

User's Manual

Copyright

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

Trademarks

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

FCC Interference Statement

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

CE Declaration of Conformity

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

The specification is subject to change without notice.

Table of Contents

Chapter 1	Introduction	3
	Functions and Features.....	3
	Packing List	5
Chapter 2	Hardware Installation.....	6
	2.1 Panel Layout	6
	2.2 Procedure for Hardware Installation	8
Chapter 3	Network Settings and Software Installation.....	9
	3.1 Make Correct Network Settings of Your Computer.....	9
Chapter 4	Configuring Broadband Router	10
	4.1 Start-up and Log in.....	11
	4.2 Status	12
	4.3 Wizard.....	13
	4.4 Basic Setting	14
	4.5 Forwarding Rules	21
	4.6 Security Settings	25
	4.7 Advanced Settings	39
	4.8 Toolbox	51
Appendix A	TCP/IP Configuration for Windows 95/98	56
Appendix B	FAQ and Troubleshooting	62
	Reset to factory Default.....	62

Chapter 1 Introduction

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

Functions and Features

Router Basic functions

I Broadband modem and NAT Router

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

I Auto-sensing Ethernet Switch

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

I Wan type supported

The router supports some wan types, Static ,Dynamic, PPPOE ,PPTP , Dynamic IP with Road Runner.

I Firewall

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

I DHCP server supported

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

I Web-based configuring

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

I Virtual Server supported

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

I User-Definable Application Sensing Tunnel

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

I DMZ Host supported

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

I Statistics of WAN Supported

Enables you to monitor inbound and outbound packets

Security functions

I Packet filter supported

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

I Domain Filter Supported

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

I URL Blocking Supported

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

I VPN Pass-through

The router also support vpn pass-through.

I SPI Mode Supported

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

I DoS Attack Detection Supported

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

Advanced functions

I System time Supported

Allow you to synchronize system time with network time server.

I E-mail Alert Supported

The router can send its info by mail.

I Dynamic dns Supported

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

I SNMP Supported

The router supports basic snmp function.

I Routing Table Supported

Now, the router supports static routing.

I Schedule Rule supported

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

Other functions

I UPNP (Universal Plug and Play) Supported

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

Packing List

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

Chapter 2 Hardware Installation

2.1 Panel Layout

2.1.1. Front Panel

LED:

LED	Function	Color	Status	Description
POWER	Power indication	Green	On	Power is being applied to this product.
Status	System status indicators	Green	Blinking	M1 is flashed once per second to indicate system is alive. When system is busy, M2 is lighted.
WAN	WAN port activity	Green	On	The WAN port is linked.
			Blinking	The WAN port is sending or receiving data.
Reset	M1	Green	Flashing	To reset system settings to factory defaults
Link/Act. 1~4	Link status	Green	On	An active station is connected to the corresponding LAN port.
			Blinking	The corresponding LAN port is sending or receiving data.
10/100	Data Rate	Green	On	Data is transmitting in 100Mbps on the corresponding LAN port.

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

2.1.2. Rear Panel

Ports:

Port	Description
9VAC	Power inlet: AC9V, 1A
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 Procedure for Hardware Installation

1. Decide where to place your Broadband Router

You can place your Broadband Router on a desk or other flat surface, or you can mount it on a wall. For optimal performance, place your Broadband Router in the center of your office (or your home) in a location that is away from any potential source of interference, such as a metal wall or microwave oven. This location must be close to power and network connection.

1. Setup LAN connection

- a. **Wired LAN connection:** connects an Ethernet cable from your computer's Ethernet port to one of the LAN ports of this product.

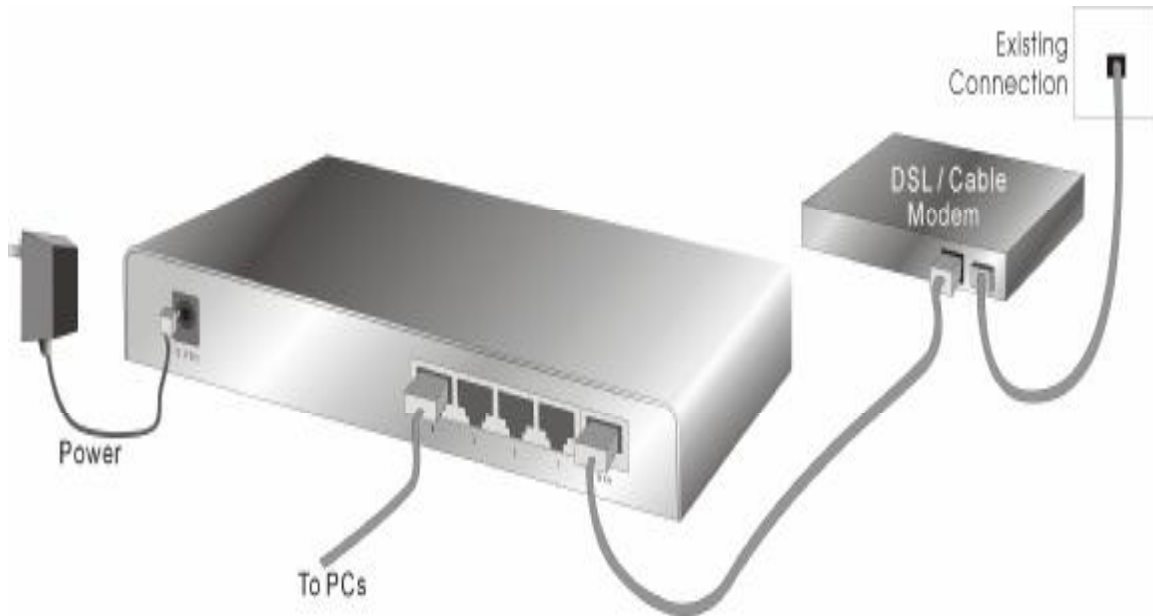


Figure 2-3 Setup of LAN and WAN connections for this product.

3. Setup WAN connection

Prepare an Ethernet cable for connecting this product to your cable/xDSL modem or Ethernet backbone. Figure 2-3 illustrates the WAN connection.

4. 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&M2 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?

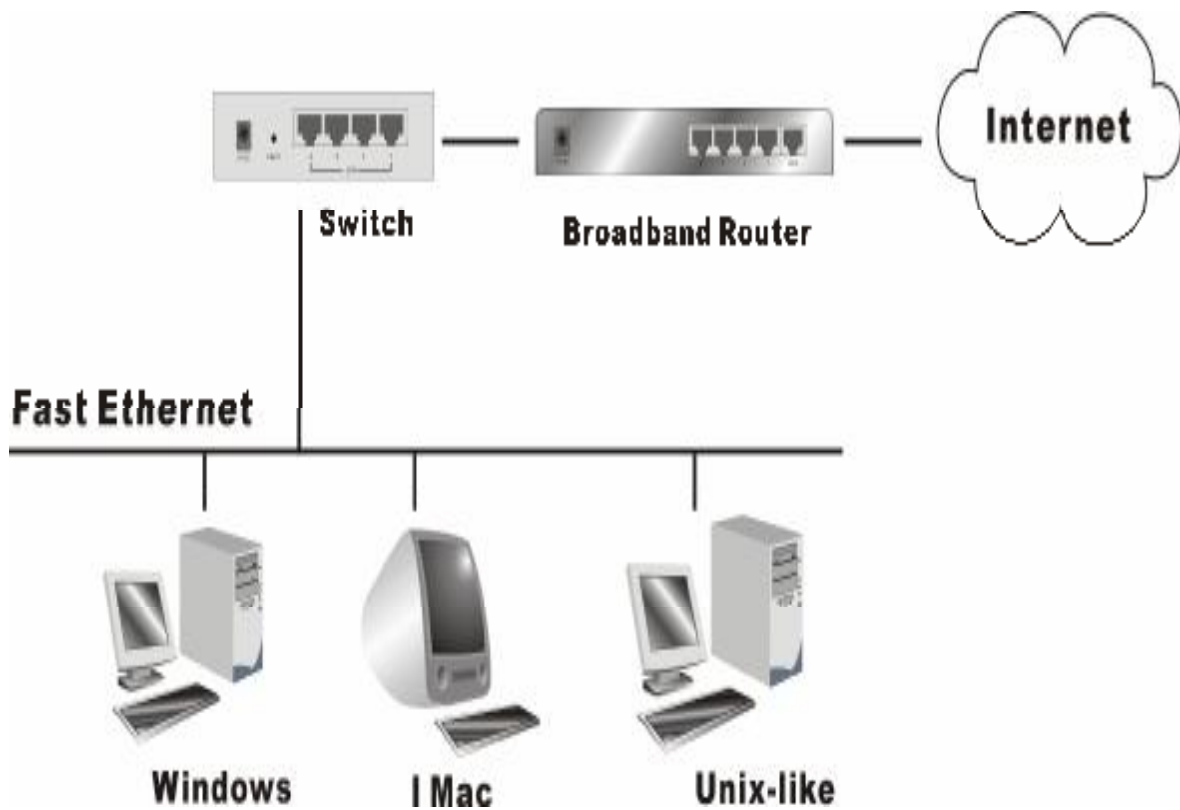
Tip: The LAN LED of this product and the link LED of network card on your computer must be lighted.

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.

Chapter 4 Configuring Broadband Router

This product provides Web based configuration scheme, that is, configuring by your Web browser, such as Netscape Communicator or Internet Explorer. This approach can be adopted in any MS Windows, Macintosh or UNIX based platforms.



4.1 Start-up and Log in

The screenshot shows the Administrator's Main Menu on the left and the System Status page on the right. The menu includes links for Status, Wizard, Basic Setting, Forwarding Rules, Security Setting, Advanced Setting, and Toolbox, along with a Log out button. The System Status page displays three tables: WAN Status, Peripheral Status, and Statistics of WAN. The WAN Status table shows Remaining Lease Time, IP Address, Subnet Mask, Gateway, and Domain Name Server. The Peripheral Status table shows a Printer that is Not ready. The Statistics of WAN table shows Octets, Unicast Packets, and Non-unicast Packets for both Inbound and Outbound directions. At the bottom, there are buttons for View Log..., Clients List..., Help, and Refresh, and the Device Time is shown as Thu Oct 09 00:02:29 2003.

Administrator's Main Menu

- [Status](#)
- [Wizard](#)
- + [Basic Setting](#)
- + [Forwarding Rules](#)
- + [Security Setting](#)
- + [Advanced Setting](#)
- + [Toolbox](#)

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	

Item	Peripheral Status	Sidenote
Printer	Not ready	

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

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

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

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

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

4.2 Status

Administrator's Main Menu

- [Status](#)
- [Wizard](#)
- + [Basic Setting](#)
- + [Forwarding Rules](#)
- + [Security Setting](#)
- + [Advanced Setting](#)
- + [Toolbox](#)

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	

Item	Peripheral Status	Sidenote
Printer	Not ready	

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

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

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

- . 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.

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

4.3 Wizard

Administrator's Main Menu

- [Status](#)
- [Wizard](#)

+ [Basic Setting](#)

+ [Forwarding Rules](#)

+ [Security Setting](#)

+ [Advanced Setting](#)

+ [Toolbox](#)

Log out

Setup Wizard

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

Next >

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

Administrator's Main Menu

- [Status](#)
- [Wizard](#)

+ [Basic Setting](#)

+ [Forwarding Rules](#)

+ [Security Setting](#)

+ [Advanced Setting](#)

+ [Toolbox](#)

Log out

Setup Wizard - Select WAN Type

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

< Back Undo Next >

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

4.4 Basic Setting

Administrator's Main Menu

- [Status](#)
- [Wizard](#)
- + [Basic Setting](#)
- + [Forwarding Rules](#)
- + [Security Setting](#)
- + [Advanced Setting](#)
- + [Toolbox](#)

[Log out](#)

Basic Setting

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

4.4.1 Primary Setup – WAN Type, Virtual Computers

The screenshot shows the 'Administrator's Main Menu' on the left and the 'Primary Setup' configuration page on the right. The menu includes options like Status, Wireless, Basic Setting, Primary Setup, DHCP Server, Wireless, Change Password, Forwarding Rules, Security Setting, Advanced Setting, and Tools. The Primary Setup page contains a table with the following items and settings:

Item	Setting
▶ LAN IP Address	[192.168.1.254]
▶ WAN Type	Dynamic IP Address <input type="button" value="Change.."/>
▶ Host Name	[] (optional)
▶ WAN MAC Address	[11:11:11:11:11:11] <input type="button" value="Restore MAC"/>
▶ Renew IP Forever	<input type="checkbox"/> Enable (Auto renew IP)

At the bottom of the Primary Setup page, there are buttons for 'Save', 'On/Off', 'Virtual Computers', and '- dp'.

Press “Change”

The screenshot shows the 'Administrator's Main Menu' on the left and the 'Choose WAN Type' configuration page on the right. The menu is similar to the previous screenshot, with 'Primary Setup' selected. The Choose WAN Type page contains a table with the following types and usages:

Type	Usage
<input type="radio"/> Static IP Address	ISP requires you to static IP address
<input checked="" type="radio"/> Dynamic IP Address	Obtain an IP address from ISP automatically
<input type="radio"/> Dynamic IP Address with Road Runner Session Management (e.g., Telstra BigPond)	
<input type="radio"/> PPP over Ethernet	Some ISPs require the use of PPPoE to connect to their services.
<input type="radio"/> PPTP	Some ISPs require the use of PPTP to connect to their services.

At the bottom of the Choose WAN Type page, there are buttons for 'Save' and 'Cancel'.

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

4.4.1.1 Static IP Address

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

4.4.1.2 Dynamic IP Address

1. Host Name: optional. Required by some ISPs, for example, @Home.
2. Renew IP Forever: this feature enables this product to renew your IP address automatically when the lease time is expiring-- even when the system is idle.

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

1. LAN IP Address is the IP address of this product. It must be the default gateway of your computers.
2. WAN Type is Dynamic IP Address. If the WAN type is not correct, change it!
3. Host Name: optional. Required by some ISPs, e.g. @Home.
4. Renew IP Forever: this feature enable this product renew IP address automatically when the lease time is being expired even the system is in idle state.

4.4.1.4 PPP over Ethernet

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

Set it to zero or enable Auto-reconnect to disable this feature.

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

MTU value is 1492.

4.4.1.5 PPTP

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

Administrator's Main Menu

- [Status](#)
- [Wizard](#)
- [Basic Setting](#)
 - [Primary Setup](#)
 - [DHCP Server](#)
 - [Wireless](#)
 - [Change Password](#)
- + [Forwarding Rules](#)
- + [Security Setting](#)
- + [Advanced Setting](#)
- + [Trunking](#)

Primary Setup

Item	Setting
▶ WAN IP Address	192.168.1.20.254
▶ WAN Type	PPTP <input type="button" value="Change..."/>
▶ My IP Address	10.0.0.140
▶ My Subnet Mask	255.255.255.0
▶ Server IP Address	10.0.0.1
▶ PPTP Account	<input type="text"/>
▶ PPTP Password	<input type="text"/>
▶ Connection ID	<input type="text"/> (optional)
▶ Maximum Idle Time	300 <input type="checkbox"/> seconds <input type="checkbox"/> Auto-reconnect

Saved! The change doesn't take effect until reboot.

4.4.1.7 Virtual Computers

The screenshot shows the 'Administrator's Main Menu' on the left and the 'Virtual Computers' configuration page on the right. The menu includes options like Status, Wizard, Basic Setting, Primary Setup, DHCP Server, WAN, Change Password, Forwarding Rules, Security Setting, Advanced Netting, and Toolbox. The 'Virtual Computers' page features a table with columns for ID, Global IP, Local IP, and Enable. Below the table are 'Save', 'Undo', and 'Help' buttons.

ID	Global IP	Local IP	Enable
1	<input type="text"/>	192.168.23 <input type="text"/>	<input type="checkbox"/>
2	<input type="text"/>	192.168.122 <input type="text"/>	<input checked="" type="checkbox"/>
3	<input type="text"/>	192.168.122 <input type="text"/>	<input type="checkbox"/>
4	<input type="text"/>	192.168.23 <input type="text"/>	<input type="checkbox"/>
5	<input type="text"/>	192.168.122 <input type="text"/>	<input checked="" type="checkbox"/>

Save Undo Help

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

Item	Setting
DHCP Server	<input type="radio"/> Disable <input checked="" type="radio"/> Enable
Lease Time	440 Minutes
IP Pool Starting Address	100
IP Pool Ending Address	199
Domain Name	amit.com
Primary DNS	192.168.123.20
Secondary DNS	198.51.101
Primary WINS	192.168.123.3
Secondary WINS	192.168.123.100
Gateway	1111.1 (optional)

Press “More>>”

The settings of a TCP/IP environment include host IP, Subnet Mask, Gateway, and DNS configurations. It is not easy to manually configure all the computers and devices in your network. Fortunately, DHCP Server provides a rather simple approach to handle all these settings. This product supports the function of DHCP server. If you enable this product’s DHCP server and configure your computers as “automatic IP allocation” mode, then when your computer is powered on, it will automatically load the proper TCP/IP settings from this product. The settings of DHCP server include the following items:

1. **DHCP Server:** Choose “Disable” or “Enable.”
2. **Lease Time:** this feature allows you to configure IP’s lease time (DHCP client).
3. **IP pool starting Address/ IP pool starting Address:** Whenever there is a request, the DHCP server will automatically allocate an unused IP address from the IP address pool to the requesting computer. You must specify the starting and ending address of the IP address pool.
4. **Domain Name:** Optional, this information will be passed to the client.
5. **Primary DNS/Secondary DNS:** This feature allows you to assign DNS Servers
6. **Primary WINS/Secondary WINS:** This feature allows you to assign WINS Servers
7. **Gateway:** The Gateway Address would be the IP address of an alternate Gateway.

This function enables you to assign another gateway to your PC, when DHCP server offers an

IP to your PC.

4.4.4 Change Password

The screenshot shows the 'Change Password' page. On the left is a blue sidebar titled 'Administrator's Main Menu' containing links for 'Status', 'Wizard', 'Basic Setting', 'Firewall Setup', 'DHCP Server', 'Wireless', 'Change Password', 'Forwarding Rules', 'Security Setting', 'Advanced Setting', and 'Toolbox'. A 'Log Out' button is at the bottom of the sidebar. The main content area is titled 'Change Password' and features a table with two columns: 'Item' and 'Setting'. The table contains three rows: 'Old Password', 'New Password', and 'Reconfirm', each with an adjacent text input field. Below the table are 'Save' and 'Cancel' buttons.

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

Save Cancel

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

4.5 Forwarding Rules

Administrator's Main Menu

- [Status](#)
- [Wizard](#)
- + [Basic Setting](#)
- [Forwarding Rules](#)
 - [Virtual Server](#)
 - [Special AP](#)
 - [Miscellaneous](#)
- + [Security Setting](#)
- + [Advanced Setting](#)
- + [Toolbox](#)

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.
 - Host Address of FTP port: You have to configure this item if you want to access an FTP server whose port number is not 21 (default value is 21).

4.5.1 Virtual Server

Administrator's Main Menu

- [Status](#)
- [Wizard](#)
- + [Basic Setting](#)
- [Forwarding Rules](#)
 - [Virtual Server](#)
 - [Special AP](#)
 - [Miscellaneous](#)
- + [Security Setting](#)
- + [Advanced Setting](#)
- + [Toolbox](#)

Virtual Server

ID	Service Ports	Server IP	Enable	Use Rule
1	<input type="text"/>	192.168.0.3 <input type="text"/>	<input type="checkbox"/>	<input type="checkbox"/>
2	<input type="text"/>	192.168.1.25 <input type="text"/>	<input type="checkbox"/>	<input type="checkbox"/>
3	<input type="text"/>	192.168.1.23 <input type="text"/>	<input type="checkbox"/>	<input type="checkbox"/>
4	<input type="text"/>	192.168.0.3 <input type="text"/>	<input type="checkbox"/>	<input type="checkbox"/>
5	<input type="text"/>	192.168.1.25 <input type="text"/>	<input type="checkbox"/>	<input type="checkbox"/>
6	<input type="text"/>	192.168.1.23 <input type="text"/>	<input type="checkbox"/>	<input type="checkbox"/>
7	<input type="text"/>	192.168.0.3 <input type="text"/>	<input type="checkbox"/>	<input type="checkbox"/>
8	<input type="text"/>	192.168.1.25 <input type="text"/>	<input type="checkbox"/>	<input type="checkbox"/>
9	<input type="text"/>	192.168.1.23 <input type="text"/>	<input type="checkbox"/>	<input type="checkbox"/>
10	<input type="text"/>	192.168.0.3 <input type="text"/>	<input type="checkbox"/>	<input type="checkbox"/>
11	<input type="text"/>	192.168.1.25 <input type="text"/>	<input type="checkbox"/>	<input type="checkbox"/>
12	<input type="text"/>	192.168.1.23 <input type="text"/>	<input type="checkbox"/>	<input type="checkbox"/>
13	<input type="text"/>	192.168.0.3 <input type="text"/>	<input type="checkbox"/>	<input type="checkbox"/>
14	<input type="text"/>	192.168.1.25 <input type="text"/>	<input type="checkbox"/>	<input type="checkbox"/>
15	<input type="text"/>	192.168.1.23 <input type="text"/>	<input type="checkbox"/>	<input type="checkbox"/>

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

Administrator's Main Menu

- Status
- Wizard
- Basic Setting
- Forwarding Rules
 - Virtual Server
 - Special AP
 - Miscellaneous
- Security Setting
- Advanced Setting
- Toolbox

Log out

Special Applications

ID	Trigger	Incoming Ports	Enable
1	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
2	<input type="text"/>	<input type="text"/>	<input checked="" type="checkbox"/>
3	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
4	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
5	<input type="text"/>	<input type="text"/>	<input checked="" type="checkbox"/>
6	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
7	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
8	<input type="text"/>	<input type="text"/>	<input checked="" type="checkbox"/>

Popular applications:

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

Administrator's Main Menu

- Status
- Wizard
- Basic Setting
- Forwarding Rules
 - Virtual Server
 - Special AP
 - Virtual IP
- Security Setting
- Advanced Setting
- Trunkless

Miscellaneous Items

Item	Setting	Enable
▶ IP Address of DMZ host	192.168.133.	<input type="checkbox"/>
▶ Non-standard FTP port		

Save Undo Help

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

Administrator's Main Menu

- [Status](#)
- [Wizard](#)

+ [Basic Setting](#)

+ [Forwarding Rules](#)

- [Security Setting](#)

- [Packet Filters](#)
- [Domain Filters](#)
- [URL Blocking](#)
- [MAC Control](#)
- [VPN](#)
- [Miscellaneous](#)

+ [Advanced Setting](#)

+ [Toolbox](#)

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**
 - VPN Settings are used to create virtual private tunnels to remote VPN gateways.
- **Miscellaneous**
 - Remote Administrator Host: In general, only Intranet user can browse the built-in web pages to perform administration task. This feature enables you to perform administration task from remote host.
 - Administrator Time-out: The amount of time of inactivity before the device will automatically close the Administrator session. Set this to zero to disable it.
 - Discard PING from WAN side: When this feature is enabled, hosts on the WAN cannot ping the Device.

4.6.1 Packet Filter

Administrator's Main Menu

- [Status](#)
- [Wizard](#)
- [+ Basic Setting](#)
- [+ Forwarding Rules](#)
- [- Security Setting](#)
 - [Packet Filters](#)
 - [Domain Filters](#)
 - [URL Blocking](#)
 - [MAC Control](#)
 - [VPN](#)
 - [Miscellaneous](#)
- [+ Advanced Setting](#)
- [+ Toolbox](#)

Outbound Packet Filter

Item	Setting
▶ Outbound Filter	<input type="checkbox"/> Enable
	<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	Use Rule#
1	<input type="text"/> : <input type="text"/>	<input type="text"/> : <input type="text"/>	<input type="checkbox"/>	<input type="text"/>
2	<input type="text"/> : <input type="text"/>	<input type="text"/> : <input type="text"/>	<input type="checkbox"/>	<input type="text"/>
3	<input type="text"/> : <input type="text"/>	<input type="text"/> : <input type="text"/>	<input type="checkbox"/>	<input type="text"/>
4	<input type="text"/> : <input type="text"/>	<input type="text"/> : <input type="text"/>	<input type="checkbox"/>	<input type="text"/>
5	<input type="text"/> : <input type="text"/>	<input type="text"/> : <input type="text"/>	<input type="checkbox"/>	<input type="text"/>
6	<input type="text"/> : <input type="text"/>	<input type="text"/> : <input type="text"/>	<input type="checkbox"/>	<input type="text"/>
7	<input type="text"/> : <input type="text"/>	<input type="text"/> : <input type="text"/>	<input type="checkbox"/>	<input type="text"/>
8	<input type="text"/> : <input type="text"/>	<input type="text"/> : <input type="text"/>	<input type="checkbox"/>	<input type="text"/>

(00)Always ID --

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

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

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

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

For source or destination IP address, you can define a single IP address (4.3.2.1) or a range of IP addresses (4.3.2.1-4.3.2.254). An empty implies all IP addresses.

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

Each rule can be enabled or disabled individually.

Inbound Filter:

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

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

Example 1:

Administrator's Main Menu

- Status
- Wizard
- 1 Basic Setting
- + Forwarding Rules
- Security Setting
 - Packet Filters
 - Domain Filter
 - Firewall Blocking
 - MAC Control
 - VPN
 - Miscellaneous
- 1 Advanced Setting
- + Trunkless

Outbound Packet Filter

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

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

Schedule rule: **Always** [Down Arrow]

(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:

Administrator's Main Menu

- [Status](#)
- [WinBox](#)
- + [Basic Setting](#)
- | [Forwarding Rules](#)
- Security Setting
 - [Packet Filter](#)
 - [Connair Filter](#)
 - [URL Filtering](#)
 - [MAC Control](#)
 - [VFI](#)
 - Miscellaneous
- + [Advanced Setting](#)
- | [Toolbox](#)
-

Outbound Packet Filter

Outbound Filter **Enable**

Allow all to pass except those match the following rules
 Deny all to pass except those match the following rules

ID	Source IP : Ports	Destination IP : Ports	Enable	Use Rule#
1	1.2.3.10-119 : 21		<input checked="" type="checkbox"/>	1
2	1.2.3.100-1.2.3.119	119	<input checked="" type="checkbox"/>	2
3			<input type="checkbox"/>	3
4			<input type="checkbox"/>	4
5			<input type="checkbox"/>	5
6			<input type="checkbox"/>	6
7			<input type="checkbox"/>	7
8			<input type="checkbox"/>	8

(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 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	Use Rule#
1	192.168.123.149 : <input type="text"/>	<input type="text"/> : 25-110	<input checked="" type="checkbox"/>	<input type="text" value="0"/>
2	192.168.123.20 : <input type="text"/>	<input type="text"/> : <input type="text"/>	<input checked="" type="checkbox"/>	<input type="text" value="0"/>
3	<input type="text"/> : <input type="text"/>	<input type="text"/> : <input type="text"/>	<input type="checkbox"/>	<input type="text" value="0"/>
4	<input type="text"/> : <input type="text"/>	<input type="text"/> : <input type="text"/>	<input type="checkbox"/>	<input type="text" value="0"/>
5	<input type="text"/> : <input type="text"/>	<input type="text"/> : <input type="text"/>	<input type="checkbox"/>	<input type="text" value="0"/>
6	<input type="text"/> : <input type="text"/>	<input type="text"/> : <input type="text"/>	<input type="checkbox"/>	<input type="text" value="0"/>
7	<input type="text"/> : <input type="text"/>	<input type="text"/> : <input type="text"/>	<input type="checkbox"/>	<input type="text" value="0"/>
8	<input type="text"/> : <input type="text"/>	<input type="text"/> : <input type="text"/>	<input type="checkbox"/>	<input type="text" value="0"/>

Schedule rule (00)Always Copy to ID --

Save
Undo
Inbound Filter...
MAC Level...
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 <input checked="" type="checkbox"/> Enable				
<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	Use Rule#
1	192.168.123.100 : <input type="text"/>	<input type="text"/> : 25	<input checked="" type="checkbox"/>	<input type="text" value="0"/>
2	192.168.123.119 : <input type="text"/>	<input type="text"/> : 119	<input checked="" type="checkbox"/>	<input type="text" value="0"/>
3	<input type="text"/> : <input type="text"/>	<input type="text"/> : <input type="text"/>	<input type="checkbox"/>	<input type="text" value="0"/>
4	<input type="text"/> : <input type="text"/>	<input type="text"/> : <input type="text"/>	<input type="checkbox"/>	<input type="text" value="0"/>
5	<input type="text"/> : <input type="text"/>	<input type="text"/> : <input type="text"/>	<input type="checkbox"/>	<input type="text" value="0"/>
6	<input type="text"/> : <input type="text"/>	<input type="text"/> : <input type="text"/>	<input type="checkbox"/>	<input type="text" value="0"/>
7	<input type="text"/> : <input type="text"/>	<input type="text"/> : <input type="text"/>	<input type="checkbox"/>	<input type="text" value="0"/>
8	<input type="text"/> : <input type="text"/>	<input type="text"/> : <input type="text"/>	<input type="checkbox"/>	<input type="text" value="0"/>

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

Save Undo Inbound Filter... MAC Level... Help

(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

Administrator's Main Menu

- [Status](#)
- [Wizard](#)
- [Basic Setting](#)
- [Forwarding Rules](#)
- [Security Setting](#)
 - [Packet Filters](#)
 - [Domain Filters](#)
 - [URL Blocking](#)
 - [MAC Control](#)
 - [VPN](#)
 - [Miscellaneous](#)
- [Advanced Setting](#)
- [Toolbox](#)

[Log out](#)

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"/> To: <input type="text"/>

ID	Domain Suffix	Action	Enable
1	<input type="text" value="www.msn.com"/>	<input checked="" type="checkbox"/> Drop <input checked="" type="checkbox"/> Log	<input checked="" type="checkbox"/>
2	<input type="text"/>	<input type="checkbox"/> Drop <input type="checkbox"/> Log	<input type="checkbox"/>
3	<input type="text"/>	<input type="checkbox"/> Drop <input type="checkbox"/> Log	<input 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	<input type="text" value="*.cherry"/>	<input type="checkbox"/> Drop <input type="checkbox"/> Log	<input type="checkbox"/>

[Save](#) [Undo](#) [Help](#)

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:

Administrator's Main Menu

- [Status](#)
- [WinBox](#)
- + [Basic Setting](#)
- | [Forwarding Rules](#)
- Security Setting
 - [Packet Filter](#)
 - [Domain Filter](#)
 - [URL Filtering](#)
 - [MAC Control](#)
 - [VPN](#)
 - [Mangle](#)
- + [Advanced Setting](#)
- | [Toolbox](#)

Domain Filter

Item	Setting
▶ Domain Filter	<input checked="" type="checkbox"/> Enable
▶ Log DNS Query	<input checked="" type="checkbox"/> Enable
▶ Privilege IP Address Range	From <input type="text" value="1"/> to <input type="text" value="20"/>

ID	Domain Suffix	Action	Enable
1	<input type="text" value="www.msn.com"/>	<input checked="" type="checkbox"/> Drop <input checked="" type="checkbox"/> Log	<input checked="" type="checkbox"/>
2	<input type="text" value="www.sina.com"/>	<input type="checkbox"/> Drop <input checked="" type="checkbox"/> Log	<input checked="" type="checkbox"/>
3	<input type="text" value="www.google.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 other)	<input type="checkbox"/> Drop <input type="checkbox"/> Log	<input type="checkbox"/>

In this example:

1. URL include “www.msn.com” will be blocked, and the action will be record in log-file.
2. URL include “www.sina.com” will not be blocked, but the action will be record in log-file.
3. URL include “www.google.com” will be blocked, but the action will not be record in log-file.
4. IP address X.X.X.1~ X.X.X.20 can access network without restriction.

4.6.3 URL Blocking

Administrator's Main Menu

- [Status](#)
- [Wizard](#)
- + [Basic Setting](#)
- + [Forwarding Rules](#)
- [Security Setting](#)
 - [Port Filter](#)
 - [Domain Filter](#)
 - [URL Blocking](#)
 - [MAD Center](#)
 - [VPN](#)
 - [Miscellaneous](#)
- + [Advanced Setting](#)
- + [Toolbox](#)

URL Blocking

URL Blocking Enable

ID	URL	Enable
1	<input type="text"/>	<input type="checkbox"/>
2	<input type="text"/>	<input type="checkbox"/>
3	<input type="text"/>	<input type="checkbox"/>
4	<input type="text"/>	<input type="checkbox"/>
5	<input type="text"/>	<input type="checkbox"/>
6	<input type="text"/>	<input type="checkbox"/>
7	<input type="text"/>	<input type="checkbox"/>
8	<input type="text"/>	<input type="checkbox"/>
9	<input type="text"/>	<input type="checkbox"/>
10	<input type="text"/>	<input type="checkbox"/>

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.

Administrator's Main Menu

- [Status](#)
- [Wizard](#)
- [Basic Setting](#)
- [Forwarding Rules](#)
- [Security Setting](#)
 - [Packet Filter](#)
 - [Domain Filter](#)
 - [URL Blocking](#)
 - [MAC Control](#)
 - [VLAN](#)
 - [Miscellaneous](#)
- [Advanced Setting](#)
- [Toolbox](#)

URL Blocking

Term	Setting
▶ URL Blocking	<input checked="" type="checkbox"/> Enable

ID	URL	Enable
1	msn	<input checked="" type="checkbox"/>
2	sina	<input checked="" type="checkbox"/>
3	cnssi	<input checked="" type="checkbox"/>
4	espn	<input checked="" type="checkbox"/>
5		<input type="checkbox"/>
6		<input type="checkbox"/>
7		<input type="checkbox"/>
8		<input type="checkbox"/>
9		<input type="checkbox"/>
10		<input type="checkbox"/>

In this example:

1. URL include “msn” will be blocked, and the action will be record in log-file.
2. URL include “sina” will be blocked, but the action will be record in log-file
3. URL include “cnssi” will not be blocked, but the action will be record in log-file.
4. URL include “espn” will be blocked, but the action will be record in log-file

4.6.4 MAC Address Control

Administrator's Main Menu

- Home
- Wizard
- Basic Setting
- Forwarding Rules
- Security Setting**
 - Packet Filter
 - Access Control
 - IP Block
 - MAC Control**
 - VLAN
 - Access Control
- Advanced Setting
- Toolbox

MAC Address Control

Enable
 Connection control: Clients with IP that do not exist on our list. If selected, select "allow" or "deny" to allow or deny the clients, whose MAC addresses are not in the "Control table" to connect.

ID	MAC Address	IP Address	C
1	<input type="text"/>	192.168.1.1 <input type="text"/>	<input type="checkbox"/>
2	<input type="text"/>	192.168.1.2 <input type="text"/>	<input checked="" type="checkbox"/>
3	<input type="text"/>	192.168.1.3 <input type="text"/>	<input type="checkbox"/>
4	<input type="text"/>	192.168.1.4 <input type="text"/>	<input type="checkbox"/>

D=CF clients:

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

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

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

Control table

ID	MAC Address	IP Address	C	A
1	<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"/>

DHCP clients ID

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

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

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

DHCP clients ID

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

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

4.6.5 Miscellaneous Items

Item	Setting	Enable
▶ Remote Administrator Host/Port	0.0.0.0/255	<input type="checkbox"/>
▶ Administration Time-out	0 seconds (0 to disable)	<input type="checkbox"/>
▶ Discard PING from WAN side		<input type="checkbox"/>
▶ SPI mode		<input type="checkbox"/>
▶ DoS Attack Detection		<input type="checkbox"/>
▶ VPN PPTP Pass-Through		<input checked="" type="checkbox"/>
▶ VPN IPSec Pass-Through		<input checked="" type="checkbox"/>

Save Undo Help

Remote Administrator Host/Port

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

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

Administrator Time-out

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

Discard PING from WAN side

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

SPI Mode

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

DoS Attack Detection

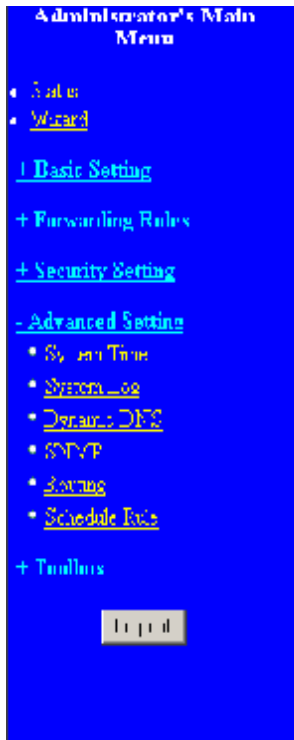
When this feature is enabled, the router will detect and log the DoS attack comes from the Internet.

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

VPN PPTP/IPSec Pass-Through

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

4.7 Advanced Settings



Advanced Setting

- **System Time**
Allow you to set device time manually to control network time from the device.
- **System Log**
Send system log to a dedicated device or email to specific recipient.
- **Dynamic DNS**
To host your server on a changing IP address, you have to use dynamic domain name service (DDNS).
- **SNMP**
Give a user the capability to remotely manage a computer network by polling and reading terminal values and manipulating network elements.
- **Routing**
If you have more than one router and subnets, you may want to enable routing table to allow packets to find proper routing path and allow different subnets to communicate with each other.
- **Schedule Rule**
Schedule Rule - Apply schedule rules to Packet Filter and Virtual Server.

4.7.1 System Time

System Time

Items	Setting
<input checked="" type="radio"/> Get Date and Time by NTP Protocol	<input type="button" value="Sync Now!"/> Time Server: <input type="text" value="time.nist.gov"/> Time Zone: <input type="text" value="(GMT-08:00) Pacific Time (US & Canada)"/>
<input type="radio"/> Get Date and Time using FQDN's Date and Time	FQDN Date and Time: <input type="text" value="2010/10/14 00:00:00"/>
<input type="radio"/> Set Date and Time manually	Date: Year: <input type="text" value="2000"/> Month: <input type="text" value="Oct"/> Day: <input type="text" value="1"/> Time: Hour: <input type="text" value="0"/> (0-23) Minute: <input type="text" value="0"/> (0-59) Second: <input type="text" value="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

4.7.2 System Log

Item	Setting
<input checked="" type="radio"/> Get Date and Time by NTP Protocol	<input type="button" value="Sync Now!"/> Time Server: <input type="text" value="time.nist.gov"/> Time Zone: <input type="text" value="(GMT-08:00) Pacific Time (US & Canada)"/>
<input type="radio"/> Set Date and Time using PC's Date and Time	PC Date and Time: <input type="text" value="2013/10/14 14:47:46"/>
<input type="radio"/> Set Date and Time manually	Date: Year: <input type="text" value="2013"/> Month: <input type="text" value="Oct"/> Day: <input type="text" value="1"/> Time: Hour: <input type="text" value="14"/> (0-23) Minute: <input type="text" value="47"/> (0-59) Second: <input type="text" value="46"/> (0-59)

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

IP Address for Syslog

Host IP of destination where syslogs will be sent to.

Check **Enable** to enable this function.

E-mail Alert Enable

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

SMTP Server IP and Port

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

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

Send E-mail alert to

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

4.7.3 Dynamic DNS

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

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

So that anyone wishing to reach your host only needs to know the name of it. Dynamic DNS will map the name of your host to your current IP address, which changes each time you connect your Internet service provider.

Before you enable **Dynamic DNS**, you need to register an account on one of these Dynamic DNS servers that we list in **provider** field.

To enable **Dynamic DNS** click the check box next to **Enable** in the **DDNS** field.

Next you can enter the appropriate information about your Dynamic DNS Server.

You have to define:

Provider

Host Name

Username/E-mail

Password/Key

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

Example:

Item	Setting
▶ DNS	<input type="radio"/> Disable <input checked="" type="radio"/> Enable
▶ Provider	<input type="text" value="DynDNS.org(Dynam..."/>
▶ Fqdn Name	<input type="text" value="kirs.cynors.org"/>
▶ Username / Password	<input type="text" value="root"/>
▶ Password / Key	<input type="text" value=""/>

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

4.7.4 SNMP Setting

Item	Setting
▶ Enable SNMP	<input checked="" type="checkbox"/> Local <input type="checkbox"/> Remote
▶ Get Community	public
▶ Set Community	public

Save Ok Cancel

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

Enable SNMP

You must check either Local or Remote or both to enable SNMP function. If Local is checked, this device will response request from LAN. If Remote is checked, this device will response request from WAN.

Get Community

Setting the community of GetRequest your device will response.

Set Community

Setting the community of SetRequest your device will accept.

4.7.5 Routing Table

Administrator's Main Menu

- [Status Wizard](#)
- + [Basic Setting](#)
- + [Forwarding Rules](#)
- + [Security Setting](#)
- [Advanced Setting](#)
 - [System Time](#)
 - [System Log](#)
 - [Dynamic DNS](#)
 - [SNMP](#)
 - [Routing](#)
 - [Schedule Rule](#)
- + [Toolbox](#)

Routing Table

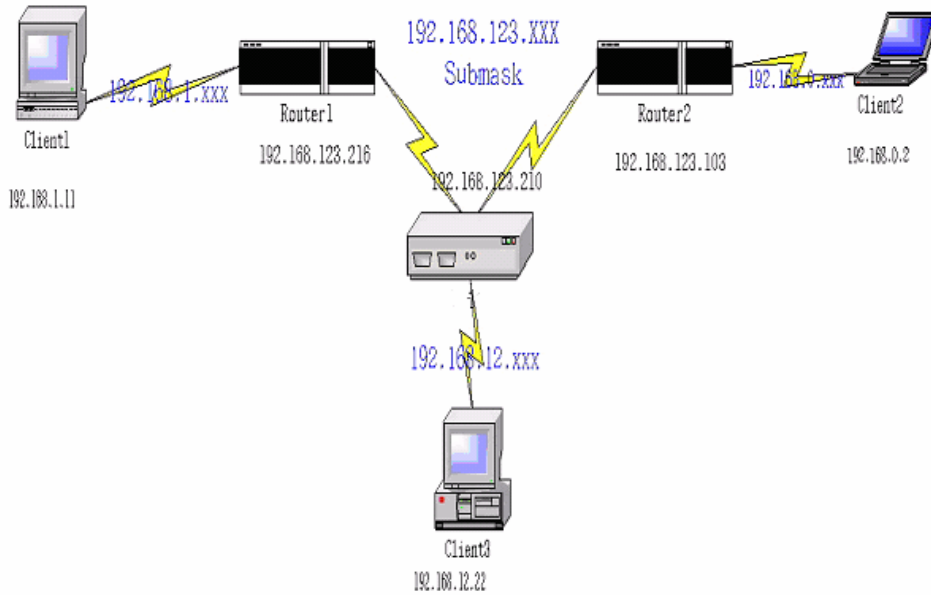
ID	Destination	Subnet Mask	Gateway	Hop	Enable
1	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
2	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
3	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
4	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
5	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
6	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
7	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
8	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>

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

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

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

Example:



Configuration on NAT Router

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

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

And if it sends Packets to 192.168.1.11 will go via 192.168.123.216

Each rule can be enabled or disabled individually.

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

4.7.6 Schedule Rule

The screenshot shows the Administration's Main Menu on the left and the Schedule Rule configuration page on the right. The menu includes options like Status, Wizard, Basic Setting, Forwarding Rules, Security Setting, Advanced Setting, System Log, System Log, Dynamic DNS, SFTP, Port, and Schedule Rule. The Schedule Rule page has a table with columns for Name and Setting, and a table with columns for Rule#, Rule Name, and Action. There are also buttons for Save, Add New Rule, and Help.

Schedule Rule	
Name	Setting
Schedule	<input checked="" type="checkbox"/> 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

Administrator's Main Menu

- [Status](#)
- [Wizard](#)
- + [Basic Setting](#)
- + [Forwarding Rules](#)
- + [Security Setting](#)
- Advanced Setting
 - [System Time](#)
 - [System Log](#)
 - [Dynamic NAT](#)
 - [NAT](#)
 - [Routing](#)
 - [Schedule Rule](#)
- + [Toolbox](#)

Schedule Rule Setting

Item	Setting
▶ Hours of Rule 1	<input type="text" value="ftp time"/>
Week Day	Start Time (hh:mm)
Sunday	<input type="text"/> : <input type="text"/>
Monday	<input type="text"/> : <input type="text"/>
Tuesday	<input type="text"/> : <input type="text"/>
Wednesday	<input type="text"/> : <input type="text"/>
Thursday	<input type="text"/> : <input type="text"/>
Friday	<input type="text"/> : <input type="text"/>
Saturday	<input type="text"/> : <input type="text"/>
Every Day	<input type="text" value="14"/> : <input type="text" value="10"/> : <input type="text" value="16"/> : <input type="text" value="20"/>

After configure Rule 1à

The screenshot displays the Administrator's Main Menu on the left and the Schedule Rule configuration interface on the right.

Administrator's Main Menu

- [Status](#)
- [Warning](#)
- [Basic Setting](#)
- [Forwarding Rules](#)
- [Security Setting](#)
- [Advanced Setting](#)
 - [System Time](#)
 - [System Log](#)
 - [Dynamic DNS](#)
 - [SNMP](#)
 - [Routing](#)
 - [Schedule Rule](#)
- [Toolbox](#)

[Log out](#)

Schedule Rule

Item	Setting
▸ Schedule	<input type="checkbox"/> enable

Rule #	Rule Name	Action
1	by time	Edit Delete

[Save](#) [Add New Rule..](#) [Help](#)

Schedule Enable

Selected if you want to Enable the Scheduler.

Edit

To edit the schedule rule.

Delete

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

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

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

Administrator's Main Menu

- Status
- Wizard
- Basic Setting**
- Forwarding Rules
 - Virtual Server
 - Special IP
 - Virtual IP
- + Security Setting
- + Advanced Setting
- + Toolbox

Virtual Server

ID	Service Ports	Server IP	Enable	Use Rule#
1	21	192.168.122.134	<input checked="" type="checkbox"/>	1
2		92.168.122.	<input type="checkbox"/>	0
3		192.168.122.	<input type="checkbox"/>	0
4		192.168.122.	<input type="checkbox"/>	1
5		92.168.122.	<input type="checkbox"/>	0
6		192.168.122.	<input type="checkbox"/>	0
7		192.168.122.	<input type="checkbox"/>	1
8		92.168.122.	<input type="checkbox"/>	0
9		192.168.122.	<input type="checkbox"/>	0
10		192.168.122.	<input type="checkbox"/>	1
11		92.168.122.	<input type="checkbox"/>	0
12		192.168.122.	<input type="checkbox"/>	0
13		192.168.122.	<input type="checkbox"/>	1
14		92.168.122.	<input type="checkbox"/>	0
15		192.168.122.	<input type="checkbox"/>	0

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

Administrator's Main Menu

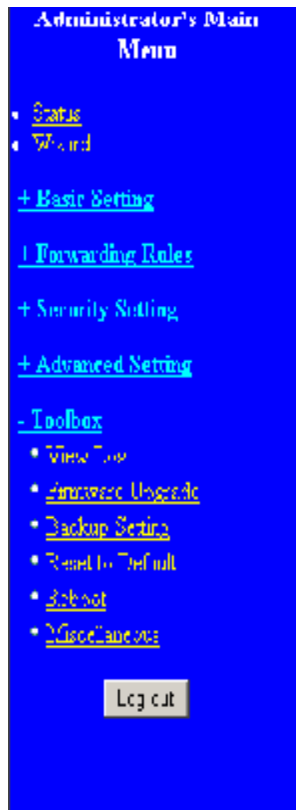
- Status
- Wizard
- Basic Setting**
- Forwarding Rules
- Security Setting
 - Packet Filters
 - Domain Filters
 - URL Blocking
 - MAC Control
 - VPN
 - Miscellaneous
- + Advanced Setting
- + Toolbox

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 type="radio"/> Deny all to pass except those match the following rules.

ID	Source IP : Ports	Destination IP : Ports	Enable	Use Rule#
1	: 21	: 21	<input checked="" type="checkbox"/>	1
2			<input type="checkbox"/>	0
3			<input type="checkbox"/>	0
4			<input type="checkbox"/>	11
5			<input type="checkbox"/>	0
6			<input type="checkbox"/>	0
7			<input type="checkbox"/>	11
8			<input type="checkbox"/>	0

4.8 Toolbox



The screenshot shows the 'Administrator's Main Menu' with a blue background. The menu items are: Status, Forward, + Basic Setting, + Forwarding Rules, + Security Setting, + Advanced Setting, - Toolbox (highlighted), View Log, Firmware Upgrade, Backup Setting, Reset to Default, Reboot, and Miscellaneous. A 'Log out' button is located at the bottom right of the menu.

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-up-LAN: Let you to power up another network device remotely.
 - Domain Name or IP Address on Ping Tool: Allow you to configure an IP and ping the device. You can ping a certain IP to test whether it is alive.

4.8.1 System Log

Administrator's Main Menu

- State
- WinBox
- [Basic Setting](#)
- + Forwarding Rules
- + Security Setting
- [Advanced Setting](#)
- Tools**
 - [View Log](#)
 - [Firmware Upgrade](#)
 - [Backup Setting](#)
 - [Export to Default](#)
 - [Reboot](#)
 - Miscellaneous

System Log

WinBox type: Dynamic: F:odshem (S: WinBox)

Display time: WinBox Oct 01 00:10:04 2003

2003年10月1日 上午 12:01:50 2003ntriggerd triggered from 192.168.1.23.125:2288 to 192.168.1.19:20186

2003年10月1日 上午 12:01:50 2003ntriggerd triggered ()

2003年10月1日 上午 12:01:54 2003ntriggerd triggered ()

2003年10月1日 上午 12:01:55 Admin from 192.168.1.23.125 login successfully

2003年10月1日 上午 12:01:58 2003ntriggerd triggered ()

2003年10月1日 上午 12:01:58 2003ntriggerd triggered ()

2003年10月1日 上午 12:02:17 2003ntriggerd triggered successfully

2003年10月1日 上午 12:02:17 2003ntriggerd triggered ()

2003年10月1日 上午 12:02:51 2003ntriggerd triggered ()

2003年10月1日 上午 12:02:55 2003ntriggerd triggered ()

2003年10月1日 上午 12:03:15 2003ntriggerd triggered ()

2003年10月1日 上午 12:03:15 2003ntriggerd triggered successfully

2003年10月1日 上午 12:03:15 2003ntriggerd triggered ()

2003年10月1日 上午 12:03:52 2003ntriggerd triggered ()

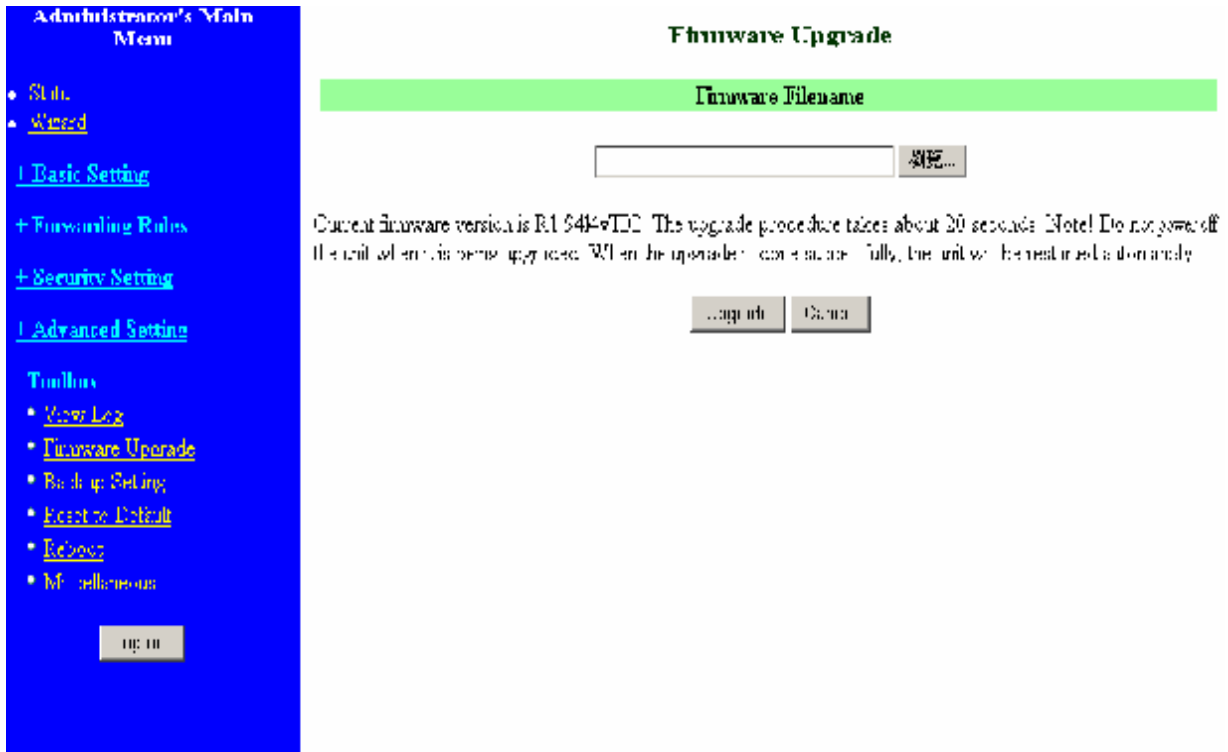
2003年10月1日 上午 12:04:00 2003ntriggerd triggered ()

2003年10月1日 上午 12:04:16 2003ntriggerd triggered ()

Back Refresh Download Clear

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

4.8.2 Firmware Upgrade



The screenshot displays the Administrator's Main Menu on the left and the Firmware Upgrade page on the right. The menu includes options like Status, Wizard, Basic Setting, Forwarding Rules, Security Setting, Advanced Setting, and Tools. The Firmware Upgrade page features a text input field for the firmware filename, a 'Browse...' button, a warning message about the upgrade process, and 'Upgrade' and 'Cancel' buttons.

Administrator's Main Menu

- [Status](#)
- [Wizard](#)
- [Basic Setting](#)
- [Forwarding Rules](#)
- [Security Setting](#)
- [Advanced Setting](#)
- **Tools**
 - [View Log](#)
 - [Firmware Upgrade](#)
 - [Backup Setting](#)
 - [Reset to Default](#)
 - [Reboot](#)
 - [Maintenance](#)

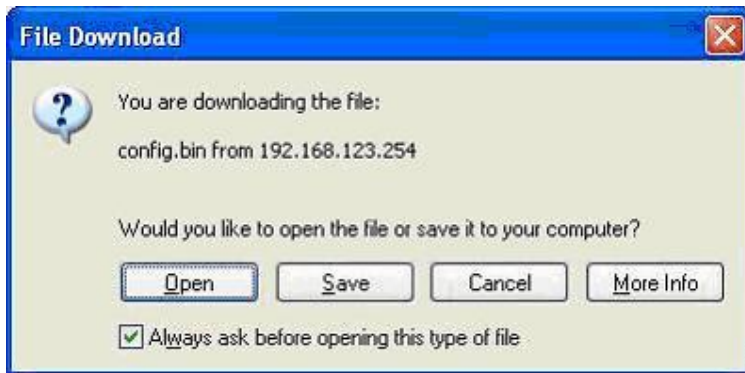
Firmware Upgrade

Firmware Filename

Current firmware version is R1.0449-110. The upgrade procedure takes about 20 seconds. **Note!** Do not power off the unit when it is being upgraded. When the upgrade is completed fully, the unit will be restarted automatically.

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

4.8.3 Backup Setting



You can backup your settings by clicking the **Backup Setting** button and save it as a bin file. Once you want to restore these settings, please click **Firmware Upgrade** button and use the bin file you saved.

4.8.4 Reset to default



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

4.8.5 Reboot



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

4.8.6 Miscellaneous Items

The image shows a screenshot of a web interface. On the left is a blue sidebar titled "Administrator's Main Menu" with a list of navigation options: "Status", "Wired", "Basic Setting", "Forwarding Rules", "Security Setting", "Advanced Setting", and a "Toolbox" section containing "View Log", "Firmware Upgrade", "Backup Setting", "Reset to Default", "Reboot", and "Miscellaneous". A "Home" button is at the bottom of the sidebar. The main content area is titled "Miscellaneous Items" and features a table with two columns: "Item" and "Setting". The table contains two rows: "MAC Address for Wake-on-LAN" with an input field and a "Wake up" button, and "Domain Name or IP address for Ping Test" with an input field and a "Ping" button. Below the table are three buttons: "Save", "Apply", and "Cancel".

Item	Setting
▶ MAC Address for Wake-on-LAN	<input type="text"/> <input type="button" value="Wake up"/>
▶ Domain Name or IP address for Ping Test	<input type="text"/> <input type="button" value="Ping"/>

MAC Address for Wake-on-LAN

Wake-on-LAN is a technology that enables you to power up a networked device remotely. In order to enjoy this feature, the target device must be Wake-on-LAN enabled and you have to know the MAC address of this device, say 00-11-22-33-44-55. Clicking "Wake up" button will make the router to send the wake-up frame to the target device immediately.

Domain Name or IP address for Ping Test

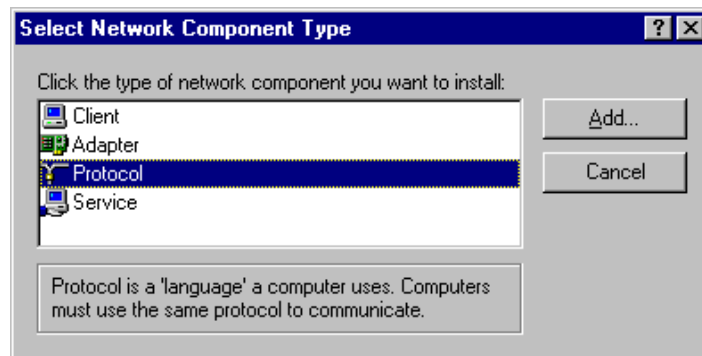
Allow you to configure an IP, and ping the device. You can ping a specific IP to test whether it is alive.

Appendix A TCP/IP Configuration for Windows 95/98

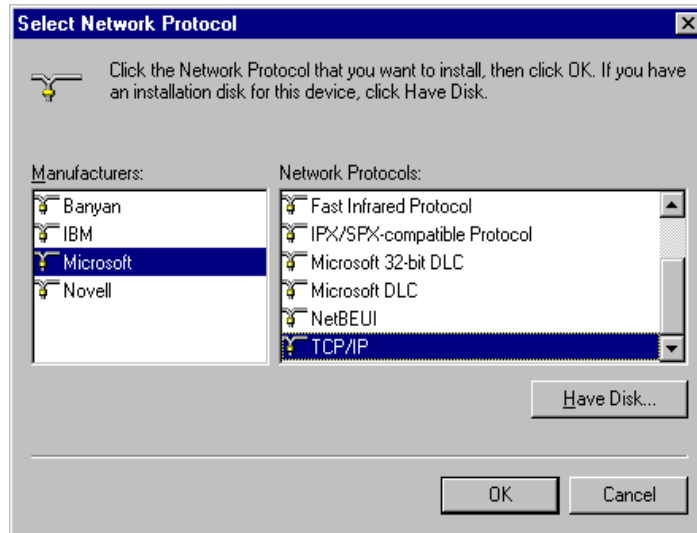
This section introduces you how to install TCP/IP protocol into your personal computer. And suppose you have been successfully installed one network card on your personal computer. If not, please refer to your network card manual. Moreover, the Section B.2 tells you how to set TCP/IP values for working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

A.1 Install TCP/IP Protocol into Your PC

1. Click **Start** button and choose **Settings**, then click **Control Panel**.
1. Double click **Network** icon and select **Configuration** tab in the Network window.
1. Click **Add** button to add network component into your PC.
1. Double click **Protocol** to add TCP/IP protocol.



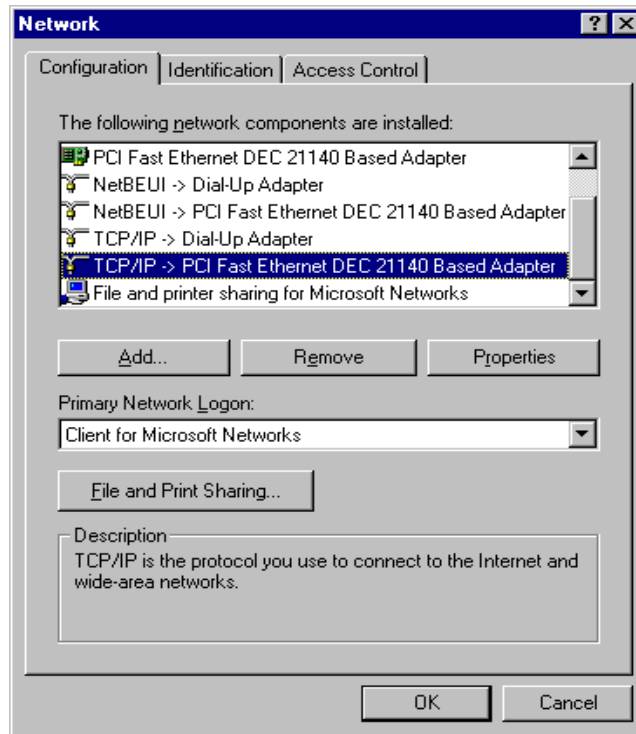
1. Select **Microsoft** item in the manufactures list. And choose **TCP/IP** in the Network Protocols.
Click **OK** button to return to Network window.



1. The TCP/IP protocol shall be listed in the Network window. Click **OK** to complete the install procedure and restart your PC to enable the TCP/IP protocol.

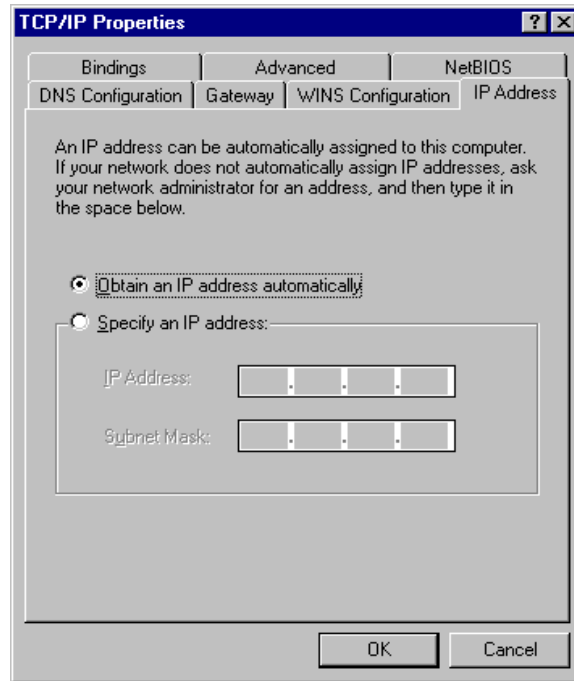
A.2 Set TCP/IP Protocol for Working with NAT Router

1. Click **Start** button and choose **Settings**, then click **Control Panel**.
2. Double click **Network** icon. Select the TCP/IP line that has been associated to your network card in the **Configuration** tab of the Network window.



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

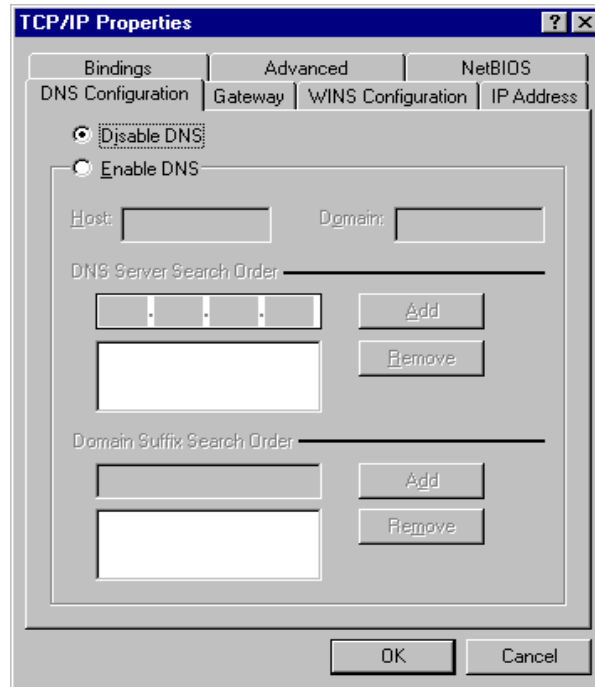
- a. Select **Obtain an IP address automatically** in the IP Address tab.



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

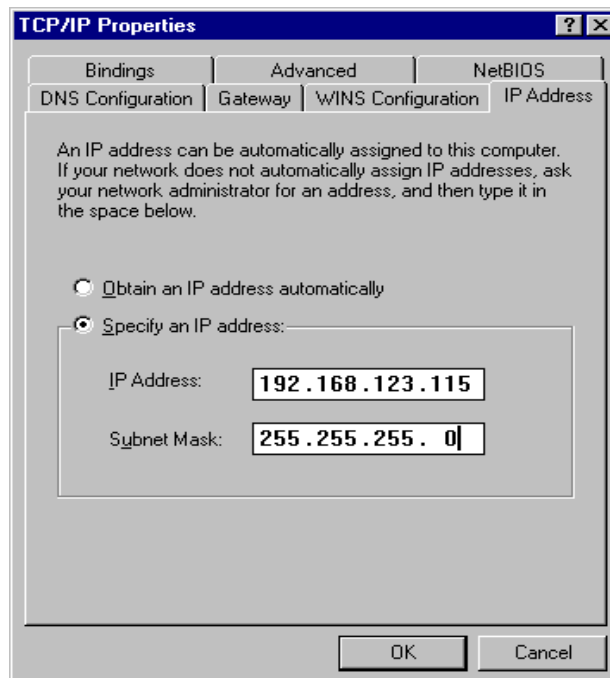


- c. Choose **Disable DNS** in the DNS Configuration tab.

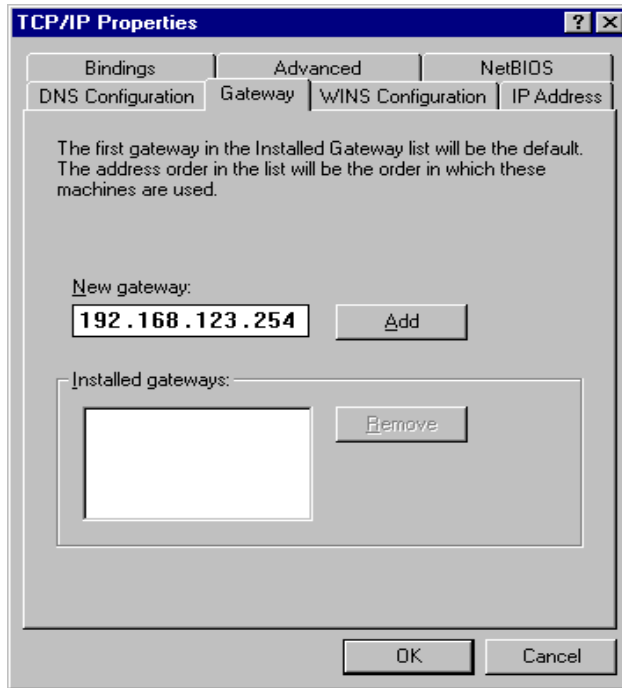


B. Configure IP manually

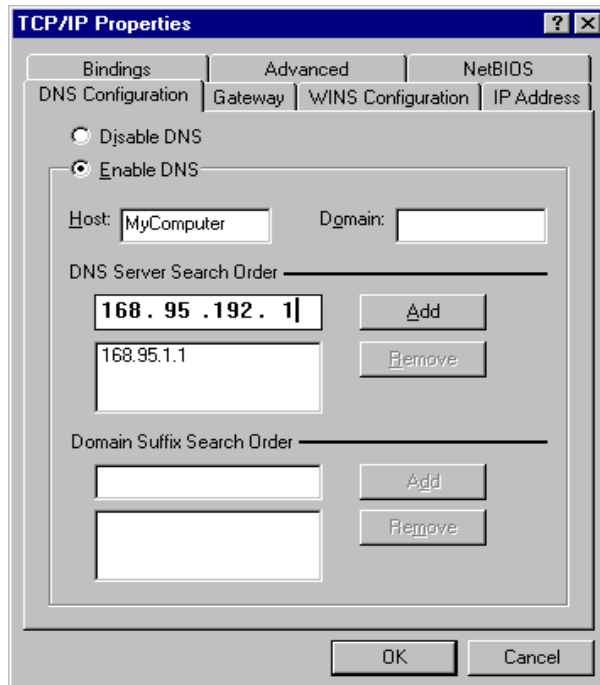
- a. Select **Specify an IP address** in the IP Address tab. The default IP address of this product is 192.168.123.254. So please use 192.168.123.xxx (xxx is between 1 and 253) for IP Address field and 255.255.255.0 for Subnet Mask field.



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



- c. In the DNS Configuration tab, add the DNS values which are provided by the ISP into DNS Server Search Order field and click **Add** button.



Appendix B FAQ and Troubleshooting

Reset to factory Default

1. Restore directly when the router power on

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