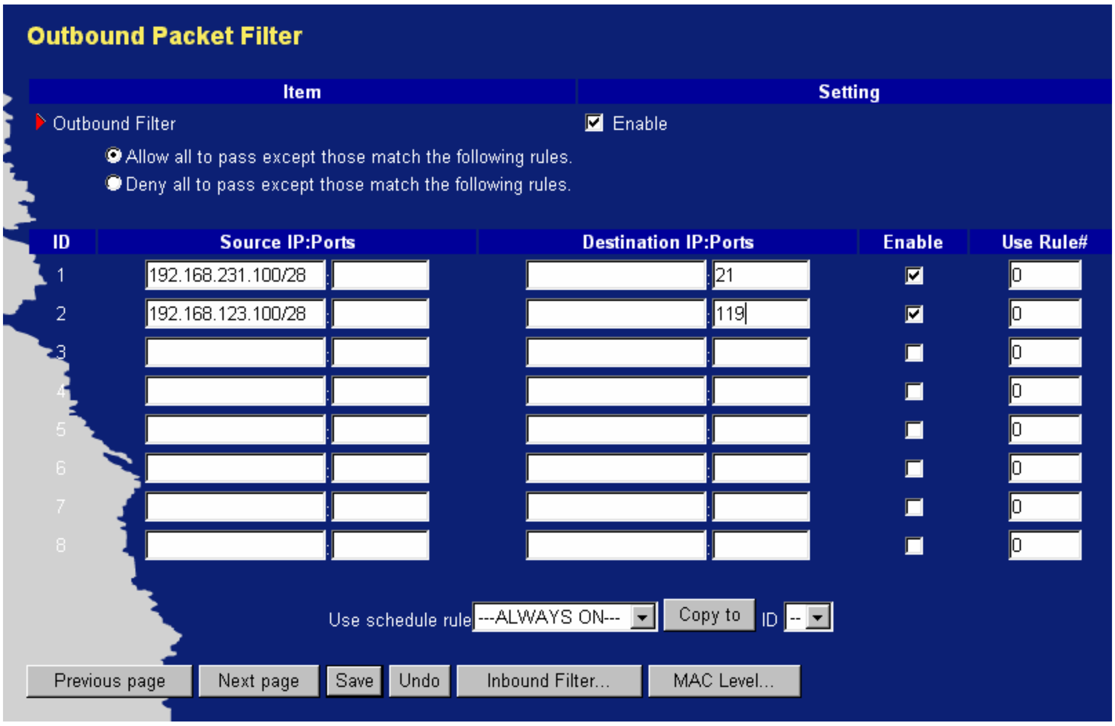
Use schedule rule ---ALWAYS ON---

(192.168.123.100/28): It stands for a subnet of IP address ranging from 192.168.123.96 to 192.168.123.111 and 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.

(192.168.123.10/29): It stands for a subnet of IP address ranging from 192.168.123.8 to 192.168.123.15 and 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	192.168.231.100/28			21	☑	0
2	192.168.123.100/28			119	☑	0
3					☐	0
4					☐	0
5					☐	0
6					☐	0
7					☐	0
8					☐	0

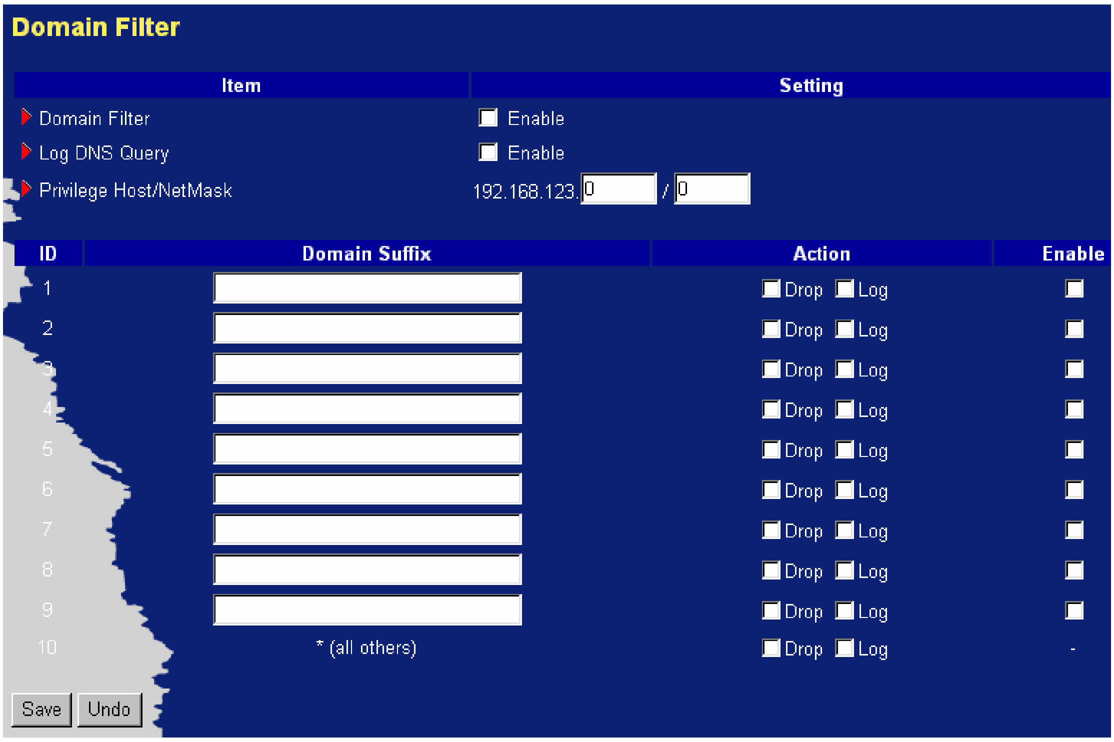
Use schedule rule ---ALWAYS ON--- Copy to ID --

(192.168.123.100/28): It stands for a subnet of IP address ranging from 192.168.123.96 to 192.168.123.111 and 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 on the **Save** button.

4.6.2 Domain Filter



Domain Filter

Item	Setting
Domain Filter	☐ Enable
Log DNS Query	☐ Enable
Privilege Host/NetMask	192.168.123. 0 / 0

ID	Domain Suffix	Action	Enable
1		☐ 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 domains.

Domain Filter Enable:

Checke if you want to enable Domain Filter.

Log DNS Query:

Checke if you want to log the action when someone accesses the specific domains.

Privilege IP Addresses Range:

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

Domain Suffix:

A suffix of domains will be restricted. For example, ".com", "xxx.com".

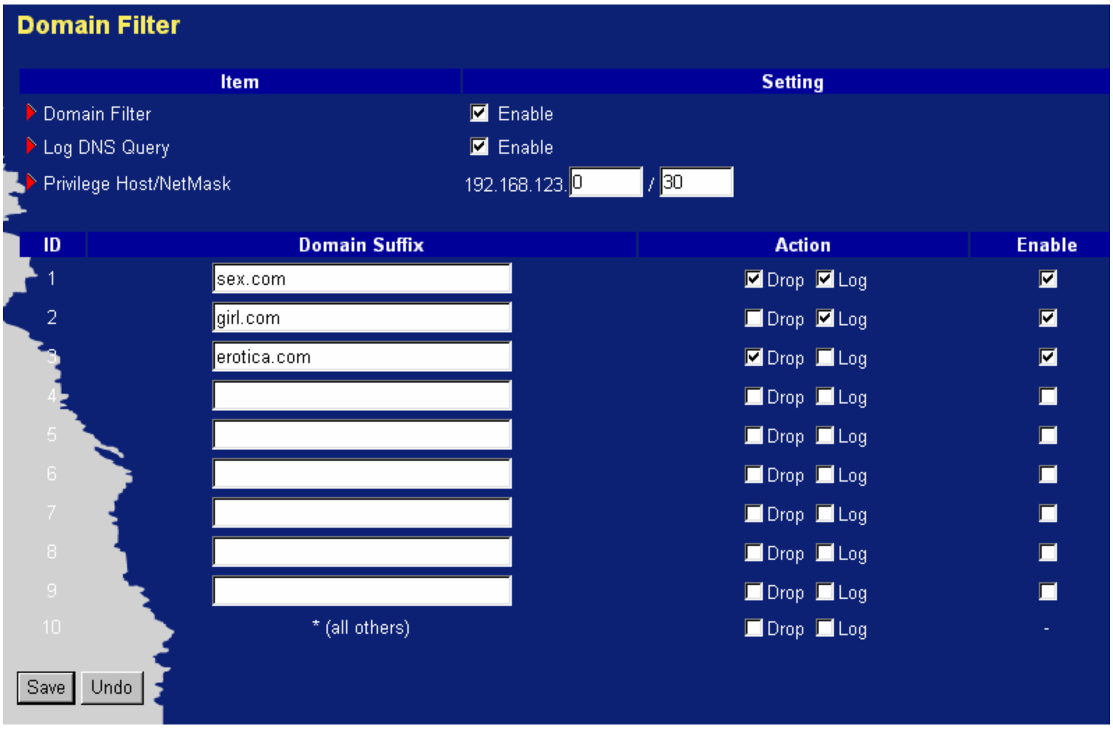
Action:

When someone is accessing the domain met the domain-suffix, what kind of action you want. *Checke* **drop** to block the access. *Checke* **log** to log these access.

Enable:

Checke **Enable** to enable each rule.

Example:



Domain Filter

Item	Setting
Domain Filter	☑ Enable
Log DNS Query	☑ Enable
Privilege Host/NetMask	192.168.123. 0 / 30

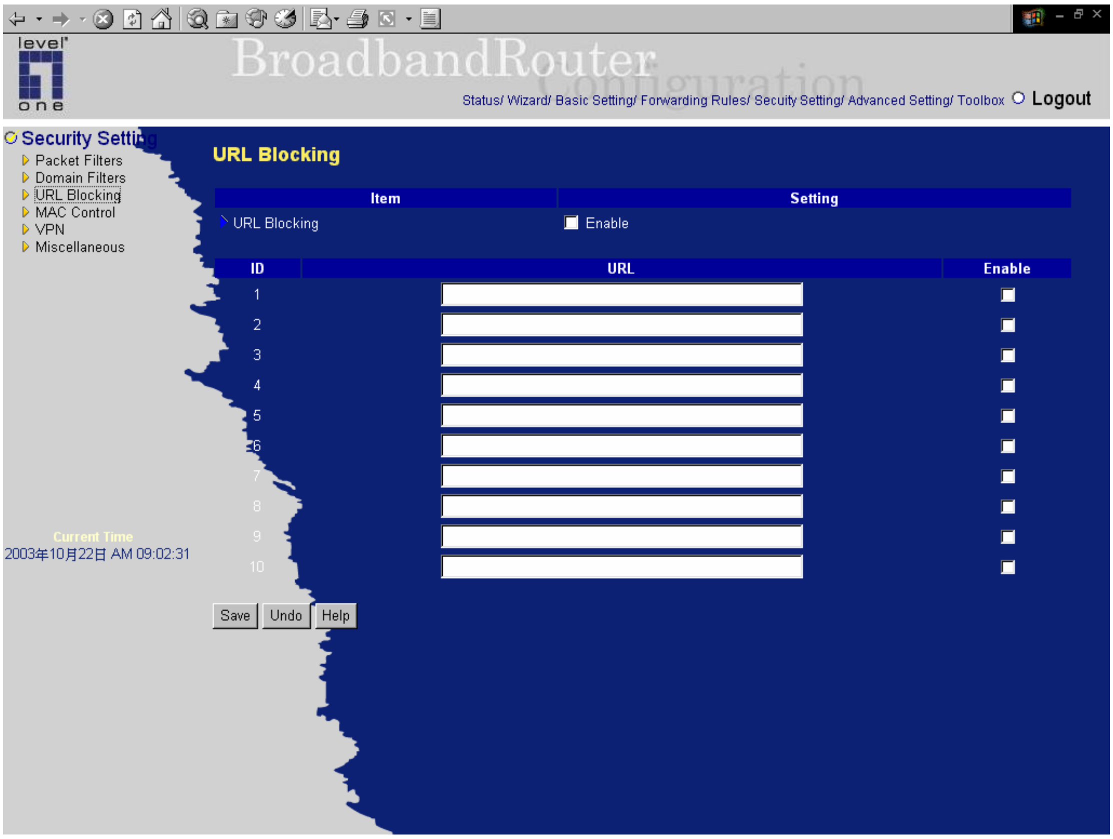
ID	Domain Suffix	Action	Enable
1	sex.com	☑ Drop ☑ Log	☑
2	girl.com	□ Drop ☑ Log	☑
3	erotica.com	☑ Drop □ Log	☑
4		□ Drop □ Log	□
5		□ Drop □ Log	□
6		□ Drop □ Log	□
7		□ Drop □ Log	□
8		□ Drop □ Log	□
9		□ Drop □ Log	□
10	* (all others)	□ Drop □ Log	-

In this example:

1. Domain include “sex.com” will be blocked, and the action will be record in log-file.
2. Domain include “girl.com” will not be blocked, but the action will be record in log-file.
3. Domain include “erotica.com” will be blocked, but the action will not be record in log-file.
4. (192.168.123.8/30): It stands for a subnet of IP address ranging from 192.168.123.8 to 192.168.123.11 and 192.168.123.8 is an element in the range set. The value of 30 stands for the netmask of subnet and 2 (=32-30) least significant bits in the last byte of IP address are unmask

bits. These LAN hosts of subnet can access network without restriction.

4.6.3 URL Blocking Blocking


level one
BroadbandRouter Configuration
Status/ Wizard/ Basic Setting/ Forwarding Rules/ Secuity Setting/ Advanced Setting/ Toolbox
Logout
Security Setting
Packet Filters
Domain Filters
URL Blocking
MAC Control
VPN
Miscellaneous
Current Time
2003年10月22日 AM 09:02:31
Save
Undo
Help

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.

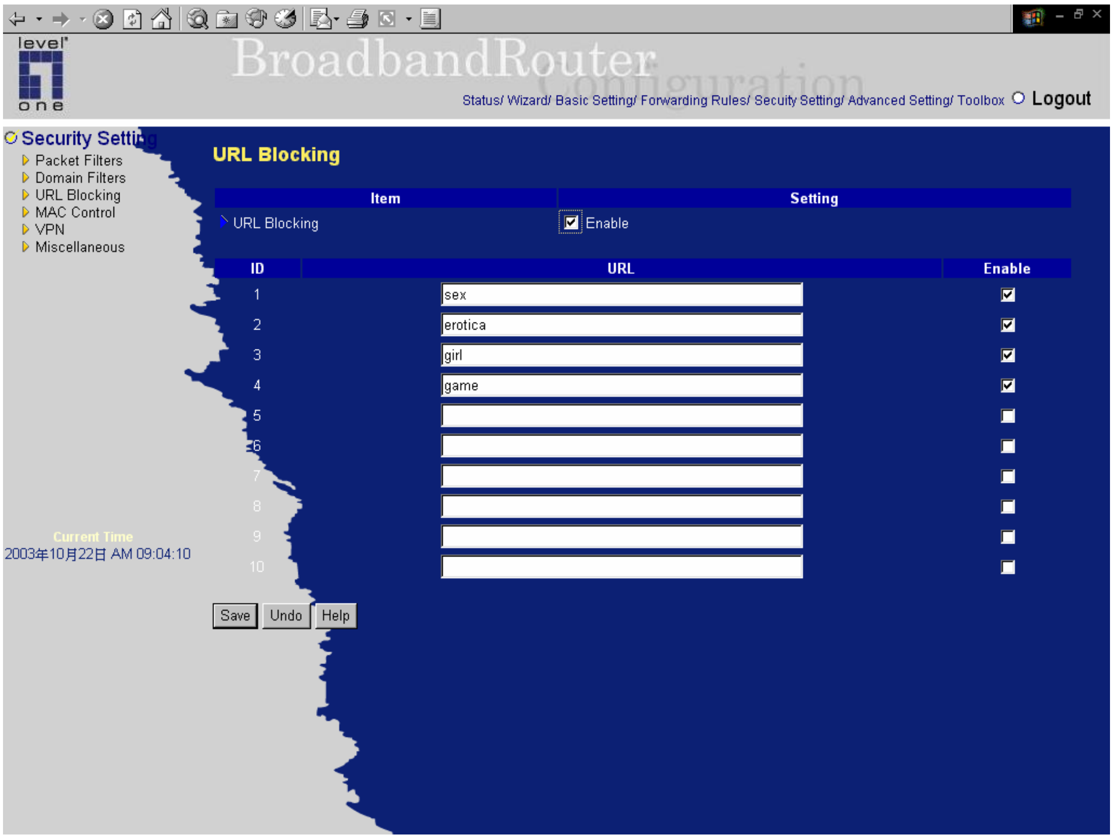
URL

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.


level one
BroadbandRouter Configuration
Status/ Wizard/ Basic Setting/ Forwarding Rules/ Secuity Setting/ Advanced Setting/ Toolbox
Logout
Security Setting
Packet Filters
Domain Filters
URL Blocking
MAC Control
VPN
Miscellaneous
Current Time
2003年10月22日 AM 09:04:10
Save
Undo
Help

URL Blocking

Item	Setting
URL Blocking	☑ Enable

ID	URL	Enable
1	sex	☑
2	erotica	☑
3	girl	☑
4	game	☑
5		□
6		□
7		□
8		□
9		□
10		□

In this example:

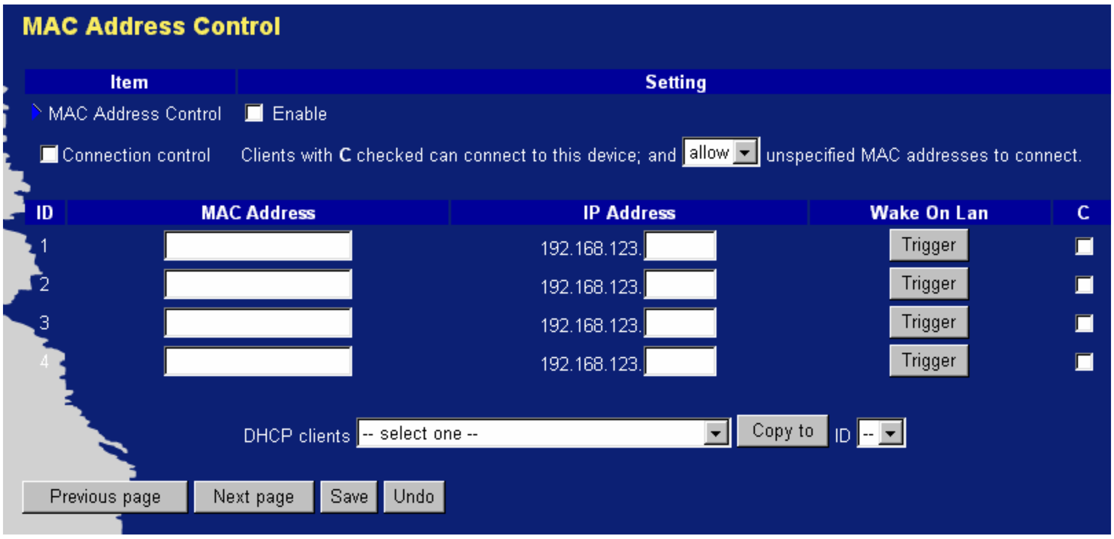
1.URL include “sex” will be blocked, and the action will be record in log-file.

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

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	Wake On Lan	C
1		192.168.123.	Trigger	□
2		192.168.123.	Trigger	□
3		192.168.123.	Trigger	□
4		192.168.123.	Trigger	□

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

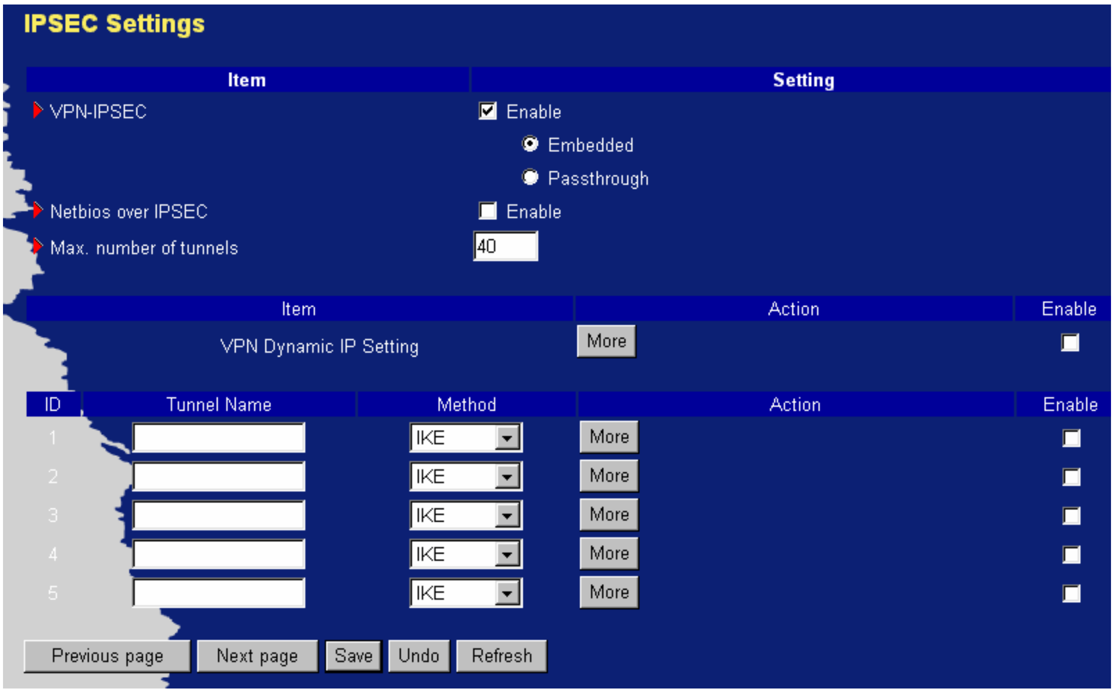
Check "**Connection control**" to enable the controlling of which clients can connect to this device. If a client is denied to connect to this device, it means the client can't access to the Internet either. Choose "allow" or "deny" to allow or deny the clients, whose MAC addresses are not in the "Control table" (please see below), to connect to this device. But note that **do not configure the router with one case resulting in none can access it.** For example, enable the MAC Address Control and Connection Control, reject unspecified MAC addresses to connect the router, but there is no entry rule for allowing some hosts to connect the router. This will result in none can access the router.

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.

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-IPSEC



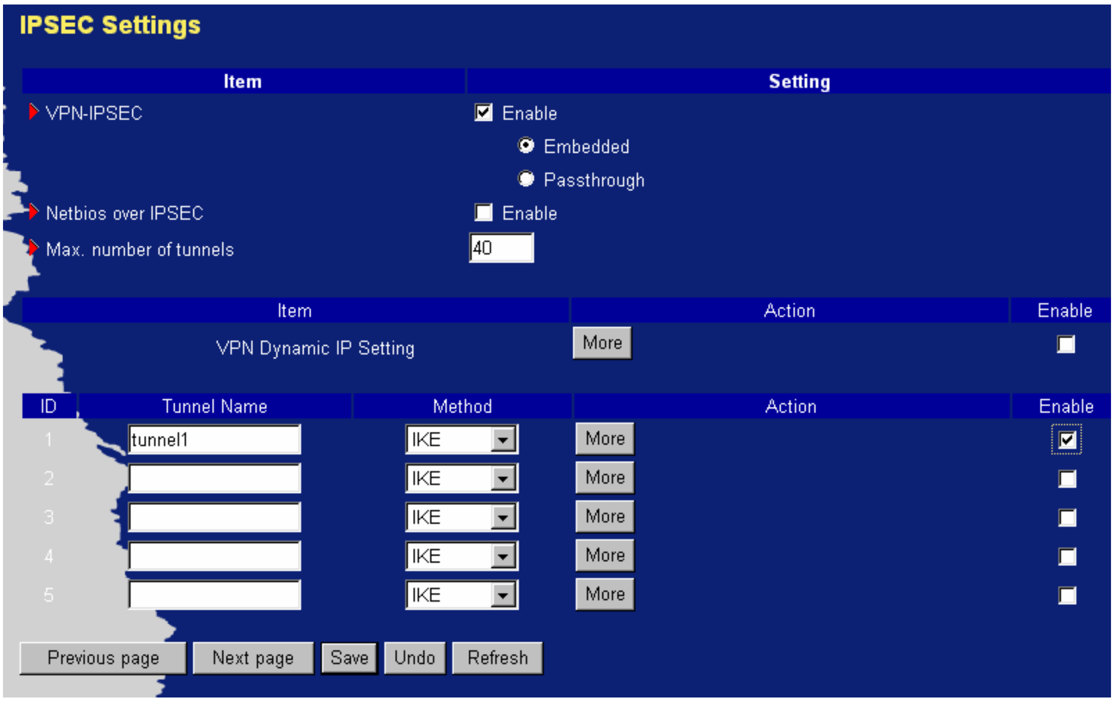
IPSEC Settings

Item	Setting
VPN-IPSEC	☑ Enable ● Embedded ○ Passthrough
Netbios over IPSEC	□ Enable
Max. number of tunnels	40

Item	Action	Enable
VPN Dynamic IP Setting	More	□

ID	Tunnel Name	Method	Action	Enable
1		IKE	More	□
2		IKE	More	□
3		IKE	More	□
4		IKE	More	□
5		IKE	More	□

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



IPSEC Settings

Item	Setting
VPN-IPSEC	☑ Enable ● Embedded ○ Passthrough
Netbios over IPSEC	□ Enable
Max. number of tunnels	40

Item	Action	Enable
VPN Dynamic IP Setting	More	□

ID	Tunnel Name	Method	Action	Enable
1	tunnel1	IKE	More	☑
2		IKE	More	□
3		IKE	More	□
4		IKE	More	□
5		IKE	More	□

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.

Embedded / Passthrough

Select **Embedded** to enable this device's VPN function, or select **Passthrough** to allow your **VPN**

Tunnel pass through this device.

Netbios over IPSEC

Enable Netbios protocol (My Network Places) between IPSEC Tunnels.

Max. number of tunnels item

Since VPN greatly degrades network throughput, the allowable maximum number of concurrent 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 40.

VPN Dynamic IP Setting

Allow user to build VPN tunnel with the device from any remote VPN gateway or host regardless of its IP information.

Tunnel name

Indicate which tunnel that is focused now.

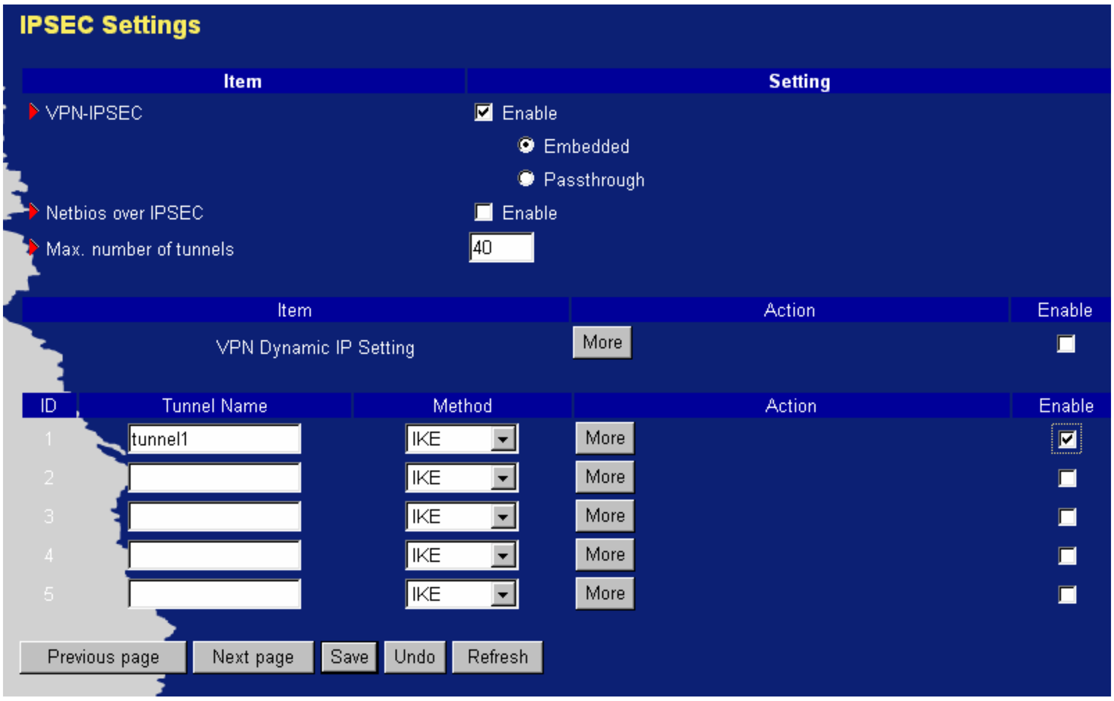
Method

IPSec VPN supports two kinds of key-obtained methods: manual key and automatic key exchange (IKE). Manual key approach indicates that two end VPN gateways setup authenticator and encryption keys 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. The detailer configuration data must be set before creating VPN tunnel.

4.6.5.1 VPN Dynamic IP Setting



IPSEC Settings

Item	Setting
VPN-IPSEC	☑ Enable ● Embedded ○ Passthrough
Netbios over IPSEC	□ Enable
Max. number of tunnels	40

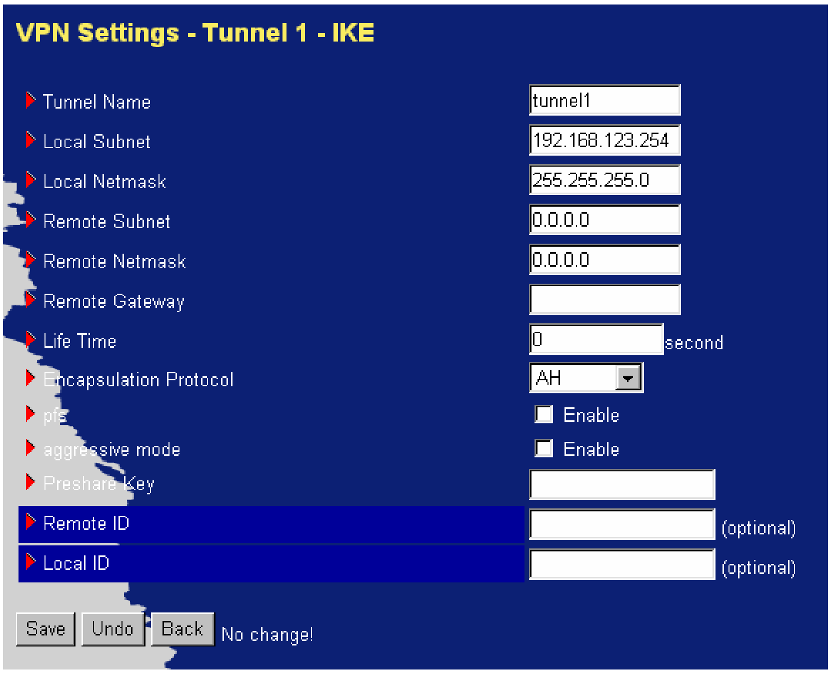
Item	Action	Enable
VPN Dynamic IP Setting	More	□

ID	Tunnel Name	Method	Action	Enable
1	tunnel1	IKE	More	☑
2		IKE	More	□
3		IKE	More	□
4		IKE	More	□
5		IKE	More	□

When using **VPN Dynamic IP Setting**, this VPN router can accept tunnel creation requests from more IPSec initiators whose IP address are dynamic except those with static IP address. By this way, the VPN router will not check VPN initiator's IP information, so user can build VPN tunnel at the VPN router from any remote VPN router or host regardless of its IP information. The setting is same with following IKE setup except some fields are not required here.

4.6.5.2 IKE setup

Press **"More"**→



VPN Settings - Tunnel 1 - IKE

Tunnel Name	tunnel1
Local Subnet	192.168.123.254
Local Netmask	255.255.255.0
Remote Subnet	0.0.0.0
Remote Netmask	0.0.0.0
Remote Gateway	
Life Time	0 second
Encapsulation Protocol	AH
pfs	□ Enable
aggressive mode	□ Enable
Preshare Key	
Remote ID	(optional)
Local ID	(optional)

No change!

IKE setup includes the setting of following items: local subnet, local netmask, remote subnet, remote netmask, remote gateway, Life Time, Encapsulation Protocol, pfs, aggressive mode, pre-shared key, remote ID and local ID. The tunnel name is derived from previous page of VPN setting.

Local subnet

It is 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 forms a subnet domain.

Remote subnet

It is 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

Remote gateway is the IP address of remote VPN gateway.

Life Time

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.

Encapsulation Protocol

There are three protocols can be selected: ESP, AH and ESP+AH.

pfs:

Perfect Forward Secrecy (PFS), allow IKE to re-exchange a key for IPSec instead of direct use ISAKMP key as the IPSec key during phase 2 of IKE negotiation. The ISAKMP key is derived at the end of phase 1 of IKE negotiation. This setting must be same between initiator and responder or a VPN tunnel can not be created.

Aggressive mode:

During phase 1 of IKE negotiation, IKE operates in main mode or aggressive mode. Aggressive mode is a reduced version of main mode and more unsafe.

Pre-shared key

It is 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.

Remote ID

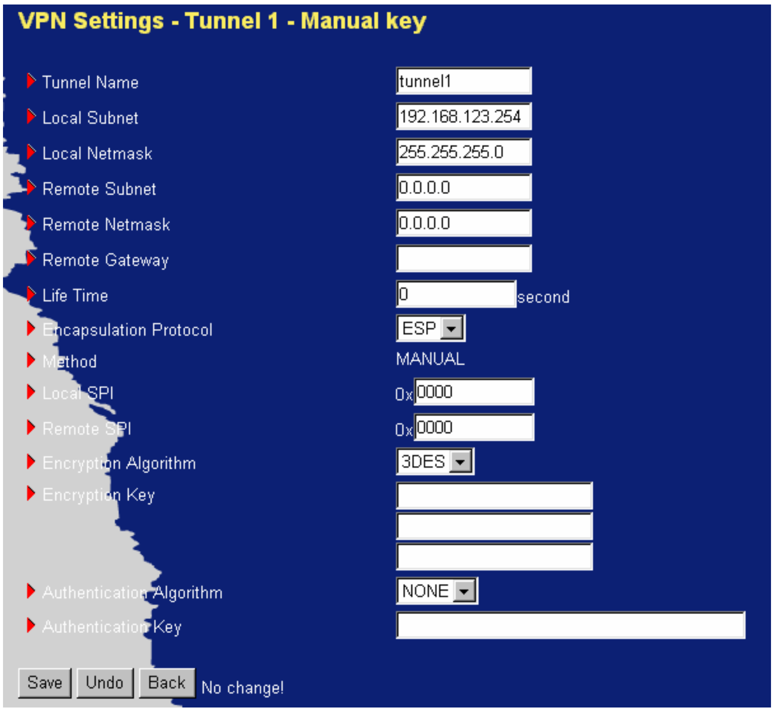
It is optional. Some VPN gateways require ID for authentication. For example, to connect to **SonicWall** VPN gateway, user should input **serial number** here. But to connect to **Cisco** VPN gateway, user should input **IP@domain**.

Local ID

It is optional. Some VPN gateways require local ID for authentication. For example, NetScreen VPN router serves as the initiator and can inquire if the responder is specific gateway or host that should be dedicated by the local ID.

4.6.5.3 Manual Key setup

Press **"More"**→



VPN Settings - Tunnel 1 - Manual key

Tunnel Name	tunnel1
Local Subnet	192.168.123.254
Local Netmask	255.255.255.0
Remote Subnet	0.0.0.0
Remote Netmask	0.0.0.0
Remote Gateway	
Life Time	0 second
Encapsulation Protocol	ESP
Method	MANUAL
Local SPI	0x 0000
Remote SPI	0x 0000
Encryption Algorithm	3DES
Encryption Key	
Authentication Algorithm	NONE
Authentication Key	

No change!

Manual key setup includes more items than **IKE setup,** like Local SPI, Remote SPI, Encryption Algorithm, Encryption Key, Authentication Algorithm, and Authentication Key.

Tunnel name

Indicate which tunnel that is focused now. The tunnel name is derived from previous page of VPN setting.

Local subnet

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

Local netmask

Local netmask combined with local subnet forms a subnet domain.

Remote subnet

It is the subnet of LAN site of remote VPN gateway; it can be a host, a partial subnet, or the whole subnet of LAN site of remote gateway.

Remote netmask

Remote netmask combined with remote subnet forms a subnet domain of remote end.

Remote gateway

The field should be filled with the IP address of remote VPN gateway.

Life time

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.

Encapsulation protocol

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

Local SPI

SPI is an important parameter during hashing. Local SPI will be included in the outbound packet transmitted from WAN interface of local gateway. The value of local SPI should be set in hex formatted.

Remote SPI

Remote SPI will be included in the inbound packet transmitted from WAN site of remote gateway. It will be used to de-hash the coming packet and check its integrity. The value of remote SPI should be set in hex formatted.

Encryption algorithm

There are three algorithms can be selected: AES, 3DES and DES (Some models only support 3DES and DES). But when the encapsulation protocol is AH, encryption algorithm is unnecessarily set.

Encryption key

Encryption key is used by the encryption algorithm. Its length is 8 bytes if encryption algorithm is DES or 24 bytes if 3DES. The key value should be set in hex formatted.

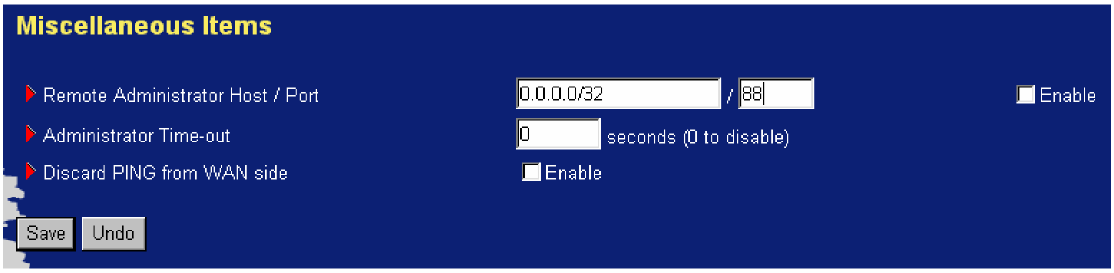
Authentication algorithm

There are two algorithms can be selected: SHA1 and MD5. But “none” also can be selected here if no hashing operation is necessary.

Authentication key

Authentication key is used by the authentication algorithm. Its length is 16 bytes if authentication algorithm is MD5 or 20 bytes if SHA1. Certainly, its length will be 0 if no authentication algorithm is chosen. The key value should be set in hex formatted.

4.6.6 Miscellaneous Items



Miscellaneous Items

Remote Administrator Host / Port: 0.0.0.0/32 / 88 □ Enable

Administrator Time-out: 0 seconds (0 to disable)

Discard PING from WAN side: □ Enable

Remote Administrator Host/Port

In general, only Intranet user can browse the built-in web pages to perform administration task. But 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 for remote administrator but no change for local administrator. You can *change web server port to other port, too.*

Administrator Time-out

It is the time of no activity on management web server to logout the administrator by router system automatically. Set it to zero to disable this feature.

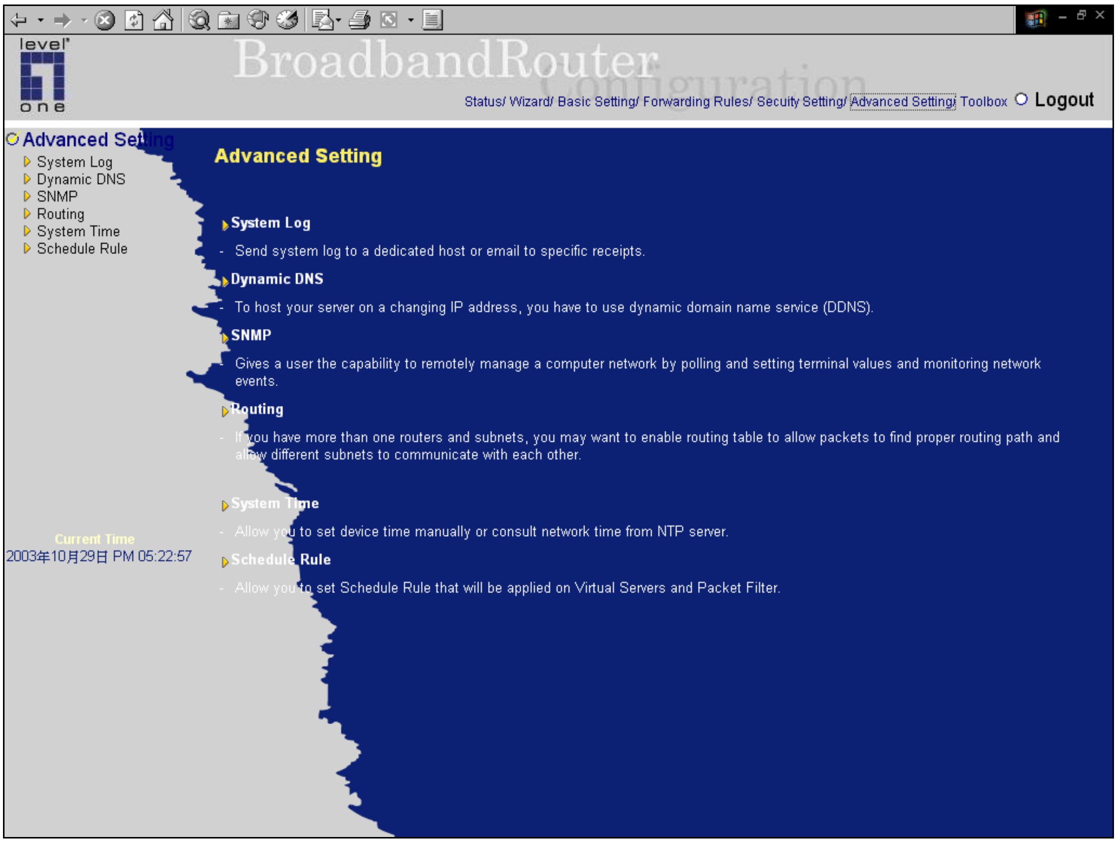
Discard PING from WAN side

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

Disable UPnp

When this feature is enabled, UPnP feature will be disabled.

4.7 Advanced Setting Chapter Home



BroadbandRouter Configuration
Status/ Wizard/ Basic Setting/ Forwarding Rules/ Secuity Setting/ Advanced Setting/ Toolbox
Logout
Advanced Setting
System Log
Dynamic DNS
SNMP
Routing
System Time
Schedule Rule
Current Time
2003年10月29日 PM 05:22:57

Advanced Setting

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.

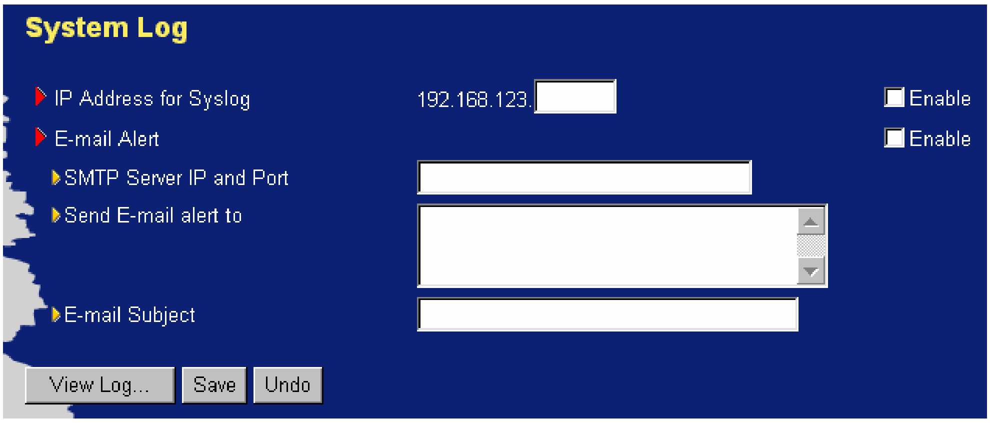
System Time

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

Schedule Rule

- Allow you to set Schedule Rule that will be applied on Virtual Servers and Packet Filter.

4.7.1 System Log



System Log

IP Address for Syslog 192.168.123. □ Enable

E-mail Alert □ Enable

SMTP Server IP and Port

Send E-mail alert to

E-mail Subject

This page supports 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 syslog will be sent. *Check* **Enable** to enable this function.

E-mail Alert Enable

Check if you want to enable Email alert (send urgent information to administrator via email).

SMTP Server IP and Port

Input the SMTP server IP and port, which are concatenated with ':'. If you do not specify port number, the default value is 25. For example, "mail.your_url.com" or "192.168.1.100:26".

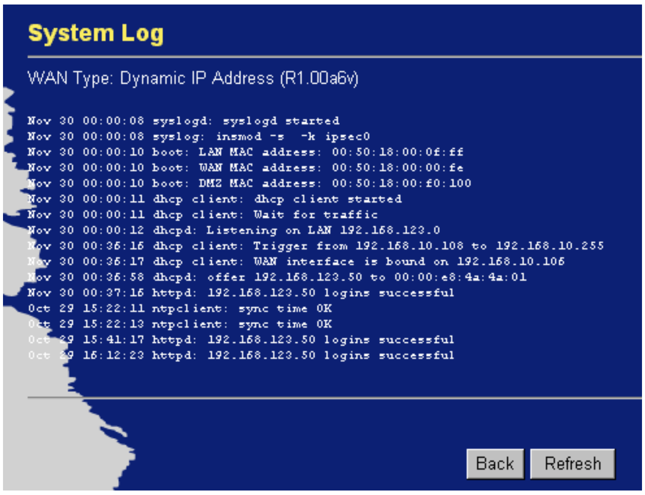
Send E-mail alert to

This field is filled with the recipients who will receive these logs. You can assign more than one recipient by using ';' or ',' to separate these email addresses.

E-mail Subject

This field is filled with the subject of email alert. This setting is optional.

View log



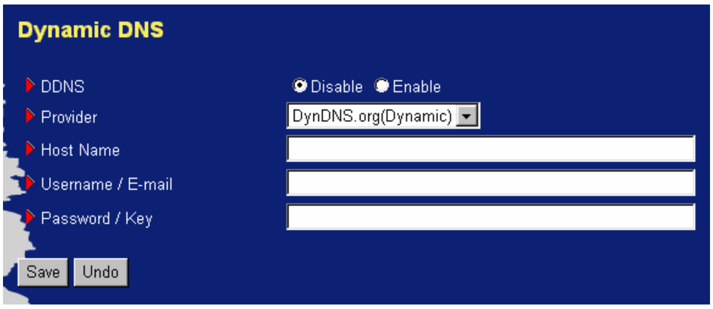
System Log

WAN Type: Dynamic IP Address (R1.00a6v)

```
Nov 30 00:00:08 syslogd: syslogd started
Nov 30 00:00:08 syslog: insmod -s  -k ipsec0
Nov 30 00:00:10 boot: LAN MAC address: 00:50:18:00:0f:ff
Nov 30 00:00:10 boot: WAN MAC address: 00:50:18:00:00:fe
Nov 30 00:00:10 boot: DMZ MAC address: 00:50:18:00:f0:100
Nov 30 00:00:11 dhcp client: dhcp client started
Nov 30 00:00:11 dhcp client: Wait for traffic
Nov 30 00:00:12 dhcpd: Listening on LAN 192.168.123.0
Nov 30 00:36:16 dhcp client: Trigger from 192.168.10.108 to 192.168.10.255
Nov 30 00:36:17 dhcp client: WAN interface is bound on 192.168.10.106
Nov 30 00:36:58 dhcpd: offer 192.168.123.50 to 00:00:e8:4a:4a:01
Nov 30 00:37:16 httpd: 192.168.123.50 logins successful
Oct 29 15:22:11 ntpclient: sync time OK
Oct 29 15:22:13 ntpclient: sync time OK
Oct 29 15:41:17 httpd: 192.168.123.50 logins successful
Oct 29 16:12:23 httpd: 192.168.123.50 logins successful
```

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

4.7.2 Dynamic DNS



Dynamic DNS

DDNS ● Disable ○ Enable

Provider DynDNS.org(Dynamic)

Host Name

Username / E-mail

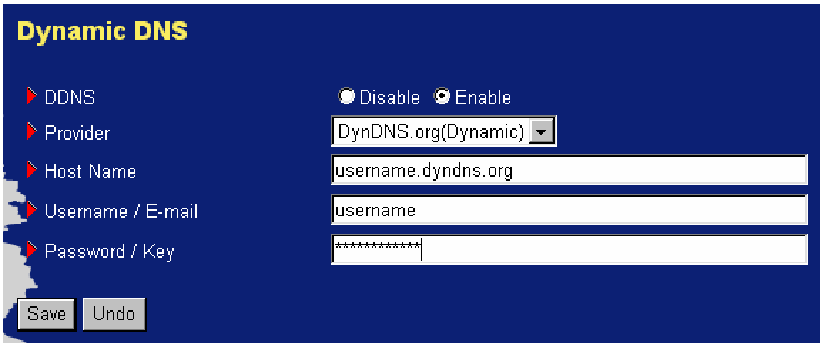
Password / Key

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

Example:



Dynamic DNS

DDNS ○ Disable ● Enable

Provider DynDNS.org(Dynamic)

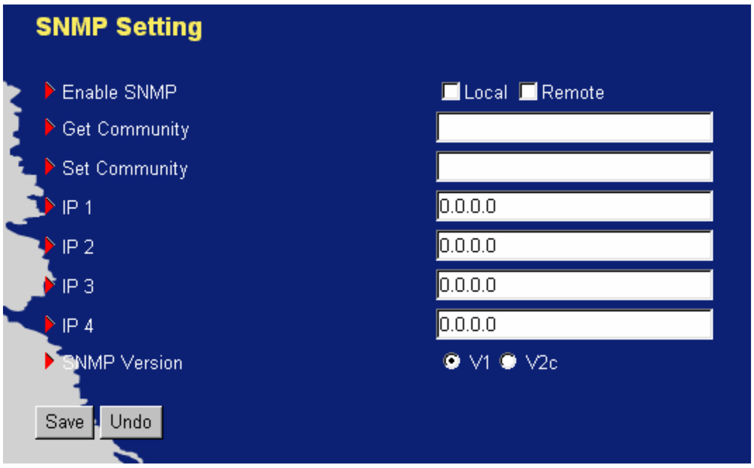
Host Name username.dyndns.org

Username / E-mail username

Password / Key *************

After Dynamic DNS setting is configured, click on the **Save** button.

4.7.3 SNMP Setting



SNMP Setting

Enable SNMP ☐ Local ☐ Remote

Get Community

Set Community

IP 1 0.0.0.0

IP 2 0.0.0.0

IP 3 0.0.0.0

IP 4 0.0.0.0

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.

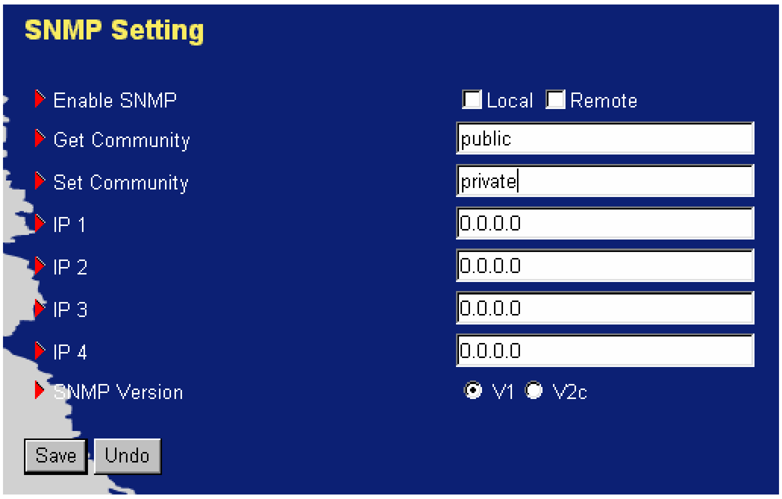
Get Community

Setting the community of Get Request your device will response.

Set Community

Setting the community of Set Request your device will accept.

Example:



SNMP Setting

Enable SNMP ☐ Local ☐ Remote

Get Community public

Set Community private

IP 1 0.0.0.0

IP 2 0.0.0.0

IP 3 0.0.0.0

IP 4 0.0.0.0

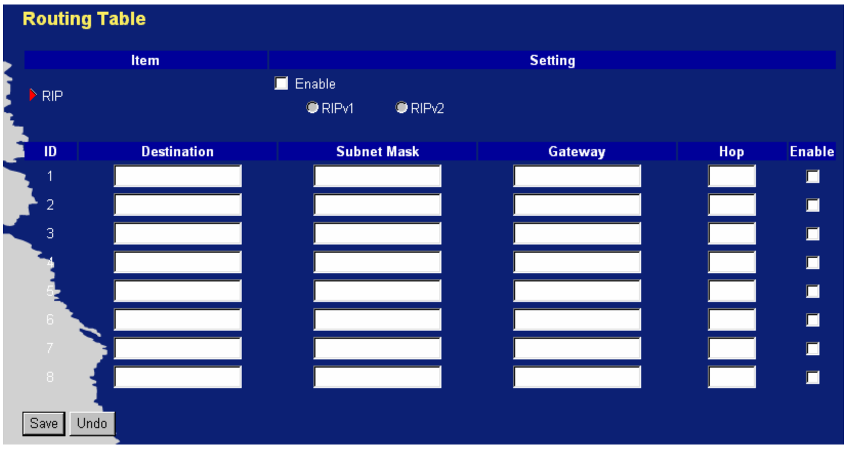
SNMP Version ● V1 ○ V2c

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

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

3. This device will response request only from LAN.

4.7.4 Routing Table

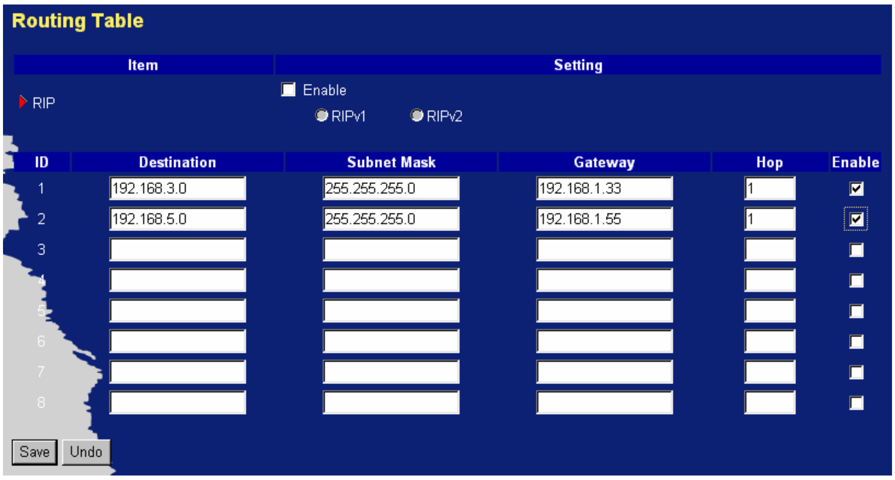


Routing Tables allow you to determine which physical interface address to use for outgoing IP data grams. If you have more than one routers and subnets, you will need to enable routing table to allow packets to find proper routing path and allow different subnets to communicate with each other. Routing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

RIP Enable: Check to enable RIP function. It supports dynamic routing information exchange.

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

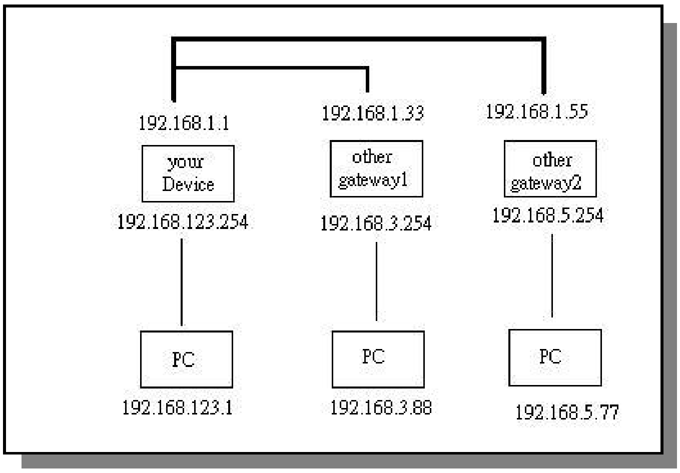
Example:



Routing Table

Item	Setting
RIP	□ Enable ○ RIPv1 ○ RIPv2

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

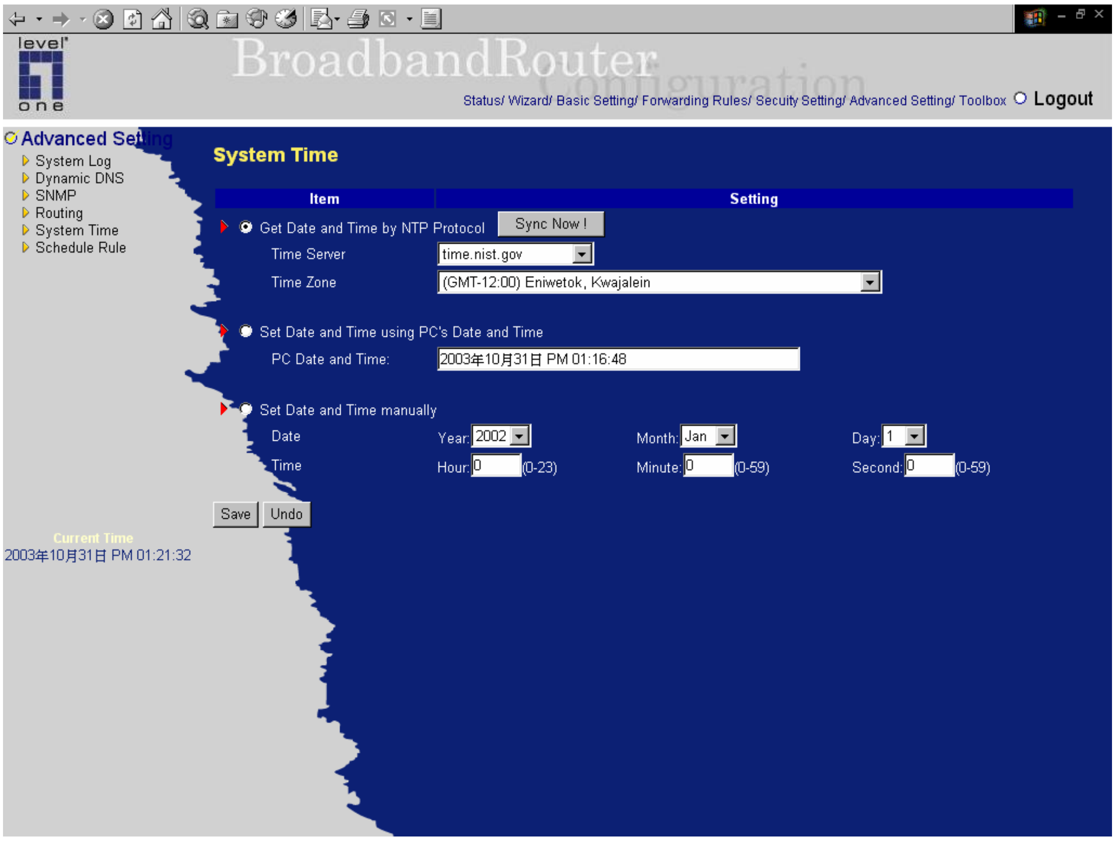


So if, for example, the host wanted to send an IP data gram to 192.168.3.88, it would use the above table to determine that it had to go via 192.168.1.33 (a gateway), and if it sends packets to 192.168.5.77 will go via 192.168.1.55.

Each rule can be enabled or disabled individually.

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

4.7.5 System Time


level one
BroadbandRouter Configuration
Status/ Wizard/ Basic Setting/ Forwarding Rules/ Secuity Setting/ Advanced Setting/ Toolbox
Logout
Advanced Setting
System Log
Dynamic DNS
SNMP
Routing
System Time
Schedule Rule
Sync Now !
Save
Undo

Current Time
2003年10月31日 PM 01:21:32

System Time

Item	Setting
● Get Date and Time by NTP Protocol	Sync Now !
Time Server	time.nist.gov
Time Zone	(GMT-12:00) Eniwetok, Kwajalein
○ Set Date and Time using PC's Date and Time	
PC Date and Time:	2003年10月31日 PM 01:16:48
○ Set Date and Time manually	
Date	Year: 2002 Month: Jan 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 time server to consult UTC time

Time Zone

Select a time zone where this device locates.

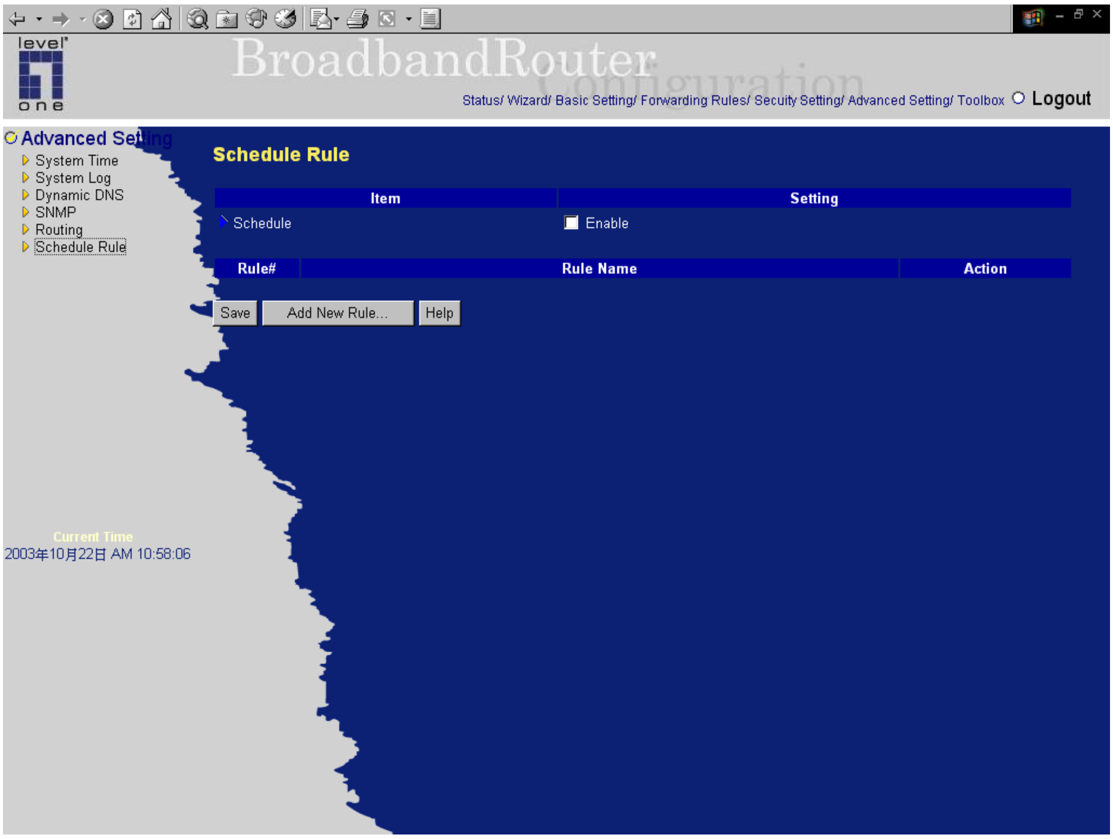
Set Date and Time manually

Selected if you want to Set Date and Time manually.

Function of Buttons

Sync Now: Synchronize system time with network time server

4.7.6 Schedule Rule



BroadbandRouter Configuration
Status/ Wizard/ Basic Setting/ Forwarding Rules/ Secuity Setting/ Advanced Setting/ Toolbox
Logout
Advanced Setting
System Time
System Log
Dynamic DNS
SNMP
Routing
Schedule Rule
Current Time
2003年10月22日 AM 10:58:06

Schedule Rule

Item	Setting
Schedule	□ Enable

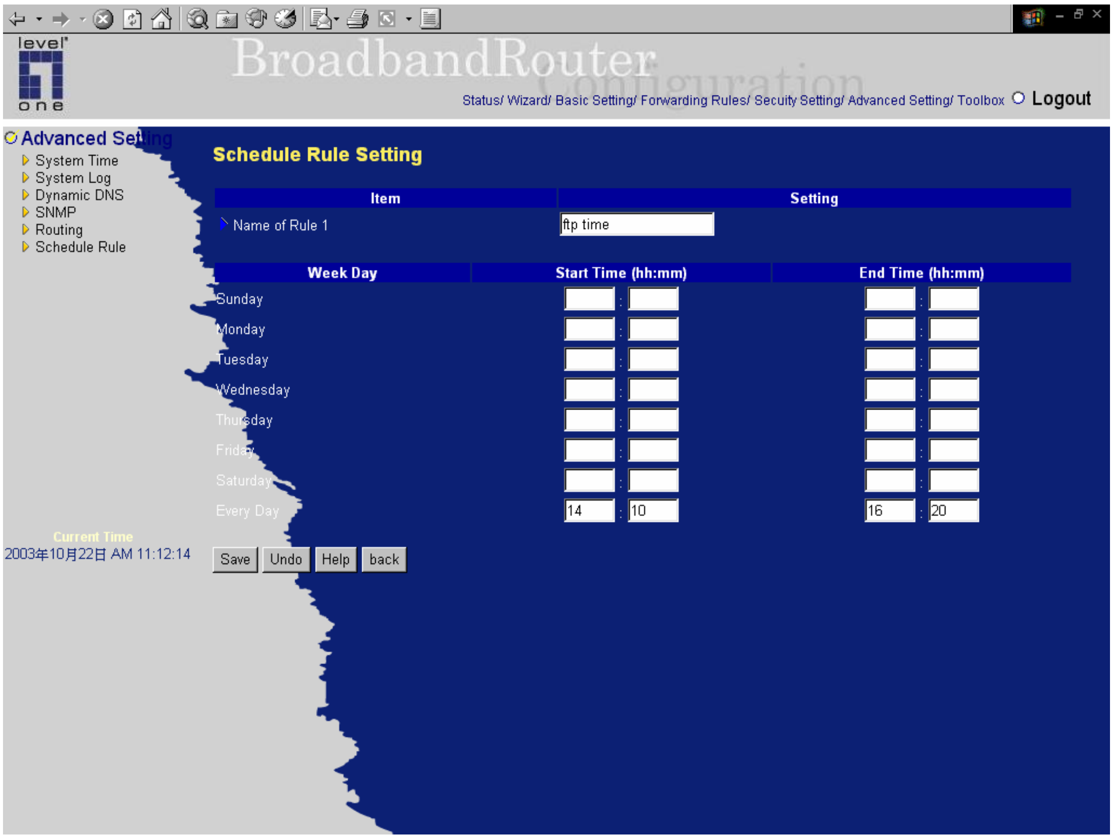
Rule#	Rule Name	Action

Save
Add New Rule...
Help

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

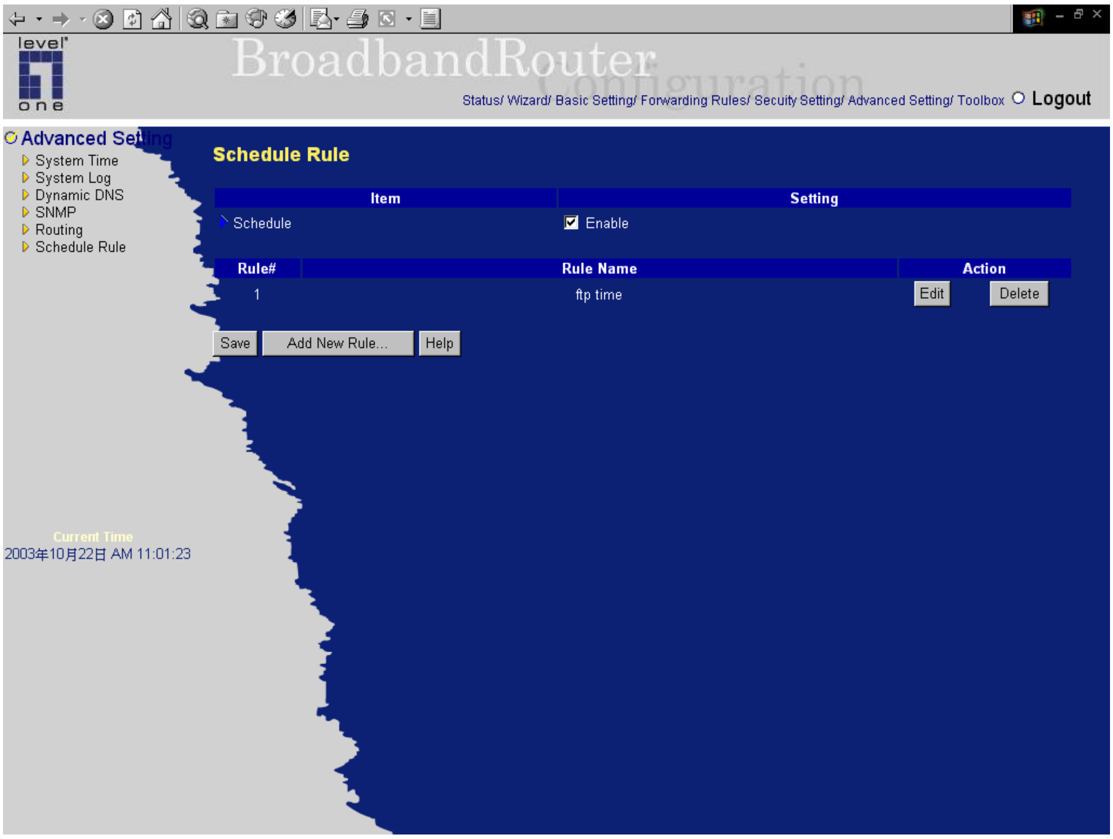

level one
BroadbandRouter Configuration
Status/ Wizard/ Basic Setting/ Forwarding Rules/ Secuity Setting/ Advanced Setting/ Toolbox
Logout
Advanced Setting
System Time
System Log
Dynamic DNS
SNMP
Routing
Schedule Rule
Current Time
2003年10月22日 AM 11:12:14
Save
Undo
Help
back

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→


level one
BroadbandRouter Configuration
Status/ Wizard/ Basic Setting/ Forwarding Rules/ Secuity Setting/ Advanced Setting/ Toolbox
Logout
Advanced Setting
System Time
System Log
Dynamic DNS
SNMP
Routing
Schedule Rule
Current Time
2003年10月22日 AM 11:01:23
Save
Add New Rule...
Help

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

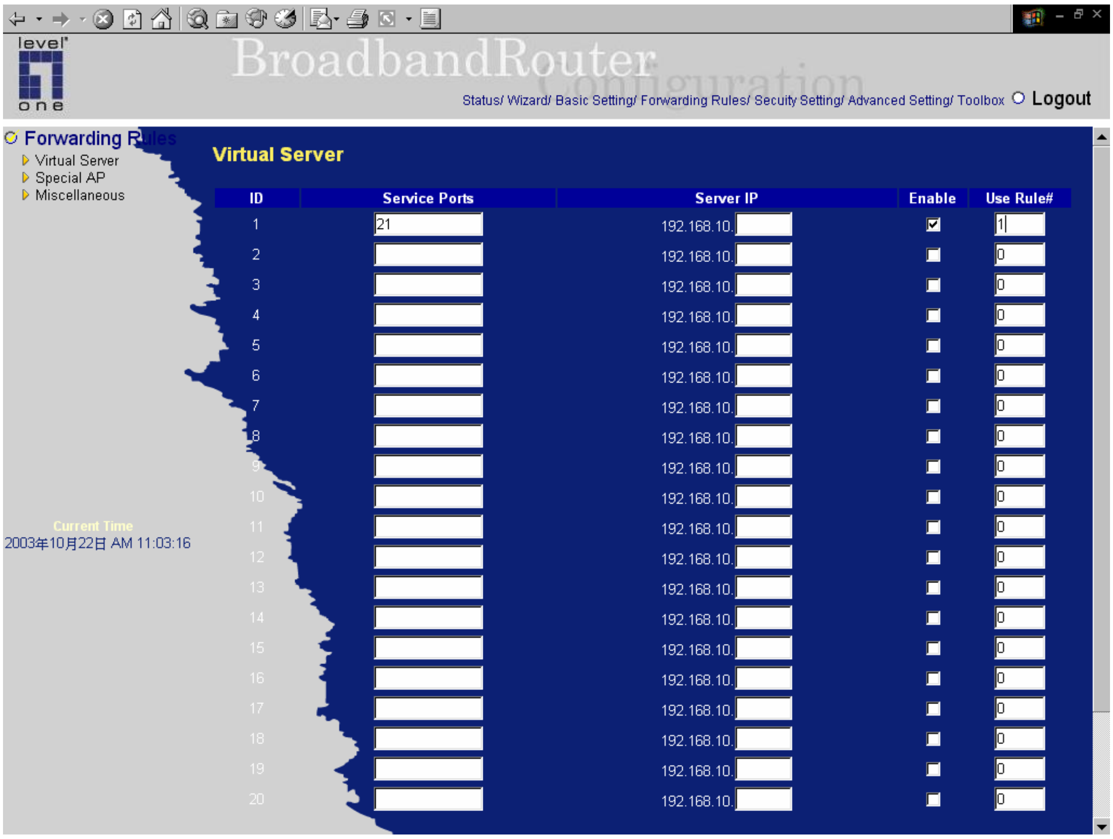
To edit the schedule rule.

Delete

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

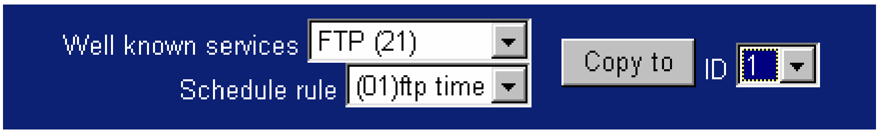
Schedule Rule can be apply to Virtual server and Packet Filter, for example:

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


level one
BroadbandRouter Configuration
Status/ Wizard/ Basic Setting/ Forwarding Rules/ Secuity Setting/ Advanced Setting/ Toolbox
Logout
Forwarding Rules
Virtual Server
Special AP
Miscellaneous
Current Time
2003年10月22日 AM 11:03:16

Virtual Server

ID	Service Ports	Server IP	Enable	Use Rule#
1	21	192.168.10.	☑	1
2		192.168.10.	☐	0
3		192.168.10.	☐	0
4		192.168.10.	☐	0
5		192.168.10.	☐	0
6		192.168.10.	☐	0
7		192.168.10.	☐	0
8		192.168.10.	☐	0
9		192.168.10.	☐	0
10		192.168.10.	☐	0
11		192.168.10.	☐	0
12		192.168.10.	☐	0
13		192.168.10.	☐	0
14		192.168.10.	☐	0
15		192.168.10.	☐	0
16		192.168.10.	☐	0
17		192.168.10.	☐	0
18		192.168.10.	☐	0
19		192.168.10.	☐	0
20		192.168.10.	☐	0

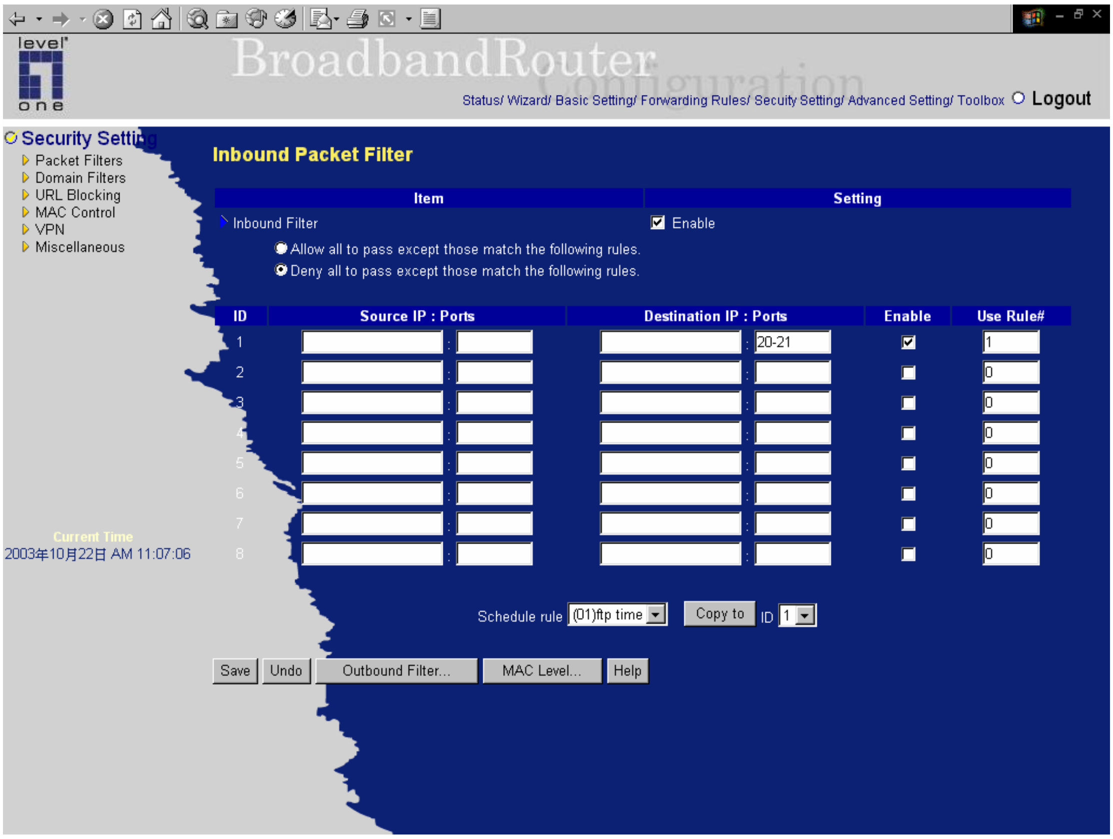


Well known services FTP (21)

Schedule rule (01)ftp time

ID 1

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



level one
BroadbandRouter Configuration
Status/ Wizard/ Basic Setting/ Forwarding Rules/ Secuity Setting/ Advanced Setting/ Toolbox
Logout
Security Setting
Packet Filters
Domain Filters
URL Blocking
MAC Control
VPN
Miscellaneous
Current Time
2003年10月22日 AM 11:07:06

Inbound Packet Filter

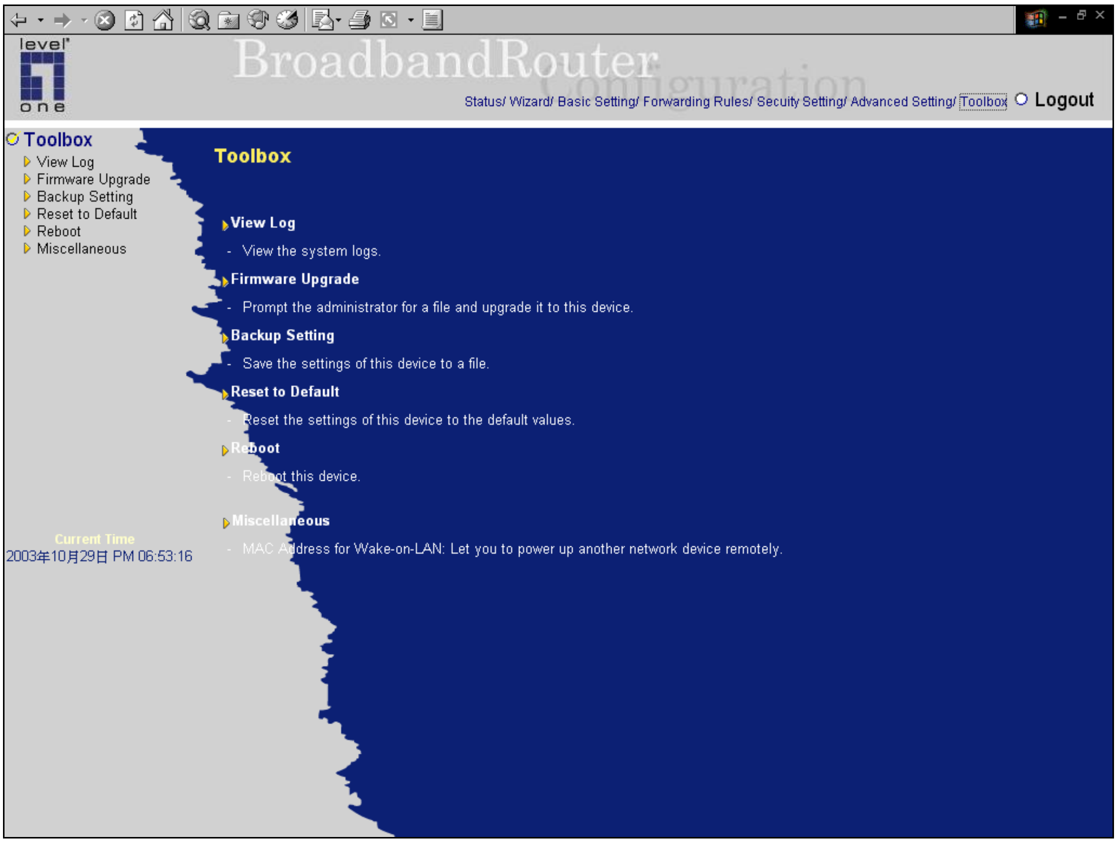
Item	Setting
Inbound Filter	☑ Enable

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

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

Schedule rule (01)ftp time   Copy to   ID 1

4.8 Toolbox Chapter Home



level one
BroadbandRouter Configuration
Status/ Wizard/ Basic Setting/ Forwarding Rules/ Secuity Setting/ Advanced Setting/ Toolbox
Logout
Toolbox
View Log
Firmware Upgrade
Backup Setting
Reset to Default
Reboot
Miscellaneous
Current Time
2003年10月29日 PM 06:53:16

Toolbox

View Log
- View the system logs.

Firmware Upgrade
- Prompt the administrator for a file and upgrade it to this device.

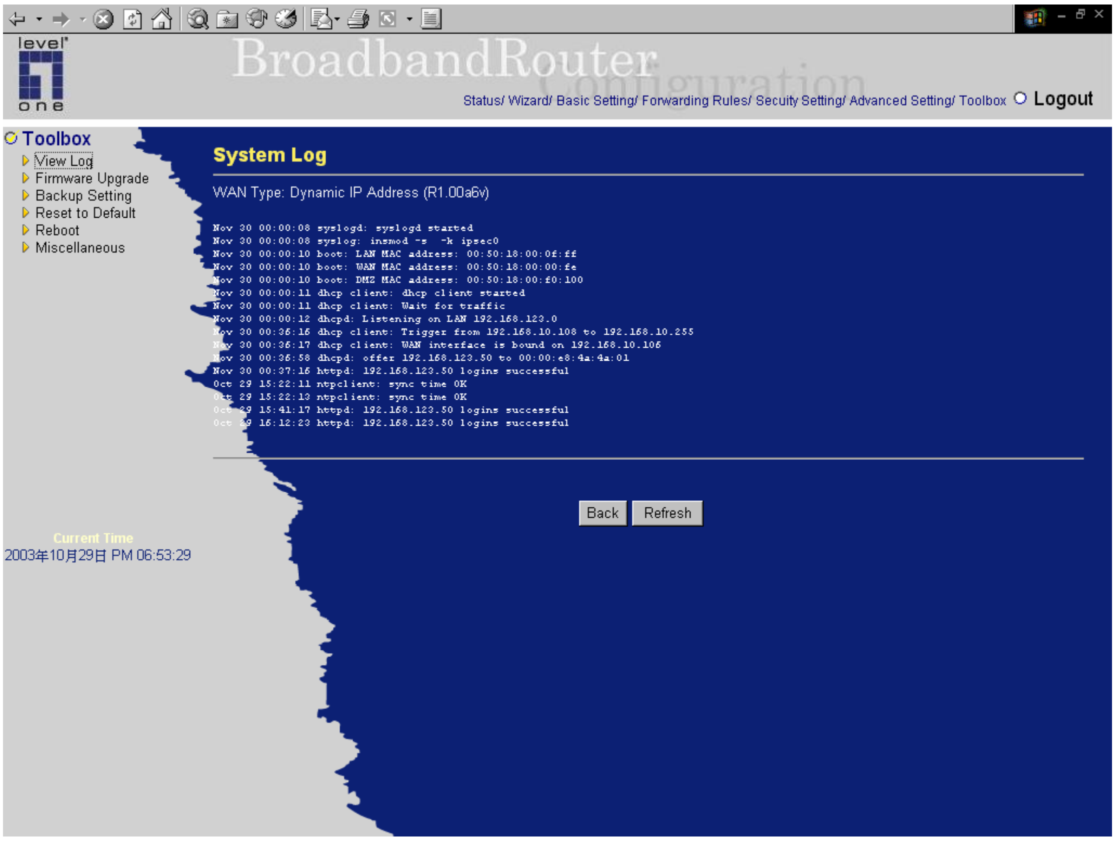
Backup Setting
- Save the settings of this device to a file.

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.

4.8.1 View log


level one
BroadbandRouter Configuration
Status/ Wizard/ Basic Setting/ Forwarding Rules/ Secuity Setting/ Advanced Setting/ Toolbox
Logout
Toolbox
View Log
Firmware Upgrade
Backup Setting
Reset to Default
Reboot
Miscellaneous
Back
Refresh
Current Time
2003年10月29日 PM 06:53:29

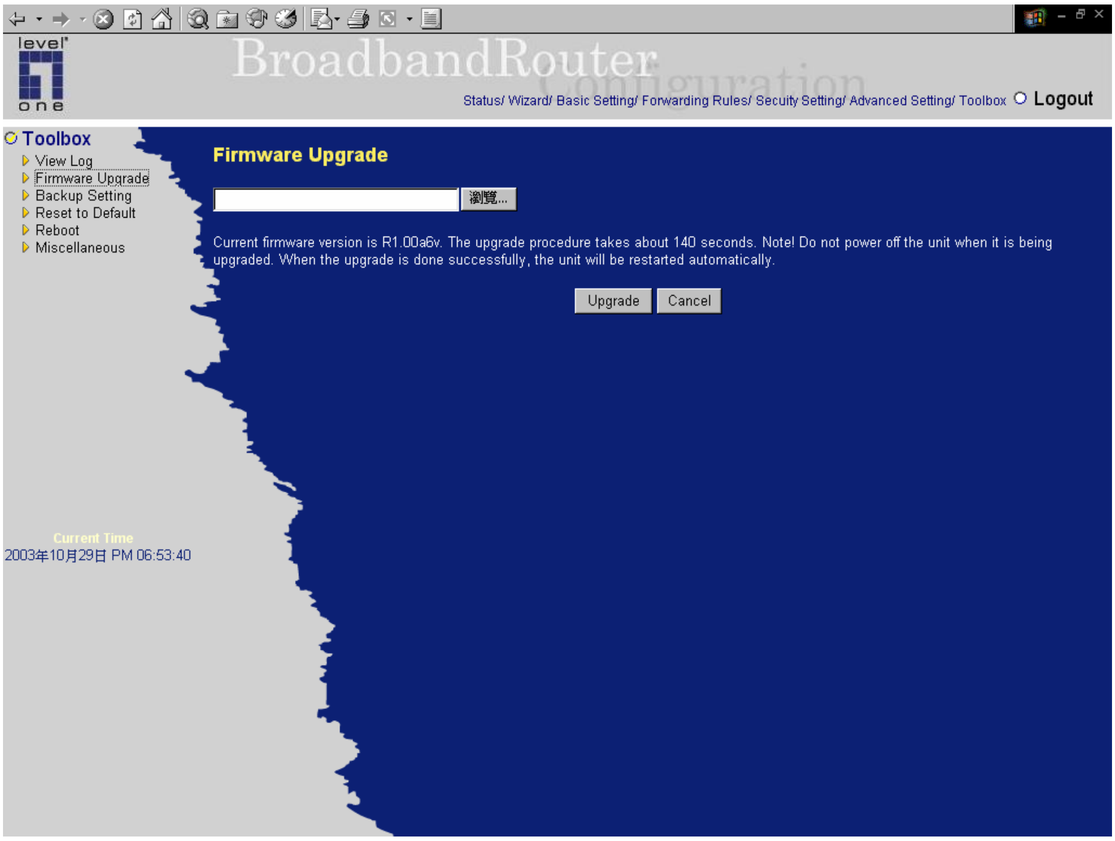
System Log

WAN Type: Dynamic IP Address (R1.00a6v)

```
Nov 30 00:00:08 syslogd: syslogd started
Nov 30 00:00:08 syslog: insmod -s  -k ipsec0
Nov 30 00:00:10 boot: LAN MAC address: 00:50:18:00:0f:ff
Nov 30 00:00:10 boot: WAN MAC address: 00:50:18:00:00:fe
Nov 30 00:00:10 boot: DMZ MAC address: 00:50:18:00:f0:100
Nov 30 00:00:11 dhcp client: dhcp client started
Nov 30 00:00:11 dhcp client: Wait for traffic
Nov 30 00:00:12 dhcpd: Listening on LAN 192.168.123.0
Nov 30 00:36:16 dhcp client: Trigger from 192.168.10.108 to 192.168.10.255
Nov 30 00:36:17 dhcp client: WAN interface is bound on 192.168.10.106
Nov 30 00:36:58 dhcpd: offer 192.168.123.50 to 00:00:e8:4a:4a:01
Nov 30 00:37:16 httpd: 192.168.123.50 logins successful
Oct 29 15:22:11 ntpclient: sync time OK
Oct 29 15:22:13 ntpclient: sync time OK
Oct 29 15:41:17 httpd: 192.168.123.50 logins successful
Oct 29 16:12:23 httpd: 192.168.123.50 logins successful
```

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

4.8.2 Firmware Upgrade

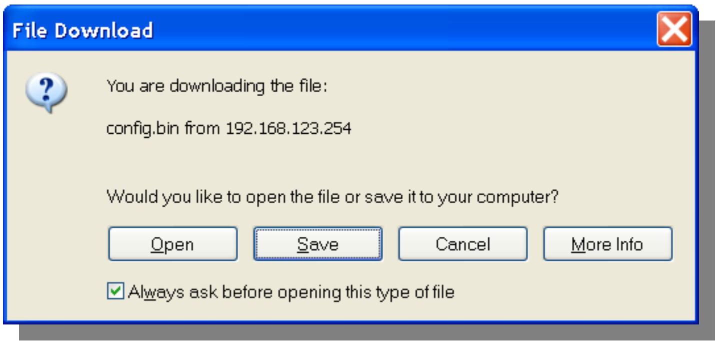

level one
BroadbandRouter Configuration
Status/ Wizard/ Basic Setting/ Forwarding Rules/ Secuity Setting/ Advanced Setting/ Toolbox
Logout
Toolbox
View Log
Firmware Upgrade
Backup Setting
Reset to Default
Reboot
Miscellaneous
瀏覽...
Upgrade
Cancel
Current Time
2003年10月29日 PM 06:53:40

Firmware Upgrade

Current firmware version is R1.00a6v. The upgrade procedure takes about 140 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:

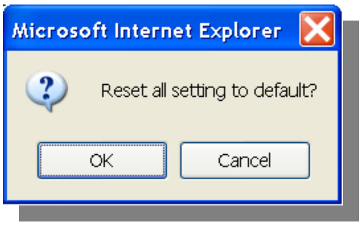
config.bin from 192.168.123.254

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

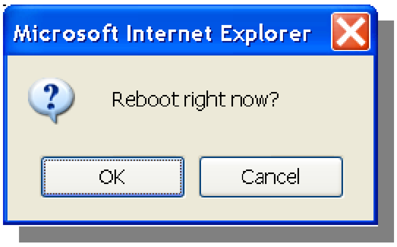


Microsoft Internet Explorer

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

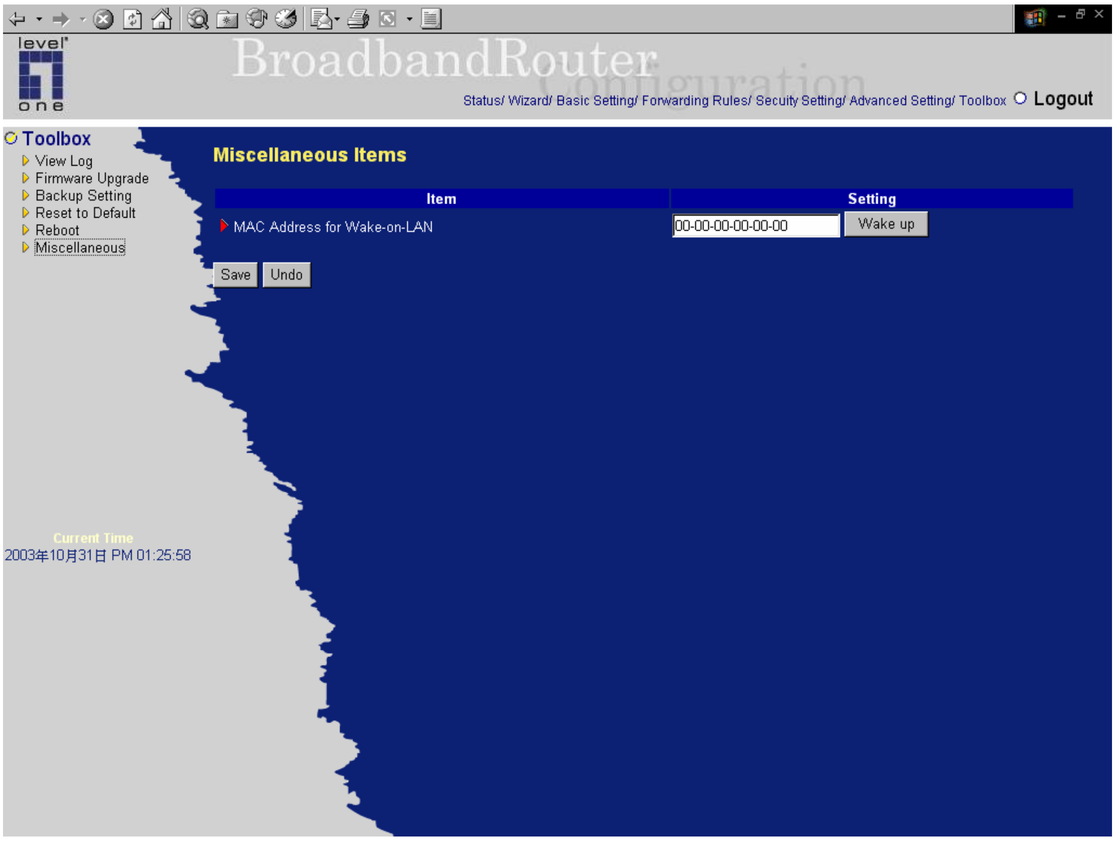


Microsoft Internet Explorer

Reboot right now?

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

4.8.6 Miscellaneous Items


BroadbandRouter Configuration
Status/ Wizard/ Basic Setting/ Forwarding Rules/ Secuity Setting/ Advanced Setting/ Toolbox
Logout
Toolbox
View Log
Firmware Upgrade
Backup Setting
Reset to Default
Reboot
Miscellaneous
Current Time
2003年10月31日 PM 01:25:58
Wake up
Save
Undo

Miscellaneous Items

Item	Setting
MAC Address for Wake-on-LAN	00-00-00-00-00-00

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.

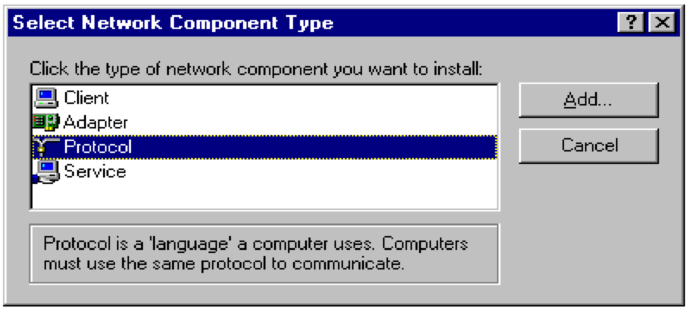
Appendix A: TCP/IP Configuration for Windows 95/98 back

Table of Contents

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.

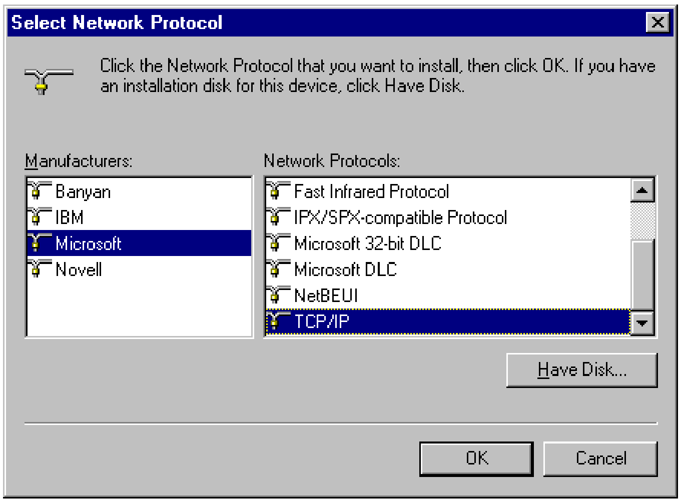


Select Network Component Type

Click the type of network component you want to install:

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.



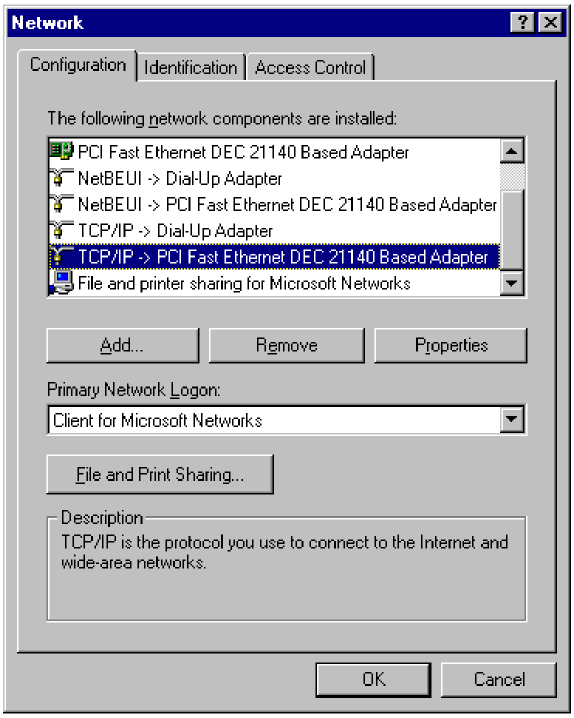
Select Network Protocol

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

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.



Network

Configuration | Identification | Access Control

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

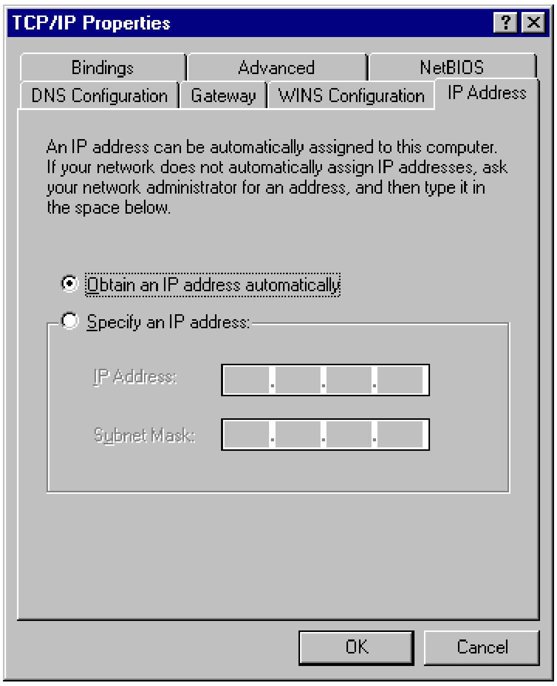
Description
TCP/IP is the protocol you use to connect to the Internet and wide-area networks.

3. Click ***Properties*** button to set the TCP/IP protocol for this NAT Router.

4. Now, you have two setting methods:

   A. Get IP via DHCP server

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



TCP/IP Properties

Bindings | Advanced | NetBIOS
DNS Configuration | Gateway | WINS Configuration | IP Address

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.

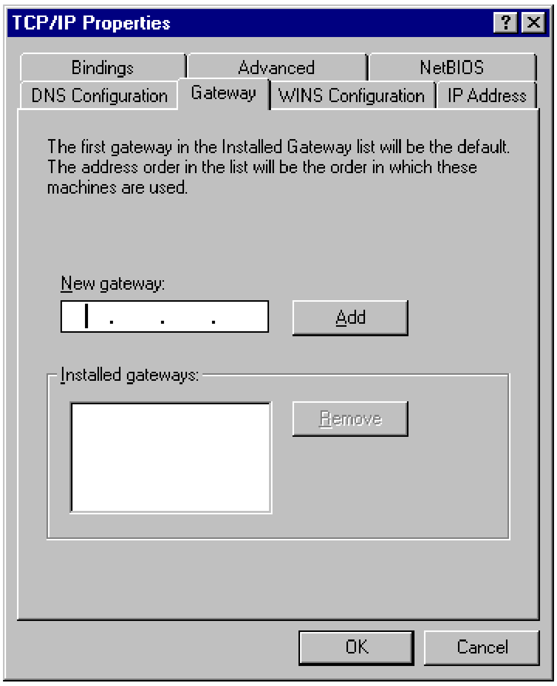
● Obtain an IP address automatically

○ Specify an IP address:

IP Address: . . .

Subnet Mask: . . .

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



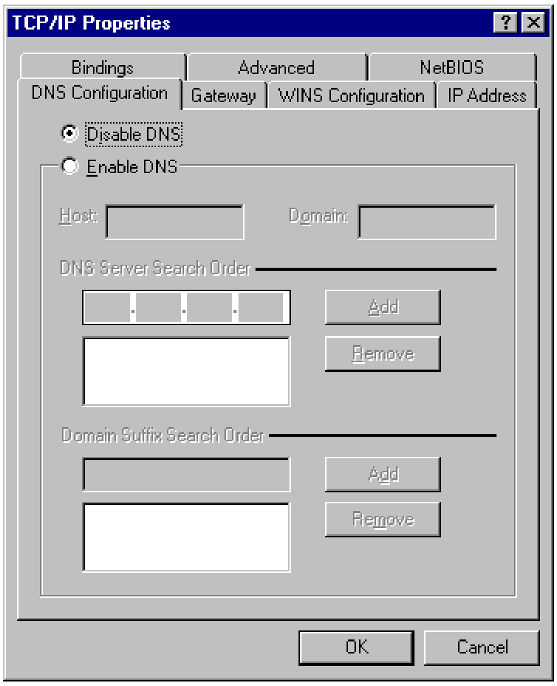
TCP/IP Properties

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: . . .

Installed gateways:

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



TCP/IP Properties

● Disable DNS

○ Enable DNS

Host:

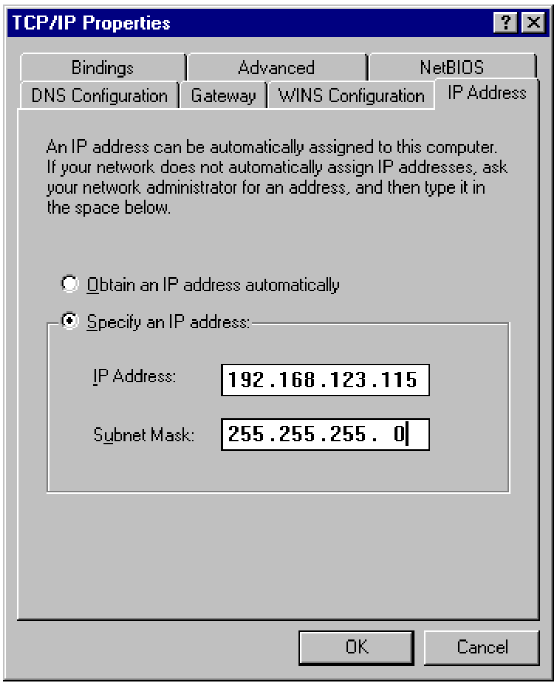
Domain:

DNS Server Search Order

Domain Suffix Search Order

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.

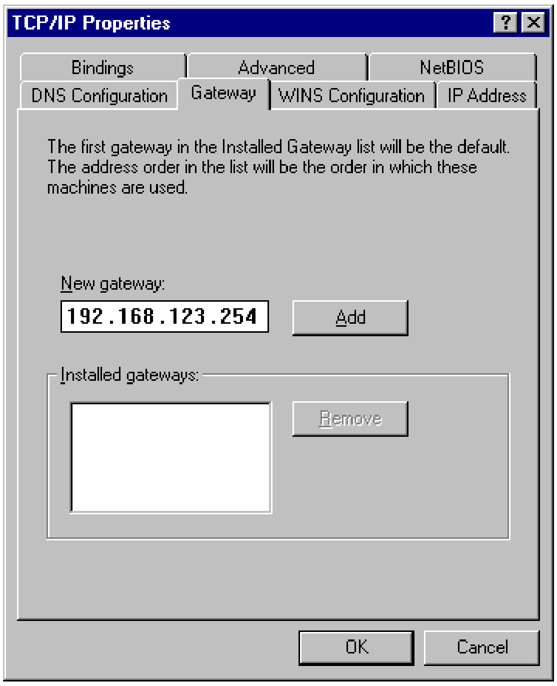
○ Obtain an IP address automatically

● 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.

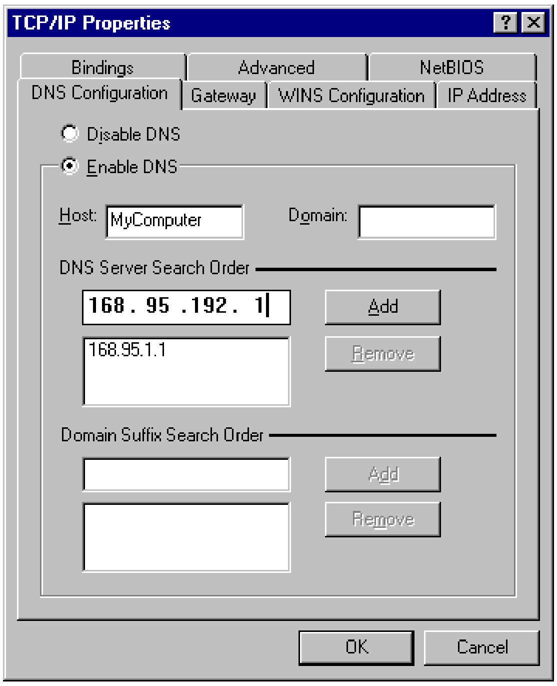


The first gateway in the Installed Gateway list will be the default. The address order in the list will be the order in which these machines are used.

New gateway: 192.168.123.254

Installed gateways:

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

Domain Suffix Search Order