

User's Manual

802.11n 4 port Broadband Router

WIQ189AM

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.....	8
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.....	29
	4.6 Security Settings	34
	4.7 Advanced Settings.....	48
	4.7.7 Qos Rule.....	59
	4.8 Toolbox	60
Appendix A	802.1x Setting.....	63
Appendix B	WPA-PSK and WPA.....	69
Appendix C	FAQ and Troubleshooting.....	81
	What can I do when I have some trouble at the first time?	81
	How do I connect router by using wireless?	84

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 80Mbps 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.

- **WDS(Wireless Distribution System):** It is a system that enables the interconnection of access points wirelessly.

- **WPS(WiFi Protection Setup):**WPS is WiFi Protection Setup which is similar to WCN-NET and offer safe and easy way in Wireless Connection.

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

Allowing inter-operation among multiple vendors.

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

Allowing inter-operation among multiple vendors.

- **IEEE 802.11n compatible**

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.

- **Qos(Quality of Service)**

Provide different priority to different users or data flows, or guarantee a certain level of performance.

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 some ddns providers,like.dyndns,no-ip 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(360), Msn Messenger, Windows Messenger and NDSL.

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

2.1.2. Rear Panel

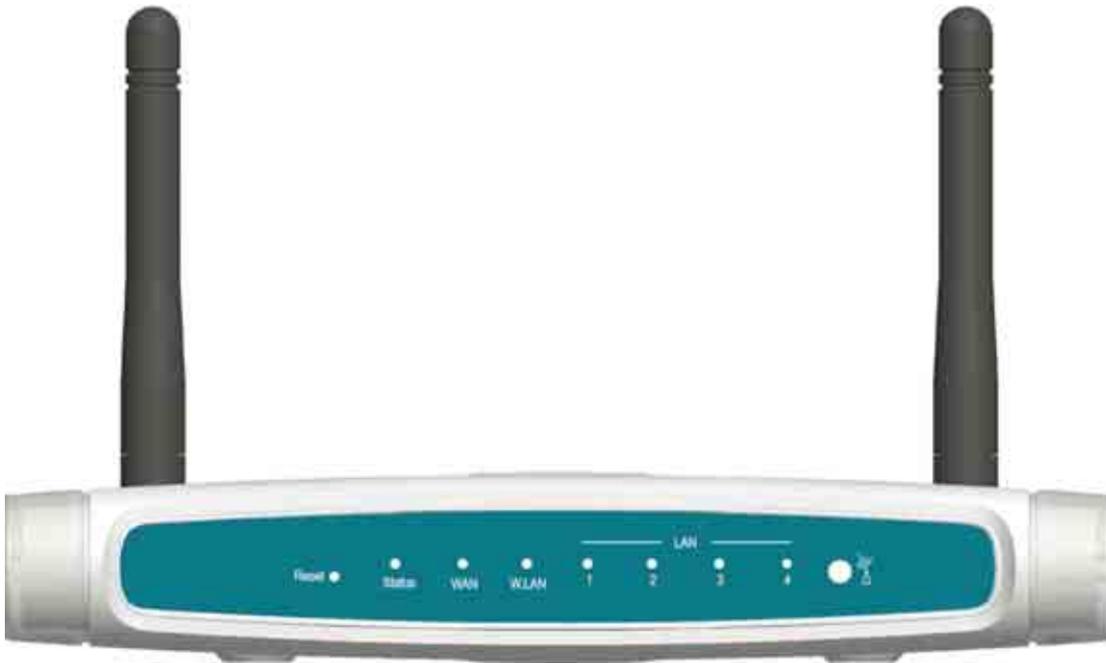


Figure 2-2 Rear Panel

LED:

LED	Function	Color	Status	Description
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
Button	Special application			

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?

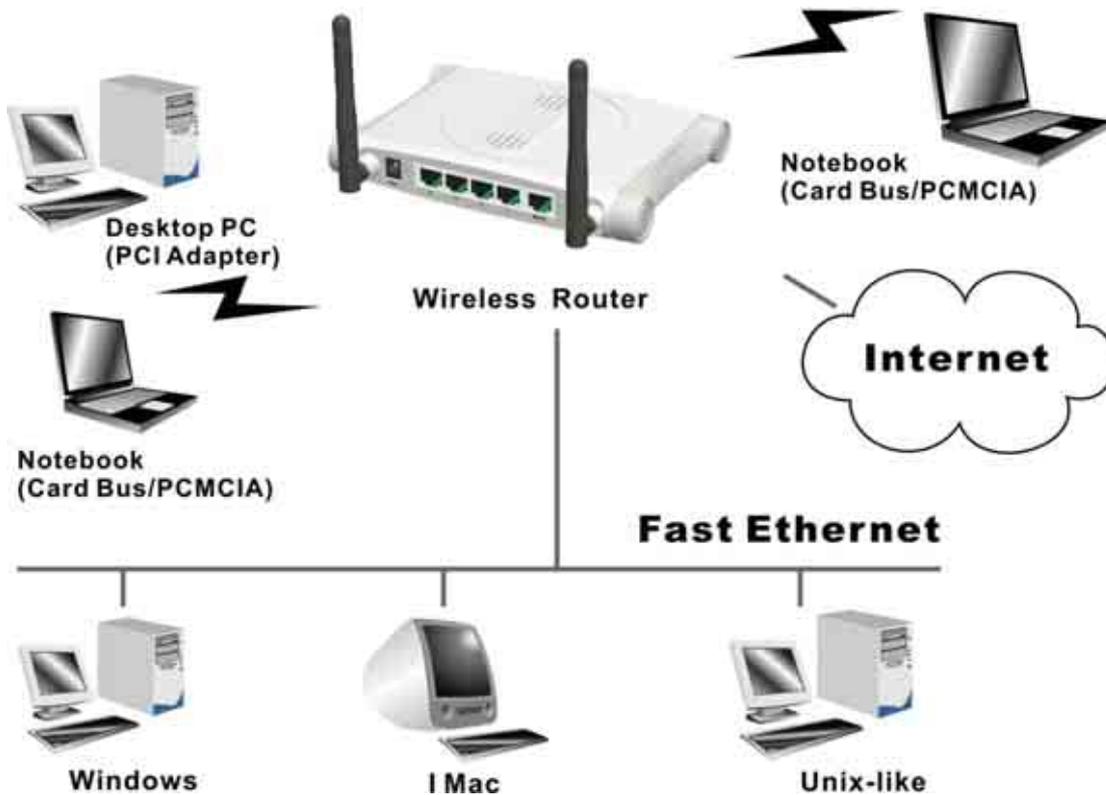
Tip: The LAN LED of this product and the link LED of network card on your computer must be lighted.

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.



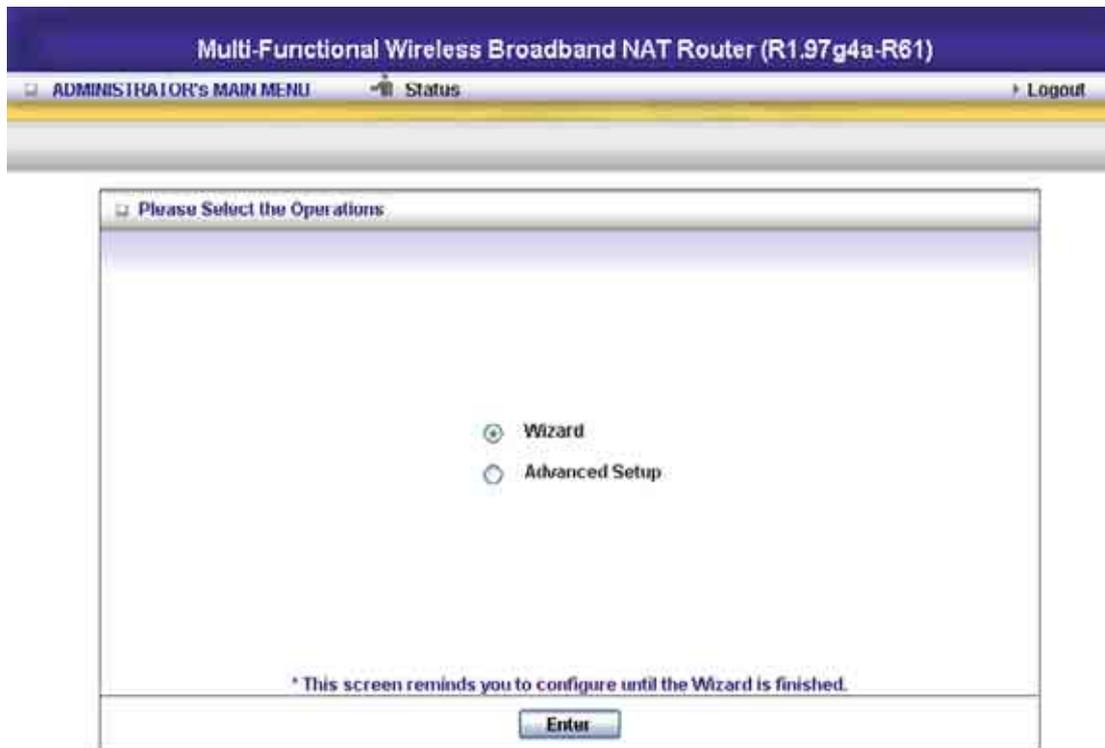
4.1 Login to Configure from Wizard

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**.

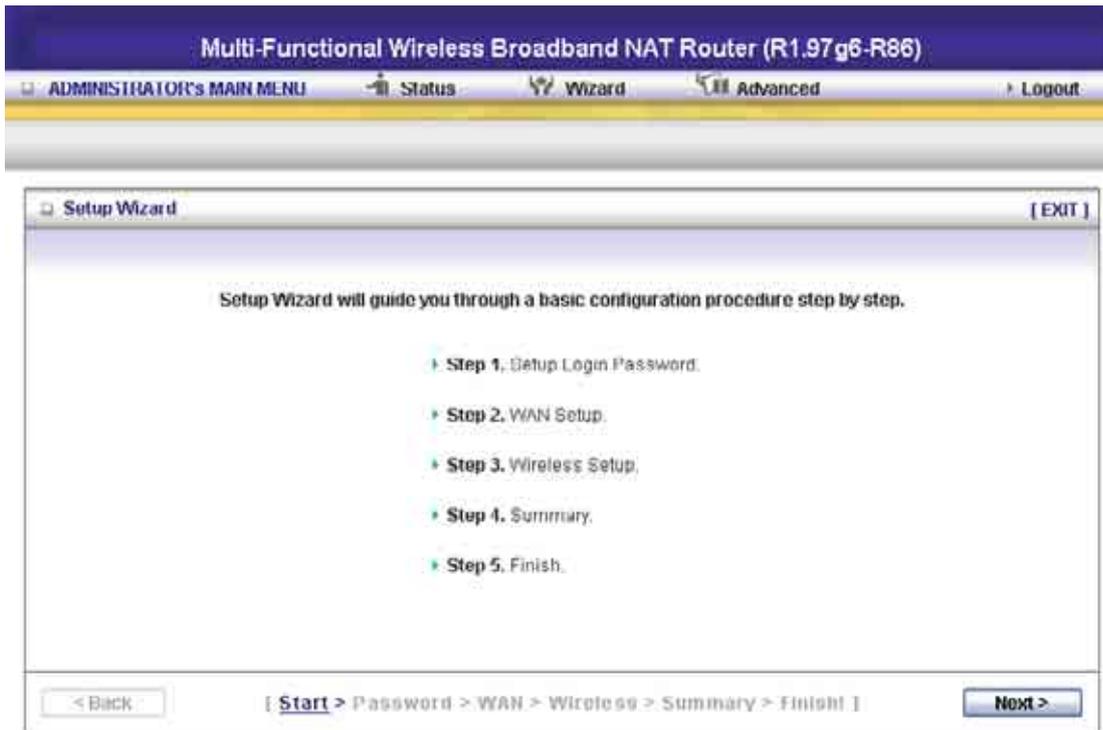
After the connection is established, you will see the web user interface of this product. There are two appearances of web user interface: for general users and for system administrator.

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 >"



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



4.2 Status

The screenshot displays the status page of a Multi-Functional Wireless Broadband NAT Router (R1.97g6-R86). The page has a blue header with the router model name and a navigation bar with links for Administrator's Main Menu, Status, Wizard, Advanced, and Logout. The main content area is divided into two sections: System Status and Wireless Status.

System Status [HELP]

Item	WAN Status	Sidenote
Remaining Lease Time	00:04:59	<input type="button" value="Renew"/>
IP Address	192.168.122.153	<input type="button" value="Release"/>
Subnet Mask	255.255.255.0	
Gateway	192.168.122.210	
Domain Name Server	192.168.122.3, 192.168.122.210	
MAC Address	00-50-10-21-C2-00	

Wireless Status

Item	WLAN Status	Sidenote
Wireless mode	Enable	
SSID	default	
Channel	3	
Security	None	

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

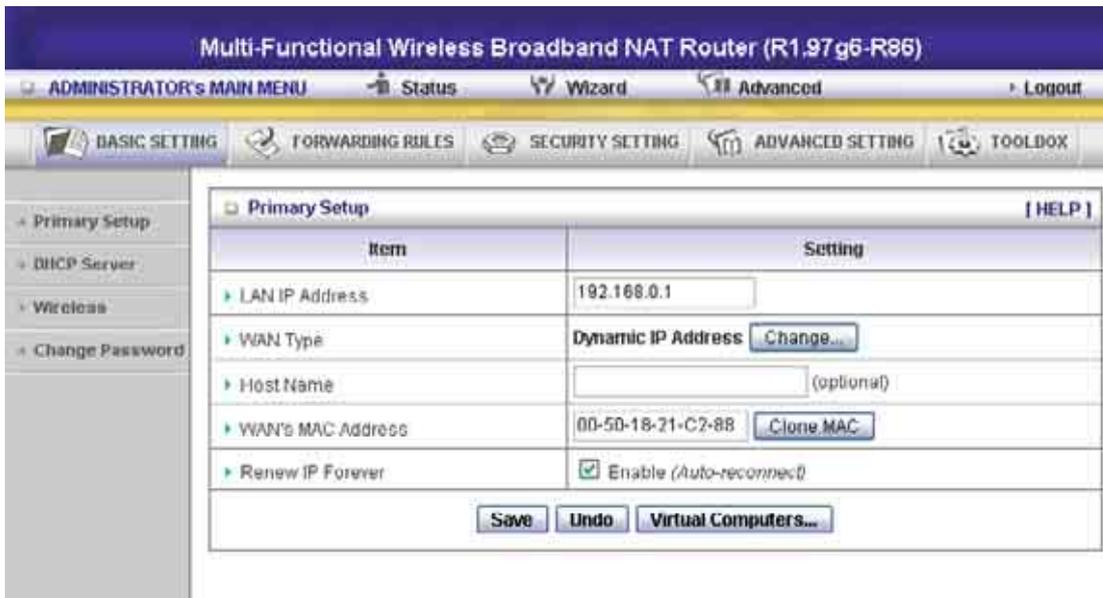
Please Select “Advanced Setup” to Setup

The screenshot displays the web interface of a Multi-Functional Wireless Broadband NAT Router (R1.97 g6-R86). The interface features a top navigation bar with the title "Multi-Functional Wireless Broadband NAT Router (R1.97 g6-R86)" and a secondary menu with "ADMINISTRATOR'S MAIN MENU", "Status", "Wizard", "Advanced", and "Logout". Below this is a primary menu with "BASIC SETTING", "FORWARDING RULES", "SECURITY SETTING", "ADVANCED SETTING", and "TOOLBOX".

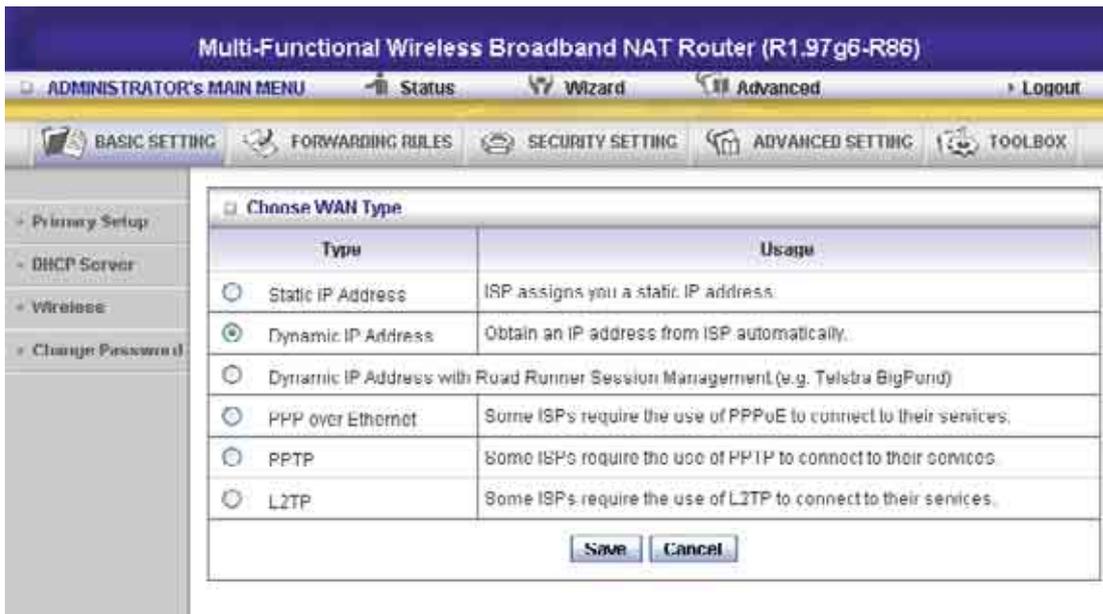
The "Basic Setting" page is active, showing a sidebar with the following options: "Primary Setup", "DHCP Server", "Wireless", and "Change Password". The main content area, titled "Basic Setting", contains the following information:

- **Primary Setup**
 - Configure LAN IP, and select WAN type.
- **DHCP Server**
 - The settings include Host IP, Subnet Mask, Gateway, DNS, and WINS configurations.
- **Wireless**
 - Wireless settings allow you to configure the wireless configuration items. The device also supports WDS(Wireless Distribution System) and WPS(WiFi Protected Setup)
- **Change Password**
 - Allow you to change system password.

4.4.1 Primary Setup – WAN Type, Virtual Computers



Press “Change”



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

1. **LAN IP Address:** the local IP address of this device. The computers on your network must use the LAN IP address of your product as their Default Gateway. You can change it if necessary.
2. **WAN Type:** WAN connection type of your ISP. You can click **Change** button to choose a correct one from the following four options:
 - A. Static IP Address: ISP assigns you a static IP address.
 - B. Dynamic IP Address: Obtain an IP address from ISP automatically.

- C. Dynamic IP Address with Road Runner Session Management.(e.g. Telstra BigPond)
- D. PPP over Ethernet: Some ISPs require the use of PPPoE to connect to their services.
- E. PPTP: Some ISPs require the use of PPTP to connect to their services.
- F. 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 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 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.

4.4.1.6 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 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.

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

The screenshot displays the configuration interface for a Multi-Functional Wireless Broadband NAT Router (R1.97g6-R86). The top navigation bar includes 'ADMINISTRATOR'S MAIN MENU', 'Status', 'Wizard', 'Advanced', and 'Logout'. Below this, a secondary menu shows 'BASIC SETTING', 'FORWARDING RULES', 'SECURITY SETTING', 'ADVANCED SETTING', and 'TOOL BOX'. The left sidebar contains a tree view with 'Primary Setup', 'DHCP Server', 'Wireless', and 'Change Password'. The main content area is titled 'Virtual Computers' and includes a '[HELP]' link. At the top of this section, there is a 'DHCP clients' dropdown menu set to '-- Select one --' and a 'Copy to ID' dropdown menu. Below this is a table with five rows, each representing a virtual computer configuration. The table has four columns: 'ID', 'Global IP', 'Local IP', and 'Enable'. The 'Local IP' column shows a default value of '192.168.0.' followed by an empty input field. At the bottom of the table are 'Save' and 'Undo' buttons. A text box on the left side of the interface reads: 'Allow you to setup the one to one mapping of multiple global IP address and local IP address.'

ID	Global IP	Local IP	Enable
1	<input type="text"/>	192.168.0. <input type="text"/>	<input type="checkbox"/>
2	<input type="text"/>	192.168.0. <input type="text"/>	<input type="checkbox"/>
3	<input type="text"/>	192.168.0. <input type="text"/>	<input type="checkbox"/>
4	<input type="text"/>	192.168.0. <input type="text"/>	<input type="checkbox"/>
5	<input type="text"/>	192.168.0. <input type="text"/>	<input type="checkbox"/>

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

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

4.4.2 DHCP Server

Item	Setting
DHCP Server	<input type="radio"/> Disable <input checked="" type="radio"/> Enable
Lease Time	30 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>>”

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

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

4.4.3 Wireless Setting, 802.1X setting and WDS

Multi-Function Wireless Broadband NAT Router (R1.97 g6-R96)

ADMINISTRATOR'S MAIN MENU | Status | Wizard | Advanced | Logout

BASIC SETTING | FORWARDING RULES | SECURITY SETTING | ADVANCED SETTING | TOOLBOX

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

Please configure 8-63 characters in preshare key field.

Item	Setting
Wireless	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Network ID(SSID)	188
Wireless Mode	<input checked="" type="radio"/> 11 b/g/n Mixed <input type="radio"/> 11n only
SSID Broadcast	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Channel	11
WDS	Enter
WPS	Enter
Security	WPA-PSK
Encryption	TKIP
Preshare Key Mode	ASCII
Preshare Key	1234567890

Save | Undo | Wireless Client List

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 shows the configuration interface for a Multi-Functional Wireless Broadband NAT Router (R1.97g6-R86). The main menu includes Administrator's Main Menu, Status, Wizard, Advanced, and Logout. The current page is the Wireless Setting page, which is part of the Security Setting section. The settings are as follows:

Item	Setting
Wireless	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Network ID (SSID)	default
Wireless Mode	<input checked="" type="radio"/> 11 b/g/n Mixed <input type="radio"/> 11n only
SSID Broadcast	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Channel	3
Security	802.1x and RADIUS
Encryption Key Length	<input checked="" type="radio"/> 64 bits <input type="radio"/> 128 bits
RADIUS Server IP	0.0.0.0
RADIUS port	1812
RADIUS Shared Key	

Buttons at the bottom include Save, Undo, WDS Setting..., MAC Address Control, and Wireless Client List.

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

Item	Setting
Wireless	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Network ID(SSID)	default
Wireless Mode	<input checked="" type="radio"/> 11 b/g/n Mixed <input type="radio"/> 11n only
SSID Broadcast	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Channel	3
Security	WPA-PSK
Encryption	TKIP
Pre-share Key Mode	ASCII
Pre-share Key	

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.

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

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.

WPA-PSK /WPA2-PSK

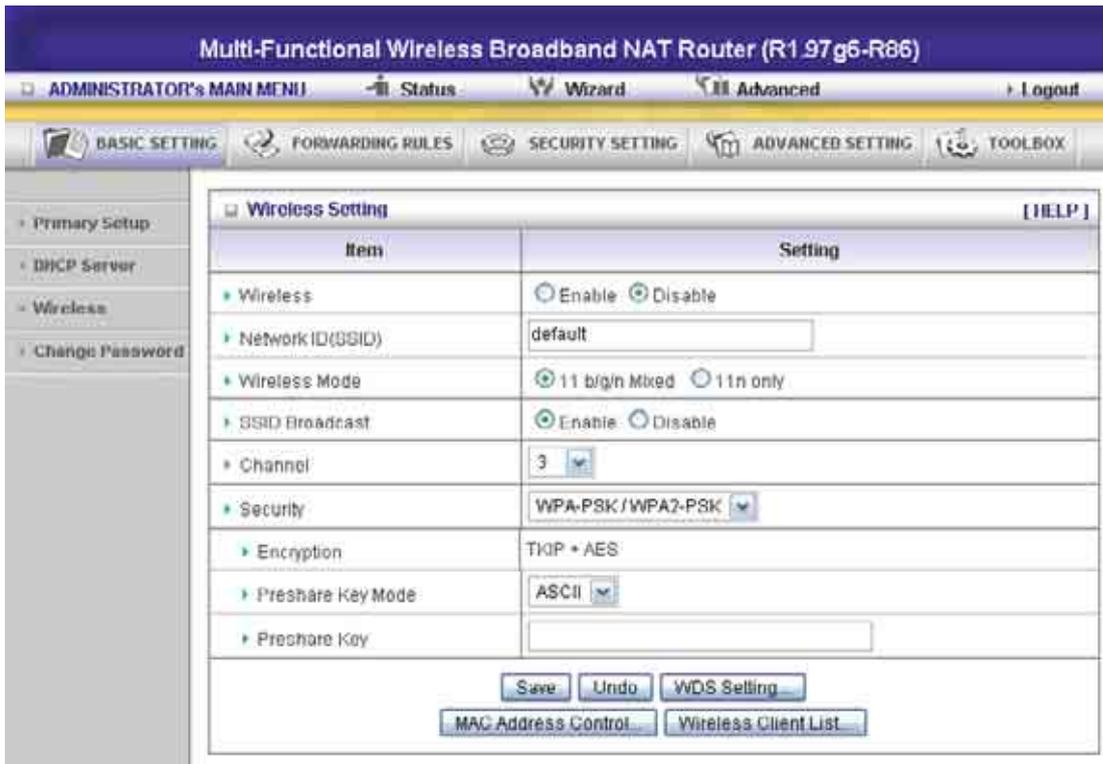
The router will detect automatically which Security type the client uses to encrypt.

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



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.

WPS(WiFi Protection Setup)

WPS is WiFi Protection Setup which is similar to WCN-NET and offers safe and easy way in Wireless Connection.

The screenshot shows the administrator interface for a Multi-Functional Wireless Broadband NAT Router (R1.97 g6-R86). The interface includes a navigation menu with options like 'ADMINISTRATOR'S MAIN MENU', 'Status', 'Wizard', 'Advanced', and 'Logout'. Below this, there are tabs for 'BASIC SETTING', 'FORWARDING RULES', 'SECURITY SETTING', 'ADVANCED SETTING', and 'TOOLBOX'. The 'WPS (WiFi Protected Setup)' configuration page is displayed, featuring a table with the following content:

Item	Setting
WPS	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Setup	<input type="radio"/> Current PIN <input checked="" type="radio"/> Configure Wireless Station
Method	<input type="radio"/> Enrollee PIN : <input type="text"/> <input type="radio"/> Software button
WPS status	WPS is invalid!

At the bottom of the configuration area, there is a button labeled 'Save and Connect'.

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.

The screenshot displays the WDS Setting page on a Multi-Functional Wireless Broadband NAT Router (R1.97g6-R86). The page includes a navigation menu with options like Administrator's Main Menu, Status, Wizard, Advanced, and Logout. The main content area is titled "WDS Setting" and contains the following configuration options:

- Wireless Bridging:** A radio button interface with "Disable" selected and "Enable" unselected.
- Remote AP MAC:** Three input fields labeled "MAC 1", "MAC 2", and "MAC 3".
- Scanned AP's MAC:** A dropdown menu currently showing "-- Select one --", a "Copy to" button, and another dropdown menu for "Remote AP MAC".

Below these settings is a table listing scanned APs with columns for SSID, Channel, and MAC Address:

SSID	Channel	MAC Address
default	1	20-50-10-40-11-44
MVA300_Q11_TOM	1	00-50-10-21-C1-5E
ELROTEL	1	00-50-10-00-0E-A8
default	1	00-50-10-00-0F-ED
SS_SbeCCD	1	00-50-10-03-03-33

4.4.4 Change Password

The screenshot displays the web interface of a Multi-Functional Wireless Broadband NAT Router (R1.97 g6-R86). The top navigation bar includes 'ADMINISTRATOR's MAIN MENU', 'Status', 'Wizard', 'Advanced', and 'Logout'. Below this, a secondary menu contains 'BASIC SETTING', 'FORWARDING RULES', 'SECURITY SETTING', 'ADVANCED SETTING', and 'TOOLBOX'. On the left, a sidebar menu lists 'Primary Setup', 'DHCP Server', 'Wireless', and 'Change Password'. The main content area is titled 'Change Password' and contains a table with the following structure:

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

At the bottom of the form, there are two buttons: 'Save' and 'Undo'.

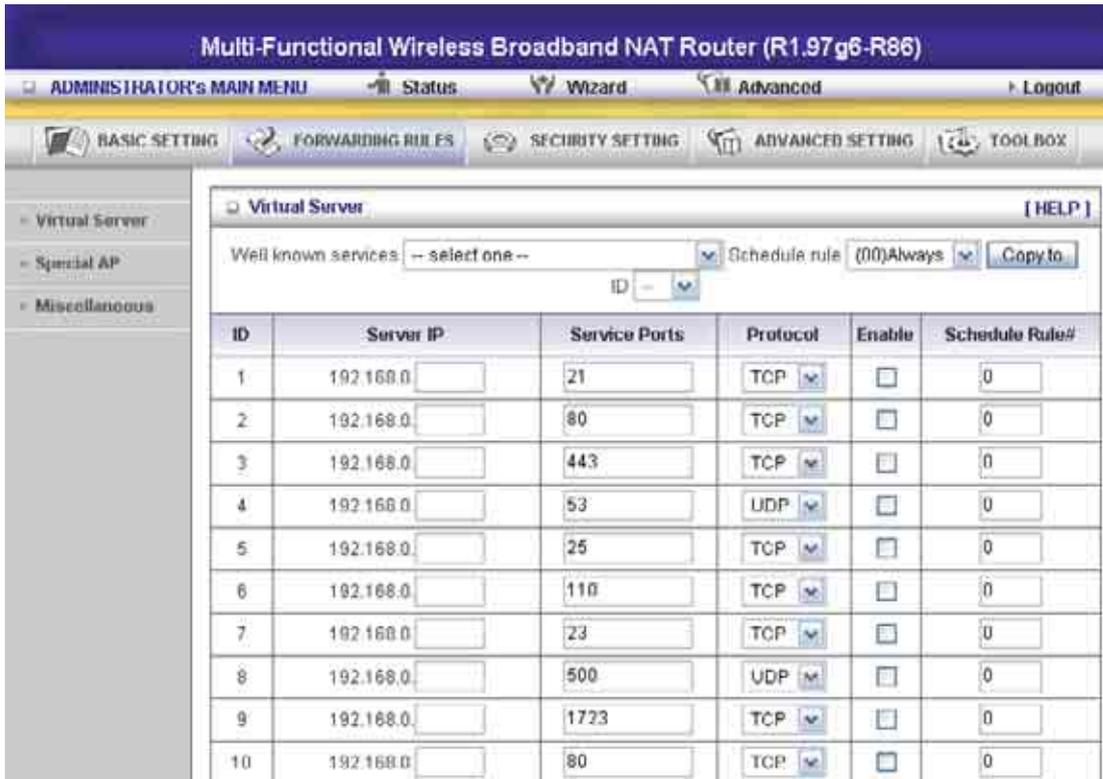
You can change Password here. We **strongly** recommend you to change the system password for security reason.

4.5 Forwarding Rules

The screenshot displays the web-based configuration interface for a Multi-Functional Wireless Broadband NAT Router (R1.97g6-R86). The interface features a top navigation bar with the title and several menu items: ADMINISTRATOR'S MAIN MENU, Status, Wizard, Advanced, and Logout. Below this is a secondary navigation bar with icons for BASIC SETTING, FORWARDING RULES (which is highlighted), SECURITY SETTING, ADVANCED SETTING, and TOOLBOX. On the left side, there is a vertical sidebar menu with options for Virtual Server, Special AP, and Miscellaneous. The main content area is titled 'Forwarding Rules' and contains three bullet points:

- **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/software.

4.5.1 Virtual Server



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

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

The screenshot shows the administrator interface of a Multi-Functional Wireless Broadband NAT Router (R1.97g6-R86). The top navigation bar includes 'ADMINISTRATOR'S MAIN MENU', 'Status', 'Wizard', 'Advanced', and 'Logout'. Below this is a secondary menu with 'BASIC SETTING', 'FORWARDING RULES', 'SECURITY SETTING', 'ADVANCED SETTING', and 'TOOL BOX'. The left sidebar has 'Virtual Server', 'Special AP', and 'Miscellaneous'. The main content area is titled 'Special Applications' and features a 'Popular applications' dropdown menu with a 'Copy to' button and an 'ID' field. Below this is a table with columns for ID, Trigger, Incoming Ports, and Enable. The table contains 8 rows of predefined applications. At the bottom of the table are 'Save' and 'Undo' buttons.

ID	Trigger	Incoming Ports	Enable
1	6112	6112	<input type="checkbox"/>
2	7175	51200-51201,51210	<input type="checkbox"/>
3	2019	2000-2039,2050-2051,2069,2085,	<input type="checkbox"/>
4	47624	2300-2400,28800-29000	<input type="checkbox"/>
5	12053	12120,12122,24150-24220	<input type="checkbox"/>
6	554	6970-6999	<input type="checkbox"/>
7			<input type="checkbox"/>
8			<input type="checkbox"/>

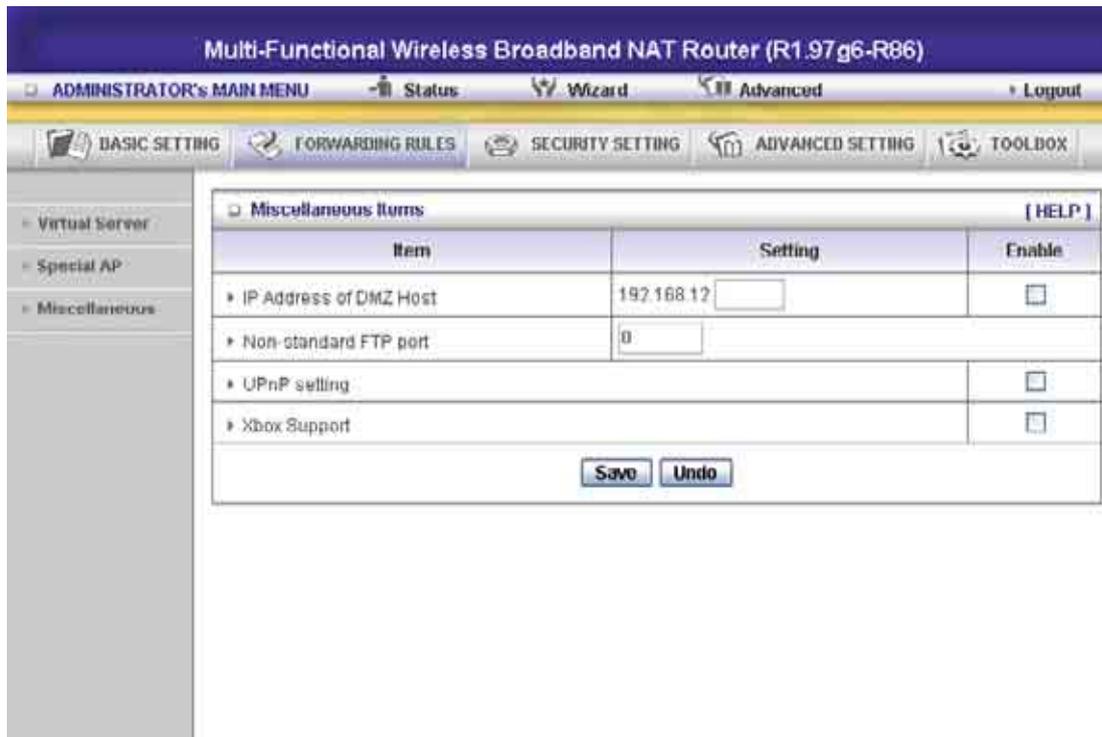
Some applications require multiple connections, like Internet games, Video conferencing, Internet telephony, etc. Because of the firewall function, these applications cannot work with a pure NAT router. The **Special Applications** feature allows some of these applications to work with this product.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

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

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

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

4.5.3 Miscellaneous Items



IP Address of DMZ Host

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

NOTE: This feature should be used only when needed.

Non-standard FTP port

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

Xbox Support

The Xbox is a video game console produced by Microsoft Corporation. Please enable this function when you play games.

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:

Internet Gateway Device UPnP [X]

A new device is now available on your network. For more information, click here.

Crazy Browser... (Untitled) - Et...

Address My Network Places

Network Tasks ^

- Add a network place
- View network connections
- Set up a home or small office network

Local Network

Internet Gateway Device UPnP

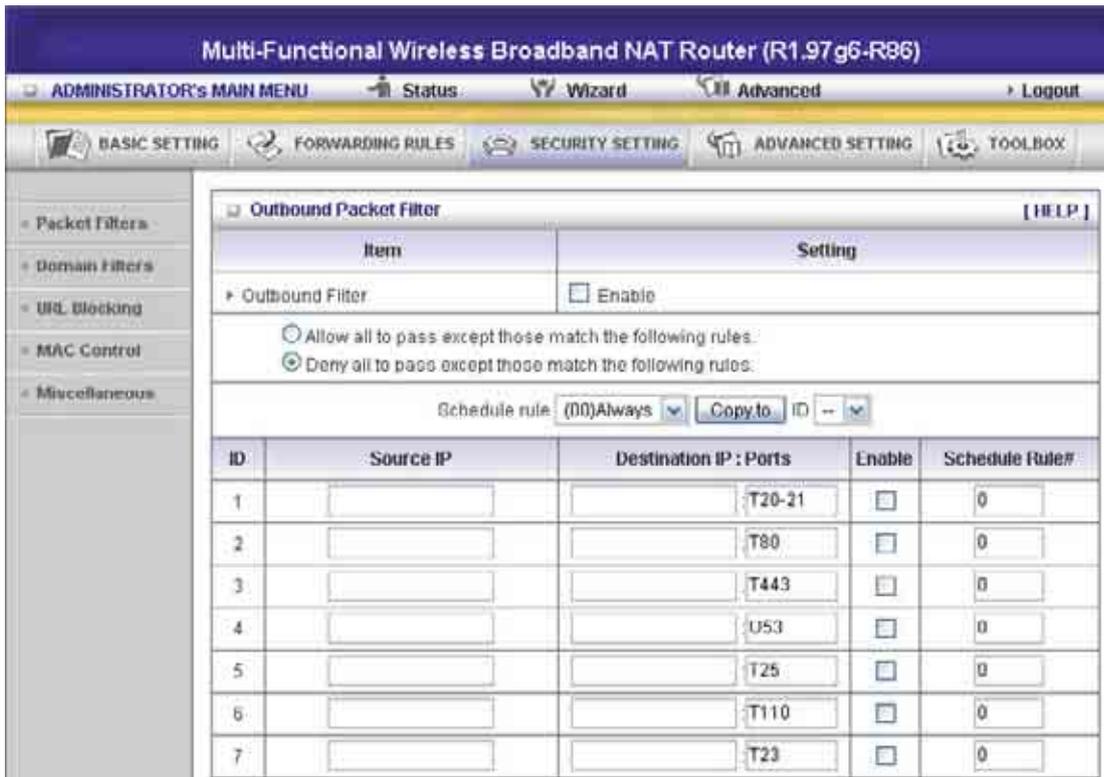
The Internet

4.6 Security Settings

The screenshot shows the 'Security Setting' page in a network device administrator interface. The top navigation bar includes 'ADMINISTRATOR's MAIN MENU', 'Status', 'Wizard', 'Advanced', and 'Logout'. Below this is a secondary navigation bar with 'BASIC SETTING', 'FORWARDING RULES', 'SECURITY SETTING' (highlighted), 'ADVANCED SETTING', and 'TOOLBOX'. On the left side, a sidebar menu lists 'Status', 'Packet Filters', 'Domain Filters', 'URL Blocking', 'MAC Control', and 'Miscellaneous'. The main content area is titled 'Security Setting' and contains a list of features:

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

4.6.1 Packet Filter



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**.

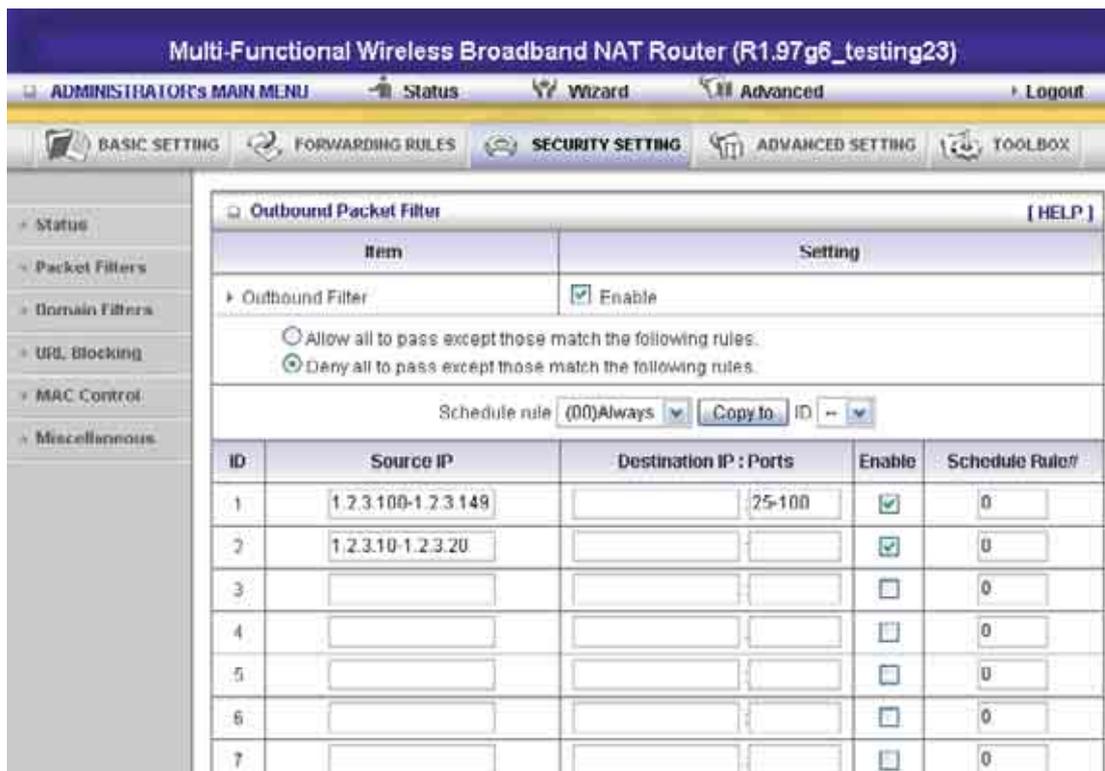
Each rule can be enabled or disabled individually.

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:

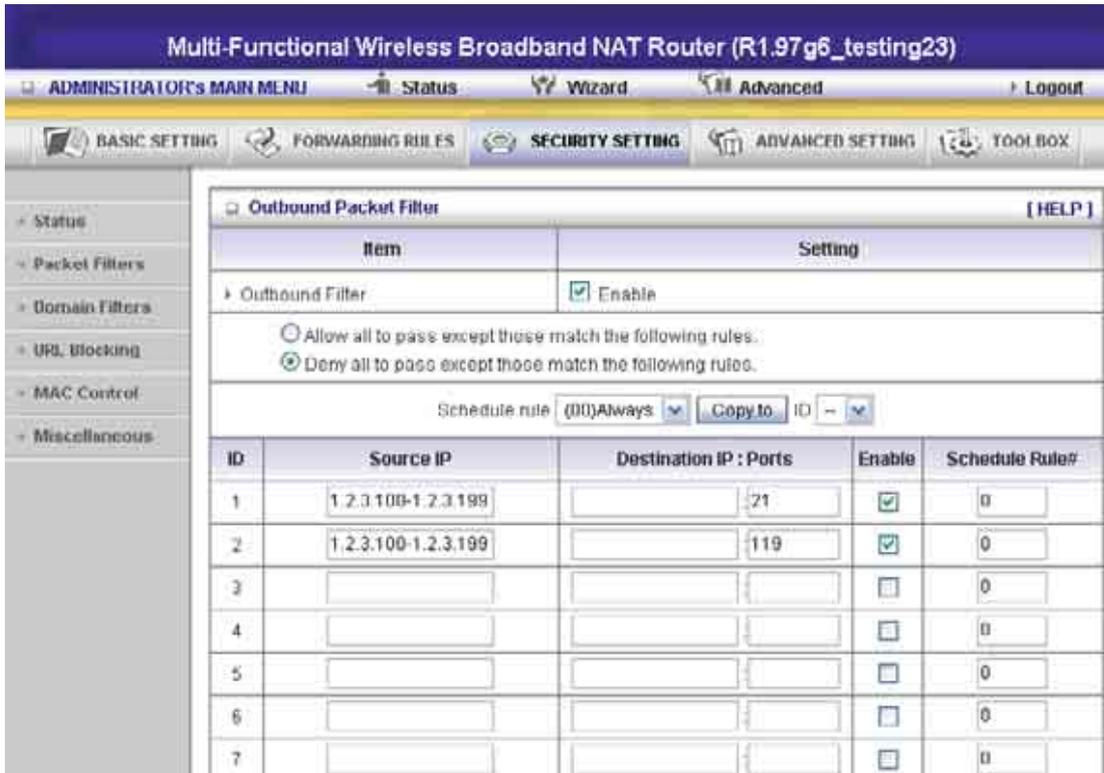


(1.2.3.100-1.2.3.149) They are allow to send mail (port 25), and browse the Internet (port 80)

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

Others are all blocked.

Example 2:



(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:

Multi-Function Wireless Broadband NAT Router (R1.97g6_testing23)

ADMINISTRATOR'S MAIN MENU Status Wizard Advanced Logout

BASIC SETTING FORWARDING RULES SECURITY SETTING ADVANCED SETTING TOOLBOX

Status
Packet Filters
Domain Filters
URL Blocking
MAC Control
Miscellaneous

Inbound Packet Filter [HELP]

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.	
Virtual Server Rule	192.168.122.13 : 20699-20700 Schedule rule (00)Always Copy to ID
1	

ID	Source IP	Destination IP : Ports	Enable	Schedule Rule#
1	10-149.168.123.149	25-100	<input checked="" type="checkbox"/>	0
2	10-149.161.123.20		<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

(149.161.123.100-149.161.123.149) 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.

(149.161.123.10-149.161.123.20) They can do everything (block nothing)

Others are all blocked.

Example 2:

The screenshot shows the configuration page for an Inbound Packet Filter on a Multi-Functional Wireless Broadband NAT Router. The page title is "Multi-Functional Wireless Broadband NAT Router (R1.97g6_testing23)". The navigation menu includes "ADMINISTRATOR'S MAIN MENU", "Status", "Wizard", "Advanced", and "Logout". The main menu has "BASIC SETTING", "FORWARDING RULES", "SECURITY SETTING", "ADVANCED SETTING", and "TOOLBOX". The left sidebar has "Status", "Packet Filters", "Domain Filters", "URL Blocking", "MAC Control", and "Miscellaneous".

The "Inbound Packet Filter" section is active, showing a table with the following data:

ID	Source IP	Destination IP : Ports	Enable	Schedule Rule#
1	149.168.123.100	:21	<input checked="" type="checkbox"/>	0
2	149.161.123.119	: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

(149.161.123.100 and 149.161.123.119) 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

The screenshot displays the web interface of a Multi-Functional Wireless Broadband NAT Router. The top navigation bar includes 'ADMINISTRATOR's MAIN MENU', 'Status', 'Wizard', 'Advanced', and 'Logout'. Below this is a secondary menu with 'BASIC SETTING', 'FORWARDING RULES', 'SECURITY SETTING', 'ADVANCED SETTING', and 'TOOLBOX'. The left sidebar lists various configuration categories: Status, Packet Filters, Domain Filters, URL Blocking, MAC Control, and Miscellaneous. The main content area is titled 'Domain Filter' and contains the following settings:

- Domain Filter:** Enable
- Log DNS Query:** Enable
- Privilege IP Addresses Range:** From To

Below the settings is a table for configuring domain filters:

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"/>

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:

Multi-Functional Wireless Broadband NAT Router (R1.97g6-R86)

ADMINISTRATOR'S MAIN MENU Status Wizard Advanced Logout

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

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

Domain Filter
[HELP]

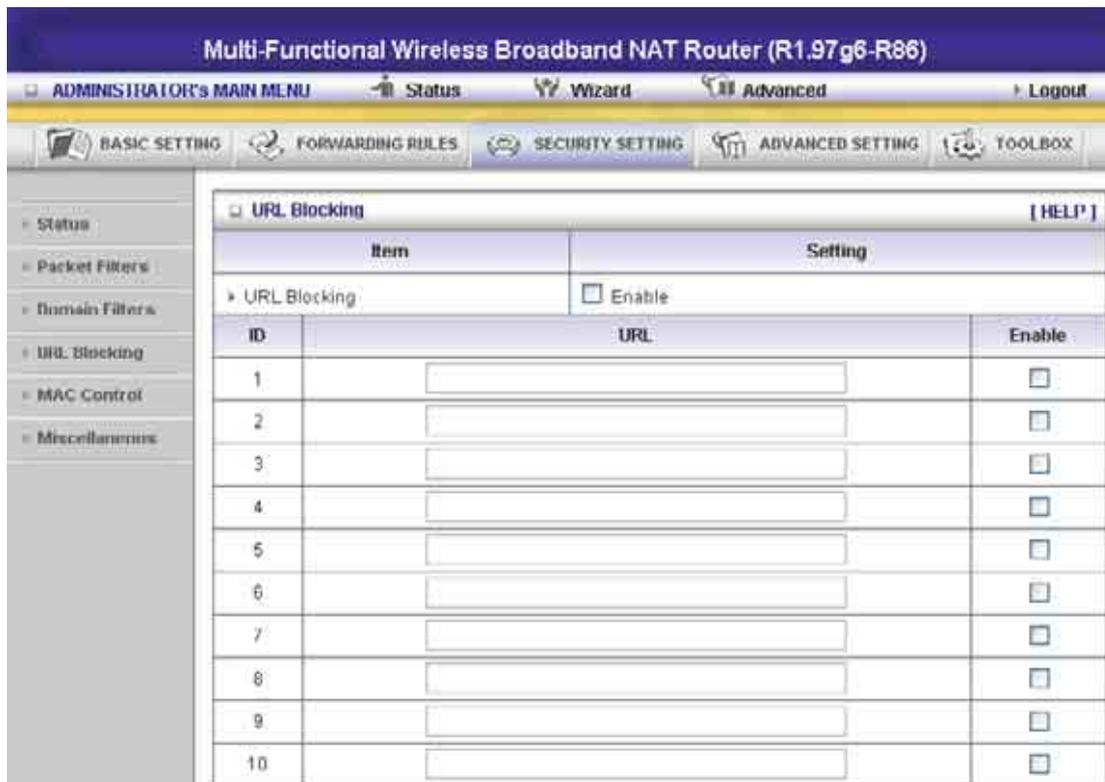
Item	Setting
» Domain Filter	<input checked="" type="checkbox"/> Enable
» Log DNS Query	<input checked="" type="checkbox"/> Enable
» Privilege IP Addresses Range	From <input type="text" value="100"/> To <input type="text" value="199"/>

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"/>

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 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.

Multi-Functional Wireless Broadband NAT Router (R1.97g6-R86)

ADMINISTRATOR'S MAIN MENU Status Wizard Advanced Logout

BASIC SETTING FORWARDING RULES SECURITY SETTING ADVANCED SETTING TOOL BOX

URL Blocking [HELP]

Item	Setting
URL Blocking <input checked="" type="checkbox"/> Enable	
ID	URL
1	<input type="text" value="msn"/>
2	<input type="text" value="sina"/>
3	<input type="text" value="cnnsi"/>
4	<input type="text" value="espn"/>
5	<input type="text"/>
6	<input type="text"/>
7	<input type="text"/>
8	<input type="text"/>
9	<input type="text"/>
10	<input type="text"/>

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

The screenshot shows the 'MAC Address Control' configuration page. At the top, there is a navigation bar with 'ADMINISTRATOR'S MAIN MENU', 'Status', 'Wizard', 'Advanced', and 'Logout'. Below this is a secondary menu with 'BASIC SETTING', 'FORWARDING RULES', 'SECURITY SETTING', 'ADVANCED SETTING', and 'TOOLBOX'. The left sidebar contains a tree view with 'Status', 'Packet Filters', 'Domain Filters', 'NAT Blocking', 'MAC Control', and 'Miscellaneous'. The main content area is titled 'MAC Address Control' and includes a '[HELP]' link.

The settings are organized into a table with two columns: 'Item' and 'Setting'. The 'MAC Address Control' item has an 'Enable' checkbox. The 'Connection control' item has a checkbox and a dropdown menu set to 'allow'. The 'Association control' item has a checkbox and a dropdown menu set to 'deny'. Below these settings is a 'DHCP clients' section with a 'Select one' dropdown and a 'Copy to ID' button.

ID	MAC Address	IP Address	C	A
1	<input type="text"/>	192.168.12. <input type="text"/>	<input type="checkbox"/>	<input type="checkbox"/>
2	<input type="text"/>	192.168.12. <input type="text"/>	<input type="checkbox"/>	<input type="checkbox"/>
3	<input type="text"/>	192.168.12. <input type="text"/>	<input type="checkbox"/>	<input type="checkbox"/>
4	<input type="text"/>	192.168.12. <input type="text"/>	<input type="checkbox"/>	<input type="checkbox"/>

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

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

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

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

addresses are not in the "Control table", to associate to the wireless LAN.

Control table

ID	MAC Address	IP Address	C	A
1	<input type="text"/>	192.168.12. <input type="text"/>	<input type="checkbox"/>	<input type="checkbox"/>
2	<input type="text"/>	192.168.12. <input type="text"/>	<input type="checkbox"/>	<input type="checkbox"/>
3	<input type="text"/>	192.168.12. <input type="text"/>	<input type="checkbox"/>	<input type="checkbox"/>
4	<input type="text"/>	192.168.12. <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:

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

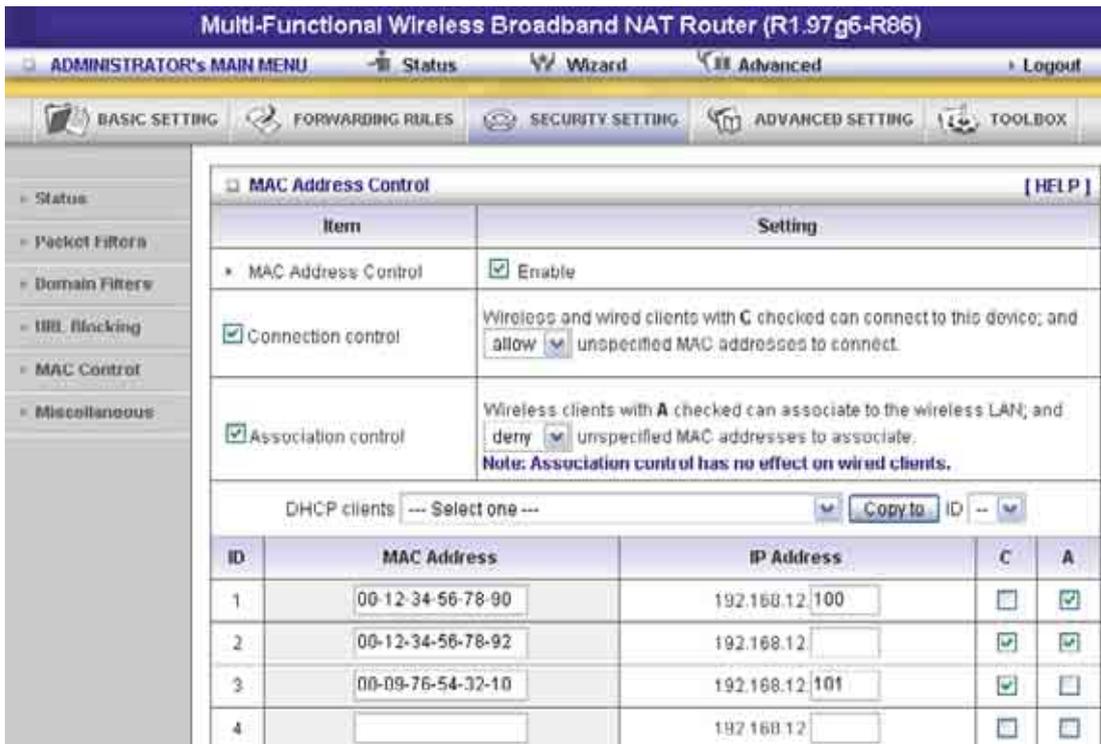
In this page, we provide the following Combobox and button to help you to input the MAC address.



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

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

Example:

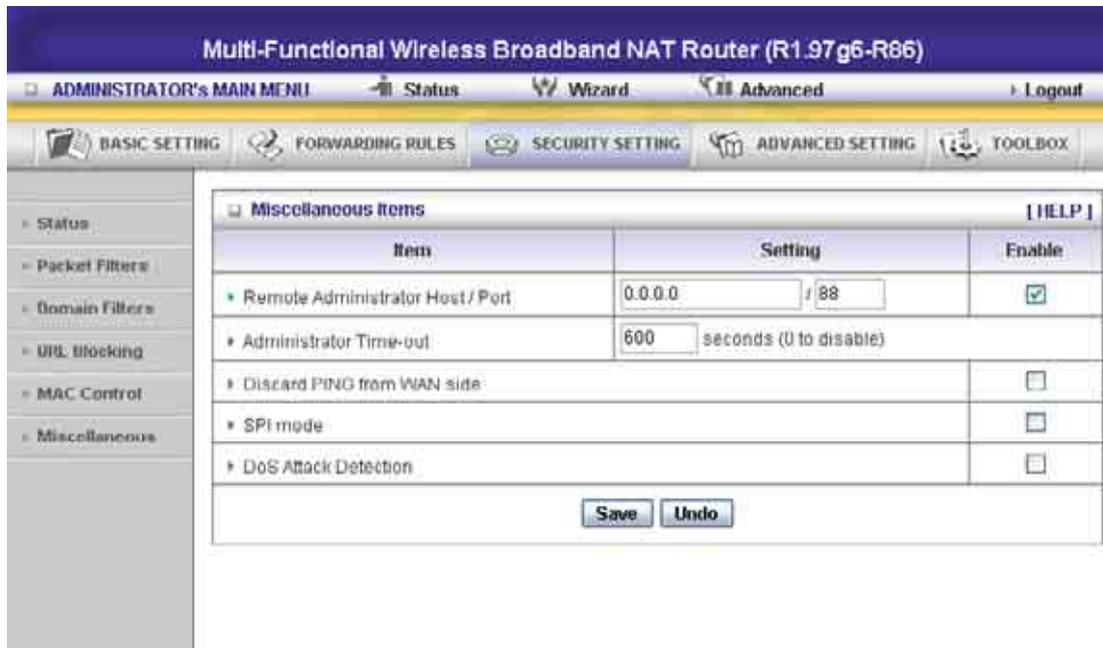


In this scenario, there are three clients listed in the Control Table. Clients 1 and 2 are wireless, and client 3 is wired.

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" --> 192.168.12.100
 - ID 3 - "00-09-76-54-32-10" --> 192.168.12.101
 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 (192.168.12.101), 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



Remote Administrator Host/Port

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

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

Administrator Time-out

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

Discard PING from WAN side

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

SPI Mode

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

DoS Attack Detection

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

4.7 Advanced Settings

Multi-Function Wireless Broadband NAT Router (R1.97.g6_testing23)

ADMINISTRATOR's MAIN MENU Status Wizard Advanced Logout

BASIC SETTING FORWARDING RULES SECURITY SETTING ADVANCED SETTING TOOLBOX

Advanced Setting

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

4.7.1 System Time

Multi-Function Wireless Broadband NAT Router (R1.97.g6_testing23)

ADMINISTRATOR's MAIN MENU Status Wizard Advanced Logout

BASIC SETTING FORWARDING RULES SECURITY SETTING ADVANCED SETTING TOOLBOX

System Time [HELP]

Item	Setting
System Time	2007年7月27日 上午 10:44:48
<input checked="" type="radio"/> Get Date and Time by NTP Protocol Sync Now!	
Time Server	time.nist.gov
Time Zone	(GMT+08:00) Beijing, Hong Kong, Singapore, Taipei
<input type="radio"/> Set Date and Time using PC's Date and Time	
PC Date and Time	2007年7月27日 上午 10:54:22
<input 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 type="radio"/> Enable <input checked="" type="radio"/> Disable
Start	Month: Jan Day: 01 Hour: 00

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

The screenshot shows the administrator interface of a Multi-Functional Wireless Broadband NAT Router (R1.97g6_testing23). The page is titled "System Log" and includes a sidebar with navigation options: Status, System Time, System Log, Dynamic DNS, SNMP, Routing, Schedule Rule, and OnS Rule. The main content area is a table with columns for Item, Setting, and Enable. The "IP Address for Syslogd" is set to 192.168.122. The "IP Address of Outgoing Mail Server" has a "Send Mail Now" button. The "Log Type" section has checkboxes for System Activity, Debug Information, Attacks, Dropped Packets, and Notice, all of which are checked. At the bottom, there are buttons for "View Log...", "Save", and "Undo".

Item	Setting	Enable
IP Address for Syslogd	192.168.122.	<input type="checkbox"/>
IP Address of Outgoing Mail Server	Send Mail Now	<input type="checkbox"/>
SMTP Server IP/Port		
E-mail addresses		
E-mail Subject		
User name		
Password		
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 the administrator interface for a Multi-Functional Wireless Broadband NAT Router (R1.97g6_testing23). The top navigation bar includes 'ADMINISTRATOR'S MAIN MENU', 'Status', 'Wizard', 'Advanced', and 'Logout'. Below this, there are tabs for 'BASIC SETTING', 'FORWARDING RULES', 'SECURITY SETTING', 'ADVANCED SETTING', and 'TOOL BOX'. The 'ADVANCED SETTING' tab is selected, and the 'Dynamic DNS' sub-tab is active. The configuration area is titled 'Dynamic DNS' and includes a '[HELP]' link. It contains a table with the following items and settings:

Item	Setting
DDNS	<input type="radio"/> Disable <input checked="" type="radio"/> Enable
Provider	No-IP.com <input type="button" value="Provider website"/>
Host Name	123.sytes.net
Username / E-mail	service@amit.com.tw
Password / Key	*****

At the bottom of the configuration area, there are 'Save' and 'Undo' buttons. A sidebar on the left contains links to 'Status', 'System Time', 'System Log', 'Dynamic DNS', 'SNMP', 'Routing', 'Schedule Rule', and 'QoS Rule'.

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

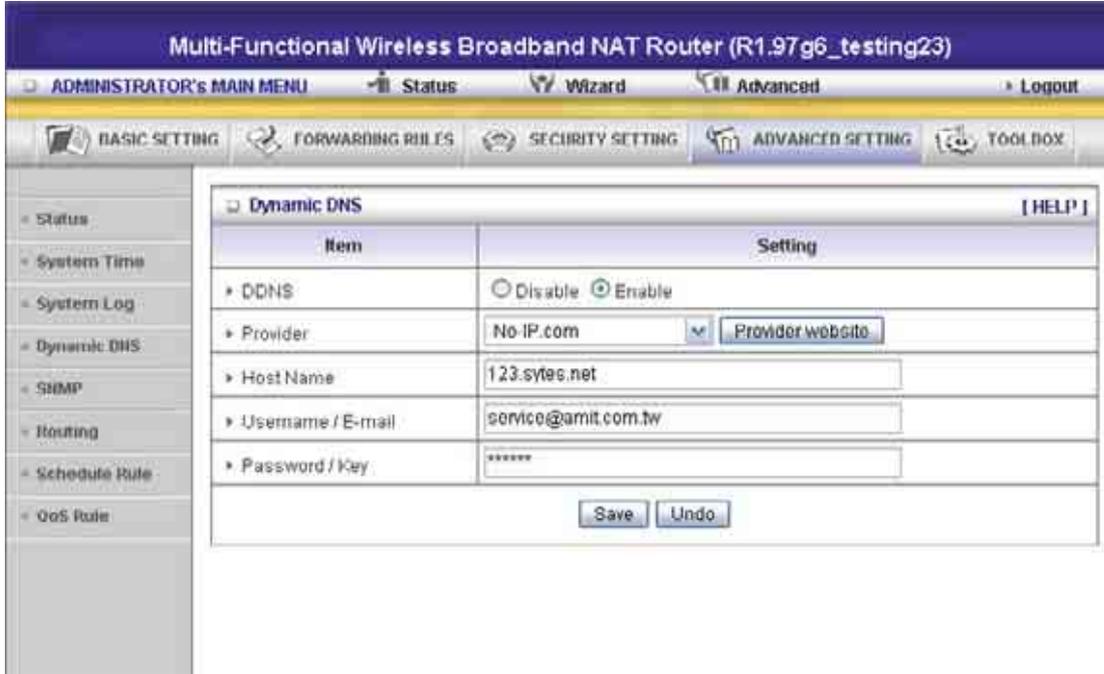
Host Name

Username/E-mail

Password/Key

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

Example:



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

4.7.4 SNMP Setting

The screenshot shows the administrator interface of a Multi-Functional Wireless Broadband NAT Router. The top navigation bar includes 'ADMINISTRATOR'S MAIN MENU', 'Status', 'Wizard', 'Advanced', and 'Logout'. Below this, there are tabs for 'BASIC SETTING', 'FORWARDING RULES', 'SECURITY SETTING', 'ADVANCED SETTING', and 'TOOL BOX'. On the left, a sidebar menu lists various system settings like 'Status', 'System Time', 'System Log', 'Dynamic DNS', 'SNMP', 'Routing', 'Schedule Rule', and 'DoS Rule'. The main content area is titled 'SNMP Setting' and contains a table with the following data:

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

At the bottom of the table, there are 'Save' and 'Undo' buttons.

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

The screenshot displays the configuration interface for a Multi-Functional Wireless Broadband NAT Router (R1.97g6_testing23). The page is titled "ADMINISTRATOR'S MAIN MENU" and includes navigation tabs for Status, Wizard, and Advanced. The main menu includes BASIC SETTING, FORWARDING RULES, SECURITY SETTING, ADVANCED SETTING, and TOOLBOX. The Routing Table settings are shown, including Dynamic Routing (Disable, RIPv1, RIPv2) and Static Routing (Disable, Enable). A table lists 8 routing rules with columns for ID, Destination, Subnet Mask, Gateway, Hop, and Enable.

Routing Table		[HELP]				
Item		Setting				
Dynamic Routing		<input checked="" type="radio"/> Disable <input type="radio"/> RIPv1 <input type="radio"/> RIPv2				
Static Routing		<input type="radio"/> Disable <input checked="" type="radio"/> Enable				
ID	Destination	Subnet Mask	Gateway	Hop	Enable	
1	192.168.0.0	255.255.0.0	192.168.122.3	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
2	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>	<input type="checkbox"/>	
3	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>	<input type="checkbox"/>	
4	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>	<input type="checkbox"/>	
5	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>	<input type="checkbox"/>	
6	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>	<input type="checkbox"/>	
7	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>	<input type="checkbox"/>	
8	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>	<input type="checkbox"/>	

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

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

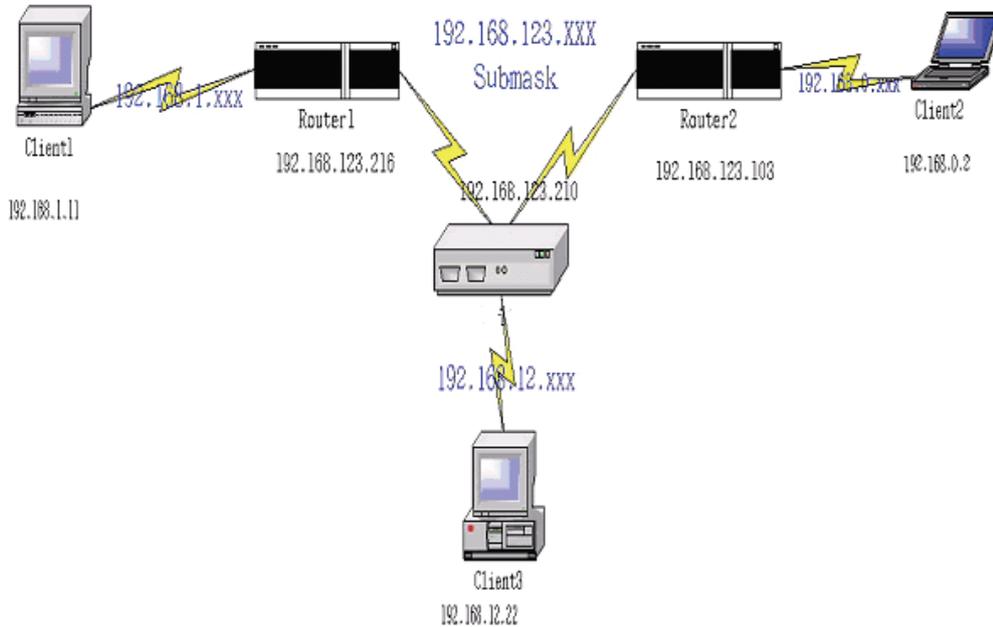
Dynamic Routing

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	✓

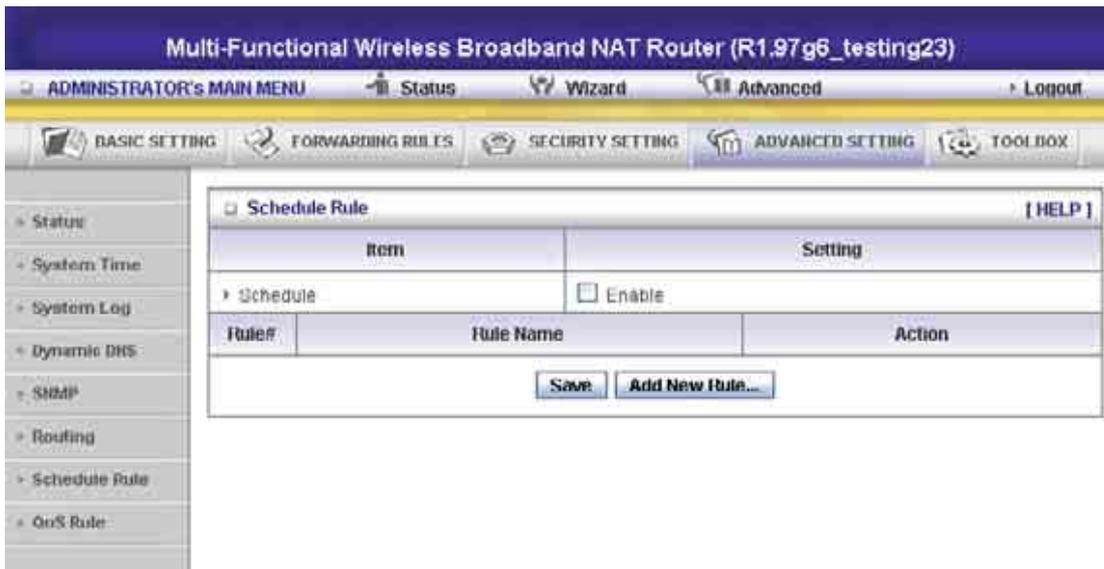
So if, for example, the client3 wanted to send an IP data gram to 192.168.0.2, it would use the above table to determine that it had to go via 192.168.123.103 (a gateway),

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.

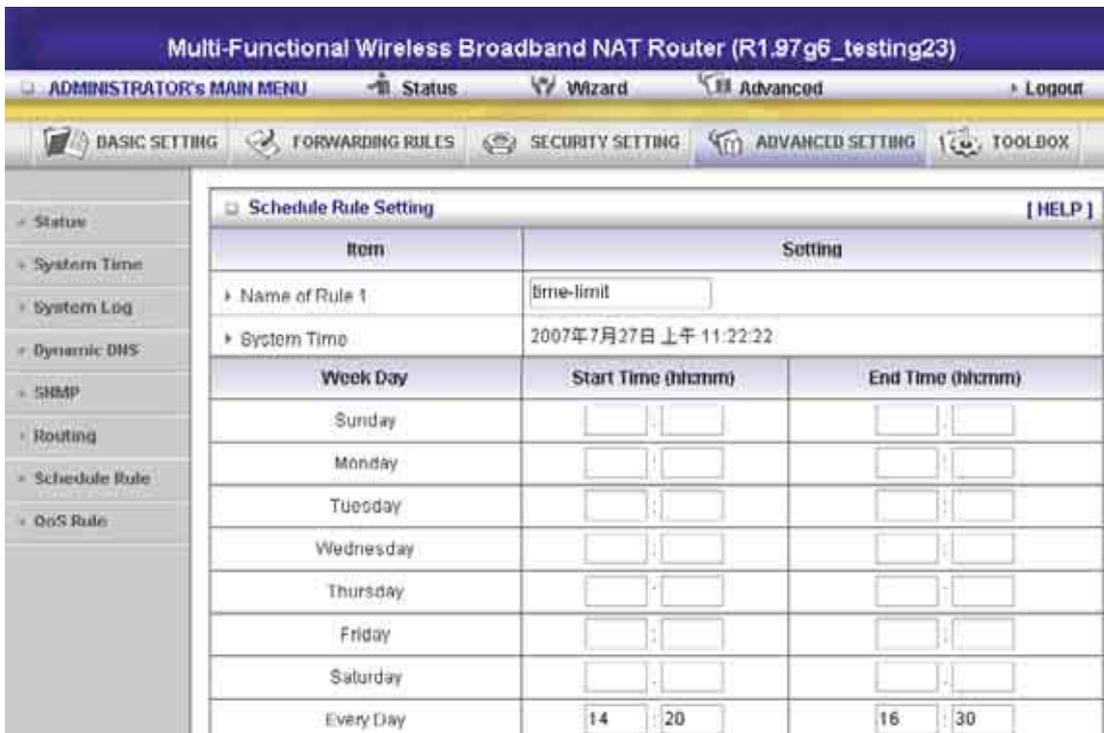
4.7.6 Schedule Rule



You can set the schedule time to decide which service will be turned on or off. Select the “enable” item.

Press “Add New Rule”

You can write a rule name and set which day and what time to schedule from “Start Time” to “End Time”. The following example configure “ftp time” as everyday 14:10 to 16:20



Schedule Enable

Selected if you want to Enable the Scheduler.

Edit

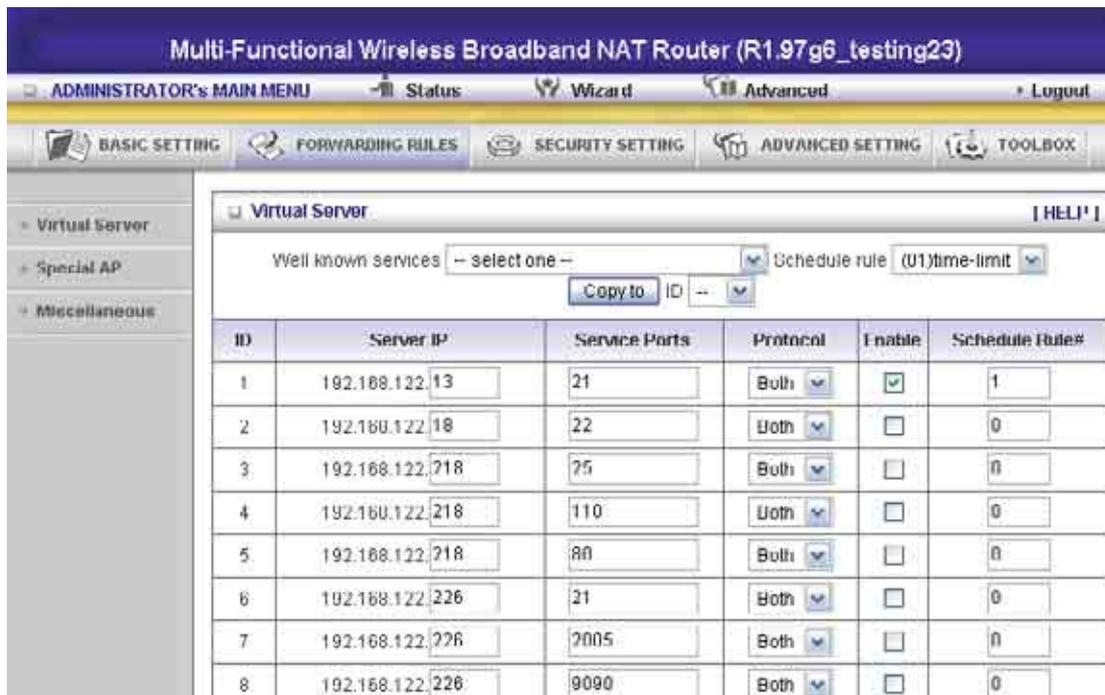
To edit the schedule rule.

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 14:20 to 16:30)



The screenshot shows the configuration page for a Multi-Function Wireless Broadband NAT Router. The page title is "Multi-Function Wireless Broadband NAT Router (R1.97g6_testing23)". The navigation menu includes "ADMINISTRATOR'S MAIN MENU", "Status", "Wizard", "Advanced", and "Logout". The main menu includes "BASIC SETTING", "FORWARDING RULES", "SECURITY SETTING", "ADVANCED SETTING", and "TOOLBOX". The "Virtual Server" section is active, showing a table of 8 entries. The table has columns for ID, Server IP, Service Ports, Protocol, Enable, and Schedule Rule#. The first entry (ID 1) is enabled and has Schedule Rule# 1. The other entries are disabled and have Schedule Rule# 0.

ID	Server IP	Service Ports	Protocol	Enable	Schedule Rule#
1	192.168.122.13	21	Both	<input checked="" type="checkbox"/>	1
2	192.168.122.18	22	Both	<input type="checkbox"/>	0
3	192.168.122.218	25	Both	<input type="checkbox"/>	0
4	192.168.122.218	110	Both	<input type="checkbox"/>	0
5	192.168.122.218	80	Both	<input type="checkbox"/>	0
6	192.168.122.226	21	Both	<input type="checkbox"/>	0
7	192.168.122.226	2005	Both	<input type="checkbox"/>	0
8	192.168.122.226	8090	Both	<input type="checkbox"/>	0

Example2: **Packet Filter** – Apply Rule#1 (ftp time: everyday 14:20 to 16:30).

Multi-Functional Wireless Broadband NAT Router (R1.97 g6_testing23)

ADMINISTRATOR'S MAIN MENU Status Wizard Advanced Logout

BASIC SETTING FORWARDING RULES SECURITY SETTING ADVANCED SETTING TOOL BOX

- Status
- 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 ID --

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

4.7.7 QoS Rule

Multi-Functional Wireless Broadband NAT Router (R1.97g6-R86)

ADMINISTRATOR'S MAIN MENU Status Wizard Advanced Logout

BASIC SETTING FORWARDING RULES SECURITY SETTING ADVANCED SETTING TOOL BOX

QoS Rule

Item	Setting				
QoS Control	<input checked="" type="checkbox"/> Enable				
Well known services -- select one --					
Schedule rule (00)Always Copy to ID --					
ID	Local IP	Remote IP : Ports	QoS Priority	Enable	Schedule Rule#
1	192.168.12.33	98.97.96.1 : 21	High	<input checked="" type="checkbox"/>	1
2			Normal	<input type="checkbox"/>	0
3			Normal	<input type="checkbox"/>	0
4			Normal	<input type="checkbox"/>	0
5			Normal	<input type="checkbox"/>	0
6			Normal	<input type="checkbox"/>	0
7			Normal	<input type="checkbox"/>	0

Local IP:

Please input Client IP,ex192.168.12.33.

Remote Priority:

Please input Global IP and port,ex:168.96.2.3 and port 21

4.8 Toolbox

The screenshot shows the administrator interface of a Multi-Functional Wireless Broadband NAT Router (R1.97 g6_testing23). The top navigation bar includes 'ADMINISTRATOR'S MAIN MENU', 'Status', 'Wizard', 'Advanced', and 'Logout'. Below this, there are tabs for 'BASIC SETTING', 'FORWARDING RULES', 'SECURITY SETTING', 'ADVANCED SETTING', and 'TOOLBOX'. The 'TOOLBOX' tab is selected, displaying a list of tools:

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

4.8.1 System Log

The screenshot shows the administrator interface of a Multi-Functional Wireless Broadband NAT Router (R1.97 g6_testing23) with the 'System Log' tab selected. The interface shows the following information:

System Log

ITEM	Info
WAN Type	Dynamic IP Address (R1.97 g6_testing23)
Display time	Fri Jul 27 11:29:10 2007
Time	Log
2007年7月26日 下午 08:20:27	Unrecognized attempt blocked from 221.234.188.53:50500 to 210.202.197.181 UDP:14333
2007年7月26日 下午 08:29:03	DHCP:renew
2007年7月26日 下午 08:29:03	DHCP:ack(DOL=1800,T1=900,T2=1575)
2007年7月26日 下午 08:44:03	DHCP:renew
2007年7月26日 下午 08:44:03	DHCP:ack(DOL=1800,T1=900,T2=1575)
2007年7月26日 下午 08:50:01	Unrecognized attempt blocked from 210.200.244.164:4364 to 210.202.197.181 TCP:135
2007年7月26日 下午 08:59:03	DHCP:renew
2007年7月26日 下午 08:59:03	DHCP:ack(DOL=1800,T1=900,T2=1575)
2007年7月26日 下午 09:09:08	Unrecognized attempt blocked from 210.193.86.250:3595 to 210.202.197.181 TCP:135

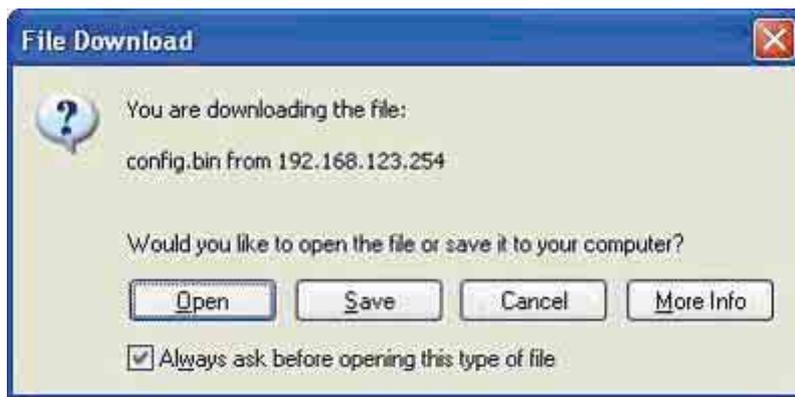
You can View system log by clicking the **View Log** button

4.8.2 Firmware Upgrade



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 802.1x Setting

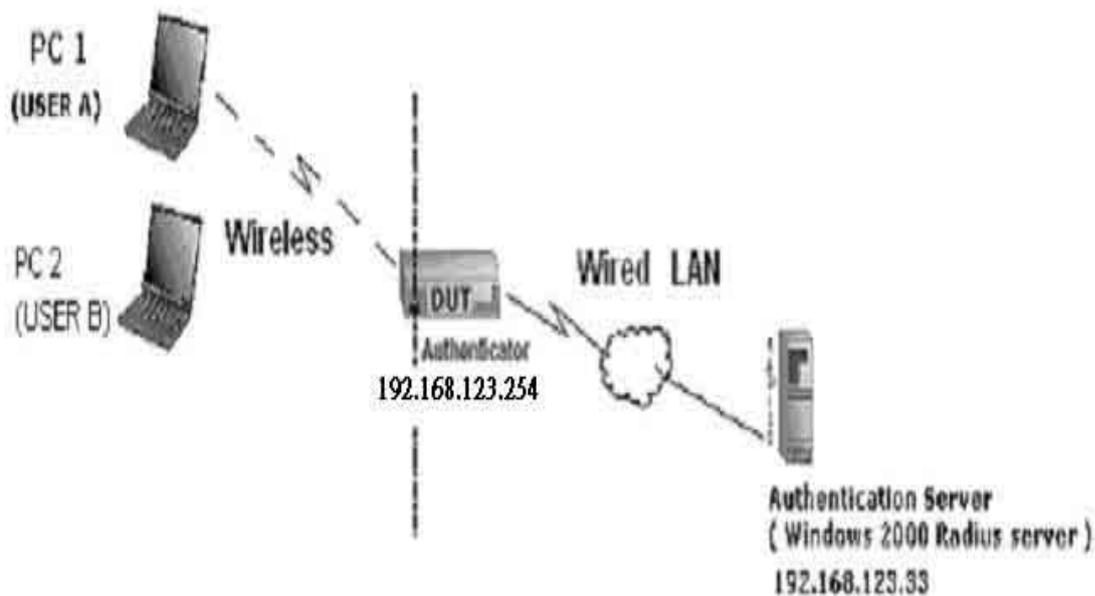


Figure 1: Testing Environment (Use Windows 2000 Radius Server)

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.

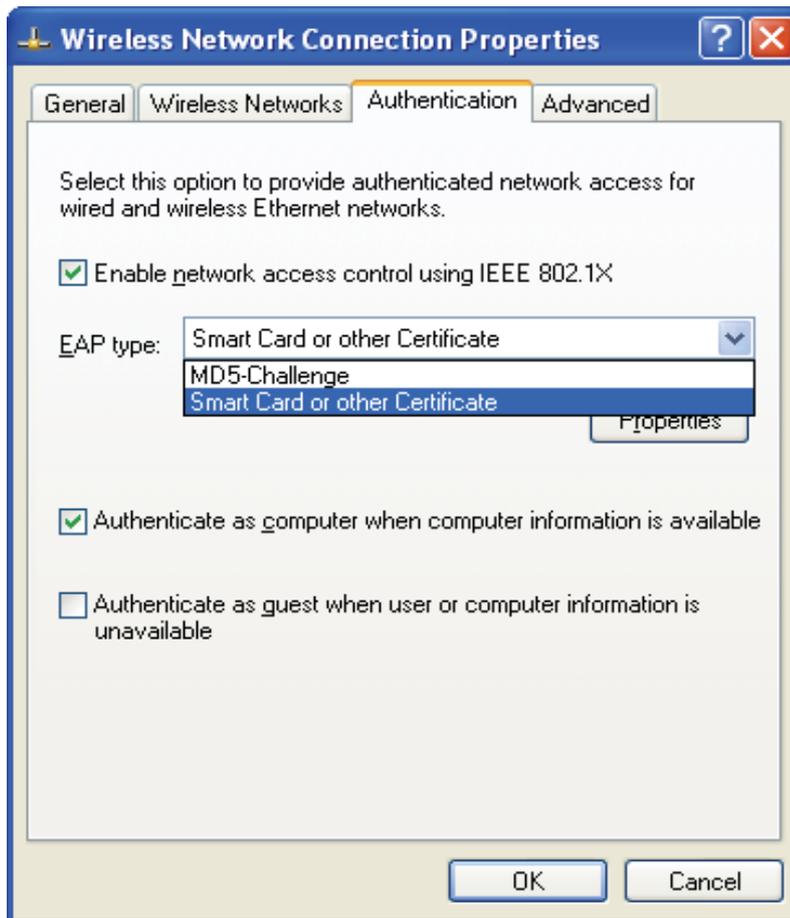


Figure 2: Enable IEEE 802.1X access control

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.

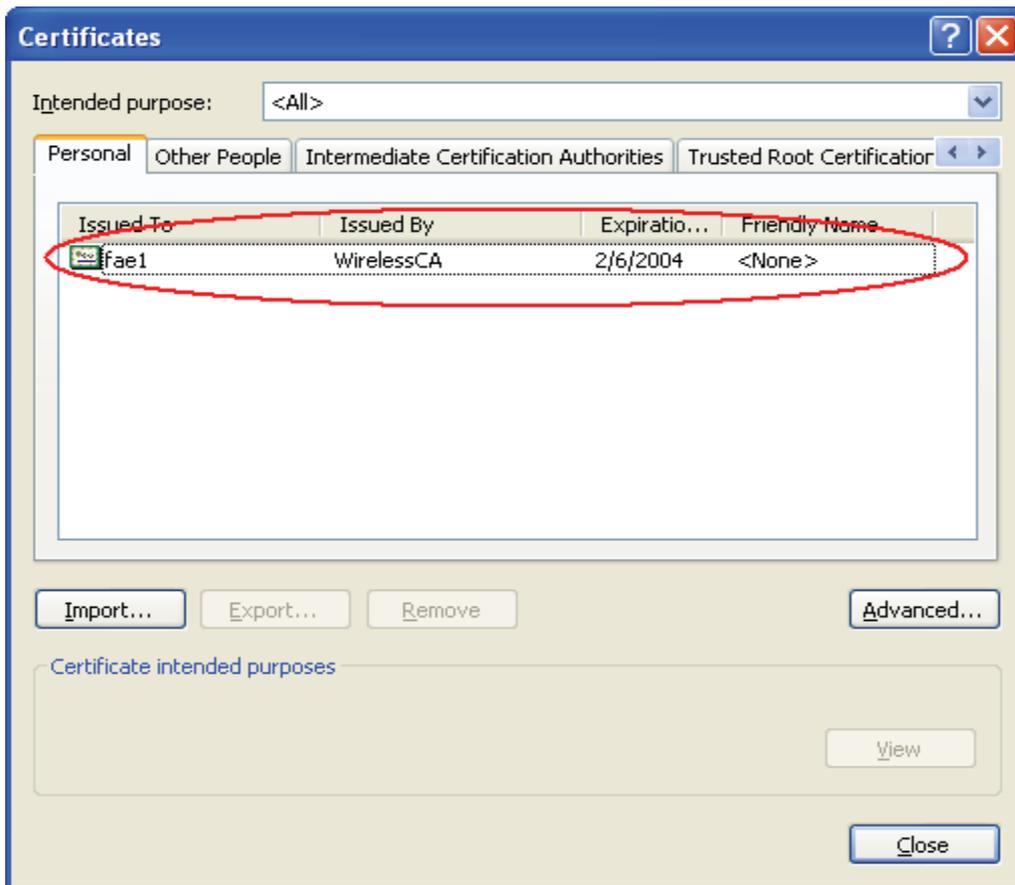


Figure 4: Certificate information on PC1

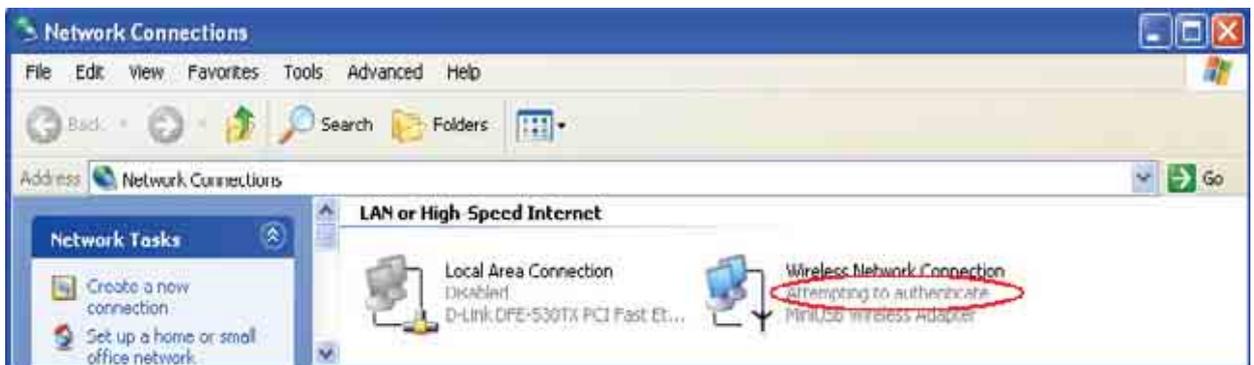


Figure 5: Authenticating

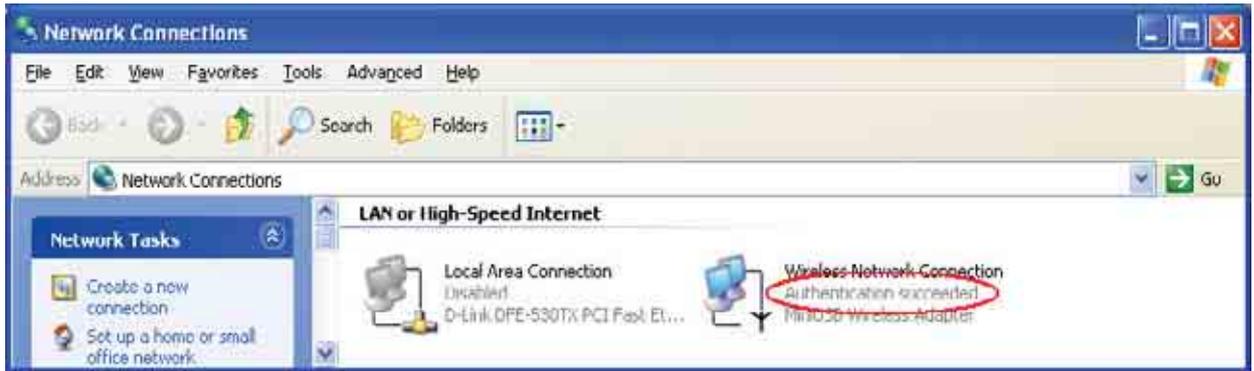


Figure 6: Authentication success

4.2DUT authenticate PC2 using PEAP-TLS.

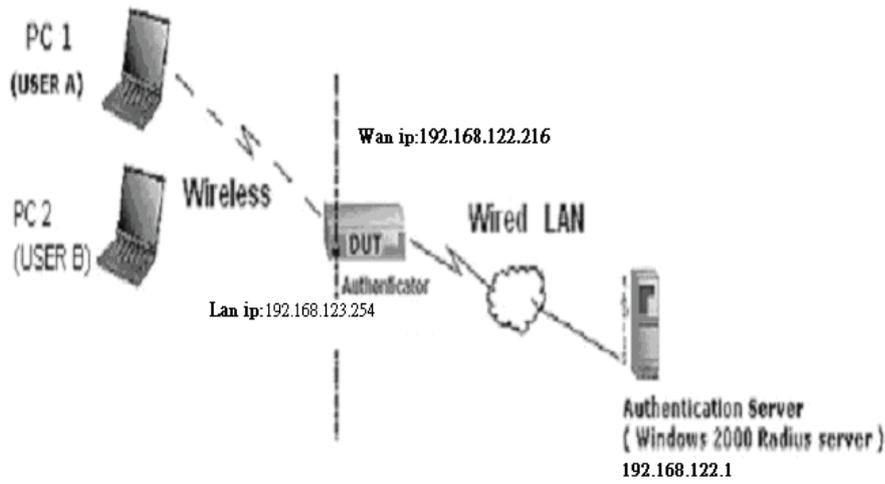
1. PC2 choose the SSID of DUT as the Access Point.
2. Set authentication type of wireless client and RADIUS server both to PEAP_TLS.
3. Disable the wireless connection and enable again.
- 4.The DUT will send the user's certificate to the RADIUS server, and then send the message of authentication result 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 B WPA-PSK and WPA



Wireless Router: LAN IP: 192.168.123.254

WAN IP: 192.168.122.216

Radius Server: 192.168.122.1

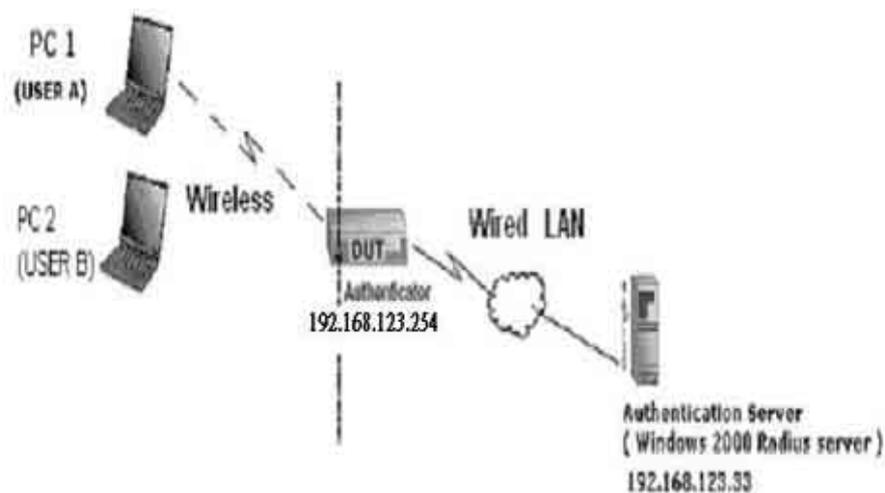
UserA : XP Wireless Card:Ti-11g

Tool: Odyssey Client Manager

Refer to: www.funk.com

Download: 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:

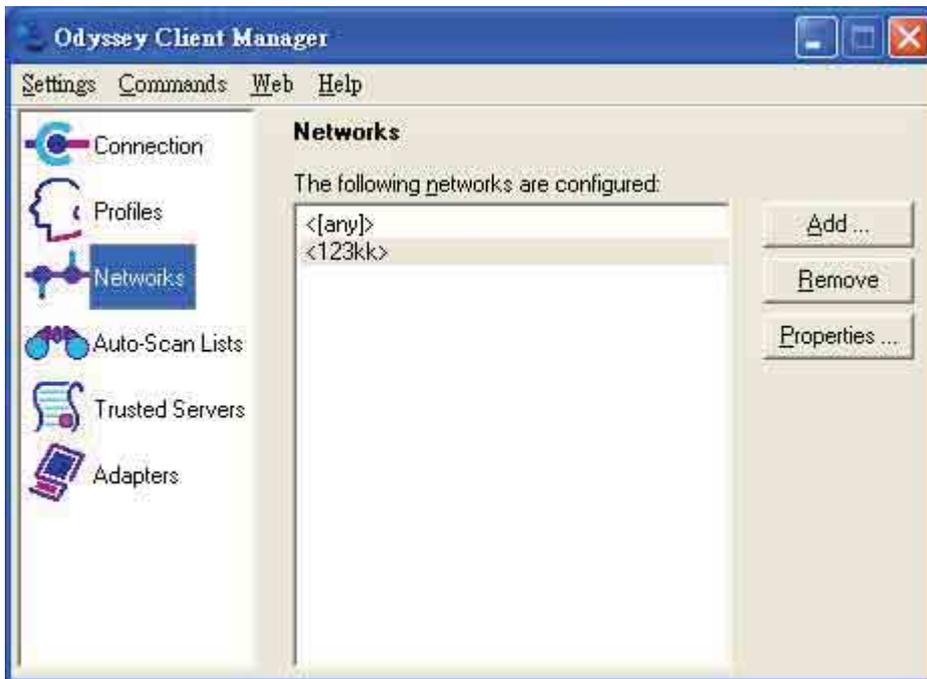
1. Go to the Web manager of Wireless Router to configure, like below:

Network ID(SSID)	<input type="text" value="123kk"/>
Channel	<input type="text" value="8"/>
Security	<input type="text" value="WPA-PSK"/>
Key Mode	<input type="text" value="ASCII"/>
Preshare Key	<input type="text" value="12345678"/>

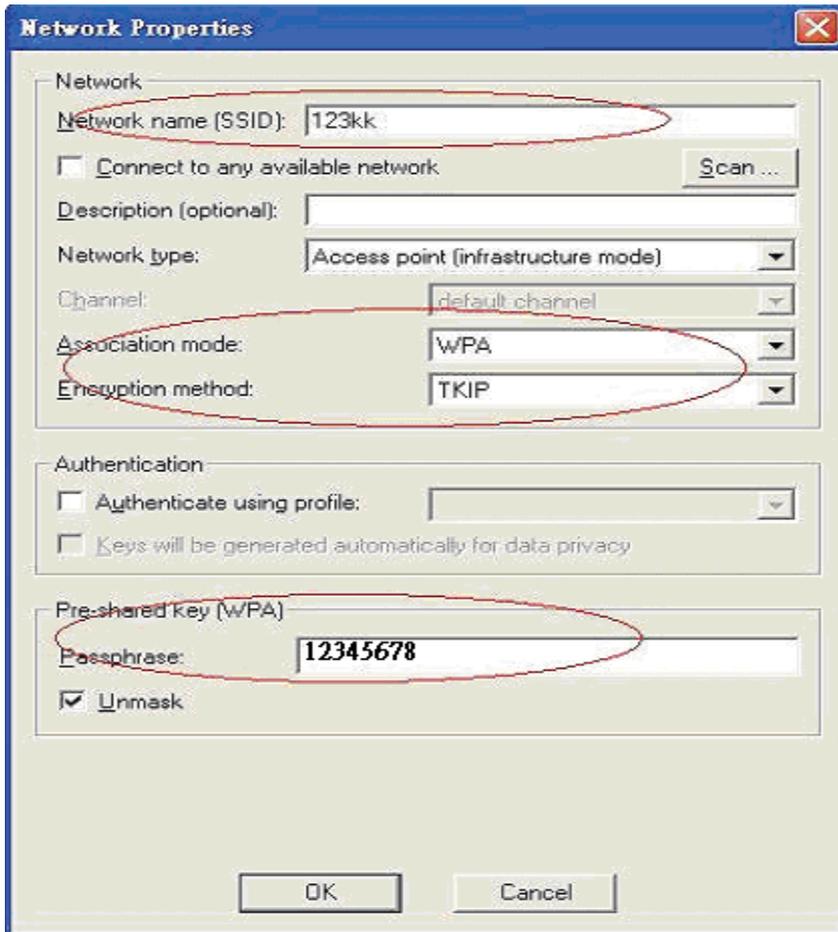
2. Go to Odyssey Client Manager, first choose “Network”

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

Open “Adapters”

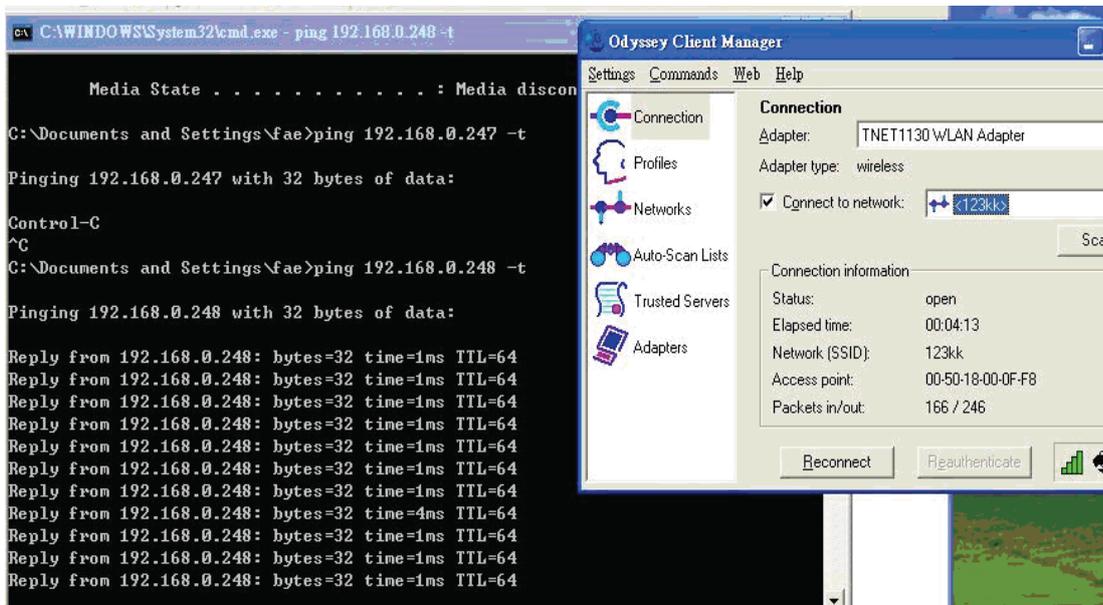


3. Add and edit some settings:



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:

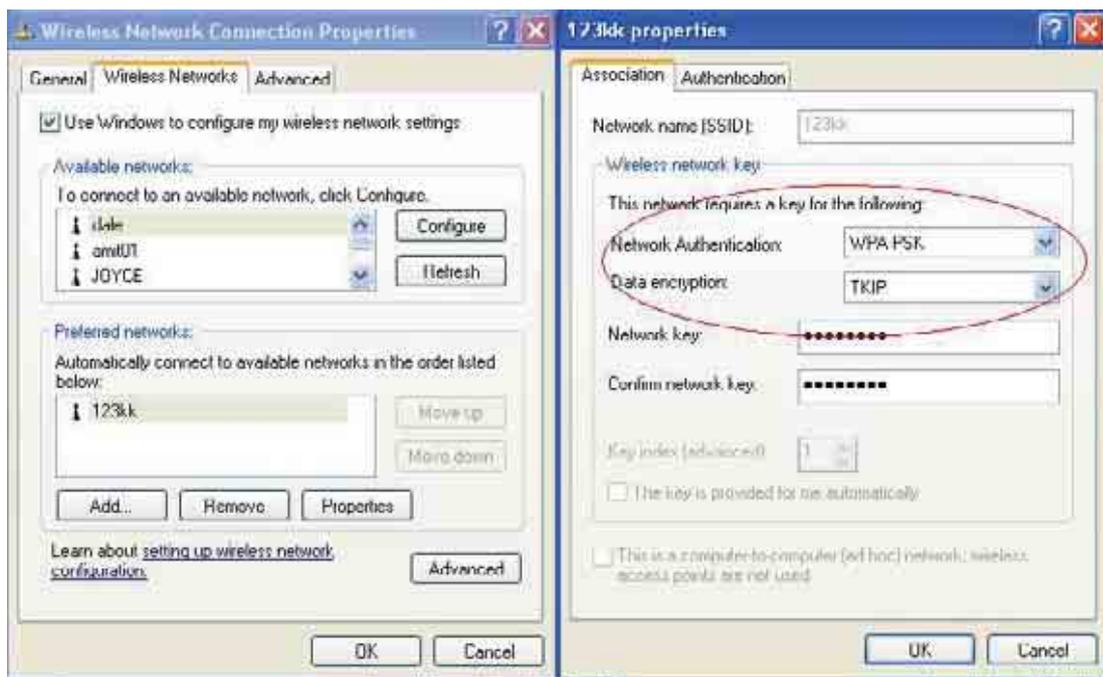
Network ID(SSID)	123kk
Channel	8
Security	WPA-PSK
Key Mode	ASCII
Preshare Key	12345678

Client:

Go to “Network Connection” and select wireless adapter.

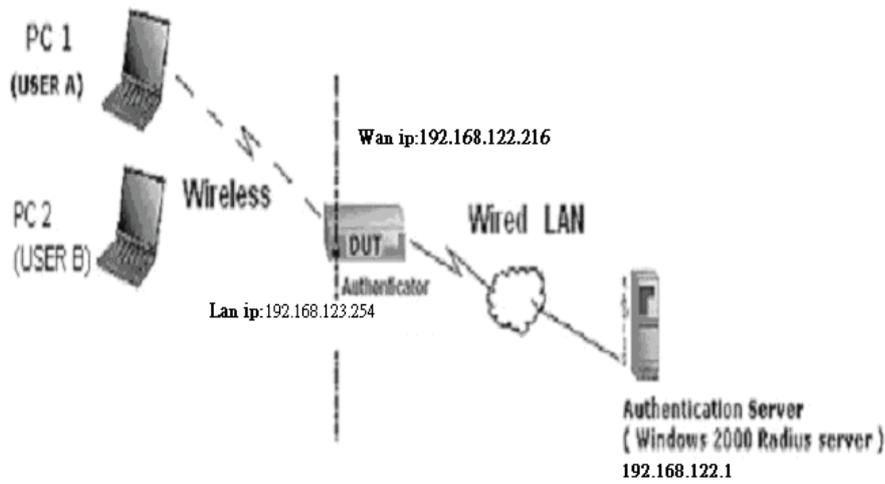
Choose “View available Wireless Networks” like below:

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

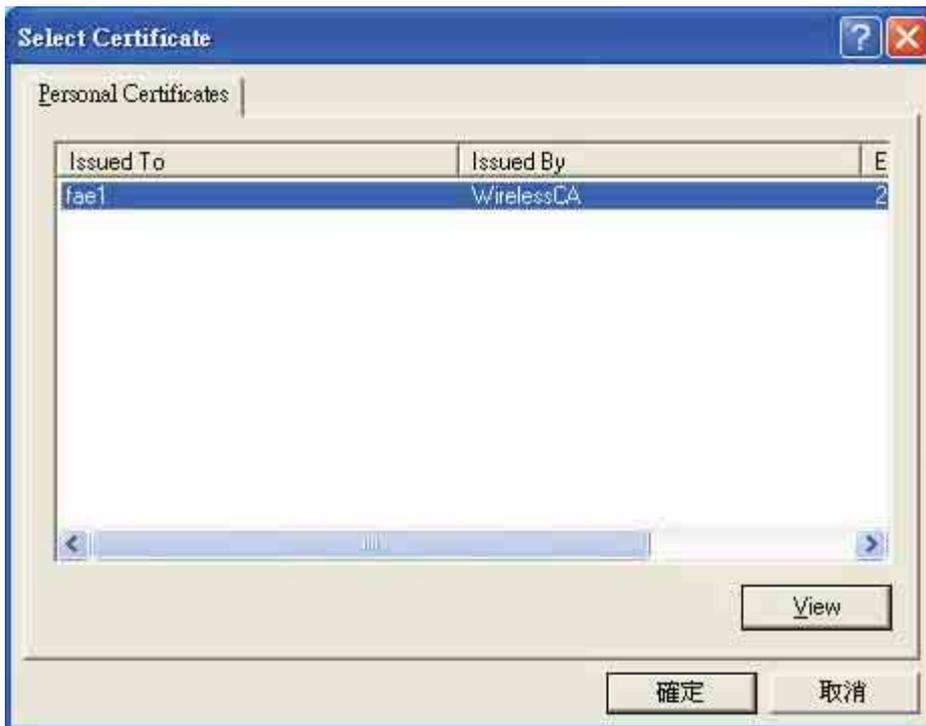
View ... Browse ...

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.



7. Go “Network” and Select “1” and ok

Network Properties

Network:

Network name (SSID): 123kk

Connect to any available network Scan ...

Description (optional):

Network type: Access point (infrastructure mode)

Channel: default channel

Association mode: WPA

Encryption method: TKIP

Authentication:

Authenticate using profile: [Profile Name]

Keys will be generated automatically for data privacy

Pre-shared key (WPA):

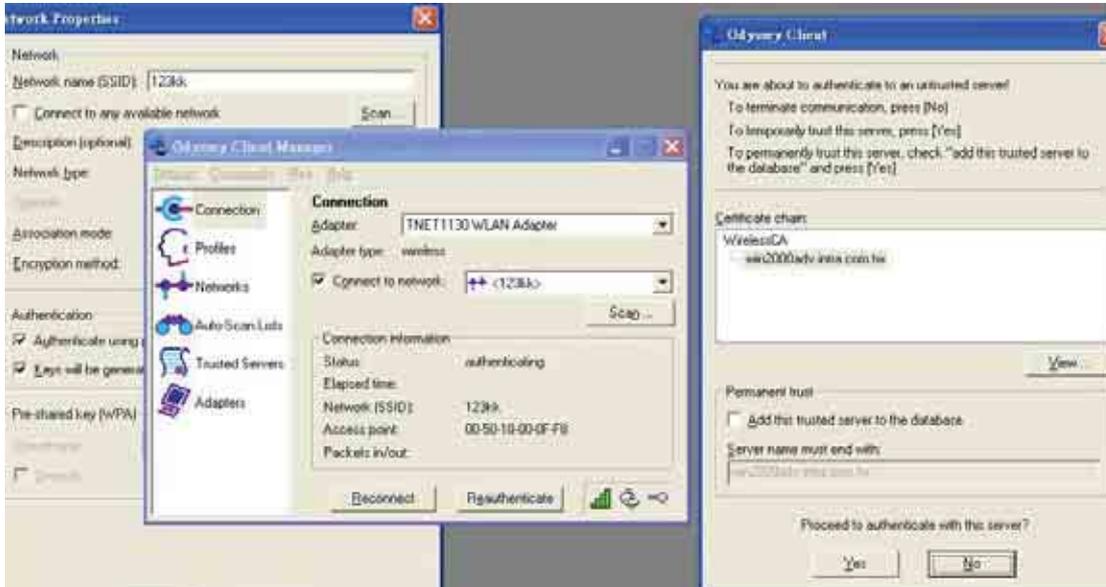
Passphrase: [Passphrase]

Unmask

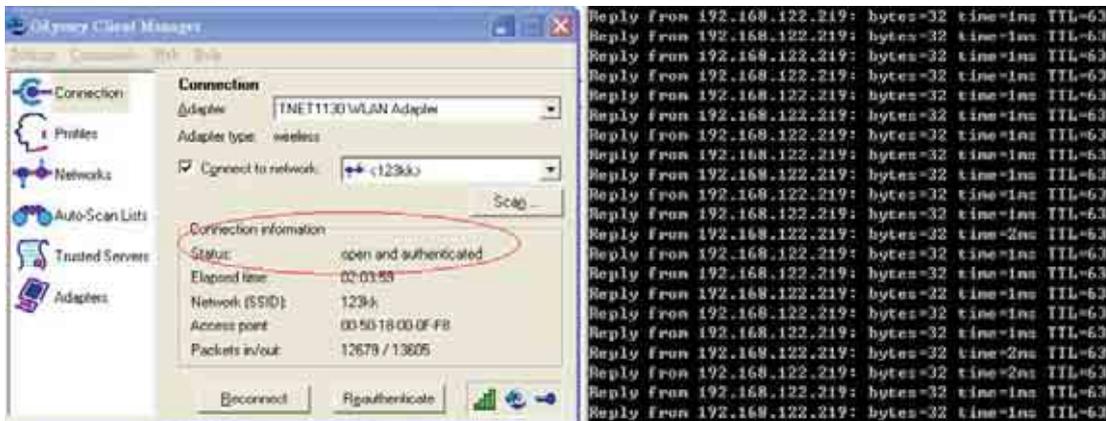
OK Cancel

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:fael

passwd:fael



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"/>

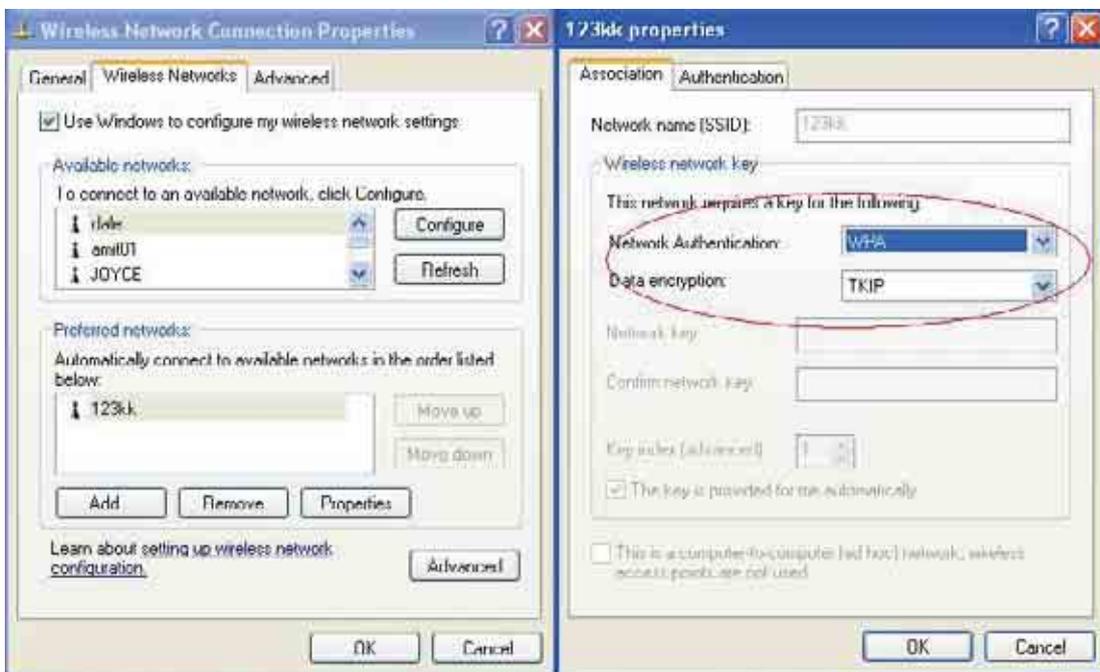
Client:

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 C 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:

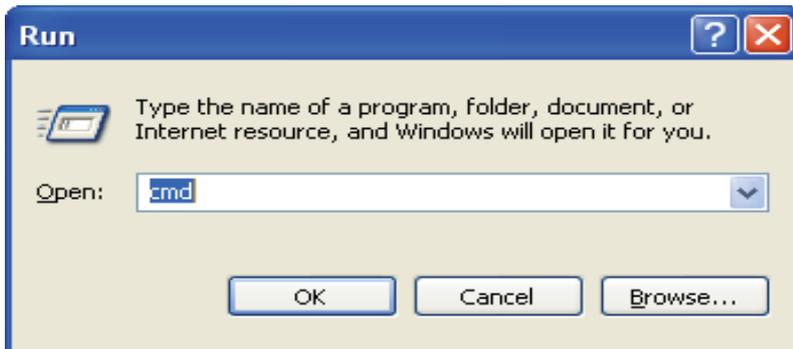
Step1:First, press the reset button and power on the router until Status blinks very ffast.

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



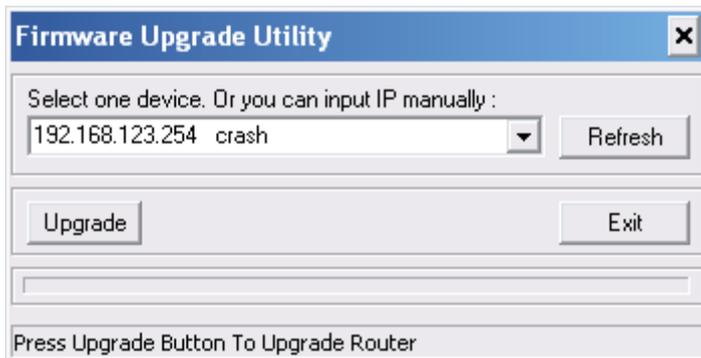
```

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)	default
Wireless Mode	<input type="radio"/> 11 b/g/n Mixed <input type="radio"/> 11n only
SSID Broadcast	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Channel	11
Security	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:

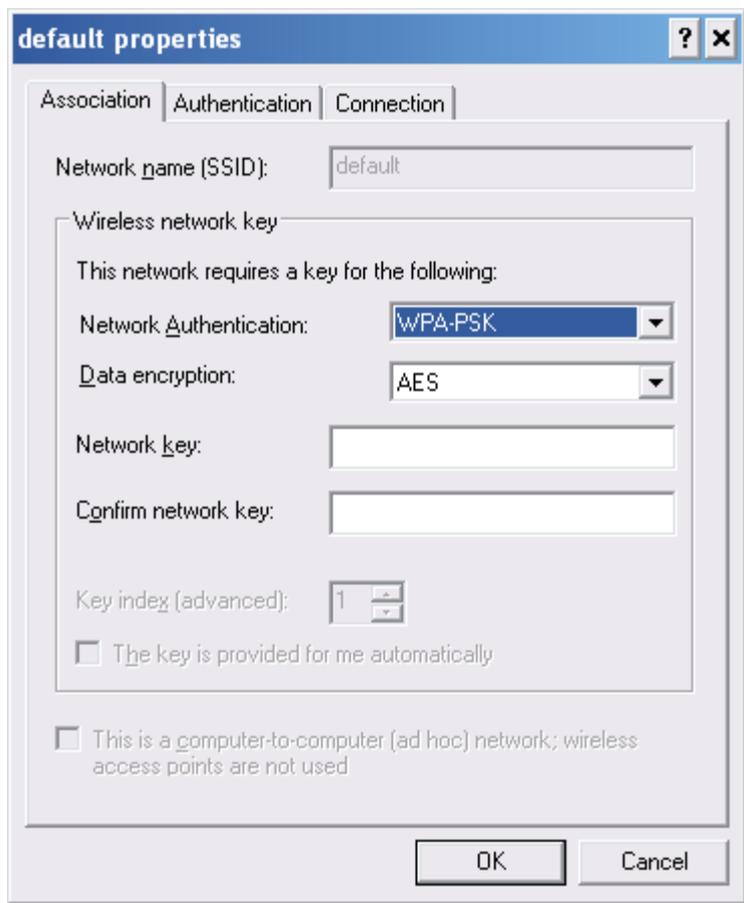
    Connection-specific DNS Suffix . : 
    IP Address . . . . . : 192.168.123.165
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.123.254
  
```

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.

FCC Caution

1. The device complies with Part 15 of the FCC rules. Operation is subject to the following two conditions:
 - (1) This device may not cause harmful interference.
 - (2) This device must accept any interference received, including interference that may cause undesired operation.

2. FCC RF Radiation Exposure Statement: The equipment complies with FCC RF radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with a minimum distance of 20 centimeters between the radiator and your body.

3. This Transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

4. Changes or modifications to this unit not expressly approved by the party responsible for compliance could void the user authority to operate the equipment.