

# 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 products, 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 .....	7
Chapter 3	Network Settings and Software Installation .....	9
	3.1 Make Correct Network Settings of Your Computer .....	9
Chapter 4	Configuring Wireless Broadband Router .....	10
	4.1 Login to Configure from Wizard .....	11
	4.2 Status .....	13
	4.4 Basic Setting .....	14
	4.5 Forwarding Rules .....	32
	4.6 Security Settings .....	36
	4.7 Advanced Settings .....	50
	4.8 Toolbox .....	63
Appendix A	TCP/IP Configuration for Windows 95/98 .....	68
Appendix B	802.1x Setting .....	73
Appendix C	WPA-PSK and WPA .....	79
Appendix D	FAQ and Troubleshooting .....	92
	What can I do when I have some trouble at the first time? .....	92
	How do I connect router by using wireless? .....	95

## **Chapter 1 Introduction**

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

### **Functions and Features**

#### **Router Basic functions**

- **Auto-sensing Ethernet Switch**  
Equipped with a 4-port auto-sensing Ethernet switch.
- **WAN type supported**  
The router supports some WAN types, Static, Dynamic, PPPoE , PPTP ,L2TP, Dynamic IP with Road Runner.
- **Firewall**  
All unwanted packets from outside intruders are blocked to protect your Intranet.
- **DHCP server supported**  
All of the networked computers can retrieve TCP/IP settings automatically from this product.
- **Web-based configuring**  
Configurable through any networked computer's web browser using Netscape or Internet Explorer.
- **Virtual Server supported**  
Enable you to expose WWW, FTP and other services on your LAN to be accessible to Internet users.
- **User-Definable Application Sensing Tunnel**  
User can define the attributes to support the special applications requiring multiple connections, like Internet gaming, video conferencing, Internet telephony and so on, then this product can sense the application type and open multi-port tunnel for it.
- **DMZ Host supported**  
Lets a networked computer be fully exposed to the Internet; this function is used when special application sensing tunnel feature is insufficient to allow an application to function correctly.
- **Statistics of WAN Supported**  
Enables you to monitor inbound and outbound packets

## Wireless functions

- **High speed for wireless LAN connection**

Up to 54Mbps data rate by incorporating Orthogonal Frequency Division Multiplexing (OFDM).

- **Roaming**

Provides seamless roaming within the IEEE 802.11b (11M) and IEEE 802.11g (54M) WLAN infrastructure.

- **IEEE 802.11b compatible (11M)**

Allowing inter-operation among multiple vendors.

- **IEEE 802.11g compatible (54M)**

Allowing inter-operation among multiple vendors.

- **Auto fallback**

54M, 48M, 36M, 24M, 18M, 12M, 6M data rate with auto fallback in 802.11g mode.

11M, 5.5M, 2M, 1M data rate with auto fallback in 802.11b mode.

## Security functions

- **Packet filter supported**

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

- **Domain Filter Supported**

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

- **URL Blocking Supported**

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

- **VPN Pass-through**

The router also supports VPN pass-through.

- **802.1X supported**

When the 802.1X function is enabled, the Wireless user must authenticate to this router first to use the Network service.

- **Support WPA-PSK and WPA version 1 and 2**

When the WPA function is enabled, the Wireless user must authenticate to this router first to use the Network service

- **SPI Mode Supported**

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

- **DoS Attack Detection Supported**

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

### **Advanced functions**

- **System time Supported**

Allow you to synchronize system time with network time server.

- **E-mail Alert Supported**

The router can send its info by mail.

- **Dynamic dns Supported**

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

- **SNMP Supported**

The router supports basic SNMP function.

- **Routing Table Supported**

Now, the router supports static routing.

- **Schedule Rule supported**

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

### **Other functions**

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

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

### **Packing List**

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

## Chapter 2 Hardware Installation

### 2.1 Panel Layout

#### 2.1.1. Front Panel



Figure 2-1 Front Panel

LED: Ports:

Port	Description
<b>PWR</b>	Power inlet
<b>WAN</b>	the port where you will connect your cable (or DSL) modem or Ethernet router.
<b>Port 1-4</b>	the ports where you will connect networked computers and other devices.

### 2.1.2. Rear Panel

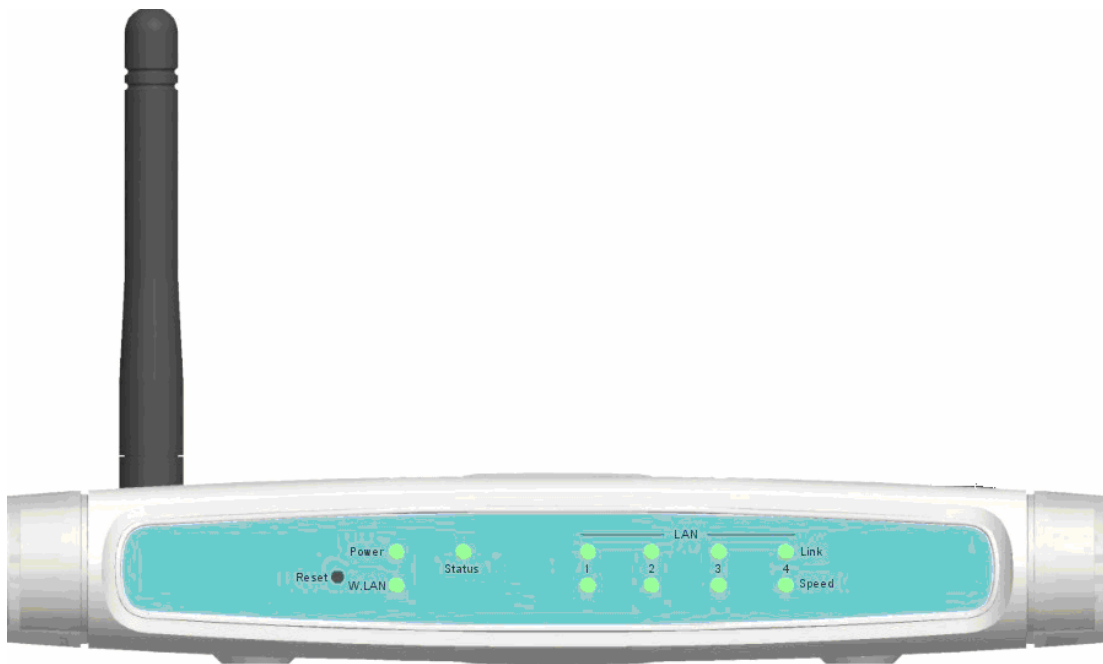


Figure 2-2 Rear Panel

LED:

LED	Function	Color	Status	Description
Power	Power indication	Green	On	Power is being applied to this product.
Status	System status	Green	Blinking	Status is flashed once per second to indicate system is alive.
WAN	WAN port activity	Green	On	The WAN port is linked.
WLAN	Wireless activity	Green	Blinking	The WAN port is sending or receiving data.
			Blinking	Sending or receiving data via wireless
Link. 1~4	Link status	Green	On	An active station is connected to the corresponding LAN port.
Speed 10/100	Data Rate	Green	Blinking	The corresponding LAN port is sending or receiving data.
			On	Data is transmitting in 100Mbps on the corresponding LAN port.
Reset				To reset system settings to factory defaults

## 2.2 Procedure for Hardware Installation

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

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

## 2. Setup LAN connection

- a. Wired LAN connection: connects an Ethernet cable from your computer's Ethernet port to one of the LAN ports of this product.
- b. Wireless LAN connection: locate this product at a proper position to gain the best transmit performance.

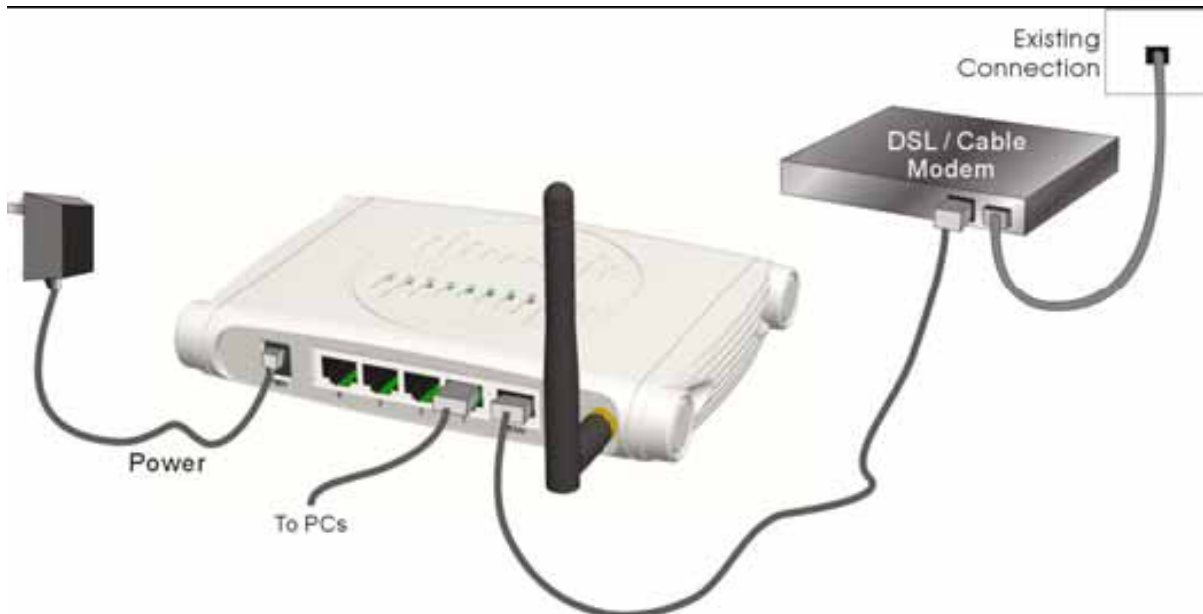


Figure 2-3 Setup of LAN and WAN connections for this product.

## 3. Setup WAN connection

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

## 4. Power on

Connecting the power cord to power inlet and turning the power switch on, this product will automatically enter the self-test phase. When it is in the self-test phase, the indicators M1 will be lighted ON for about 10 seconds, and then M1 will be flashed 3 times to indicate that the self-test operation has finished. Finally, the M1 will be continuously flashed once per second to indicate that this product is in normal operation.



## Chapter 3 Network Settings and Software Installation

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

### 3.1 Make Correct Network Settings of Your Computer

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

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

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

**ping 192.168.123.254**

If the following messages appear:

**Pinging 192.168.123.254 with 32 bytes of data:**

**Reply from 192.168.123.254: bytes=32 time=2ms TTL=64**

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

**Pinging 192.168.123.254 with 32 bytes of data:**

**Request timed out.**

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

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

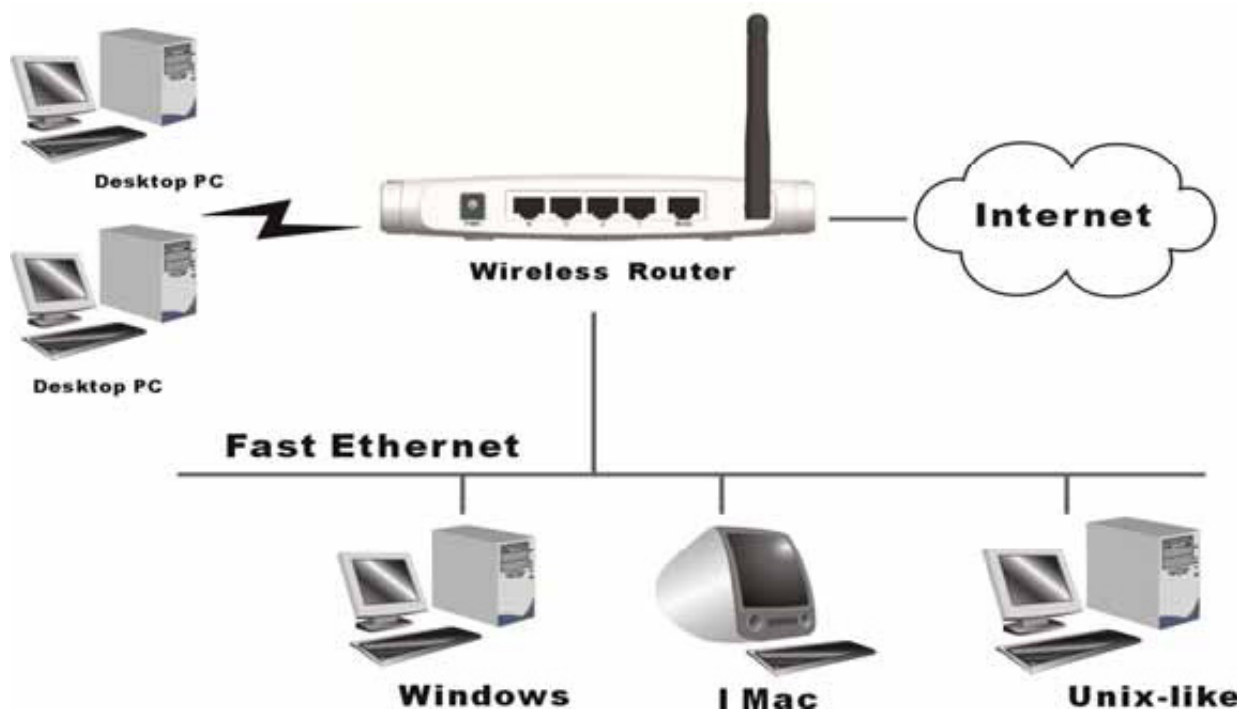
**Tip:** The LAN LED of this product and the link LED of network card on your computer must be lighted.

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

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

## Chapter 4 Configuring Wireless Broadband Router

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



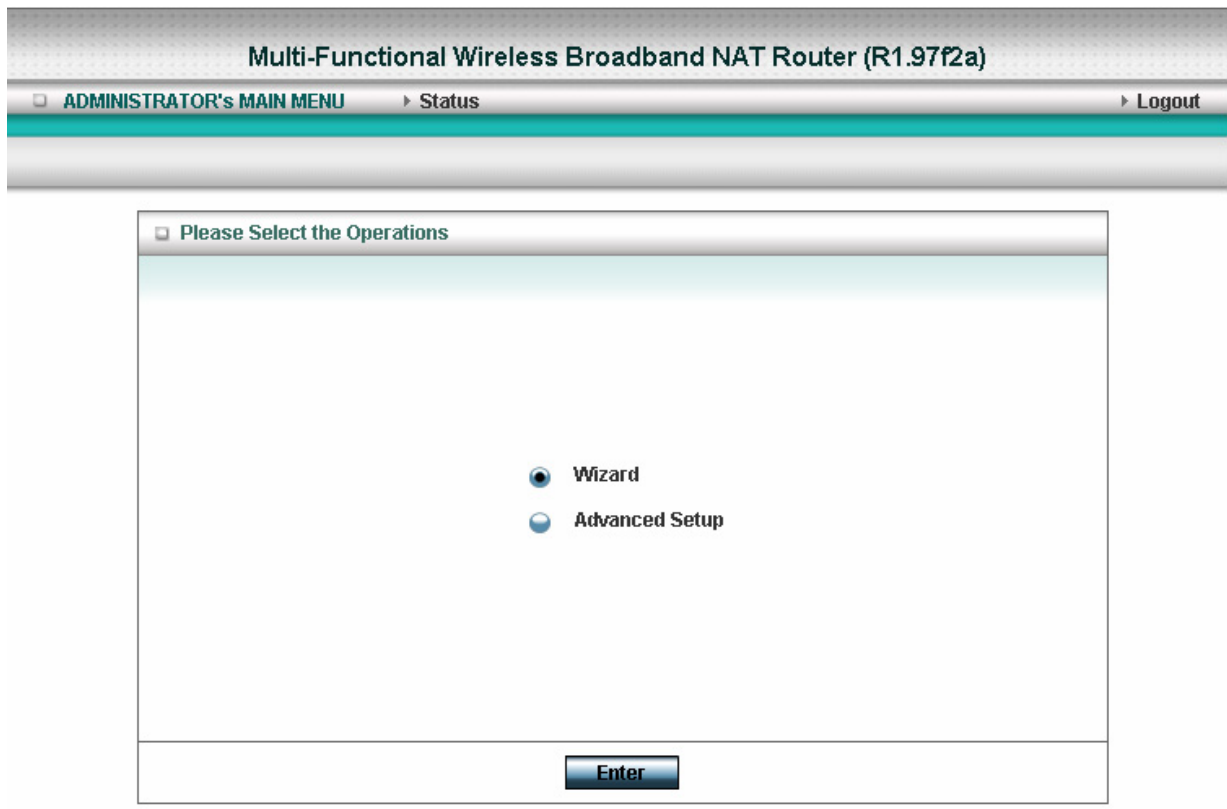
## 4.1 Login to Configure from Wizard

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.

The user can setup step by step to finish the connection with Wizard.



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

Multi-Functional Wireless Broadband NAT Router (R1.97f2a)

ADMINISTRATOR's MAIN MENU
Status
Wizard
Logout

BASIC SETTING
FORWARDING RULES
SECURITY SETTING
ADVANCED SETTING
TOOLBOX

Setup Wizard - Setup Wizard

[ EXIT ]

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

Step 1. Set Password.
Step 2. WAN Setup.
Step 3. Wireless Setup.
Step 4. Summary.
Step 5. Finish.

< Back

[ [Start](#) > Password > WAN > Wireless > Summary > Finish! ]

Next >

If the user finishes those steps and the router shows as below. It means that customers can enjoy Internet.

Multi-Functional Wireless Broadband NAT Router (R1.97f2a)

ADMINISTRATOR's MAIN MENU
Status
Wizard
Logout

BASIC SETTING
FORWARDING RULES
SECURITY SETTING
ADVANCED SETTING
TOOLBOX

Setup Wizard - WAN Connection Test

[ EXIT ]

**Congratulations!!**

The Internet connection is established.

Connection information are

WAN Type	Dynamic IP Address
IP Address	210.202.197.182
Subnet Mask	255.255.255.240
Gateway	210.202.197.190
Domain Name Server	192.168.123.10, 192.168.122.3

< Back

[ Start > Password > WAN > Wireless > Summary > [Finish!](#) ]

Finish

12

## 4.2 Status

Multi-Functional Wireless Broadband NAT Router (R1.97f1)

ADMINISTRATOR's MAIN MENU

Status

Logout

Wizard

Advanced Setup

System Status

[ HELP ]

Item	WAN Status	Sidenote
IP Address	211.74.184.162	PPPoE
Subnet Mask	255.255.255.255	
Gateway	211.74.184.162	
Domain Name Server	168.95.1.1	
Connection Time	03:10:14	<div>Disconnect</div>
MAC Address	00-04-61-4A-8A-33	

Wireless Status

Item	WLAN Status	Sidenote
SSID	default	
Channel	11	
Security	None	
MAC Address	00-50-18-00-0F-DA	

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

A. WAN Port Status.

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

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

## 4.4 Basic Setting

Please Select “Advanced Setup” to Setup

Multi-Functional Wireless Broadband NAT Router (R1.97f2a)

ADMINISTRATOR's MAIN MENU

Status

Wizard

Logout

BASIC SETTING

FORWARDING RULES

SECURITY SETTING

ADVANCED SETTING

TOOLBOX

System Status

[ HELP ]

Item	WAN Status	Sidenote
Remaining Lease Time	00:24:30	<div>Renew</div>
IP Address	210.202.197.182	<div>Release</div>
Subnet Mask	255.255.255.240	
Gateway	210.202.197.190	
Domain Name Server	192.168.123.10, 192.168.122.3	
MAC Address	00-50-18-AF-BE-CD	

Wireless Status

Item	WLAN Status	Sidenote
SSID	default	
Channel	11	
Security	None	
MAC Address	00-50-18-AF-BE-CE	

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

Multi-Functional Wireless Broadband NAT Router (R1.97f2a)

ADMINISTRATOR's MAIN MENU

Status

Wizard

Logout

BASIC SETTING

FORWARDING RULES

SECURITY SETTING

ADVANCED SETTING

TOOLBOX

Primary Setup

DHCP Server

Wireless

Change Password

Primary Setup

[ HELP ]

Item	Setting
▶ LAN IP Address	192.168.122.217
▶ WAN Type	Dynamic IP Address <div>Change...</div>
▶ Host Name	<div></div> (optional)
▶ WAN's MAC Address	00-50-18-AF-BE-CD <div>Clone MAC</div>
▶ Renew IP Forever	<input checked="" type="checkbox"/> Enable (Auto-reconnect)
<div>Save</div> <div>Undo</div> <div>Virtual Computers...</div>	

Press “Change”

**Multi-Functional Wireless Broadband NAT Router (R1.97f2a)**

ADMINISTRATOR's MAIN MENU    ▶ Status    ▶ Wizard    ▶ Logout

**BASIC SETTING**    FORWARDING RULES    SECURITY SETTING    ADVANCED SETTING    TOOLBOX

• Primary Setup  
• DHCP Server  
• Wireless  
• Change Password

**Choose WAN Type**

Type	Usage
<input type="radio"/> Static IP Address	ISP assigns you a 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.
<input type="radio"/> L2TP	Some ISPs require the use of L2TP to connect to their services.

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

1. **LAN IP Address:** the local IP address of this device. The computers on your network must use the LAN IP address of your product as their Default Gateway. You can change it if necessary.
2. **WAN Type:** WAN connection type of your ISP. You can click **Change** button to choose a correct one from the following four options:
  - A. Static IP Address: ISP assigns you a static IP address.
  - B. Dynamic IP Address: Obtain an IP address from ISP automatically.
  - C. Dynamic IP Address with Road Runner Session Management.(e.g. Telstra BigPond)
  - D. PPP over Ethernet: Some ISPs require the use of PPPoE to connect to their services.
  - E. PPTP: Some ISPs require the use of PPTP to connect to their services.
  - F. L2TP: Some ISPs require the use of L2TP 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.
5. Connection Control: There are 3 modes to select:

Connect-on-demand: The device will link up with ISP when the clients send outgoing packets.

Auto-Reconnect(Always-on): The device will link upw with ISP until the connection is established.

Manually: The device will not make the link until someone clicks the connect-button in the Staus-page.

#### **4.4.1.5 PPTP**

First, Please check your ISP assigned and Select Static IP Address or Dynamic IP Address.

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 connect to ISP automatically, after system is restarted or connection is dropped.
5. Connection Control: There are 3 modes to select:  
  
Connect-on-demand: The device will link up with ISP when the clients send outgoing packets.  
  
Auto-Reconnect(Always-on): The device will link up with ISP until the connection is established.  
  
Manually: The device will not make the link until someone clicks the connect-button in the Staus-page.

**Multi-Functional Wireless Broadband NAT Router (R1.97f2a)**

ADMINISTRATOR's MAIN MENU   Status   Wizard   Logout

BASIC SETTING   FORWARDING RULES   SECURITY SETTING   ADVANCED SETTING   TOOLBOX

- Primary Setup
- DHCP Server
- Wireless
- Change Password

Primary Setup [ HELP ]

Item	Setting
▶ LAN IP Address	<input type="text" value="192.168.122.217"/>
▶ WAN Type	PPTP <span style="background-color: #0056b3; color: white; padding: 2px 5px; border: 1px solid black;">Change...</span>
▶ IP Mode	<div style="border: 1px solid black; padding: 2px;"> Static IP Address ▼ </div>
▶ My IP Address	<div style="border: 1px solid black; padding: 2px;"> Dynamic IP Address  Static IP Address </div>
▶ My Subnet Mask	<input type="text" value="255.255.255.0"/>
▶ Gateway IP	<input type="text" value="0.0.0.0"/>
▶ Server IP Address/Name	<input type="text"/>
▶ PPTP Account	<input type="text"/>
▶ PPTP Password	<input type="text"/>
▶ Connection ID	<input type="text"/> (optional)
▶ Maximum Idle Time	<input type="text" value="600"/> seconds
▶ Connection Control	<div style="border: 1px solid black; padding: 2px;"> Auto reconnect(Always-on) ▼ </div>
▶ MTU	<input type="text" value="1460"/>

#### 4.4.1.6 L2TP

First, Please check your ISP assigned and Select Static IP Address or Dynamic IP Address.

For example: Use Static

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

connect to ISP automatically, after system is restarted or connection is dropped.

6. Connection Control: There are 3 modes to select:

Connect-on-demand: The device will link up with ISP when the clients send outgoing packets.

Auto-Reconnect(Always-on): The device will link up with ISP until the connection is established.

Manually: The device will not make the link until someone clicks the connect-button in the Status-page.

Multi-Functional Wireless Broadband NAT Router (R1.97f2a)

ADMINISTRATOR's MAIN MENU

Status

Wizard

Logout

BASIC SETTING

FORWARDING RULES

SECURITY SETTING

ADVANCED SETTING

TOOLBOX

Primary Setup

DHCP Server

Wireless

Change Password

Primary Setup [ HELP ]

Item	Setting
▶ LAN IP Address	192.168.122.217
▶ WAN Type	PPTP <a href="#">Change...</a>
▶ IP Mode	Static IP Address
▶ My IP Address	10.0.0.100
▶ My Subnet Mask	255.255.255.0
▶ Gateway IP	10.0.0.1
▶ Server IP Address/Name	
▶ PPTP Account	
▶ PPTP Password	
▶ Connection ID	(optional)
▶ Maximum Idle Time	600 seconds
▶ Connection Control	Auto reconnect(Always-on)
▶ MTU	1460

#### 4.4.1.7 Virtual Computers(Only for Static and dynamic IP address Wan type)

Multi-Functional Wireless Broadband NAT Router (R1.97f2a)

ADMINISTRATOR's MAIN MENU

Status

Wizard

Logout

BASIC SETTING

FORWARDING RULES

SECURITY SETTING

ADVANCED SETTING

TOOLBOX

Primary Setup

DHCP Server

Wireless

Change Password

Virtual Computers

[ HELP ]

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

Save

Undo

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

Multi-Functional Wireless Broadband NAT Router (R1.97f2a)

ADMINISTRATOR's MAIN MENU   Status   Wizard   Logout

BASIC SETTING   FORWARDING RULES   SECURITY SETTING   ADVANCED SETTING   TOOLBOX

Primary Setup  
DHCP Server  
Wireless  
Change Password

**DHCP Server** [HELP]

Item	Setting
DHCP Server	<input checked="" type="radio"/> Disable <input type="radio"/> Enable
Lease Time	0 Minutes
IP Pool Starting Address	100
IP Pool Ending Address	199
Domain Name	
Primary DNS	0.0.0.0
Secondary DNS	0.0.0.0
Primary WINS	0.0.0.0
Secondary WINS	0.0.0.0
Gateway	0.0.0.0 (optional)

Save   Undo   Clients List...   Fixed Mapping...

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. **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.
3. **Domain Name:** Optional, this information will be passed to the client.
4. **Primary DNS/Secondary DNS:** This feature allows you to assign DNS Servers
5. **Primary WINS/Secondary WINS:** This feature allows you to assign WINS Servers
6. **Gateway:** The Gateway Address would be the IP address of an alternate Gateway.  
This function enables you to assign another gateway to your PC, when DHCP server offers an IP to your PC.

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

Multi-Functional Wireless Broadband NAT Router (R1.97f2a)

ADMINISTRATOR's MAIN MENU   Status   Wizard   Logout

BASIC SETTING   FORWARDING RULES   SECURITY SETTING   ADVANCED SETTING   TOOLBOX

Primary Setup  
DHCP Server  
Wireless  
Change Password

Wireless Setting [ HELP ]

Item	Setting
Wireless	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Network ID(SSID)	default
Wireless Mode	<input type="radio"/> Mixed <input checked="" type="radio"/> 11g only
SSID broadcast	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Channel	11
Security	None

Save   Undo   WPS Control...

- None
- WEP
- 802.1x and RADIUS
- WPA-PSK
- WPA
- WPA2-PSK(AES)
- WPA2(AES)
- WPA-PSK / WPA2-PSK
- WPA1/WPA2

Wireless settings allow you to set the wireless configuration items.

**Wireless :** The user can enable or disable wireless function.

**Network ID (SSID):** Network ID is used for identifying the Wireless LAN (WLAN). Client stations can roam freely over this product and other Access Points that have the same Network ID. (The factory setting is “default”)

**SSID Broadcast:** The router will Broadcast beacons that have some information, including ssid so that The wireless clients can know how many ap devices by scanning function in the network. Therefore, This function is disabled, the wireless clients can not find the device from beacons.

**Channel:** The radio channel number. The permissible channels depend on the Regulatory Domain. The factory setting is as follow: **channel 6** for North America; **channel 7** for European (ETSI); **channel 7** for Japan.

**Security:** Select the data privacy algorithm you want. Enabling the security can protect your data while

it is transferred from one station to another.

## There are several security types to use:

### WEP :

When you enable the 128 or 64 bit WEP key security, please select one WEP key to be used and input 26 or 10 hexadecimal (0, 1, 2...8, 9, A, B...F) digits.

### 802.1X

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

RADIUS Server

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

RADIUS Shared Key

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

The screenshot displays the configuration interface of a Multi-Functional Wireless Broadband NAT Router (R1.97f2a). The top navigation bar includes links for ADMINISTRATOR's MAIN MENU, Status, Wizard, and Logout. Below this, a tabbed interface shows BASIC SETTING, FORWARDING RULES, SECURITY SETTING, ADVANCED SETTING, and TOOLBOX. The left sidebar lists navigation options: Primary Setup, DHCP Server, Wireless, and Change Password. The main content area is titled 'Wireless Setting' and contains a table with the following items and settings:

Item	Setting
Wireless	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Network ID(SSID)	default
Wireless Mode	<input type="radio"/> Mixed <input checked="" type="radio"/> 11g only
SSID broadcast	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Channel	11
Security	802.1x and RADIUS
Encryption Key Length	<input checked="" type="radio"/> 64 bits <input type="radio"/> 128 bits
RADIUS Server IP	192.168.123.33
RADIUS port	1812
RADIUS Shared Key	

At the bottom of the table, there are four buttons: Save, Undo, WDS Setting..., and MAC Address Control...



## WPA-PSK

1. Select Encryption and Pre-share Key Mode

If you select HEX, you have to fill in 64 hexadecimal (0, 1, 2...8, 9, A, B...F) digits

If ASCII, the length of pre-share key is from 8 to 63.

2. Fill in the key, Ex 12345678

The screenshot shows the configuration interface of a Multi-Functional Wireless Broadband NAT Router (R1.97f2a). The top navigation bar includes 'ADMINISTRATOR's MAIN MENU', 'Status', 'Wizard', and 'Logout'. Below this, a tabbed interface shows 'BASIC SETTING' as the active tab, with other tabs for 'FORWARDING RULES', 'SECURITY SETTING', 'ADVANCED SETTING', and 'TOOLBOX'. On the left, a sidebar lists 'Primary Setup', 'DHCP Server', 'Wireless', and 'Change Password'. The main content area is titled 'Wireless Setting' and contains a table with the following items and settings:

Item	Setting
Wireless	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Network ID(SSID)	default
Wireless Mode	<input type="radio"/> Mixed <input checked="" type="radio"/> 11g only
SSID broadcast	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Channel	11
Security	WPA-PSK
Encryption	<input checked="" type="radio"/> TKIP <input type="radio"/> AES
Preshare Key Mode	ASCII
Preshare Key	

At the bottom of the table, there are four buttons: 'Save', 'Undo', 'WDS Setting...', and 'MAC Address Control...'.

## WPA

Check Box was used to switch the function of the WPA. When the WPA function is enabled, the Wireless user must **authenticate** to this router first to use the Network service. RADIUS Server

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

Select Encryption and RADIUS Shared Key

If you select HEX, you have to fill in 64 hexadecimal (0, 1, 2...8, 9, A, B...F) digits

If ASCII, the length of pre-share key is from 8 to 63.

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

**Multi-Functional Wireless Broadband NAT Router (R1.97f2a)**

ADMINISTRATOR's MAIN MENU   Status   Wizard   Logout

BASIC SETTING   FORWARDING RULES   SECURITY SETTING   ADVANCED SETTING   TOOLBOX

- Primary Setup
- DHCP Server
- Wireless
- Change Password

Wireless Setting [ HELP ]

Item	Setting
▶ Wireless	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
▶ Network ID(SSID)	<input type="text" value="default"/>
▶ Wireless Mode	<input type="radio"/> Mixed <input checked="" type="radio"/> 11g only
▶ SSID broadcast	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
▶ Channel	<input type="text" value="11"/> ▼
▶ Security	<input type="text" value="WPA"/> ▼
▶ Encryption	<input checked="" type="radio"/> TKIP <input type="radio"/> AES
▶ RADIUS Server IP	<input type="text" value="192.168.123.33"/>
▶ RADIUS port	<input type="text" value="1812"/>
▶ RADIUS Shared Key	<input type="text" value="1234"/>

Save   Undo   WDS Setting...   MAC Address Control...

## WPA2-PSK(AES)

### 1. Select Pre-share Key Mode

If you select HEX, you have to fill in 64 hexadecimal (0, 1, 2...8, 9, A, B...F) digits

If ASCII, the length of Pre-share key is from 8 to 63.

### 2. Fill in the key, Ex 12345678

Multi-Functional Wireless Broadband NAT Router (R1.97f2a)

ADMINISTRATOR's MAIN MENU   Status   Wizard   Logout

BASIC SETTING   FORWARDING RULES   SECURITY SETTING   ADVANCED SETTING   TOOLBOX

- Primary Setup
- DHCP Server
- Wireless
- Change Password

Wireless Setting
[ HELP ]

Item	Setting
▶ Wireless	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
▶ Network ID(SSID)	<input style="width: 100%;" type="text" value="default"/>
▶ Wireless Mode	<input type="radio"/> Mixed <input checked="" type="radio"/> 11g only
▶ SSID broadcast	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
▶ Channel	<input style="width: 50%;" type="text" value="11"/> ▼
▶ Security	<input style="width: 80%;" type="text" value="WPA2-PSK(AES)"/> ▼
▶ Preshare Key Mode	<input style="width: 50%;" type="text" value="ASCII"/> ▼
▶ Preshare Key	<input style="width: 100%;" type="text"/>

Save
Undo
WDS Setting...
MAC Address Control...

## WPA2(AES)

Check Box was used to switch the function of the WPA. When the WPA function is enabled, the Wireless user must **authenticate** to this router first to use the Network service. RADIUS Server

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

Select RADIUS Shared Key

If you select HEX, you have to fill in 64 hexadecimal (0, 1, 2...8, 9, A, B...F) digits

If ASCII, the length of Pre-share key is from 8 to 63.

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

**Multi-Functional Wireless Broadband NAT Router (R1.97f2a)**

ADMINISTRATOR's MAIN MENU   Status   Wizard   Logout

BASIC SETTING   FORWARDING RULES   SECURITY SETTING   ADVANCED SETTING   TOOLBOX

- Primary Setup
- DHCP Server
- Wireless
- Change Password

Wireless Setting [ HELP ]

Item	Setting
▶ Wireless	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
▶ Network ID(SSID)	<input type="text" value="default"/>
▶ Wireless Mode	<input type="radio"/> Mixed <input checked="" type="radio"/> 11g only
▶ SSID broadcast	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
▶ Channel	<input type="text" value="11"/> ▼
▶ Security	<input type="text" value="WPA2(AES)"/> ▼
▶ RADIUS Server IP	<input type="text" value="0.0.0.0"/>
▶ RADIUS port	<input type="text" value="1812"/>
▶ RADIUS Shared Key	<input type="text"/>

## WPA-PSK /WPA2-PSK

The router will detect automatically which Security type the client uses to encrypt.

### 1. Select Pre-share Key Mode

If you select HEX, you have to fill in 64 hexadecimal (0, 1, 2...8, 9, A, B...F) digits

If ASCII, the length of Pre-share key is from 8 to 63.

### 2. Fill in the key, Ex 12345678

**Multi-Functional Wireless Broadband NAT Router (R1.97f2a)**

ADMINISTRATOR's MAIN MENU
Status Wizard
Logout

BASIC SETTING
FORWARDING RULES
SECURITY SETTING
ADVANCED SETTING
TOOLBOX

- Primary Setup
- DHCP Server
- **Wireless**
- Change Password

Wireless Setting
[ HELP ]

Item	Setting
▶ Wireless	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
▶ Network ID(SSID)	<input type="text" value="default"/>
▶ Wireless Mode	<input type="radio"/> Mixed <input checked="" type="radio"/> 11g only
▶ SSID broadcast	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
▶ Channel	<input type="text" value="11"/> ▼
▶ Security	<input type="text" value="WPA-PSK / WPA2-PSK"/> ▼
▶ Preshare Key Mode	<input type="text" value="ASCII"/> ▼
▶ Preshare Key	<input type="text"/>

Save
Undo
WDS Setting...
MAC Address Control...

## WPA/WPA2

Check Box was used to switch the function of the WPA. When the WPA function is enabled, the Wireless user must **authenticate** to this router first to use the Network service. RADIUS Server

The router will detect automatically which Security type(Wpa-psk version 1 or 2) the client uses to encrypt.

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

Select RADIUS Shared Key

If you select HEX, you have to fill in 64 hexadecimal (0, 1, 2...8, 9, A, B...F) digits

If ASCII, the length of Pre-share key is from 8 to 63.

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

**Multi-Functional Wireless Broadband NAT Router (R1.97f2a)**

ADMINISTRATOR's MAIN MENU   Status   Wizard   Logout

BASIC SETTING   FORWARDING RULES   SECURITY SETTING   ADVANCED SETTING   TOOLBOX

- Primary Setup
- DHCP Server
- Wireless
- Change Password

Wireless Setting [ HELP ]

Item	Setting
▶ Wireless	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
▶ Network ID(SSID)	<input type="text" value="default"/>
▶ Wireless Mode	<input type="radio"/> Mixed <input checked="" type="radio"/> 11g only
▶ SSID broadcast	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
▶ Channel	<input type="text" value="11"/> ▼
▶ Security	<input type="text" value="WPA1/WPA2"/> ▼
▶ RADIUS Server IP	<input type="text" value="0.0.0.0"/>
▶ RADIUS port	<input type="text" value="1812"/>
▶ RADIUS Shared Key	<input type="text"/>

Save
Undo
WDS Setting...
MAC Address Control...

### WDS(Wireless Distribution System)

WDS operation as defined by the IEEE802.11 standard has been made available. Using WDS it is possible to wirelessly connect Access Points, and in doing so extend a wired infrastructure to locations where cabling is not possible or inefficient to implement.

#### 4.4.4 Change Password

Multi-Functional Wireless Broadband NAT Router (R1.97f2a)

ADMINISTRATOR's MAIN MENU

Status

Wizard

Logout

BASIC SETTING

FORWARDING RULES

SECURITY SETTING

ADVANCED SETTING

TOOLBOX

Primary Setup

DHCP Server

Wireless

Change Password

Change Password

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

Save

Undo

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

## 4.5 Forwarding Rules

The screenshot displays the web interface of a Multi-Functional Wireless Broadband NAT Router (R1.97f2a). The top navigation bar includes links for ADMINISTRATOR's MAIN MENU, Status, Wizard, and Logout. Below this, a secondary menu highlights FORWARDING RULES, with other options like BASIC SETTING, SECURITY SETTING, ADVANCED SETTING, and TOOLBOX. On the left side, a sidebar menu lists Virtual Server, Special AP, and Miscellaneous. The main content area, titled 'Forwarding Rules', provides a detailed overview of the features:

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



## 4.5.1 Virtual Server

**Multi-Functional Wireless Broadband NAT Router (R1.97f2a)**

ADMINISTRATOR's MAIN MENU   Status   Wizard   Logout

BASIC SETTING   **FORWARDING RULES**   SECURITY SETTING   ADVANCED SETTING   TOOLBOX

Virtual Server   Special AP   Miscellaneous

**Virtual Server** [ HELP ]

Well known services -- select one -- use Schedule rule (00)Always Copy to ID --

ID	Server IP	Service Ports	Protocol	Enable	Schedule Rule#
1	192.168.122.13	14333	Both	<input checked="" type="checkbox"/>	0
2	192.168.122.13	20699-20700	Both	<input checked="" type="checkbox"/>	0
3	192.168.122.226	21	Both	<input checked="" type="checkbox"/>	0
4	192.168.122.229	2005	Both	<input checked="" type="checkbox"/>	0
5	192.168.122.218	25	Both	<input checked="" type="checkbox"/>	0
6	192.168.122.218	110	Both	<input checked="" type="checkbox"/>	0
7	192.168.122.218	22	Both	<input checked="" type="checkbox"/>	0
8	192.168.122.218	80	Both	<input checked="" type="checkbox"/>	0
9	192.168.122.13	4662-4663	Both	<input checked="" type="checkbox"/>	0
10	192.168.122.		Both	<input type="checkbox"/>	0

Next >>   Save   Undo

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

Multi-Functional Wireless Broadband NAT Router (R1.97f2a)

ADMINISTRATOR's MAIN MENU   Status   Wizard   Logout

BASIC SETTING   **FORWARDING RULES**   SECURITY SETTING   ADVANCED SETTING   TOOLBOX

Virtual Server  
Special AP  
Miscellaneous

**Special Applications** [ HELP ]

Popular applications Battle.net [ Copy to ] ID 1

ID	Trigger	Incoming Ports	Enable
1	6112	6112	<input checked="" type="checkbox"/>
2			<input type="checkbox"/>
3			<input type="checkbox"/>
4			<input type="checkbox"/>
5			<input type="checkbox"/>
6			<input type="checkbox"/>
7			<input type="checkbox"/>
8			<input type="checkbox"/>

Save   Undo

Saved! Changes take effect immediately!

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

Multi-Functional Wireless Broadband NAT Router (R1.97f2a)

ADMINISTRATOR's MAIN MENU   Status   Wizard   Logout

BASIC SETTING   **FORWARDING RULES**   SECURITY SETTING   ADVANCED SETTING   TOOLBOX

Virtual Server  
Special AP  
Miscellaneous

**Miscellaneous Items** [ HELP ]

Item	Setting	Enable
▶ IP Address of DMZ Host	192.168.122. <input type="text"/>	<input type="checkbox"/>
▶ Non-standard FTP port	<input type="text" value="0"/>	
▶ UPnP setting		<input type="checkbox"/>

Save   Undo

#### IP Address of DMZ Host

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

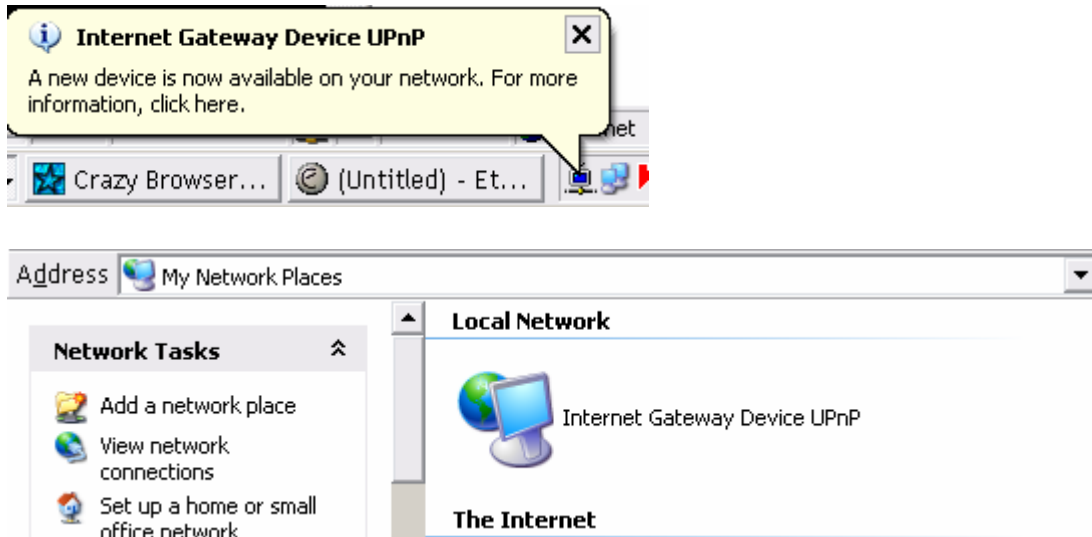
NOTE: This feature should be used only when needed.

#### Non-standard FTP port

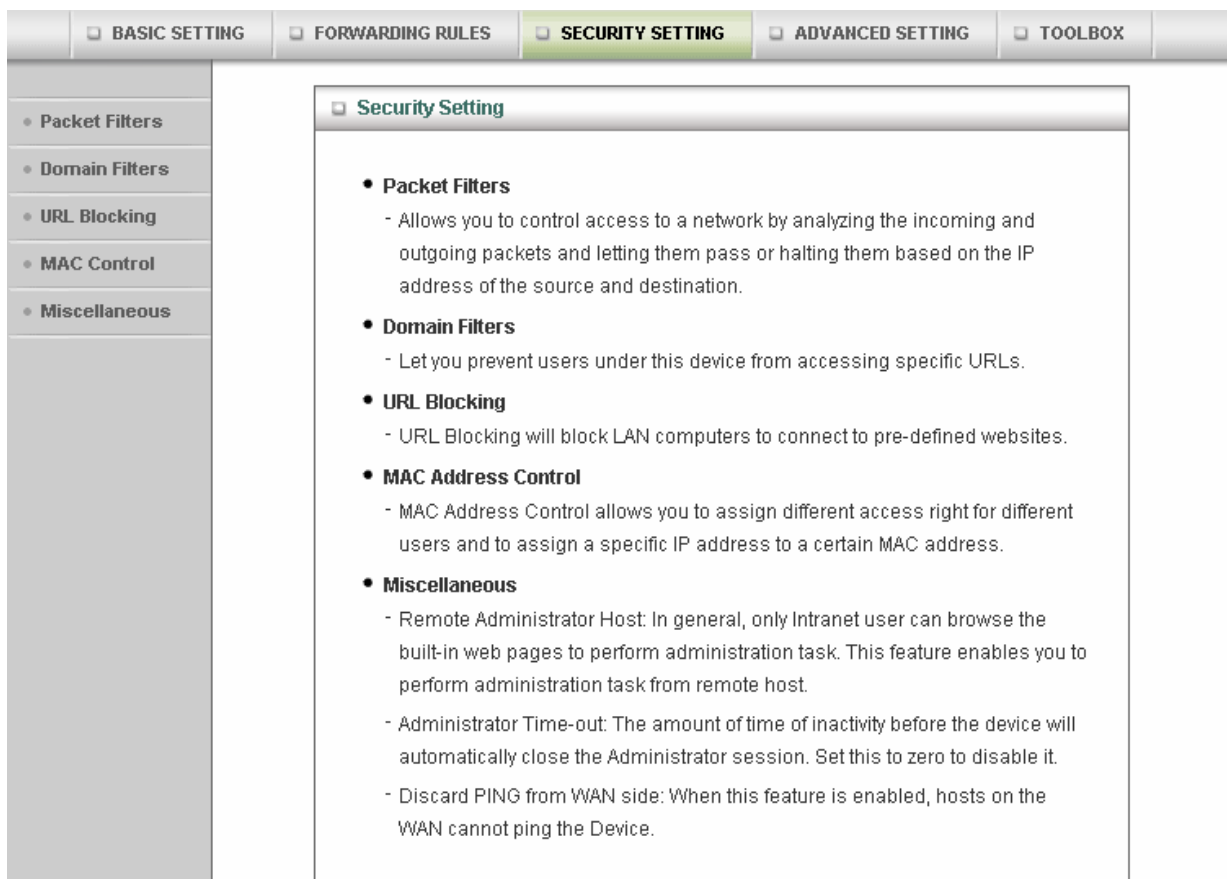
You have to configure this item if you want to access an FTP server whose port number is not 21. This setting will be lost after rebooting.

#### UpnP Setting

The device also supports this function. If the OS supports this function enable it, like Windows Xp. When the user gets IP from Device and will see icon as below:



## 4.6 Security Settings



## 4.6.1 Packet Filter

Multi-Functional Wireless Broadband NAT Router (R1.97f2a)

ADMINISTRATOR's MAIN MENU

Status

Wizard

Logout

BASIC SETTING

FORWARDING RULES

SECURITY SETTING

ADVANCED SETTING

TOOLBOX

Packet Filters

Domain Filters

URL Blocking

MAC Control

Miscellaneous

Outbound Packet Filter

[ HELP ]

Item	Setting			
Outbound Filter	<input type="checkbox"/> Enable			
<div><div><input type="radio"/> Allow all to pass except those match the following rules.</div><div><input checked="" type="radio"/> Deny all to pass except those match the following rules.</div></div>				
Schedule rule (00)Always <input type="button" value="Copy to ID"/> -- <input type="button" value="ID"/>				
ID	Source IP : Ports	Destination IP : Ports	Enable	Schedule Rule#
1	192.168.122.13 : <input type="text"/>	<input type="text"/> : <input type="text"/>	<input type="checkbox"/>	0 <input type="text"/>
2	192.168.122.18 : <input type="text"/>	<input type="text"/> : <input type="text"/>	<input type="checkbox"/>	0 <input type="text"/>
3	192.168.122.226 : <input type="text"/>	<input type="text"/> : <input type="text"/>	<input type="checkbox"/>	0 <input type="text"/>
4	192.168.122.218 : <input type="text"/>	<input type="text"/> : <input type="text"/>	<input type="checkbox"/>	0 <input type="text"/>
5	192.168.122.229 : <input type="text"/>	<input type="text"/> : <input type="text"/>	<input type="checkbox"/>	0 <input type="text"/>
6	<input type="text"/> : <input type="text"/>	<input type="text"/> : <input type="text"/>	<input type="checkbox"/>	0 <input type="text"/>
7	<input type="text"/> : <input type="text"/>	<input type="text"/> : <input type="text"/>	<input type="checkbox"/>	0 <input type="text"/>
8	<input type="text"/> : <input type="text"/>	<input type="text"/> : <input type="text"/>	<input type="checkbox"/>	0 <input type="text"/>

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:

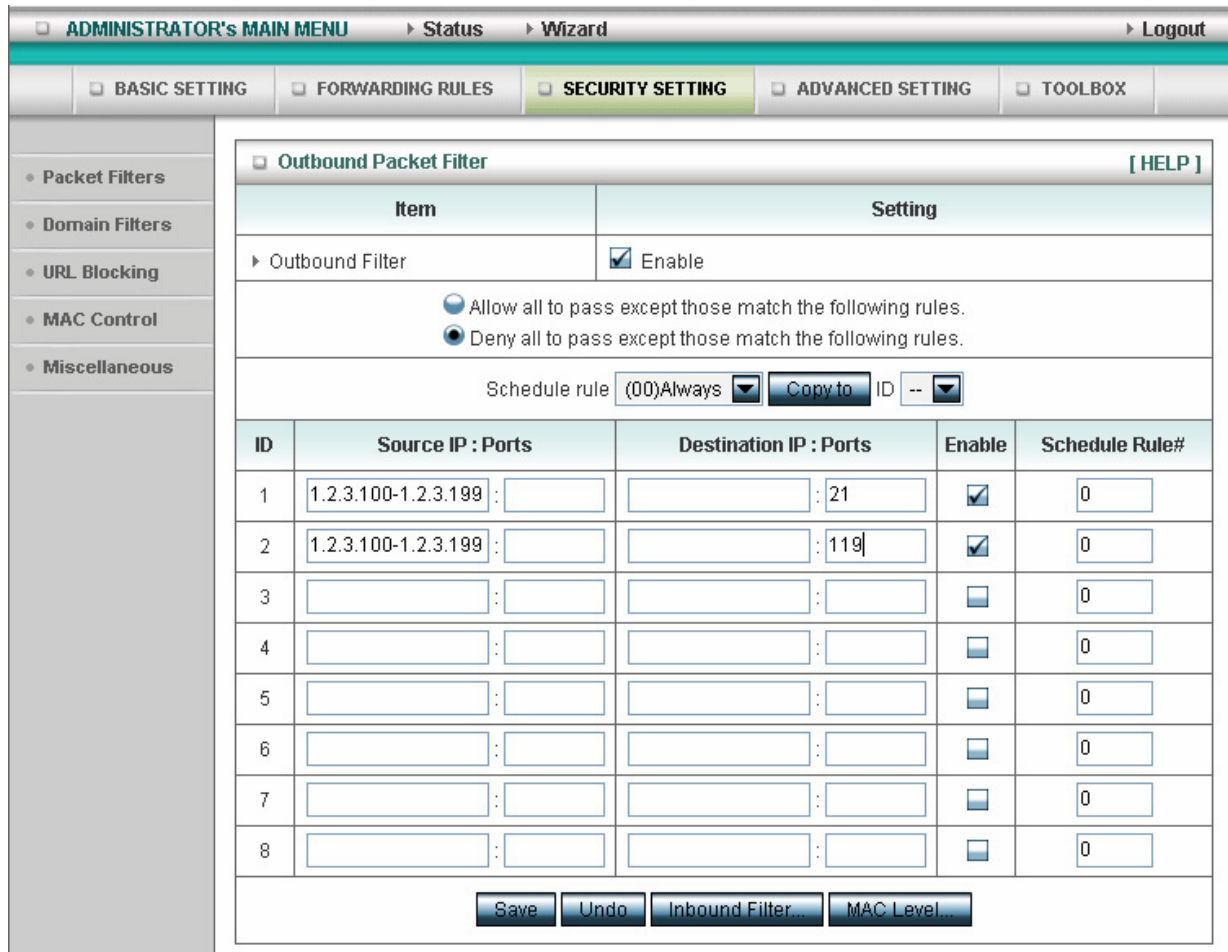
BASIC SETTING		FORWARDING RULES		SECURITY SETTING		ADVANCED SETTING		TOOLBOX																																																						
<div> <div> <ul style="list-style-type: none"> <li>Packet Filters</li> <li>Domain Filters</li> <li>URL Blocking</li> <li>MAC Control</li> <li>Miscellaneous</li> </ul> </div> <div> <div> <div>Outbound Packet Filter</div> <div>[ HELP ]</div> </div> <table border="1"> <thead> <tr> <th>Item</th> <th>Setting</th> </tr> </thead> <tbody> <tr> <td>Outbound Filter</td> <td><input checked="" type="checkbox"/> Enable</td> </tr> <tr> <td colspan="2"> <input type="radio"/> Allow all to pass except those match the following rules.  <input checked="" type="radio"/> Deny all to pass except those match the following rules. </td> </tr> <tr> <td colspan="2"> Schedule rule (00)Always <input type="button" value="Copy to"/> ID -- <input type="button" value="ID"/> </td> </tr> <tr> <th>ID</th> <th>Source IP : Ports</th> <th>Destination IP : Ports</th> <th>Enable</th> <th>Schedule Rule#</th> </tr> <tr> <td>1</td> <td>1.2.3.100-1.2.3.149 : <input type="text"/></td> <td><input type="text"/> : 25-100</td> <td><input checked="" type="checkbox"/></td> <td>0 <input type="text"/></td> </tr> <tr> <td>2</td> <td>1.2.3.10-1.2.3.20 : <input type="text"/></td> <td><input type="text"/> : <input type="text"/></td> <td><input checked="" type="checkbox"/></td> <td>0 <input type="text"/></td> </tr> <tr> <td>3</td> <td><input type="text"/> : <input type="text"/></td> <td><input type="text"/> : <input type="text"/></td> <td><input type="checkbox"/></td> <td>0 <input type="text"/></td> </tr> <tr> <td>4</td> <td><input type="text"/> : <input type="text"/></td> <td><input type="text"/> : <input type="text"/></td> <td><input type="checkbox"/></td> <td>0 <input type="text"/></td> </tr> <tr> <td>5</td> <td><input type="text"/> : <input type="text"/></td> <td><input type="text"/> : <input type="text"/></td> <td><input type="checkbox"/></td> <td>0 <input type="text"/></td> </tr> <tr> <td>6</td> <td><input type="text"/> : <input type="text"/></td> <td><input type="text"/> : <input type="text"/></td> <td><input type="checkbox"/></td> <td>0 <input type="text"/></td> </tr> <tr> <td>7</td> <td><input type="text"/> : <input type="text"/></td> <td><input type="text"/> : <input type="text"/></td> <td><input type="checkbox"/></td> <td>0 <input type="text"/></td> </tr> <tr> <td>8</td> <td><input type="text"/> : <input type="text"/></td> <td><input type="text"/> : <input type="text"/></td> <td><input type="checkbox"/></td> <td>0 <input type="text"/></td> </tr> </tbody> </table> <div> <input type="button" value="Save"/> <input type="button" value="Undo"/> <input type="button" value="Inbound Filter..."/> <input type="button" value="MAC Level..."/> </div> </div> </div>										Item	Setting	Outbound Filter	<input checked="" type="checkbox"/> Enable	<input type="radio"/> Allow all to pass except those match the following rules. <input checked="" type="radio"/> Deny all to pass except those match the following rules.		Schedule rule (00)Always <input type="button" value="Copy to"/> ID -- <input type="button" value="ID"/>		ID	Source IP : Ports	Destination IP : Ports	Enable	Schedule Rule#	1	1.2.3.100-1.2.3.149 : <input type="text"/>	<input type="text"/> : 25-100	<input checked="" type="checkbox"/>	0 <input type="text"/>	2	1.2.3.10-1.2.3.20 : <input type="text"/>	<input type="text"/> : <input type="text"/>	<input checked="" type="checkbox"/>	0 <input type="text"/>	3	<input type="text"/> : <input type="text"/>	<input type="text"/> : <input type="text"/>	<input type="checkbox"/>	0 <input type="text"/>	4	<input type="text"/> : <input type="text"/>	<input type="text"/> : <input type="text"/>	<input type="checkbox"/>	0 <input type="text"/>	5	<input type="text"/> : <input type="text"/>	<input type="text"/> : <input type="text"/>	<input type="checkbox"/>	0 <input type="text"/>	6	<input type="text"/> : <input type="text"/>	<input type="text"/> : <input type="text"/>	<input type="checkbox"/>	0 <input type="text"/>	7	<input type="text"/> : <input type="text"/>	<input type="text"/> : <input type="text"/>	<input type="checkbox"/>	0 <input type="text"/>	8	<input type="text"/> : <input type="text"/>	<input type="text"/> : <input type="text"/>	<input type="checkbox"/>	0 <input type="text"/>
Item	Setting																																																													
Outbound Filter	<input checked="" type="checkbox"/> Enable																																																													
<input type="radio"/> Allow all to pass except those match the following rules. <input checked="" type="radio"/> Deny all to pass except those match the following rules.																																																														
Schedule rule (00)Always <input type="button" value="Copy to"/> ID -- <input type="button" value="ID"/>																																																														
ID	Source IP : Ports	Destination IP : Ports	Enable	Schedule Rule#																																																										
1	1.2.3.100-1.2.3.149 : <input type="text"/>	<input type="text"/> : 25-100	<input checked="" type="checkbox"/>	0 <input type="text"/>																																																										
2	1.2.3.10-1.2.3.20 : <input type="text"/>	<input type="text"/> : <input type="text"/>	<input checked="" type="checkbox"/>	0 <input type="text"/>																																																										
3	<input type="text"/> : <input type="text"/>	<input type="text"/> : <input type="text"/>	<input type="checkbox"/>	0 <input type="text"/>																																																										
4	<input type="text"/> : <input type="text"/>	<input type="text"/> : <input type="text"/>	<input type="checkbox"/>	0 <input type="text"/>																																																										
5	<input type="text"/> : <input type="text"/>	<input type="text"/> : <input type="text"/>	<input type="checkbox"/>	0 <input type="text"/>																																																										
6	<input type="text"/> : <input type="text"/>	<input type="text"/> : <input type="text"/>	<input type="checkbox"/>	0 <input type="text"/>																																																										
7	<input type="text"/> : <input type="text"/>	<input type="text"/> : <input type="text"/>	<input type="checkbox"/>	0 <input type="text"/>																																																										
8	<input type="text"/> : <input type="text"/>	<input type="text"/> : <input type="text"/>	<input type="checkbox"/>	0 <input type="text"/>																																																										

(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   Wizard   Logout

BASIC SETTING   FORWARDING RULES   **SECURITY SETTING**   ADVANCED SETTING   TOOLBOX

Packet Filters  
Domain Filters  
URL Blocking  
MAC Control  
Miscellaneous

**Outbound Packet Filter** [ HELP ]

**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.

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

ID	Source IP : Ports	Destination IP : Ports	Enable	Schedule Rule#
1	1.2.3.100-1.2.3.199 :	: 21	<input checked="" type="checkbox"/>	0
2	1.2.3.100-1.2.3.199 :	: 119	<input checked="" type="checkbox"/>	0
3	:	:	<input type="checkbox"/>	0
4	:	:	<input type="checkbox"/>	0
5	:	:	<input type="checkbox"/>	0
6	:	:	<input type="checkbox"/>	0
7	:	:	<input type="checkbox"/>	0
8	:	:	<input type="checkbox"/>	0

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

(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:

BASIC SETTING		FORWARDING RULES		SECURITY SETTING		ADVANCED SETTING		TOOLBOX																																																						
<ul style="list-style-type: none"> <li>• Packet Filters</li> <li>• Domain Filters</li> <li>• URL Blocking</li> <li>• MAC Control</li> <li>• Miscellaneous</li> </ul>		<div> <div>Inbound Packet Filter</div> <div>[ HELP ]</div> </div> <table border="1"> <thead> <tr> <th>Item</th> <th>Setting</th> </tr> </thead> <tbody> <tr> <td>▶ Inbound Filter</td> <td><input checked="" type="checkbox"/> Enable</td> </tr> <tr> <td colspan="2"> <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.                 </td> </tr> <tr> <td colspan="2">                     Schedule rule (00)Always <input type="button" value="Copy to ID"/> ID -- <input type="button" value="ID"/> </td> </tr> <tr> <th>ID</th> <th>Source IP : Ports</th> <th>Destination IP : Ports</th> <th>Enable</th> <th>Schedule Rule#</th> </tr> <tr> <td>1</td> <td>192.168.123.149 : <input type="text"/></td> <td><input type="text"/> : 25-100</td> <td><input checked="" type="checkbox"/></td> <td><input type="text" value="0"/></td> </tr> <tr> <td>2</td> <td>192.168.123.20 : <input type="text"/></td> <td><input type="text"/> : <input type="text"/></td> <td><input checked="" type="checkbox"/></td> <td><input type="text" value="0"/></td> </tr> <tr> <td>3</td> <td><input type="text"/> : <input type="text"/></td> <td><input type="text"/> : <input type="text"/></td> <td><input type="checkbox"/></td> <td><input type="text" value="0"/></td> </tr> <tr> <td>4</td> <td><input type="text"/> : <input type="text"/></td> <td><input type="text"/> : <input type="text"/></td> <td><input type="checkbox"/></td> <td><input type="text" value="0"/></td> </tr> <tr> <td>5</td> <td><input type="text"/> : <input type="text"/></td> <td><input type="text"/> : <input type="text"/></td> <td><input type="checkbox"/></td> <td><input type="text" value="0"/></td> </tr> <tr> <td>6</td> <td><input type="text"/> : <input type="text"/></td> <td><input type="text"/> : <input type="text"/></td> <td><input type="checkbox"/></td> <td><input type="text" value="0"/></td> </tr> <tr> <td>7</td> <td><input type="text"/> : <input type="text"/></td> <td><input type="text"/> : <input type="text"/></td> <td><input type="checkbox"/></td> <td><input type="text" value="0"/></td> </tr> <tr> <td>8</td> <td><input type="text"/> : <input type="text"/></td> <td><input type="text"/> : <input type="text"/></td> <td><input type="checkbox"/></td> <td><input type="text" value="0"/></td> </tr> </tbody> </table> <div> <input type="button" value="Save"/> <input type="button" value="Undo"/> <input type="button" value="Outbound Filter..."/> <input type="button" value="MAC Level..."/> </div>								Item	Setting	▶ Inbound 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.		Schedule rule (00)Always <input type="button" value="Copy to ID"/> ID -- <input type="button" value="ID"/>		ID	Source IP : Ports	Destination IP : Ports	Enable	Schedule Rule#	1	192.168.123.149 : <input type="text"/>	<input type="text"/> : 25-100	<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"/>
Item	Setting																																																													
▶ Inbound 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.																																																														
Schedule rule (00)Always <input type="button" value="Copy to ID"/> ID -- <input type="button" value="ID"/>																																																														
ID	Source IP : Ports	Destination IP : Ports	Enable	Schedule Rule#																																																										
1	192.168.123.149 : <input type="text"/>	<input type="text"/> : 25-100	<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"/>																																																										

(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:

<input type="checkbox"/> BASIC SETTING <input type="checkbox"/> FORWARDING RULES <input checked="" type="checkbox"/> SECURITY SETTING <input type="checkbox"/> ADVANCED SETTING <input type="checkbox"/> TOOLBOX																																																						
<ul style="list-style-type: none"> <li>• Packet Filters</li> <li>• Domain Filters</li> <li>• URL Blocking</li> <li>• MAC Control</li> <li>• Miscellaneous</li> </ul>	<div> <input checked="" type="checkbox"/> Inbound Packet Filter           <span>[ HELP ]</span> </div> <table border="1"> <thead> <tr> <th>Item</th> <th>Setting</th> </tr> </thead> <tbody> <tr> <td>▶ Inbound Filter</td> <td><input checked="" type="checkbox"/> Enable</td> </tr> <tr> <td colspan="2"> <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.               </td> </tr> <tr> <td colspan="2">                 Schedule rule (00)Always <input type="button" value="Copy to ID"/> -- <input type="button" value="ID"/> </td> </tr> <tr> <th>ID</th> <th>Source IP : Ports</th> <th>Destination IP : Ports</th> <th>Enable</th> <th>Schedule Rule#</th> </tr> <tr> <td>1</td> <td>192.168.123.100 : <input type="text"/></td> <td><input type="text"/> : 21</td> <td><input checked="" type="checkbox"/></td> <td><input type="text" value="0"/></td> </tr> <tr> <td>2</td> <td>192.168.123.119 : <input type="text"/></td> <td><input type="text"/> : 119</td> <td><input checked="" type="checkbox"/></td> <td><input type="text" value="0"/></td> </tr> <tr> <td>3</td> <td><input type="text"/> : <input type="text"/></td> <td><input type="text"/> : <input type="text"/></td> <td><input type="checkbox"/></td> <td><input type="text" value="0"/></td> </tr> <tr> <td>4</td> <td><input type="text"/> : <input type="text"/></td> <td><input type="text"/> : <input type="text"/></td> <td><input type="checkbox"/></td> <td><input type="text" value="0"/></td> </tr> <tr> <td>5</td> <td><input type="text"/> : <input type="text"/></td> <td><input type="text"/> : <input type="text"/></td> <td><input type="checkbox"/></td> <td><input type="text" value="0"/></td> </tr> <tr> <td>6</td> <td><input type="text"/> : <input type="text"/></td> <td><input type="text"/> : <input type="text"/></td> <td><input type="checkbox"/></td> <td><input type="text" value="0"/></td> </tr> <tr> <td>7</td> <td><input type="text"/> : <input type="text"/></td> <td><input type="text"/> : <input type="text"/></td> <td><input type="checkbox"/></td> <td><input type="text" value="0"/></td> </tr> <tr> <td>8</td> <td><input type="text"/> : <input type="text"/></td> <td><input type="text"/> : <input type="text"/></td> <td><input type="checkbox"/></td> <td><input type="text" value="0"/></td> </tr> </tbody> </table> <div> <input type="button" value="Save"/> <input type="button" value="Undo"/> <input type="button" value="Outbound Filter..."/> <input type="button" value="MAC Level..."/> </div>	Item	Setting	▶ Inbound 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.		Schedule rule (00)Always <input type="button" value="Copy to ID"/> -- <input type="button" value="ID"/>		ID	Source IP : Ports	Destination IP : Ports	Enable	Schedule Rule#	1	192.168.123.100 : <input type="text"/>	<input type="text"/> : 21	<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"/>
	Item	Setting																																																				
	▶ Inbound 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.																																																					
	Schedule rule (00)Always <input type="button" value="Copy to ID"/> -- <input type="button" value="ID"/>																																																					
	ID	Source IP : Ports	Destination IP : Ports	Enable	Schedule Rule#																																																	
1	192.168.123.100 : <input type="text"/>	<input type="text"/> : 21	<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"/>																																																		

(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

Logout

BASIC SETTING

FORWARDING RULES

SECURITY SETTING

ADVANCED SETTING

TOOLBOX

• Packet Filters

• Domain Filters

• URL Blocking

• MAC Control

• Miscellaneous

Domain Filter

[ HELP ]

Item	Setting
Domain Filter	<input checked="" type="checkbox"/> Enable
Log DNS Query	<input checked="" type="checkbox"/> Enable
Privilege IP Addresses Range	From <input type="text" value="0"/> To <input type="text" value="0"/>

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

### 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:

<input type="checkbox"/> BASIC SETTING <input type="checkbox"/> FORWARDING RULES <input checked="" type="checkbox"/> SECURITY SETTING <input type="checkbox"/> ADVANCED SETTING <input type="checkbox"/> TOOLBOX																																																						
<ul style="list-style-type: none"> <li>• Packet Filters</li> <li>• Domain Filters</li> <li>• URL Blocking</li> <li>• MAC Control</li> <li>• Miscellaneous</li> </ul>	<div> <input checked="" type="checkbox"/> Domain Filter           <span>[ HELP ]</span> </div> <table border="1"> <thead> <tr> <th>Item</th> <th>Setting</th> </tr> </thead> <tbody> <tr> <td>▶ Domain Filter</td> <td><input checked="" type="checkbox"/> Enable</td> </tr> <tr> <td>▶ Log DNS Query</td> <td><input checked="" type="checkbox"/> Enable</td> </tr> <tr> <td>▶ Privilege IP Addresses Range</td> <td>From <input type="text" value="1"/> To <input type="text" value="20"/></td> </tr> </tbody> </table> <table border="1"> <thead> <tr> <th>ID</th> <th>Domain Suffix</th> <th>Action</th> <th>Enable</th> </tr> </thead> <tbody> <tr> <td>1</td> <td><input type="text" value="www.msn.com"/></td> <td><input checked="" type="checkbox"/> Drop <input checked="" type="checkbox"/> Log</td> <td><input checked="" type="checkbox"/></td> </tr> <tr> <td>2</td> <td><input type="text" value="www.sina.com"/></td> <td><input type="checkbox"/> Drop <input checked="" type="checkbox"/> Log</td> <td><input checked="" type="checkbox"/></td> </tr> <tr> <td>3</td> <td><input type="text" value="www.google.com"/></td> <td><input checked="" type="checkbox"/> Drop <input type="checkbox"/> Log</td> <td><input checked="" type="checkbox"/></td> </tr> <tr> <td>4</td> <td><input type="text"/></td> <td><input type="checkbox"/> Drop <input type="checkbox"/> Log</td> <td><input type="checkbox"/></td> </tr> <tr> <td>5</td> <td><input type="text"/></td> <td><input type="checkbox"/> Drop <input type="checkbox"/> Log</td> <td><input type="checkbox"/></td> </tr> <tr> <td>6</td> <td><input type="text"/></td> <td><input type="checkbox"/> Drop <input type="checkbox"/> Log</td> <td><input type="checkbox"/></td> </tr> <tr> <td>7</td> <td><input type="text"/></td> <td><input type="checkbox"/> Drop <input type="checkbox"/> Log</td> <td><input type="checkbox"/></td> </tr> <tr> <td>8</td> <td><input type="text"/></td> <td><input type="checkbox"/> Drop <input type="checkbox"/> Log</td> <td><input type="checkbox"/></td> </tr> <tr> <td>9</td> <td><input type="text"/></td> <td><input type="checkbox"/> Drop <input type="checkbox"/> Log</td> <td><input type="checkbox"/></td> </tr> <tr> <td>10</td> <td>* (all others)</td> <td><input type="checkbox"/> Drop <input type="checkbox"/> Log</td> <td>-</td> </tr> </tbody> </table> <div> <input type="button" value="Save"/> <input type="button" value="Undo"/> </div>		Item	Setting	▶ Domain Filter	<input checked="" type="checkbox"/> Enable	▶ Log DNS Query	<input checked="" type="checkbox"/> Enable	▶ Privilege IP Addresses Range	From <input type="text" value="1"/> To <input type="text" value="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 others)	<input type="checkbox"/> Drop <input type="checkbox"/> Log	-
	Item	Setting																																																				
	▶ Domain Filter	<input checked="" type="checkbox"/> Enable																																																				
	▶ Log DNS Query	<input checked="" type="checkbox"/> Enable																																																				
	▶ Privilege IP Addresses Range	From <input type="text" value="1"/> To <input type="text" value="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 others)	<input type="checkbox"/> Drop <input type="checkbox"/> Log	-																																																			

In this example:

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

### 4.6.3 URL Blocking

URL Blocking [ HELP ]		
Item		Setting
▶ URL Blocking		<input type="checkbox"/> 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"/>
<input type="button" value="Save"/> <input type="button" value="Undo"/>		

**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
Logout

BASIC SETTING
FORWARDING RULES
SECURITY SETTING
ADVANCED SETTING
TOOLBOX

- Packet Filters
- Domain Filters
- URL Blocking
- MAC Control
- Miscellaneous

URL Blocking [ HELP ]

Item		Setting
URL Blocking		<input checked="" type="checkbox"/> Enable
ID	URL	Enable
1	msn	<input checked="" type="checkbox"/>
2	sina	<input checked="" type="checkbox"/>
3	cnnsi	<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"/>

Save
Undo

In this example:

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

## 4.6.4 MAC Address Control

Multi-Functional Wireless Broadband NAT Router (R1.97f2a)

ADMINISTRATOR's MAIN MENU

Status

Wizard

Logout

BASIC SETTING

FORWARDING RULES

SECURITY SETTING

ADVANCED SETTING

TOOLBOX

Packet Filters

Domain Filters

URL Blocking

MAC Control

Miscellaneous

MAC Address Control [HELP]

Item	Setting			
MAC Address Control	<input checked="" type="checkbox"/> Enable			
<input checked="" type="checkbox"/> Connection control	Wireless and wired clients with <b>C</b> checked can connect to this device; and <input type="text" value="deny"/> unspecified MAC addresses to connect.			
<input type="checkbox"/> Association control	Wireless clients with <b>A</b> checked can associate to the wireless LAN; and <input type="text" value="deny"/> unspecified MAC addresses to associate.			
DHCP clients <input type="text" value="--- Select one ---"/> <input type="button" value="Copy to"/> ID <input type="text" value="--"/>				
ID	MAC Address	IP Address	C	A
1	<input type="text" value="00-90-CC-1D-9D-40"/>	192.168.122. <input type="text" value="13"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
2	<input type="text" value="00-50-BA-24-05-E7"/>	192.168.122. <input type="text" value="18"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
3	<input type="text" value="00-90-CC-15-79-DC"/>	192.168.122. <input type="text" value="218"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
4	<input type="text" value="00-50-18-FF-12-34"/>	192.168.122. <input type="text" value="226"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<div><input type="button" value="=&lt; Previous"/> <input type="button" value="Next &gt;="/> <input type="button" value="Save"/> <input type="button" value="Undo"/></div>				

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

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

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

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

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

#### Control table

ID	MAC Address	IP Address	C	A
9	<input type="text"/>	192.168.122. <input type="text"/>	<input type="checkbox"/>	<input type="checkbox"/>
10	<input type="text"/>	192.168.122. <input type="text"/>	<input type="checkbox"/>	<input type="checkbox"/>
11	<input type="text"/>	192.168.122. <input type="text"/>	<input type="checkbox"/>	<input type="checkbox"/>
12	<input type="text"/>	192.168.122. <input type="text"/>	<input type="checkbox"/>	<input type="checkbox"/>

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

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

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

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.

**Example:**

**Multi-Functional Wireless Broadband NAT Router (R1.97f2a)**

☐ ADMINISTRATOR's MAIN MENU    ▶ Status    ▶ Wizard    ▶ Logout

☐ BASIC SETTING    ☐ FORWARDING RULES    ☒ SECURITY SETTING    ☐ ADVANCED SETTING    ☐ TOOLBOX

- Packet Filters
- Domain Filters
- URL Blocking
- **MAC Control**
- Miscellaneous

☒ **MAC Address Control** [ HELP ]

Item	Setting			
▶ MAC Address Control	<input checked="" type="checkbox"/> Enable			
<input checked="" type="checkbox"/> Connection control	Wireless and wired clients with <b>C</b> checked can connect to this device; and <input type="text" value="allow"/> unspecified MAC addresses to connect.			
<input checked="" type="checkbox"/> Association control	Wireless clients with <b>A</b> checked can associate to the wireless LAN; and <input type="text" value="deny"/> unspecified MAC addresses to associate.			
DHCP clients <input type="text" value="--- Select one ---"/> <input type="button" value="Copy to"/> ID <input type="text" value="--"/>				
ID	MAC Address	IP Address	C	A
9	<input type="text" value="00-12-34-56-78-90"/>	192.168.122. <input type="text" value="100"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
10	<input type="text" value="00-12-34-56-78-92"/>	192.168.122. <input type="text"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
11	<input type="text" value="00-09-76-54-32-10"/>	192.168.122. <input type="text" value="101"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
12	<input type="text"/>	192.168.122. <input type="text"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="button" value=" &lt;&lt; Previous"/> <input type="button" value="Next &gt;&gt;"/> <input type="button" value="Save"/> <input type="button" value="Undo"/>				

In this scenario, there are three clients listed in the Control Table. Clients 1 and 2 are wireless, and client 3 is wired.

- 1.The "MAC Address Control" function is enabled.
- 2."Connection control" is enabled, and all of the wired and wireless clients not listed in the "Control table" are "allowed" to connect to this device.
- 3."Association control" is enabled, and all of the wireless clients not listed in the "Control table" are "denied" to associate to the wireless LAN.
- 4.Clients 1 and 3 have fixed IP addresses either from the DHCP server of this device or manually assigned:

ID 1 - "00-12-34-56-78-90" --> 192.168.122.100

ID 3 - "00-98-76-54-32-10" --> 192.168.122.101

Client 2 will obtain its IP address from the IP Address pool specified in the "DHCP Server" page or can use a manually assigned static IP address.

If, for example, client 3 tries to use an IP address different from the address listed in the Control table (192.168.122.101), it will be denied to connect to this device.



5. Clients 2 and 3 and other wired clients with a MAC address unspecified in the Control table are all allowed to connect to this device. But client 1 is denied to connect to this device.
6. Clients 1 and 2 are allowed to associate to the wireless LAN, but a wireless client with a MAC address not specified in the Control table is denied to associate to the wireless LAN. Client 3 is a wired client and so is not affected by Association control.

#### 4.6.5 Miscellaneous Items

**Multi-Functional Wireless Broadband NAT Router (R1.97f2a)**

ADMINISTRATOR's MAIN MENU   Status   Wizard   Logout

BASIC SETTING   FORWARDING RULES   **SECURITY SETTING**   ADVANCED SETTING   TOOLBOX

Packet Filters  
Domain Filters  
URL Blocking  
MAC Control  
Miscellaneous

**Miscellaneous Items** [ HELP ]

Item	Setting	Enable
▶ Remote Administrator Host / Port	0.0.0.0 / 8089	<input checked="" type="checkbox"/>
▶ Administrator Time-out	600 seconds (0 to disable)	
▶ Discard PING from WAN side		<input type="checkbox"/>
▶ SPI mode		<input type="checkbox"/>
▶ DoS Attack Detection		<input type="checkbox"/>

Save Undo

##### 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 specify 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.

## 4.7 Advanced Settings

The screenshot displays the web interface of a Multi-Functional Wireless Broadband NAT Router (R1.97f2a). The top navigation bar includes links for ADMINISTRATOR's MAIN MENU, Status, Wizard, and Logout. Below this, a secondary menu highlights the ADVANCED SETTING tab, alongside BASIC SETTING, FORWARDING RULES, SECURITY SETTING, and TOOLBOX. On the left side, a vertical sidebar lists various configuration options: System Time, System Log, Dynamic DNS, SNMP, Routing, and Schedule Rule. The main content area, titled 'Advanced Setting', provides detailed descriptions for each of these options:

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

## 4.7.1 System Time

<input type="checkbox"/> BASIC SETTING		<input type="checkbox"/> FORWARDING RULES	<input type="checkbox"/> SECURITY SETTING	<input checked="" type="checkbox"/> <b>ADVANCED SETTING</b>	<input type="checkbox"/> TOOLBOX
--	--	---	---	---	----------------------------------

<ul style="list-style-type: none"><li>• System Time</li><li>• System Log</li><li>• Dynamic DNS</li><li>• SNMP</li><li>• Routing</li><li>• Schedule Rule</li></ul>	<input checked="" type="checkbox"/> <b>System Time</b> <span style="float: right;">[ HELP ]</span>	
	<b>Item</b>	<b>Setting</b>
	▶ System Time	2006年6月24日 下午 05:40:49
	▶ <input checked="" type="radio"/> Get Date and Time by NTP Protocol	<input type="button" value="Sync Now !"/>
	Time Server	time.nist.gov ▼
	Time Zone	(GMT-08:00) Pacific Time (US & Canada) ▼
	▶ <input type="radio"/> Set Date and Time using PC's Date and Time	
	PC Date and Time	2006年10月5日 上午 11:10:01
	▶ <input checked="" type="radio"/> Set Date and Time manually	
	Date	Year: 2006 ▼ Month: Jun ▼ Day: 01 ▼
	Time	Hour: 0 (0-23) Minute: 0 (0-59) Second: 0 (0-59)
	▶ Daylight Saving	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Start	Month: Jan ▼ Day: 01 ▼ Hour: 00 ▼	
End	Month: Jan ▼ Day: 01 ▼ Hour: 00 ▼	
<input type="button" value="Save"/> <input type="button" value="Undo"/>		

### 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.

#### 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

**Daylight Saving:** Set up where the location is.

## 4.7.2 System Log

Multi-Functional Wireless Broadband NAT Router (R1.97f2a)

ADMINISTRATOR's MAIN MENU   Status   Wizard   Logout

BASIC SETTING   FORWARDING RULES   SECURITY SETTING   **ADVANCED SETTING**   TOOLBOX

System Time  
System Log  
Dynamic DNS  
SNMP  
Routing  
Schedule Rule

**System Log** [ HELP ]

Item	Setting	Enable
▶ IP Address for Syslogd	192.168.122. <input type="text"/>	<input type="checkbox"/>
▶ IP Address of Outgoing Mail Server	<input type="button" value="Send Mail Now"/>	<input type="checkbox"/>
• SMTP Server IP/Port	<input type="text"/>	
• E-mail addresses	<input type="text"/>	
• E-mail Subject	<input type="text"/>	
• User name	<input type="text"/>	
• Password	<input type="text"/>	
▶ Log Type	<input checked="" type="checkbox"/> System Activity <input checked="" type="checkbox"/> Debug Information <input checked="" type="checkbox"/> Attacks <input checked="" type="checkbox"/> Dropped Packets <input checked="" type="checkbox"/> Notice	

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

The screenshot shows a web-based configuration interface. At the top, there is a navigation bar with 'ADMINISTRATOR's MAIN MENU', 'Status', 'Wizard', and 'Logout'. Below this is a tabbed menu with 'BASIC SETTING', 'FORWARDING RULES', 'SECURITY SETTING', 'ADVANCED SETTING' (which is selected), and 'TOOLBOX'. On the left side, there is a sidebar menu with 'System Time', 'System Log', 'Dynamic DNS' (selected), 'SNMP', 'Routing', and 'Schedule Rule'. The main content area is titled 'Dynamic DNS' with a '[ HELP ]' link. It contains a table with two columns: 'Item' and 'Setting'. The table has five rows: 'DDNS' with radio buttons for 'Disable' and 'Enable' (where 'Enable' is selected); 'Provider' with a dropdown menu showing 'No-IP.com'; 'Host Name' with a text input field; 'Username / E-mail' with a text input field; and 'Password / Key' with a text input field. At the bottom of the table are 'Save' and 'Undo' buttons.

Item	Setting
▶ DDNS	<input type="radio"/> Disable <input checked="" type="radio"/> Enable
▶ Provider	No-IP.com ▼
▶ Host Name	<input type="text"/>
▶ Username / E-mail	<input type="text"/>
▶ Password / Key	<input type="text"/>

Save Undo

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

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

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

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

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

You have to define:

Provider

Host Name

Username/E-mail

Password/Key

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

**Example:**

The screenshot shows the web interface of a Multi-Functional Wireless Broadband NAT Router (R1.97f2a). The top navigation bar includes 'ADMINISTRATOR's MAIN MENU', 'Status', 'Wizard', and 'Logout'. Below this is a secondary menu with 'BASIC SETTING', 'FORWARDING RULES', 'SECURITY SETTING', 'ADVANCED SETTING' (highlighted), and 'TOOLBOX'. On the left, a sidebar lists various settings: 'System Time', 'System Log', 'Dynamic DNS' (selected), 'SNMP', 'Routing', and 'Schedule Rule'. The main content area is titled 'Dynamic DNS' with a '[ HELP ]' link. It contains a table with two columns: 'Item' and 'Setting'. The table has five rows: 'DDNS' with radio buttons for 'Disable' and 'Enable' (the latter is selected); 'Provider' with a dropdown menu showing 'No-IP.com'; 'Host Name' with a text input field containing 'faelinux.no-ip.com'; 'Username / E-mail' with a text input field containing 'costra@amit.com.tw'; and 'Password / Key' with a text input field containing six asterisks. At the bottom of the table are 'Save' and 'Undo' buttons.

Item	Setting
DDNS	<input type="radio"/> Disable <input checked="" type="radio"/> Enable
Provider	No-IP.com
Host Name	faelinux.no-ip.com
Username / E-mail	costra@amit.com.tw
Password / Key	*****

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

#### 4.7.4 SNMP Setting

The screenshot shows the 'SNMP Setting' configuration page. It has a title bar with 'SNMP Setting' and a '[ HELP ]' link. Below is a table with two columns: 'Item' and 'Setting'. The table has four rows: 'Enable SNMP' with checkboxes for 'Local' (checked) and 'Remote'; 'Get Community' with a text input field containing 'public'; 'Set Community' with a text input field containing 'private'; and 'WAN Access IP Address' with a text input field containing '0.0.0.0'. At the bottom of the table are 'Save' and 'Undo' buttons.

Item	Setting
Enable SNMP	<input checked="" type="checkbox"/> Local <input type="checkbox"/> Remote
Get Community	public
Set Community	private
WAN Access IP Address	0.0.0.0

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.

#### **WAN Access IP Address**

IF the user wants to limit to specific the ip address to access,please input in the item.The default 0.0.0.0 and means every ip of Internet can get some information of device with snmp protocol.

## 4.7.5 Routing

Multi-Functional Wireless Broadband NAT Router (R1.97f2a)

ADMINISTRATOR's MAIN MENU

Status

Wizard

Logout

BASIC SETTING

FORWARDING RULES

SECURITY SETTING

ADVANCED SETTING

TOOLBOX

• System Time

• System Log

• Dynamic DNS

• SNMP

• Routing

• Schedule Rule

Routing Table [ HELP ]

Dynamic Routing

☒ Disable

☐ RIPv1

☐ RIPv2

Static Routing

☐ Disable

☒ Enable

ID	Destination	Subnet Mask	Gateway	Hop	Enable
1	192.168.123.0	255.255.255.0	192.168.122.3	1	<input checked="" type="checkbox"/>
2	192.168.19.0	255.255.255.0	192.168.122.18	1	<input checked="" type="checkbox"/>
3					<input type="checkbox"/>
4					<input type="checkbox"/>
5					<input type="checkbox"/>
6					<input type="checkbox"/>
7					<input type="checkbox"/>
8					<input type="checkbox"/>

Save

Undo

**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.

### Dynamic Routing

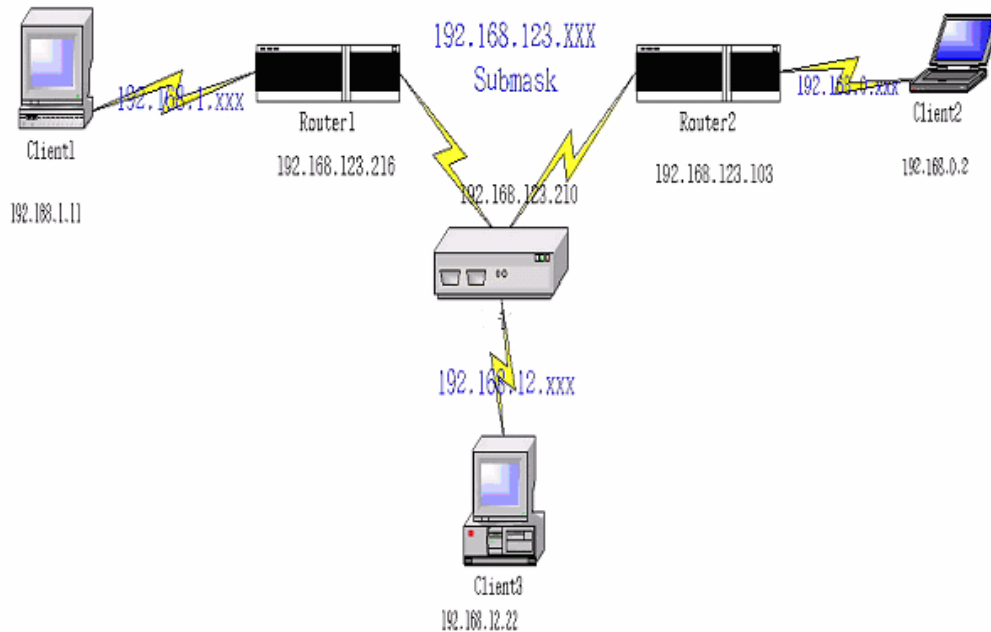
Routing Information Protocol (RIP) will exchange information about destinations for computing routes throughout the network. Please select RIPv2 only if you have different subnet in your network.

Otherwise, please select RIPv1 if you need this protocol.

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



### Example:



### Configuration on NAT Router

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

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

And if it sends Packets to 192.168.1.11 will go via 192.168.123.216

Each rule can be enabled or disabled individually.

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

## 4.7.6 Schedule Rule

ADMINISTRATOR's MAIN MENU

Status

Wizard

Logout

BASIC SETTING

FORWARDING RULES

SECURITY SETTING

ADVANCED SETTING

TOOLBOX

• System Time

• System Log

• Dynamic DNS

• SNMP

• Routing

• Schedule Rule

Schedule Rule

[ HELP ]

Item		Setting
Schedule		<input type="checkbox"/> Enable
Rule#	Rule Name	Action
		<div>SaveAdd New Rule...</div>

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
Logout

BASIC SETTING
FORWARDING RULES
SECURITY SETTING
ADVANCED SETTING
TOOLBOX

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

Schedule Rule Setting
[ HELP ]

Item	Setting	
▶ Name of Rule 1	<input type="text"/>	
▶ System Time	2006年6月24日 下午 06:07:06	
Week Day	Start Time (hh:mm)	End Time (hh:mm)
Sunday	<input type="text"/> : <input type="text"/>	<input type="text"/> : <input type="text"/>
Monday	<input type="text"/> : <input type="text"/>	<input type="text"/> : <input type="text"/>
Tuesday	<input type="text"/> : <input type="text"/>	<input type="text"/> : <input type="text"/>
Wednesday	<input type="text"/> : <input type="text"/>	<input type="text"/> : <input type="text"/>
Thursday	<input type="text"/> : <input type="text"/>	<input type="text"/> : <input type="text"/>
Friday	<input type="text"/> : <input type="text"/>	<input type="text"/> : <input type="text"/>
Saturday	<input type="text"/> : <input type="text"/>	<input type="text"/> : <input type="text"/>
Every Day	14 : 10	16 : 20

Save
Undo
Back

**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
Logout

BASIC SETTING
**FORWARDING RULES**
SECURITY SETTING
ADVANCED SETTING
TOOLBOX

- Virtual Server
- Special AP
- Miscellaneous

Virtual Server [ HELP ]

Well known services -- select one -- use Schedule rule (00)Always Copy to ID --

ID	Server IP	Service Ports	Protocol	Enable	Schedule Rule#
1	192.168.122.33	21	Both	<input checked="" type="checkbox"/>	1
2	192.168.122.13		Both	<input type="checkbox"/>	0
3	192.168.122.226		Both	<input type="checkbox"/>	0
4	192.168.122.229		Both	<input type="checkbox"/>	0
5	192.168.122.218		Both	<input type="checkbox"/>	0
6	192.168.122.218		Both	<input type="checkbox"/>	0
7	192.168.122.218		Both	<input type="checkbox"/>	0
8	192.168.122.218		Both	<input type="checkbox"/>	0
9	192.168.122.13		Both	<input type="checkbox"/>	0
10	192.168.122.		Both	<input type="checkbox"/>	0

Next >>
Save
Undo

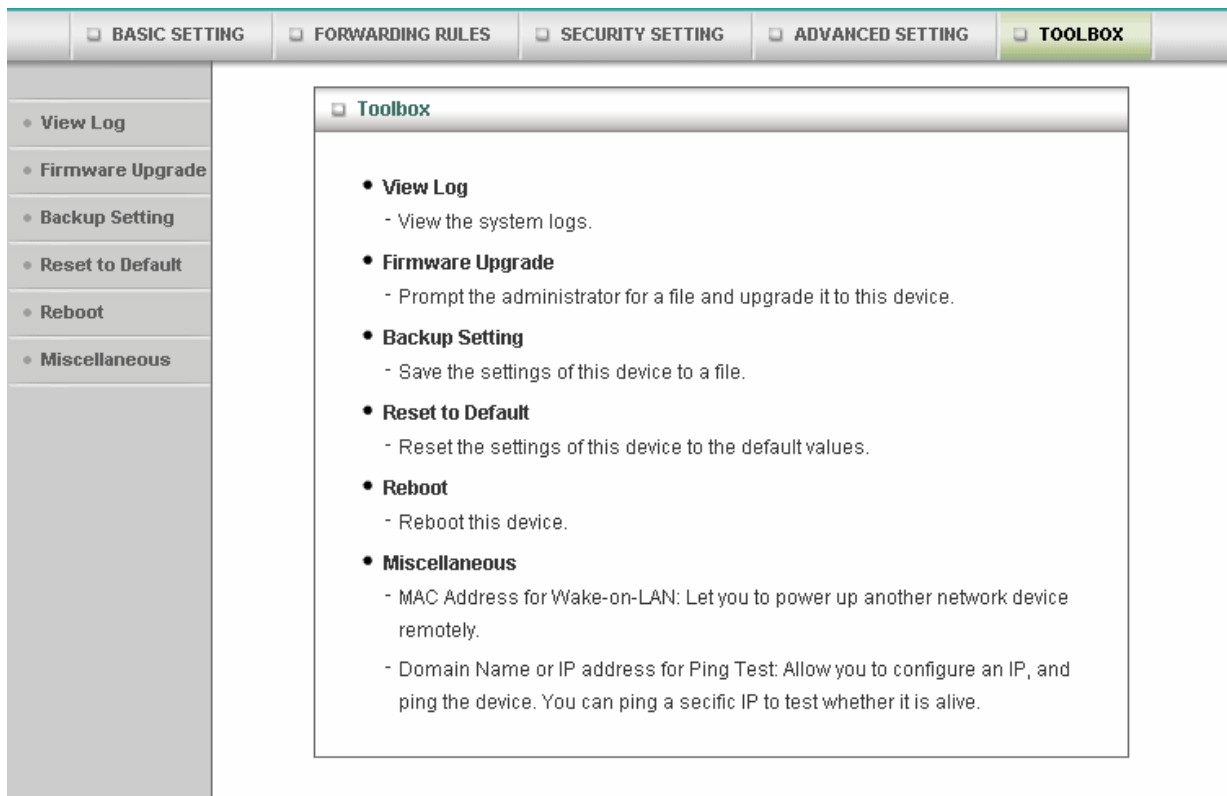
Example2: **Packet Filter** – Apply Rule#1 (ftp time: everyday 14:10 to 16:20).

Outbound Packet Filter

[ HELP ]

Item	Setting			
► Outbound Filter	<input checked="" type="checkbox"/> Enable			
<input type="radio"/> Allow all to pass except those match the following rules. <input checked="" type="radio"/> Deny all to pass except those match the following rules.				
Schedule rule (00)Always   ID --				
ID	Source IP : Ports	Destination IP : Ports	Enable	Schedule Rule#
1	<input type="text"/> : <input type="text"/>	<input type="text"/> : 20-21	<input checked="" type="checkbox"/>	<input type="text" value="1"/>
2	<input type="text"/> : <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 checked="" type="checkbox"/>	<input type="text" value="0"/>
4	<input type="text"/> : <input type="text"/>	<input type="text"/> : <input type="text"/>	<input checked="" type="checkbox"/>	<input type="text" value="0"/>
5	<input type="text"/> : <input type="text"/>	<input type="text"/> : <input type="text"/>	<input checked="" 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"/>

## 4.8 Toolbox



### 4.8.1 System Log

System Log	
ITEM	Info
WAN Type	Dynamic IP Address (R1.97f2a)
Display time	Sat Jun 24 18:15:35 2006
Time	Log
2006年6月24日 下午 06:12:00	Block 00-E0-18-06-BF-24 because deny all
2006年6月24日 下午 06:12:00	Block 00-50-BA-04-D9-B5 because deny all
2006年6月24日 下午 06:12:00	Block 00-20-ED-5F-F8-35 because deny all
2006年6月24日 下午 06:12:01	Block 00-50-8D-50-C6-CA because deny all
2006年6月24日 下午 06:12:01	Block 00-E0-18-06-BF-24 because deny all
2006年6月24日 下午 06:12:01	Block 00-50-18-00-0F-FA because deny all
2006年6月24日 下午 06:12:01	Block 00-50-BA-04-D9-B5 because deny all
2006年6月24日 下午 06:12:01	Block 00-20-ED-5F-F8-35 because deny all
2006年6月24日 下午 06:12:02	Block 00-13-D4-29-7A-D5 because deny all
2006年6月24日 下午 06:12:02	Block 00-50-BA-04-D9-B5 because deny all
2006年6月24日 下午 06:12:02	Block 00-50-BA-04-D9-B5 because deny all
2006年6月24日 下午 06:12:02	Block 00-20-ED-5F-F8-35 because deny all
2006年6月24日 下午 06:12:02	Block 00-50-BA-04-D9-B5 because deny all
2006年6月24日 下午 06:12:02	Block 00-50-18-00-0F-F6 because deny all
2006年6月24日 下午 06:12:02	Block 00-13-D4-BA-23-93 because deny all

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



#### 4.8.2 Firmware Upgrade

Firmware Upgrade

Firmware Filename

瀏覽...

Current firmware version is R1.97f2a. The upgrade procedure takes about 20 seconds.

Note! Do not power off the unit when it is being upgraded.

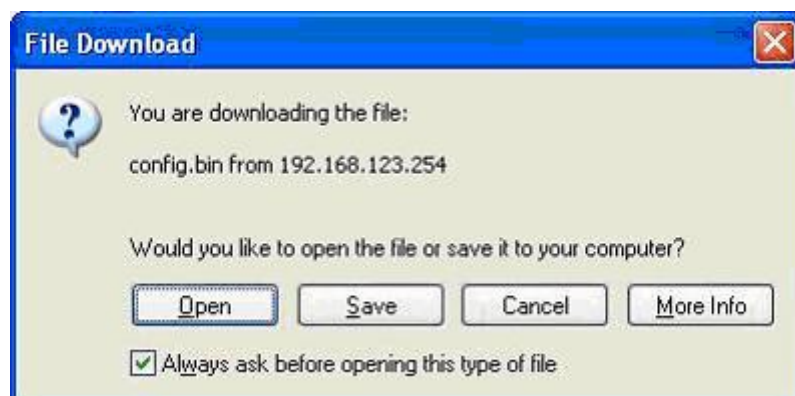
When the upgrade is done successfully, the unit will be restarted automatically.

Upgrade

Cancel

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

Miscellaneous Items [ HELP ]	
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 Test

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

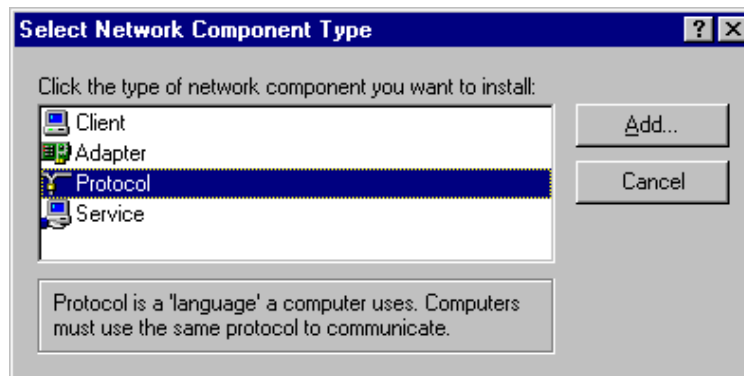


## Appendix A TCP/IP Configuration for Windows 95/98

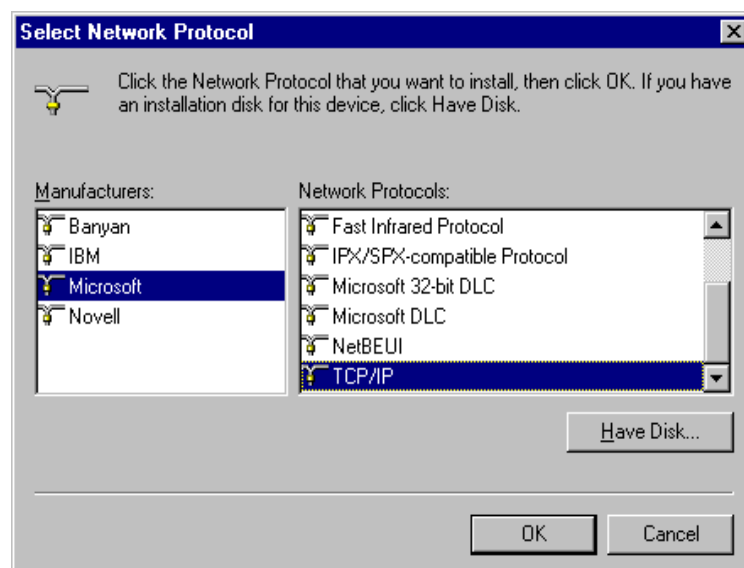
This section introduces you how to install TCP/IP protocol into your personal computer. And suppose you have been successfully installed one network card on your personal computer. If not, please refer to your network card manual. Moreover, the Section B.2 tells you how to set TCP/IP values for working 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**.
2. Double click **Network** icon and select **Configuration** tab in the Network window.
3. Click **Add** button to add network component into your PC.
4. Double click **Protocol** to add TCP/IP protocol.



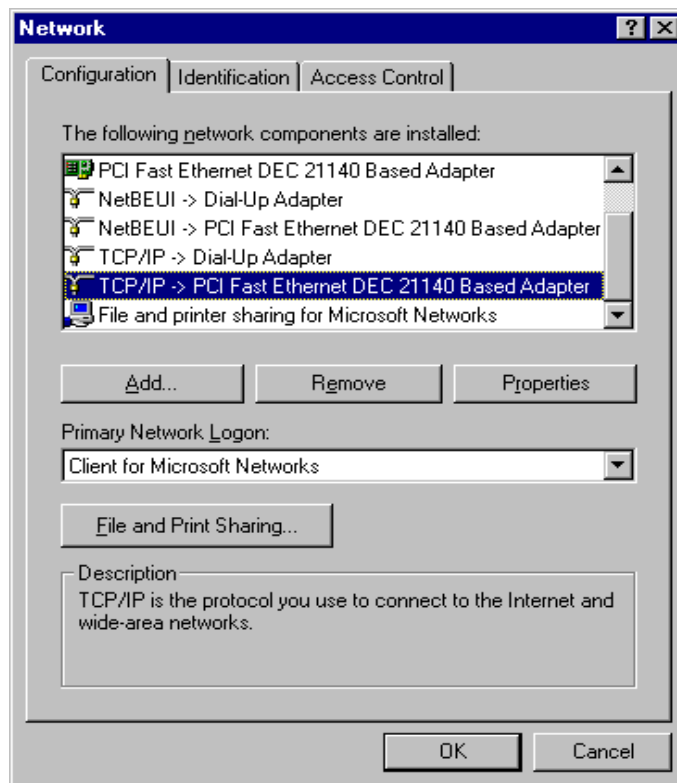
5. Select **Microsoft** item in the manufactures list. And choose **TCP/IP** in the Network Protocols. Click **OK** button to return to Network window.



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

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

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



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

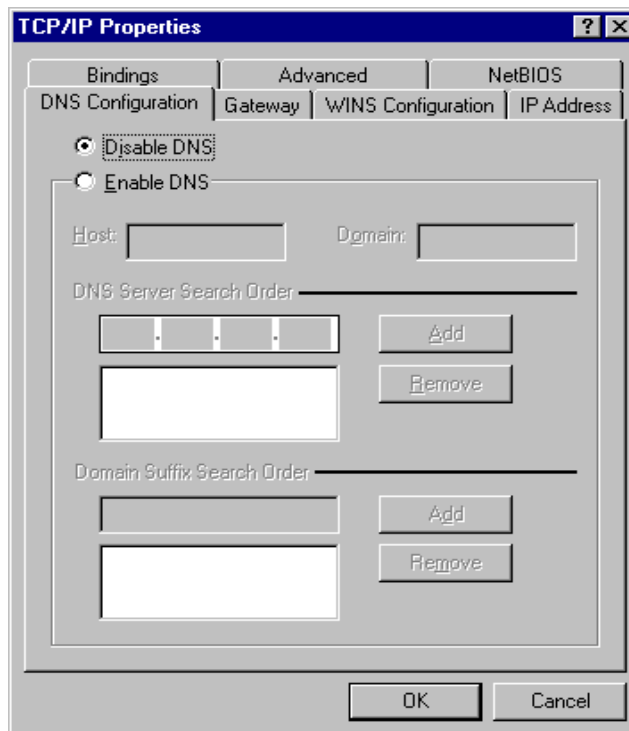
- a. Select **Obtain an IP address automatically** in the IP Address tab.

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

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

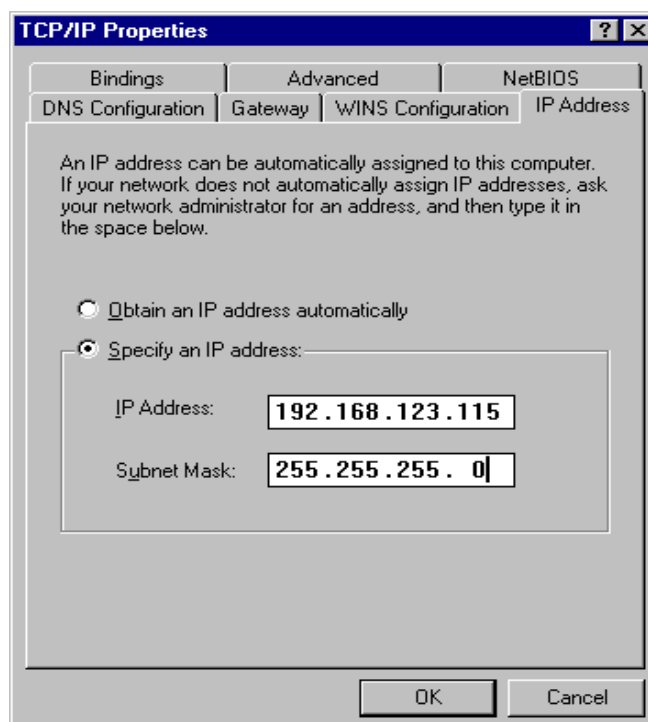
The screenshot shows the 'TCP/IP Properties' dialog box with the 'Gateway' tab selected. The dialog has a title bar with a question mark and a close button. Below the title bar are four tabs: 'Bindings', 'Advanced', 'NetBIOS', and 'Gateway'. The 'Gateway' tab is active, showing a text area with instructions: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

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

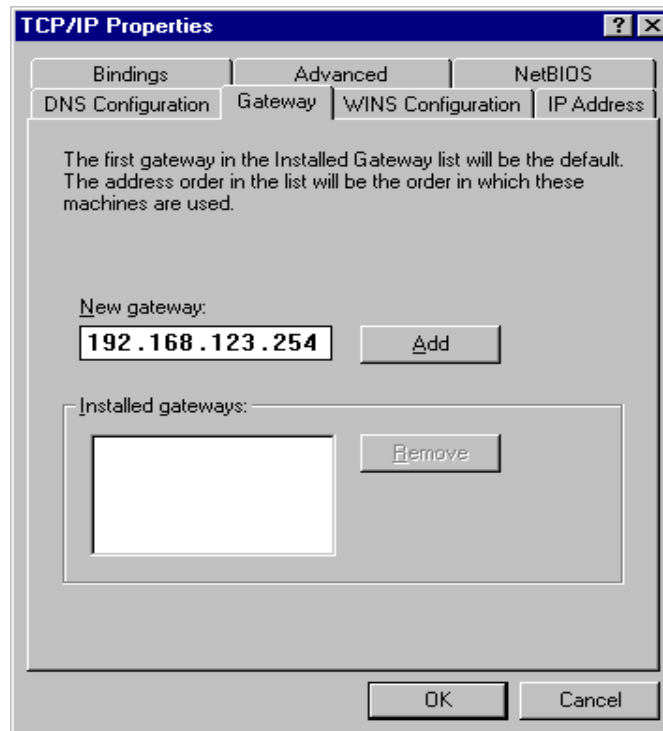


B. Configure IP manually

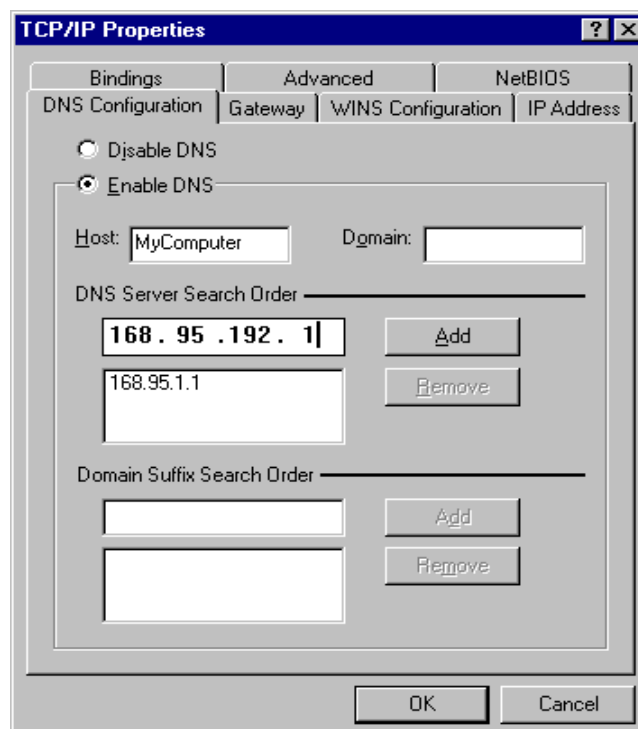
- a. Select **Specify an IP address** in the IP Address tab. The default IP address of this product is 192.168.123.254. So please use 192.168.123.xxx (xxx is between 1 and 253) for IP Address field and 255.255.255.0 for Subnet Mask field.



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



- 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 802.1x Setting

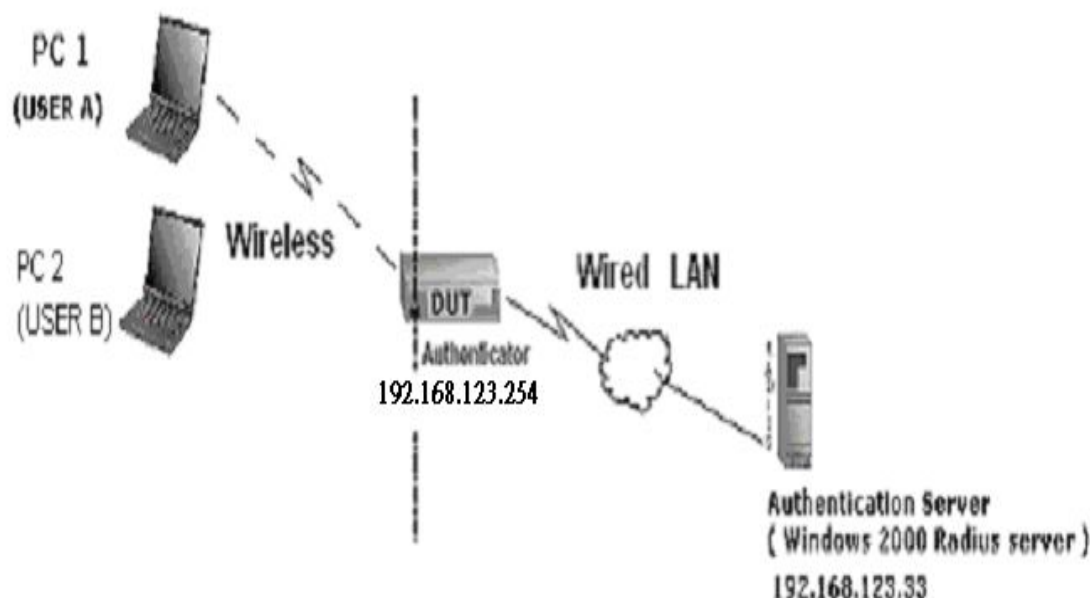


Figure 1: Testing Environment (Use Windows 2000 Radius Server)

### 1 Equipment Details

#### PC1:

Microsoft Windows XP Professional without Service Pack 1.

AMIT 531C Wireless Cardbus:3.0.3.0

Driver version:

#### PC2:

Microsoft Windows XP Professional with Service Pack 1a or latter.

AMIT 561C Wireless Cardbus:1.0.1.0

Driver version: 1.7.29.0 (Driver date: 10.20.2001)

Authentication Server: Windows 2000 RADIUS server with Service Pack 3 and HotFix Q313664.

Note. Windows 2000 RADIUS server only supports PEAP after upgrade to service pack 3 and

HotFix Q313664 (You can get more information from

<http://support.microsoft.com/default.aspx?scid=kb;en-us;313664>)

### 2 DUT

#### Configuration:

- 1.Enable DHCP server.
- 2.WAN setting: static IP address.
- 3.LAN IP address: 192.168.123.254/24.
- 4.Set RADIUS server IP.
- 5.Set RADIUS server shared key.
- 6.Configure WEP key and 802.1X setting.

The following test will use the inbuilt 802.1X authentication method such as ,EAP\_TLS, PEAP\_CHAPv2(Windows XP with SP1 only), and PEAP\_TLS(Windows XP with SP1 only) using the Smart Card or other Certificate of the Windows XP Professional.

### **3. DUT and Windows 2000 Radius Server Setup**

#### **3-1-1. Setup Windows 2000 RADIUS Server**

We have to change authentication method to MD5\_Challenge or using smart card or other certificate on RADIUS server according to the test condition.

#### **3-1-2. Setup DUT**

- 1.Enable the 802.1X (check the “Enable checkbox“).
- 2.Enter the RADIUS server IP.
- 3.Enter the shared key. (The key shared by the RADIUS server and DUT).
- 4.We will change 802.1X encryption key length to fit the variable test condition.

#### **3-1-3. Setup Network adapter on PC**

- 1.Choose the IEEE802.1X as the authentication method. (Fig 2)

Note.

Figure 2 is a setting picture of Windows XP without service pack 1. If users upgrade to service pack 1, then they can't see MD5-Challenge from EAP type list any more, but they will get a new Protected EAP (PEAP) option.

- 2.Choose MD5-Challenge or Smart Card or other Certificate as the EAP type.
- 3.If choosing use smart card or the certificate as the EAP type, we select to use a certificate on this computer. (Fig 3)

4. We will change EAP type to fit the variable test condition.

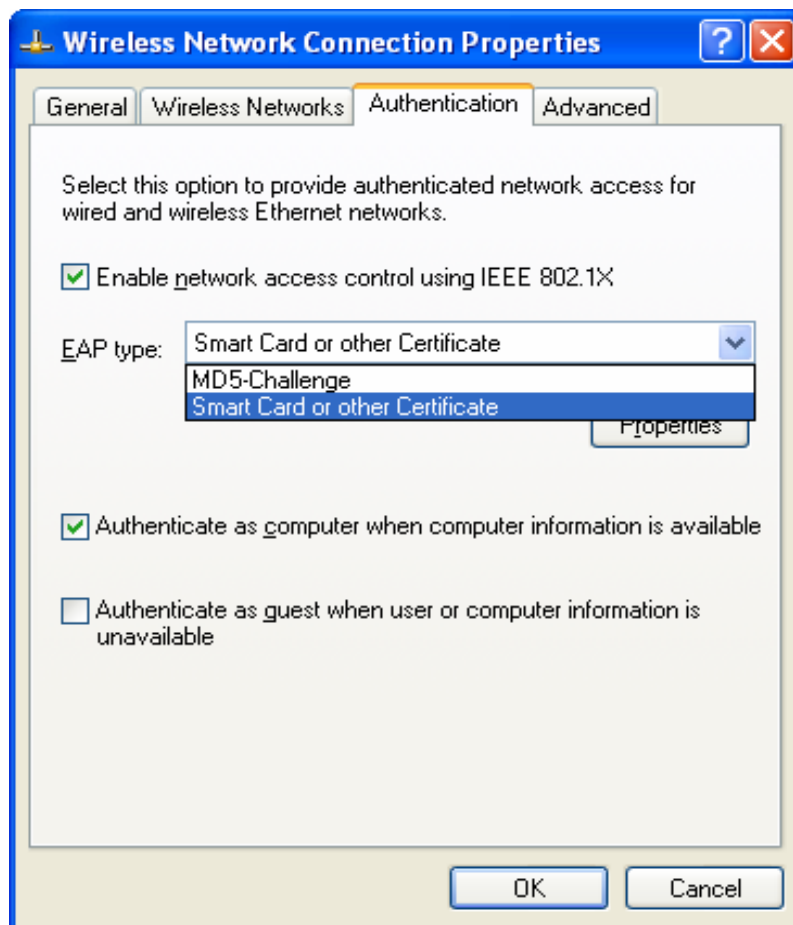


Figure 2: Enable IEEE 802.1X access control

**Figure 3: Smart card or certificate properties**

**4. Windows 2000 RADIUS server Authentication testing:**

4.1 DUT authenticate PC1 using certificate. (PC2 follows the same test procedures.)

1. Download and install the certificate on PC1. (Fig 4)
2. PC1 choose the SSID of DUT as the Access Point.
3. Set authentication type of wireless client and RADIUS server both to EAP\_TLS.
4. Disable the wireless connection and enable again.
5. The DUT will send the user's certificate to the RADIUS server, and then send the message of authentication result to PC1. (Fig 5)
6. Windows XP will prompt that the authentication process is success or fail and end the authentication procedure. ( Fig 6)
7. Terminate the test steps when PC1 get dynamic IP and PING remote host successfully.

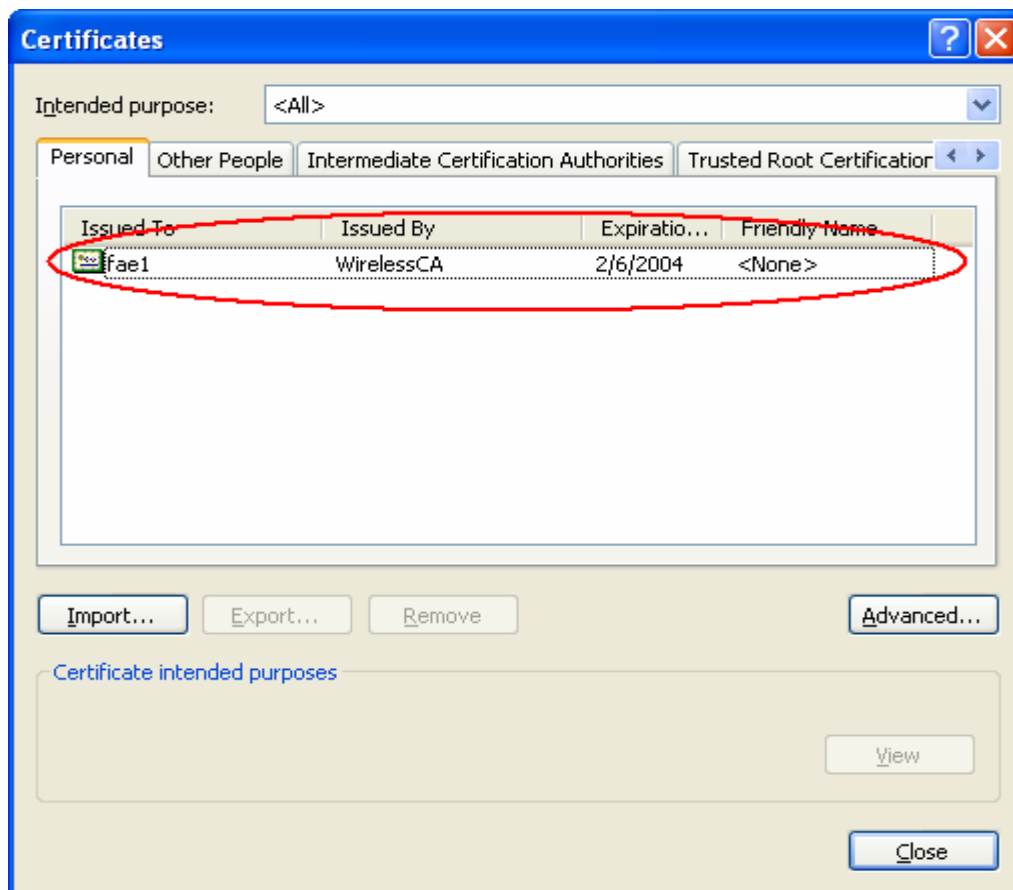


Figure 4: Certificate information on PC1

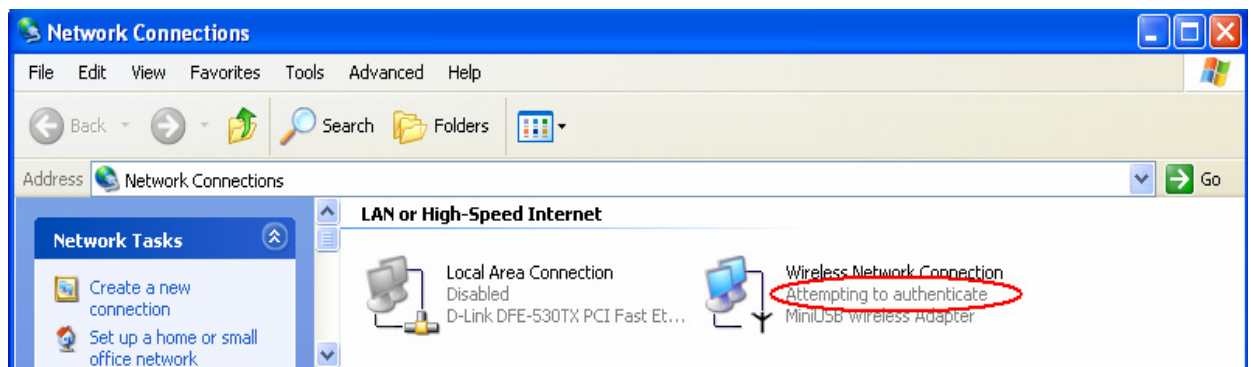
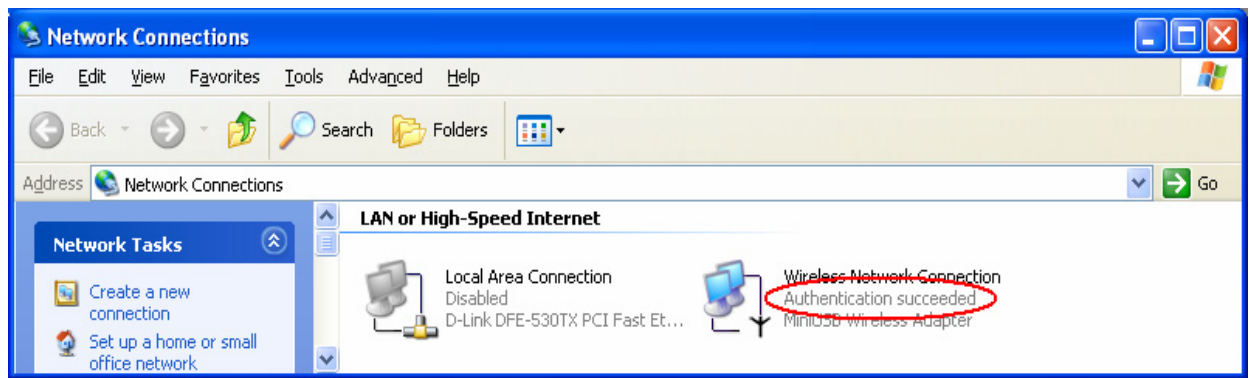


Figure 5: Authenticating



**Figure 6: Authentication success**

#### 4.2DUT authenticate PC2 using PEAP-TLS.

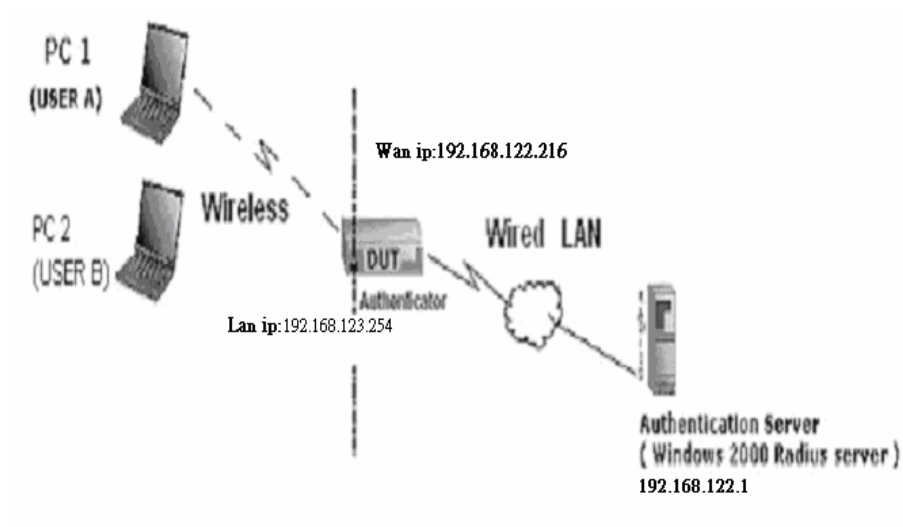
1. PC2 choose the SSID of DUT as the Access Point.
2. Set authentication type of wireless client and RADIUS server both to PEAP\_TLS.
3. Disable the wireless connection and enable again.
4. The DUT will send the user's certificate to the RADIUS server, and then send the message of authentication result to PC2.
5. Windows XP will prompt that the authentication process is success or fail and end the authentication procedure.
6. Terminate the test steps when PC2 get dynamic IP and PING remote host successfully.

**Support Type: The router supports the types of 802.1x Authentication: PEAP-CHAPv2 and PEAP-TLS.**

Note.

1. PC1 is on Windows XP platform without Service Pack 1.
2. PC2 is on Windows XP platform with Service Pack 1a.
3. PEAP is supported on Windows XP with Service Pack 1 only.
4. Windows XP with Service Pack 1 allows 802.1x authentication only when data encryption function is enable.

## Appendix C WPA-PSK and WPA



Wireless Router: LAN IP: 192.168.123.254

WAN IP: 192.168.122.216

Radius Server: 192.168.122.1

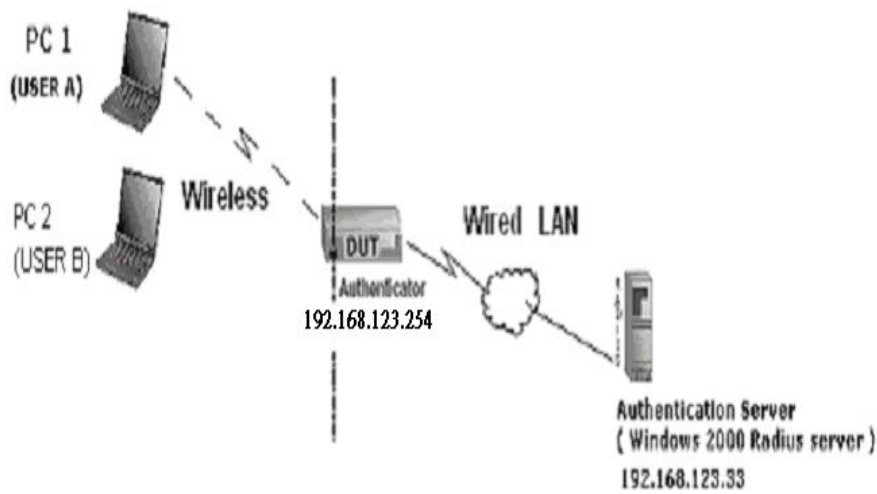
UserA : XP Wireless Card:Ti-11g

Tool: Odyssey Client Manager

Refer to: [www.funk.com](http://www.funk.com)

Download: [http://www.funk.com/News&Events/ody\\_c\\_wpa\\_preview\\_pn.asp](http://www.funk.com/News&Events/ody_c_wpa_preview_pn.asp)

Or Another Configuration:



## WPA-PSK

In fact, it is not necessary for this function to authenticate by Radius Server, the client and wireless Router authenticate by themselves.

Method1:

1. Go to the Web manager of Wireless Router to configure, like below:

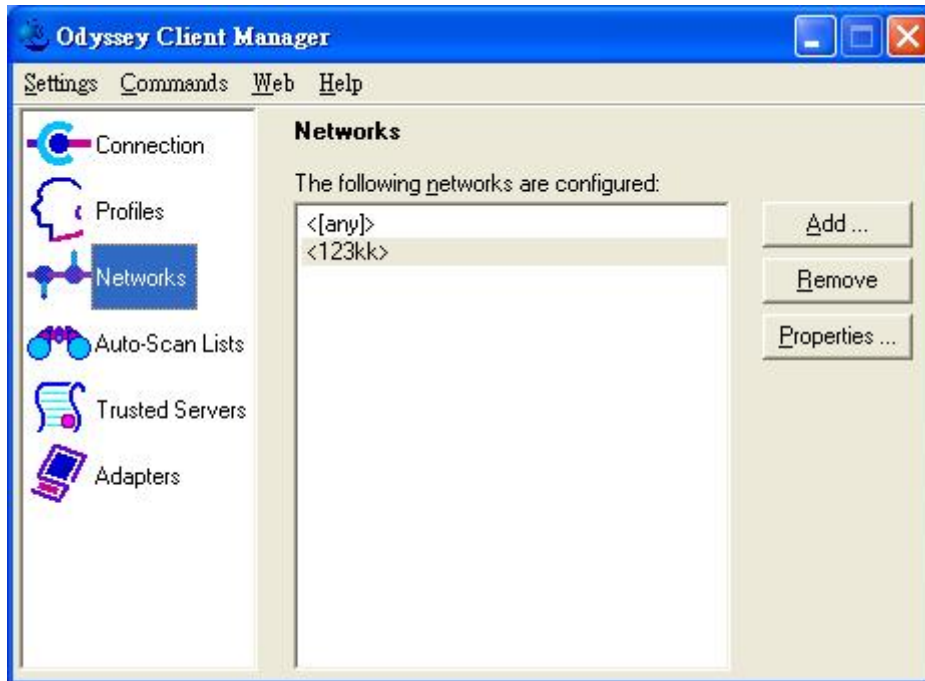
Network ID(SSID)	123kk
Channel	8
Security	WPA-PSK
Key Mode	ASCII
Preshare Key	12345678

2. Go to Odyssey Client Manager, first choose "Network"

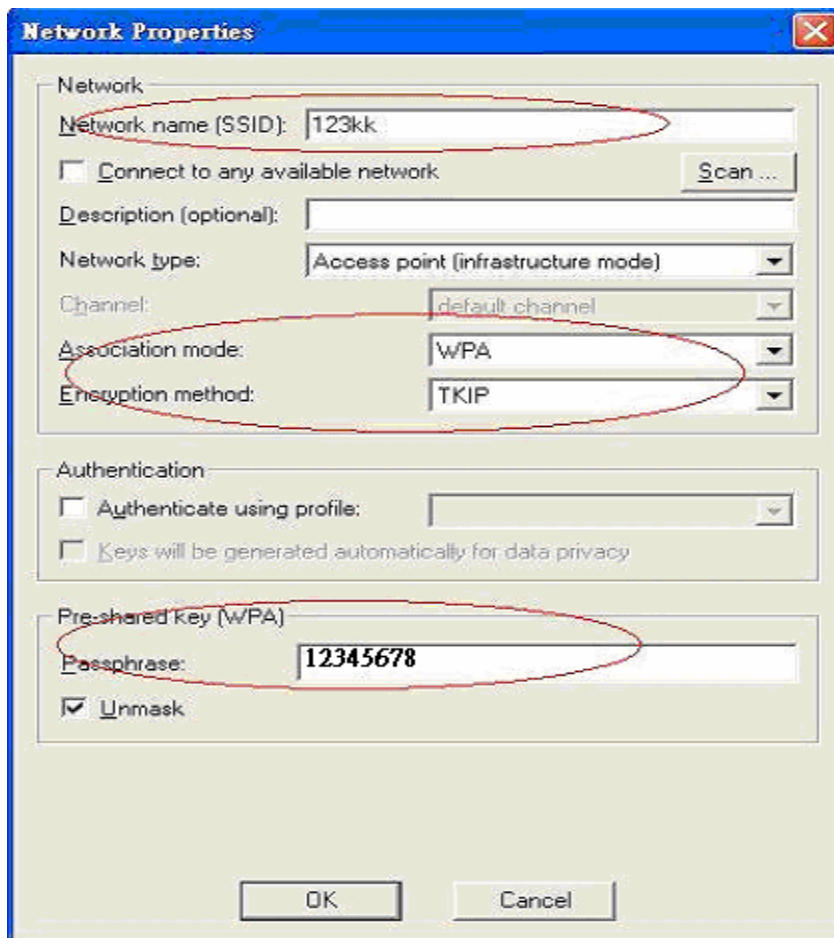
Before doing that, you should verify if the software can show the wireless card.

Open "Adapters"



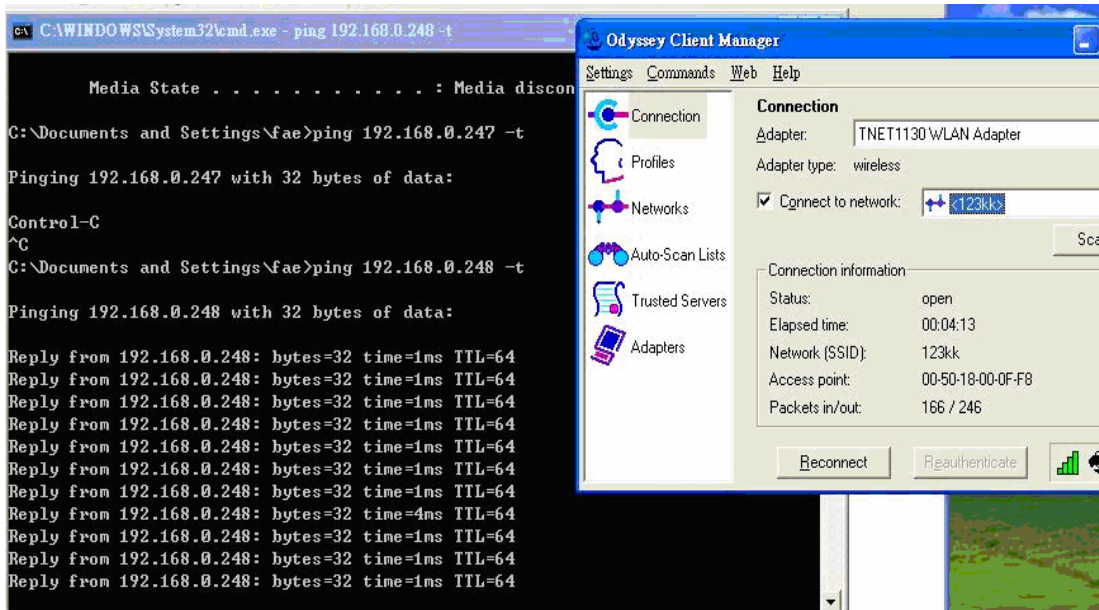


3. Add and edit some settings:



#### 4. Back to Connection:

Then Select “Connect to network” You will see:



#### Method2:

1. First, patch windows XP and have to install “Service package 1”

Patch:

<http://www.microsoft.com/downloads/details.aspx?displaylang=en&FamilyID=5039ef4a-61e0-4c44-94f0-c25c9de0ace9>

2. Then reboot.

3. Setting on the router and client:

Router:

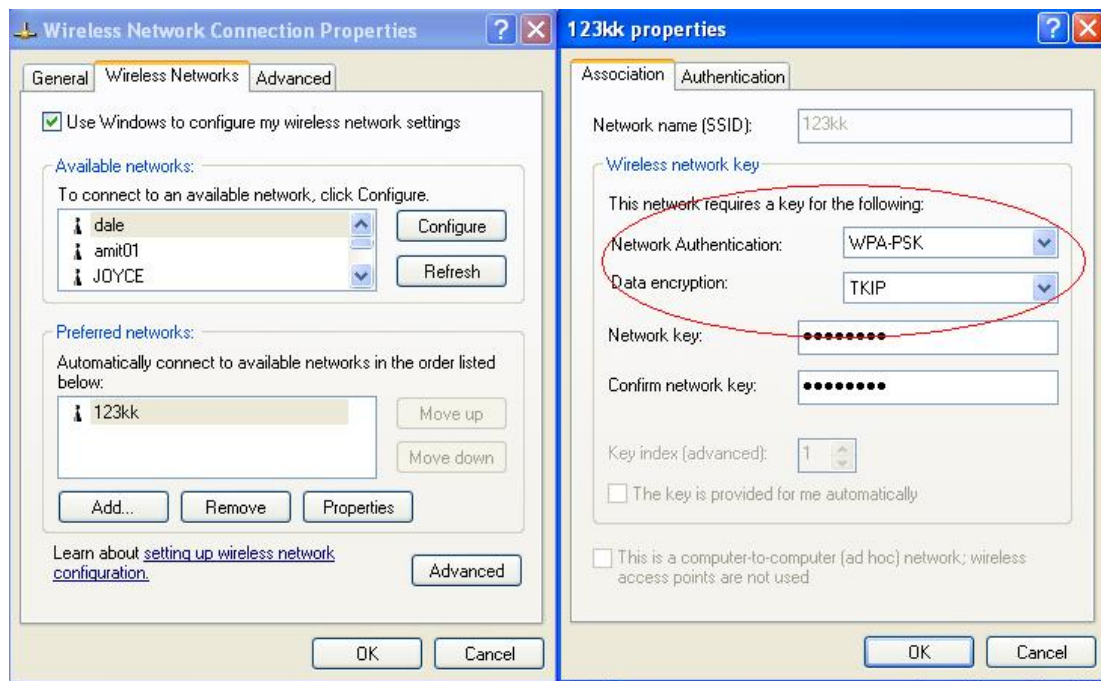
Network ID(SSID)	123kk
Channel	8
Security	WPA-PSK
Key Mode	ASCII
Preshare Key	12345678

Client:

Go to “Network Connection” and select wireless adapter.

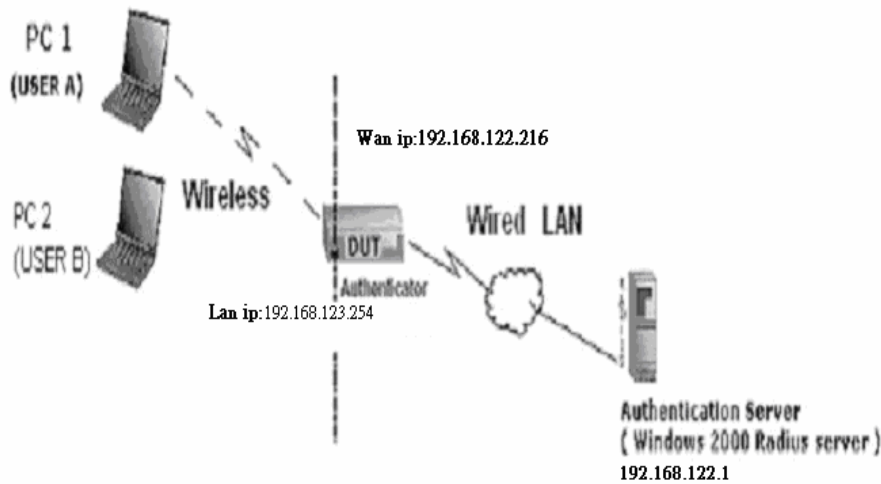
Choose “View available Wireless Networks” like below:

Advanced→ choose “123kk”



## WPA:

For this function, we need the server to authenticate. This function is like 802.1x.



The above is our environment:

Method 1:

1. The UserA or UserB have to get certificate from Radius, first.

<http://192.168.122.1/certsrv>

account : fael

passwd : fael



2. Then, Install this certificate and finish.

3. Go to the Web manager of Wireless Router to configure, like below:

Network ID(SSID)	123kk
Channel	8
Security	WPA

#### 802.1X Settings

RADIUS Server IP	192.168.122.1
RADIUS port	1812
RADIUS Shared Key	costra

4. Go to Odyssey Client Manager, choose “Profiles” and Setup Profile name as “1”

**Add Profile**

Profile name: 1

User Info | Authentication | ITLS Settings | PEAP Settings

Login name: fae1

Password

☒ Permit login using password

☐ use Windows password

☐ prompt for password

☒ use the following password:

fae1

☒ Unmask

Certificate

☒ Permit login using my certificate:

fae1

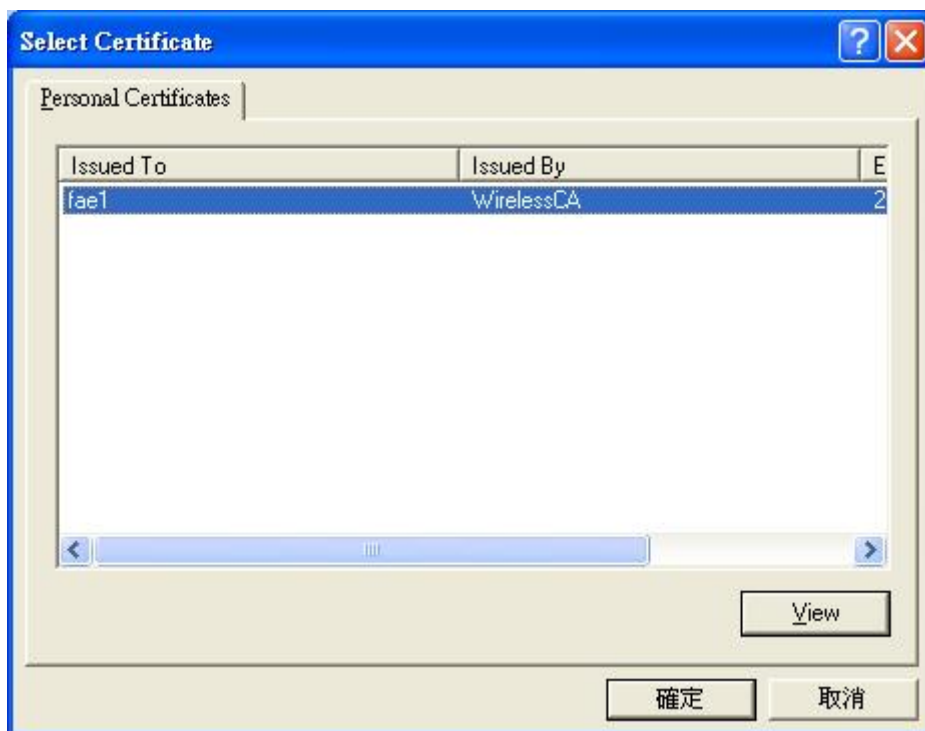
View ... Browse ...

OK Cancel

Login name and passwd are fae1 and fae1.

Remember that you get certificate from Radius in Step1.

5. Then Choose “certificate” like above.



6. Then go to Authentication and first Remove EAP/ TLS and Add EAP/TLS again.

The screenshot shows the 'Edit Profile Properties' dialog box with the 'Authentication' tab selected. The 'Profile name' field contains the number '1'. The 'Authentication protocols, in order of preference:' list contains 'EAP / TLS'. To the right of the list are buttons for 'Add ...' and 'Remove'. Below the list is a checked checkbox labeled 'Validate server certificate'. At the bottom of the dialog are 'OK' and 'Cancel' buttons.

Profile name: 1

User Info Authentication ITLS Settings PEAP Settings

Authentication protocols, in order of preference:

EAP / TLS

↑ ↓

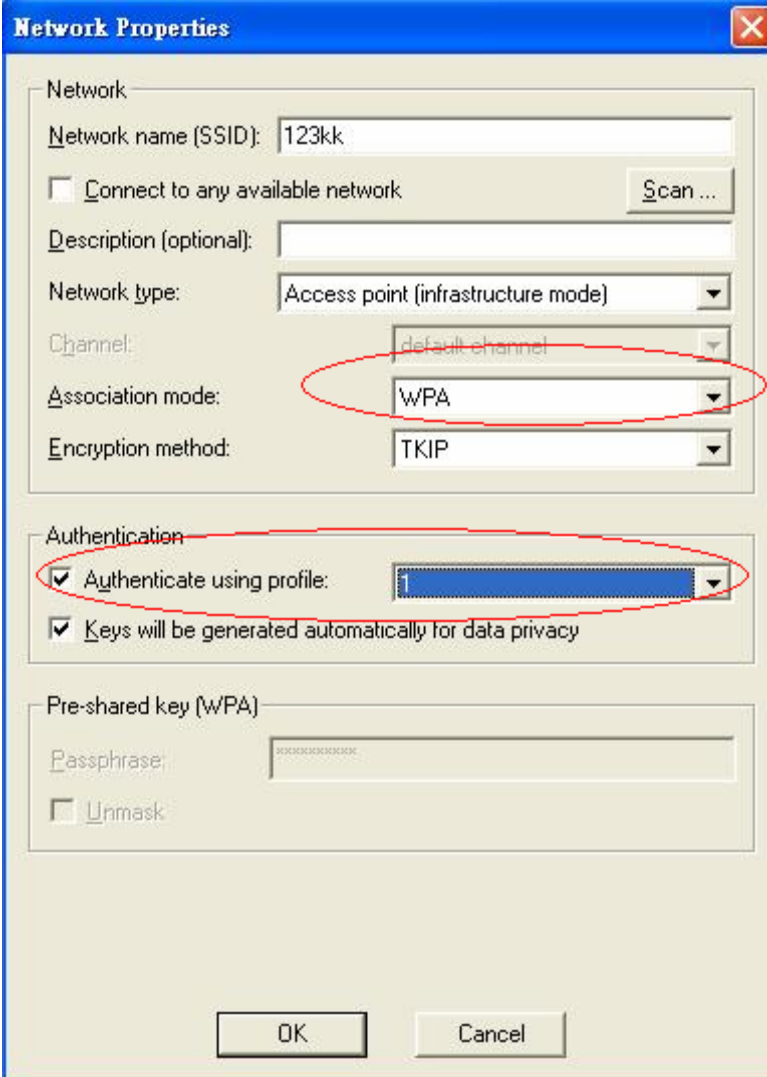
Add ...

Remove

☒ Validate server certificate

OK Cancel

7. Go “Network” and Select “1” and ok



The image shows a Windows XP-style "Network Properties" dialog box. It has a blue title bar with the text "Network Properties" and a close button. The dialog is divided into three main sections: "Network", "Authentication", and "Pre-shared key (WPA)".

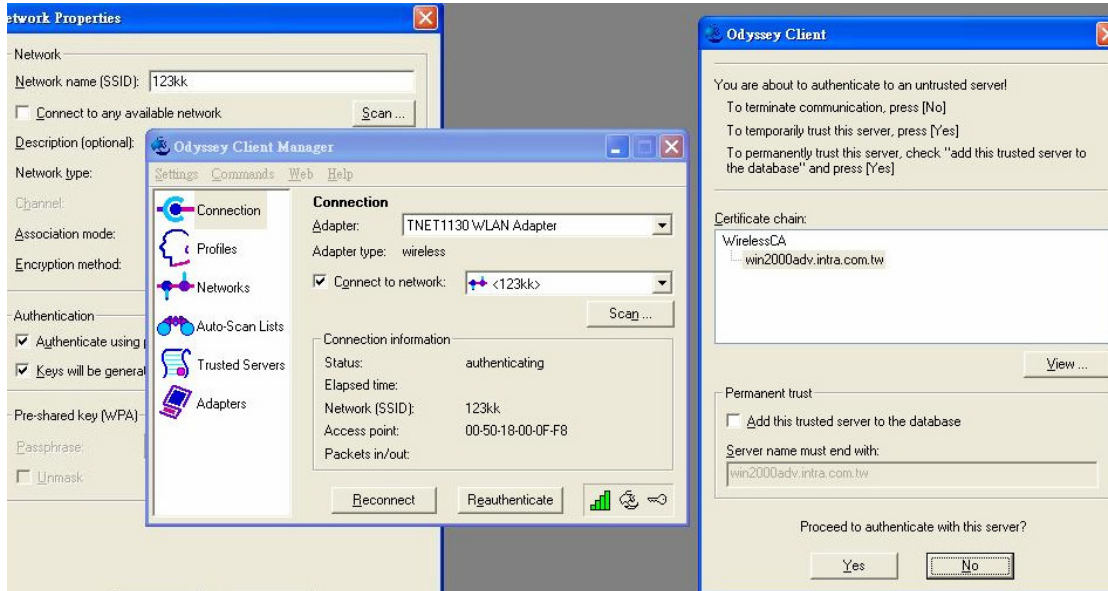
- Network section:**
  - Network name (SSID):** A text box containing "123kk".
  - Connect to any available network:** An unchecked checkbox.
  - Description (optional):** An empty text box.
  - Network type:** A dropdown menu showing "Access point (infrastructure mode)".
  - Channel:** A dropdown menu showing "default channel".
  - Association mode:** A dropdown menu showing "WPA". This dropdown is circled in red.
  - Encryption method:** A dropdown menu showing "TKIP".
- Authentication section:**
  - Authenticate using profile:** A checked checkbox followed by a dropdown menu. This entire row is circled in red.
  - Keys will be generated automatically for data privacy:** A checked checkbox.
- Pre-shared key (WPA) section:**
  - Passphrase:** A text box with masked characters (dots).
  - Unmask:** An unchecked checkbox.

At the bottom of the dialog are two buttons: "OK" and "Cancel".

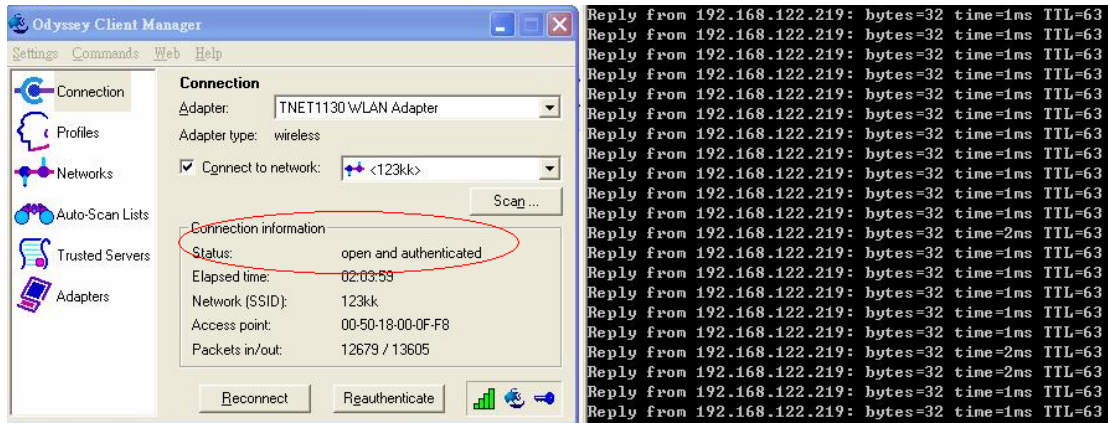


8. Back to Connection and Select “123kk.

If **successfully**, the wireless client has to authenticate with Radius Server, like below:



9.Result:



Method 2:

1. The UserA or UserB have to get certificate from Radius,first.

<http://192.168.122.1/certsrv>

account:fae1

passwd:fae1



2. Then Install this certificate and finish.

3. Setting on the router and client:

Router:

Network ID(SSID)	<input type="text" value="123kk"/>
Channel	<input type="text" value="8"/>
Security	<input type="text" value="WPA"/>

#### 802.1X Settings

RADIUS Server IP	<input type="text" value="192.168.122.1"/>
RADIUS port	<input type="text" value="1812"/>
RADIUS Shared Key	<input type="text" value="costra"/>

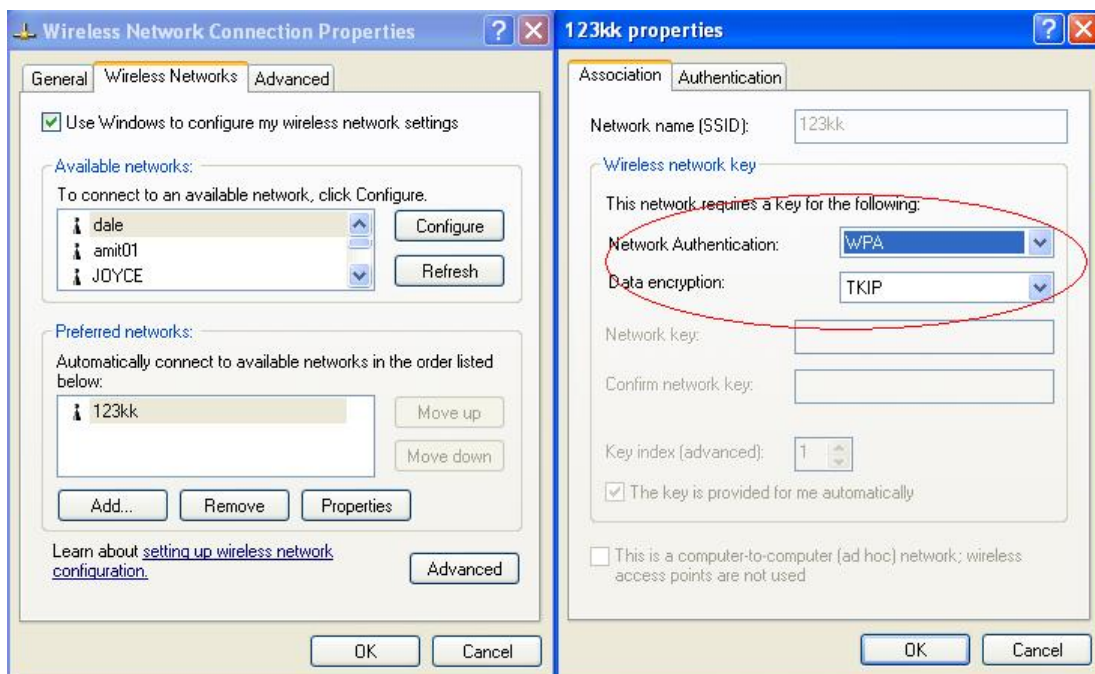
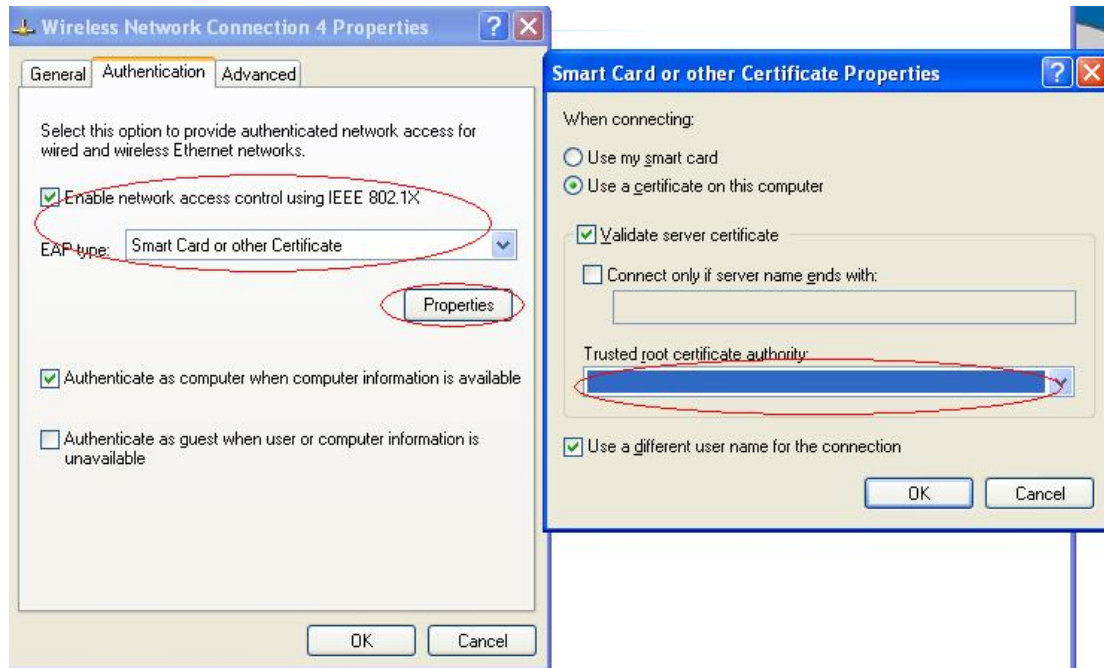
Client:

Go to “Network Connection” and select wireless adapter.

Choose “View available Wireless Networks” like below:

Advanced→ choose “123kk”

Select “WirelessCA and Enable” in Trusted root certificate authority:



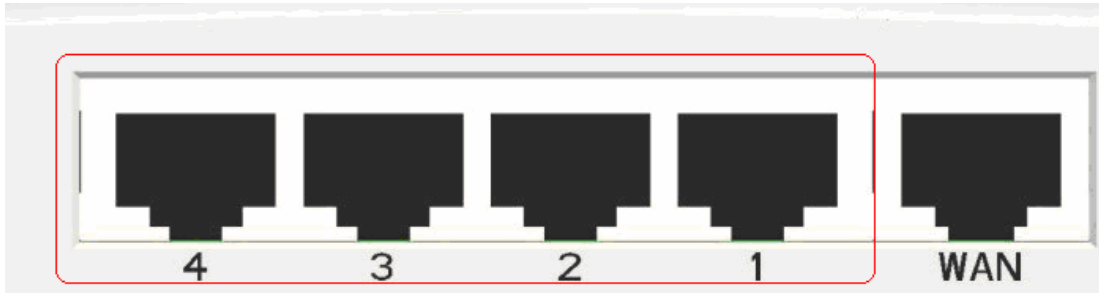
Then, if the wireless client wants to associate, it has to request to authenticate.

## Appendix D FAQ and Troubleshooting

### What can I do when I have some trouble at the first time?

**1. Why can I not configure the router even if the cable is plugged in the ports of Router and the led is also light?**

**A:** First, make sure that which port is plugged. If the cable is in the Wan port, please change to plug in Lan port 1 or Lan port 4:



Then, please check if the Pc gets ip address from Router. Use command mode as below:

```
C:\>ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  . : 
    IP Address. . . . .               : 192.168.123.115
    Subnet Mask . . . . .             : 255.255.255.0
    Default Gateway . . . . .         : 192.168.123.254
```

If yes, please execute Browser, like Mozilla and key 192.168.123.254 in address.

If not, please ipconfig /release, then ipconfig /renew.

```
C:\>ipconfig /release

Windows IP Configuration

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  . : 
    IP Address. . . . .               : 0.0.0.0
    Subnet Mask . . . . .             : 0.0.0.0
    Default Gateway . . . . .         : 

C:\>ipconfig /renew

Windows IP Configuration

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  . : 
    IP Address. . . . .               : 192.168.123.115
    Subnet Mask . . . . .             : 255.255.255.0
    Default Gateway . . . . .         : 192.168.123.254
```

Whatever I setup, the pc can not get ip. Please check Status Led and refer to the Q2:

**2. Why can I not connect the router even if the cable is plugged in Lan port and**

## the led is light?

**A:** First, please check Status Led. If the device is normal, the led will blink per second.

If not, please check How blinking Status led shows.

There are many abnormal symptoms as below:

**Status Led is bright or dark in work:** The system hanged up .Suggest powering off and on the router. But this symptom often occurs, please reset to default or upgrade latest fw to try again.

**Status led flashes irregularly:** Maybe the root cause is Flash rom and please press reset Button to reset to default or try to use Recovery mode.(Refer to Q3 and Q4)

**Status flashes very fast while powering on:** Maybe the router is the recovery mode and please refer to Q4.

## 3.How to reset to factory default?

**A:** There are 2 methods to reset to default.

### 1. Restore with RESET button

First, turn off the router and press the RESET button in. And then, power on the router and push the RESET button down until the M1 and or M2 LED (or Status LED) start flashing, then remove the finger. If LED flashes about 8 times, the RESTORE process is completed. However, if LED flashes 2 times, repeat.

### 2. Restore directly when the router power on

First, push the RESET button about 5 seconds (Status will start flashing about 5 times), remove the finger. The RESTORE process is completed.

## 4.How to do recovery mode when the router is abnormal ?

**A:** Allocate a Static IP Address on your computer as below:

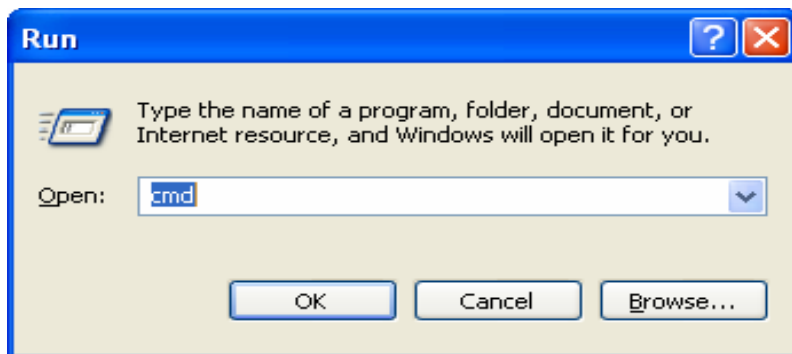
**Step1:**First, press the reset button and power on the router until Status blinks very ffast.

**Step2:**Find the **Inter Protocol(TCP/IP)** Properties from **My Network Places** and check **Properties of Local Area Network Connection**. And click the **“General”** icon and assign one **IP address** which can be from 192.168.123.1 to 192.168.123.253. Here we use the 192.168.123.88 as the IP address. The **Subnet mask** must be 255.255.255.0, and the **Default gateway** must be 192.168.123.254. Then click **“OK”** button to complete TCP/IP setup.

☐ Obtain an IP address automatically  
☒ Use the following IP address:

IP address:	192 . 168 . 123 . 88
Subnet mask:	255 . 255 . 255 . 0
Default gateway:	192 . 168 . 123 . 254

**Step2:** Open the command mode and input “cmd” then check if the router replies to ping 192.168.123.254



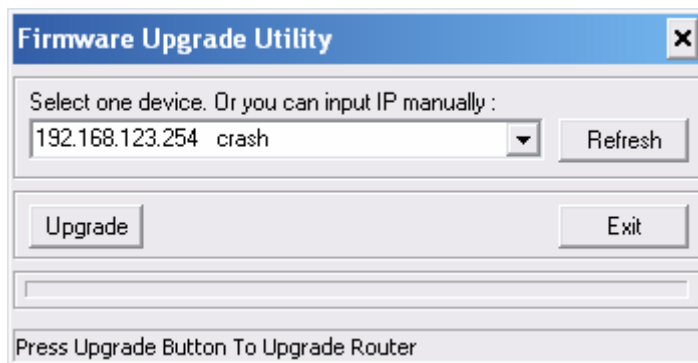
```

C:\>ping 192.168.123.254

Pinging 192.168.123.254 with 32 bytes of data:

Reply from 192.168.123.254: bytes=32 time<1ms TTL=64
Reply from 192.168.123.254: bytes=32 time<1ms TTL=64
Reply from 192.168.123.254: bytes=32 time<1ms TTL=64
  
```

**Step3:**Please use the exe-file of fw and click as below:



Then click” Upgrade” if necessary, please input password ”admin” .Then reset to default and refer to Q1 How to connect Router.

However, if those methods can not make the router normal, please send the unit to the seller to check, thanks.

**5.Why can I not connect Internet even though the cables are plugged in Wan port and Lan port and the leds are blink. In addition, Status led is also normal and I can configure web management?**

**A:** Make sure that the network cable from DSL or Cable modem is plugged in Wan port of Router and that the network cable from Lan port of router is plugged in Ethernet adapter. Then, please check which wan type you use. If you are not sure, please call the isp. Then please go to this page to input the information isp is assigned.

Choose WAN Type	
Type	Usage
<input type="radio"/> Static IP Address	ISP assigns you a 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.
<input type="radio"/> L2TP	Some ISPs require the use of L2TP to connect to their services.

**6. When I use Static IP Address to roam Internet, I can access or ping global IP 202.93.91.218, But I can not access the site that inputs domain name, for example <http://espn.com> ?**

**A:** Please check the dns configuration of Static IP Address. Please refer to the information of ISP and assign one or two in dns item.

## How do I connect router by using wireless?

### 1. How to start to use wireless?

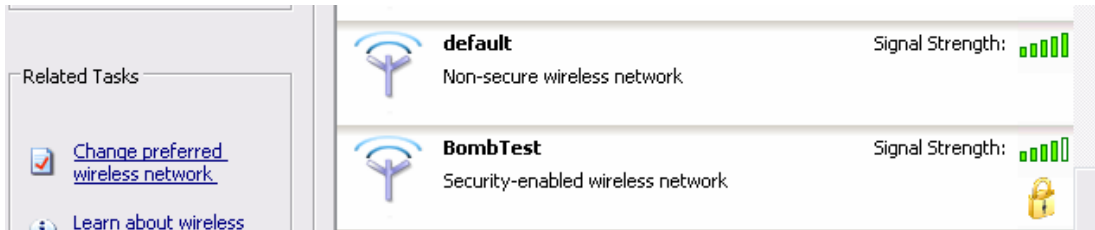
**A:** First, make sure that you already installed wireless client device in your computer. Then check the Configuration of wireless router. The default is as below:

Wireless Setting [ HELP ]	
Item	Setting
▶ Wireless	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
▶ Network ID(SSID)	<input type="text" value="default"/>
▶ Wireless Mode	<input type="radio"/> Mixed <input checked="" type="radio"/> 11g only
▶ SSID broadcast	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
▶ Channel	<input type="text" value="11"/> ▼
▶ Security	<input type="text" value="None"/> ▼

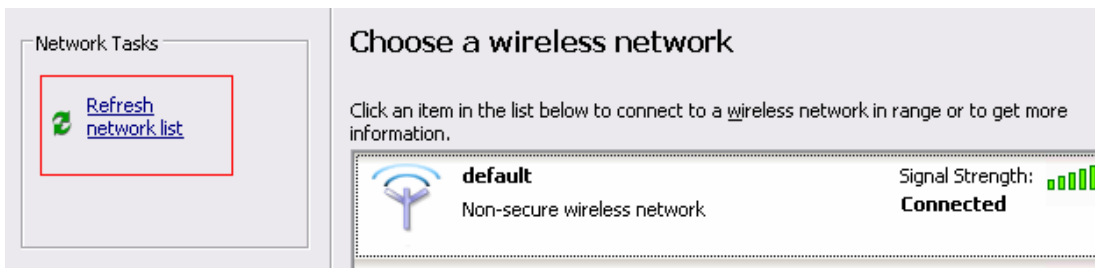
About wireless client, you will see wireless icon:



Then click and will see the ap list that wireless client can be accessed:



If the client can not access your wireless router, please refresh network list again. However, I still can not find the device which ssid is “default”, please refer to Q3.



Choose the one that you will want to connect and Connect:



If successfully, the computer will show



and get ip from router:



```

Ethernet adapter Wireless Network Connection 5:

    Connection-specific DNS Suffix  . : 
    IP Address. . . . .               : 192.168.123.165
    Subnet Mask . . . . .             : 255.255.255.0
    Default Gateway . . . . .         : 192.168.123.254

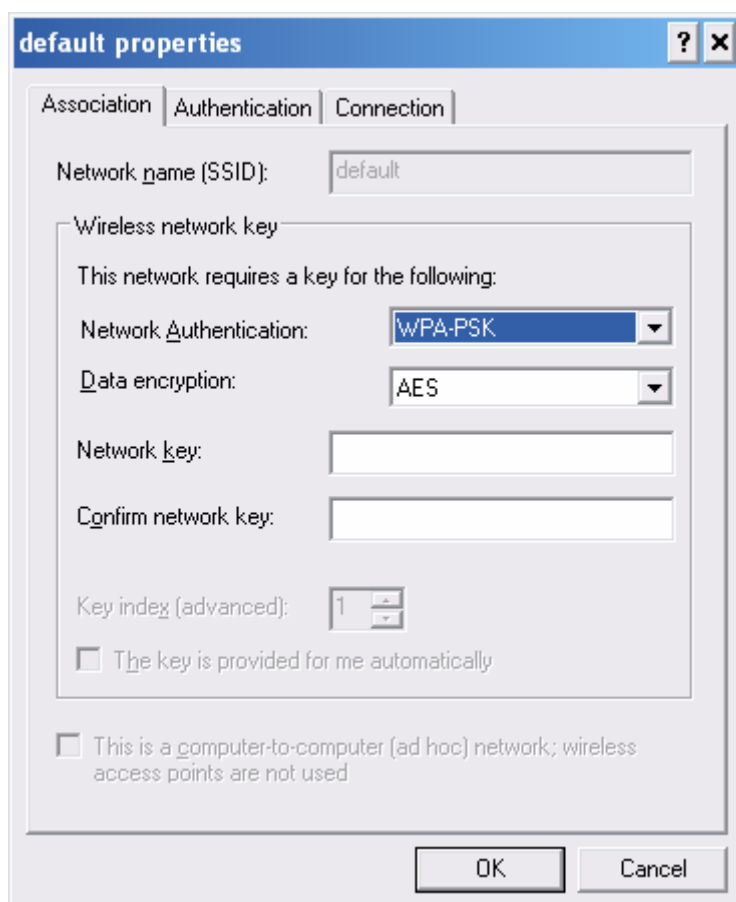
```

## 2. When I use AES encryption of WPA-PSK to connect even if I input the correct pre-share key?

**A:** First, you must check if the driver of wireless client supports AES encryption. Please refer to the below:



If SSID is default and click “Properties” to check if the driver of wireless client supports AES encryption.



**3. When I use wireless to connect the router, but I find the signal is very low even if I am close to the router?**

**A:** Please check if the wireless client is normal, first. If yes, please send the unit to the seller and verify what the problem is.