

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

ADMINISTRATOR's MAIN MENU    ▶ Status    ▶ Wizard    ▶ Logout

BASIC SETTING   
 FORWARDING RULES   
 SECURITY SETTING   
 ADVANCED SETTING   
 TOOLBOX

- Primary Setup
- DHCP Server
- Wireless
- Change Password

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

### WPA2-PSK(AES)

1. Select Pre-share Key Mode

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

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

2. Fill in the key, Ex 12345678

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

ADMINISTRATOR's MAIN MENU    ▶ Status    ▶ Wizard    ▶ Logout

BASIC SETTING   
 FORWARDING RULES   
 SECURITY SETTING   
 ADVANCED SETTING   
 TOOLBOX

Primary Setup  
 DHCP Server  
 Wireless  
 Change Password

**Wireless Setting** [ HELP ]

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

### WPA2(AES)

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

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

Select RADIUS Shared Key

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

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

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

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

ADMINISTRATOR's MAIN MENU    ▶ Status    ▶ Wizard    ▶ Logout

BASIC SETTING   
 FORWARDING RULES   
 SECURITY SETTING   
 ADVANCED SETTING   
 TOOLBOX

**Wireless Setting** [ HELP ]

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

### WPA-PSK /WPA2-PSK

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

1. Select Pre-share Key Mode

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

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

2. Fill in the key, Ex 12345678

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

ADMINISTRATOR's MAIN MENU    ▶ Status    ▶ Wizard    ▶ Logout

BASIC SETTING    FORWARDING RULES    SECURITY SETTING    ADVANCED SETTING    TOOLBOX

Primary Setup  
DHCP Server  
Wireless  
Change Password

**Wireless Setting** [ HELP ]

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

## WPA/WPA2

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

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

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

Select RADIUS Shared Key

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

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

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

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

ADMINISTRATOR's MAIN MENU    ▶ Status    ▶ Wizard    ▶ Logout

BASIC SETTING   
 FORWARDING RULES   
 SECURITY SETTING   
 ADVANCED SETTING   
 TOOLBOX

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

**Wireless Setting** [ HELP ]

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

**WDS(Wireless Distribution System)**

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

## 4.4.4 Change Password

The screenshot displays the administrator interface for a Multi-Functional Wireless Broadband NAT Router (R1.97f2a). The top navigation bar includes 'ADMINISTRATOR's MAIN MENU', 'Status', 'Wizard', and 'Logout'. Below this, a menu bar contains 'BASIC SETTING', 'FORWARDING RULES', 'SECURITY SETTING', 'ADVANCED SETTING', and 'TOOLBOX'. The left sidebar lists navigation options: 'Primary Setup', 'DHCP Server', 'Wireless', and 'Change Password'. The main content area is titled '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 interface of a Multi-Functional Wireless Broadband NAT Router (R1.97f2a). The top navigation bar includes 'ADMINISTRATOR's MAIN MENU', 'Status', 'Wizard', and 'Logout'. Below this is a secondary menu with 'BASIC SETTING', 'FORWARDING RULES' (highlighted), 'SECURITY SETTING', 'ADVANCED SETTING', and 'TOOLBOX'. On the left side, there is a sidebar menu with 'Virtual Server', 'Special AP', and 'Miscellaneous'. The main content area is titled 'Forwarding Rules' and contains the following information:

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

## 4.5.1 Virtual Server

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

ADMINISTRATOR's MAIN MENU    ▶ Status    ▶ Wizard    ▶ Logout

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

Virtual Server    Special AP    Miscellaneous

**Virtual Server** [HELP]

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

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

Next >>    Save    Undo

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

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

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

Service Port	Server IP	Enable
21	192.168.123.1	V
80	192.168.123.2	V
1723	192.168.123.6	V



## 4.5.2 Special AP

The screenshot shows the administrator interface for a Multi-Functional Wireless Broadband NAT Router (R1.97f2a). The main menu includes 'ADMINISTRATOR's MAIN MENU', 'Status', 'Wizard', and 'Logout'. The sub-menu includes 'BASIC SETTING', 'FORWARDING RULES' (selected), 'SECURITY SETTING', 'ADVANCED SETTING', and 'TOOLBOX'. The left sidebar has 'Virtual Server', 'Special AP' (selected), and 'Miscellaneous'. The main content area is titled 'Special Applications' and includes a 'Popular applications' dropdown set to 'Battle.net', a 'Copy to' button, and an 'ID' dropdown set to '1'. Below this is a table with columns 'ID', 'Trigger', 'Incoming Ports', and 'Enable'.

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

At the bottom of the configuration area, there are 'Save' and 'Undo' buttons, and a message: 'Saved! Changes take effect immediately!'.

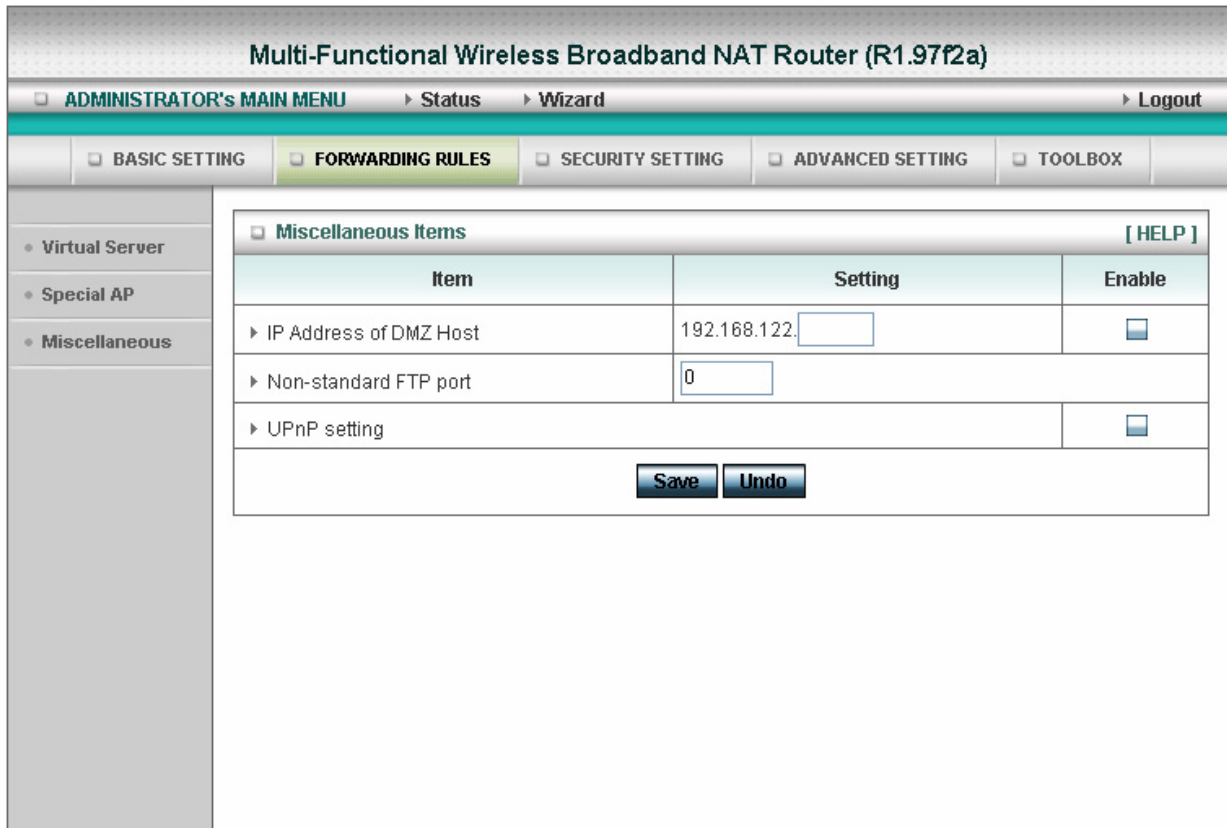
Some applications require multiple connections, like Internet games, Video conferencing, Internet telephony, etc. Because of the firewall function, these applications cannot work with a pure NAT router. The **Special Applications** feature allows some of these applications to work with this product.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

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

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

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

### 4.5.3 Miscellaneous Items



#### IP Address of DMZ Host

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

NOTE: This feature should be used only when needed.

#### Non-standard FTP port

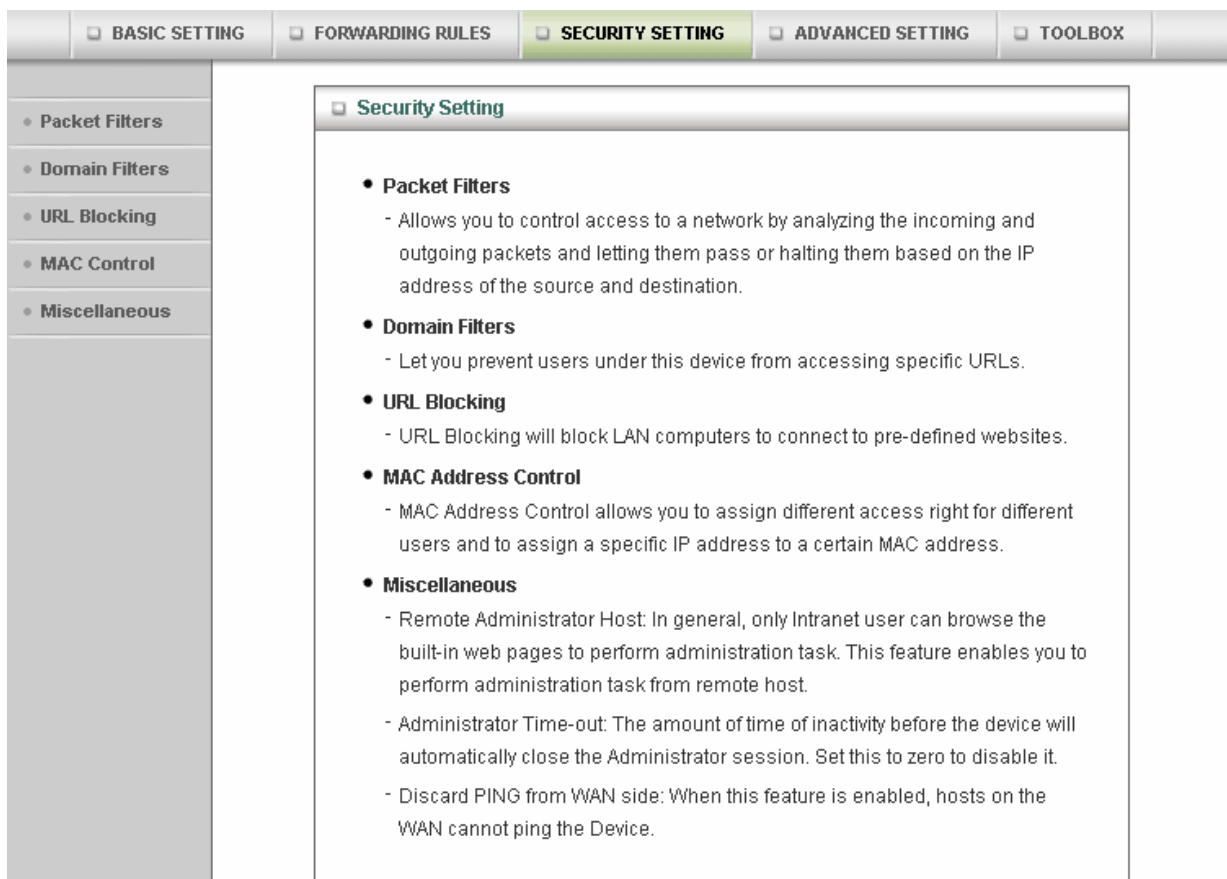
You have to configure this item if you want to access an FTP server whose port number is not 21. This setting will be lost after rebooting.

#### UpnP Setting

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



## 4.6 Security Settings



## 4.6.1 Packet Filter

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

ADMINISTRATOR's MAIN MENU    Status    Wizard    Logout

BASIC SETTING    FORWARDING RULES    SECURITY SETTING    ADVANCED SETTING    TOOLBOX

Packet Filters    Domain Filters    URL Blocking    MAC Control    Miscellaneous

Outbound Packet Filter [ HELP ]

Item	Setting			
▶ Outbound Filter	<input type="checkbox"/> Enable			
<input type="radio"/> Allow all to pass except those match the following rules. <input checked="" type="radio"/> Deny all to pass except those match the following rules.				
Schedule rule: (00)Always ▼ <span style="background-color: #d0e0d0;">Copy to</span> ID -- ▼				
ID	Source IP : Ports	Destination IP : Ports	Enable	Schedule Rule#
1	192.168.122.13 : <input type="text"/>	<input type="text"/> : <input type="text"/>	<input type="checkbox"/>	0 <input type="text"/>
2	192.168.122.18 : <input type="text"/>	<input type="text"/> : <input type="text"/>	<input type="checkbox"/>	0 <input type="text"/>
3	192.168.122.226 : <input type="text"/>	<input type="text"/> : <input type="text"/>	<input type="checkbox"/>	0 <input type="text"/>
4	192.168.122.218 : <input type="text"/>	<input type="text"/> : <input type="text"/>	<input type="checkbox"/>	0 <input type="text"/>
5	192.168.122.229 : <input type="text"/>	<input type="text"/> : <input type="text"/>	<input type="checkbox"/>	0 <input type="text"/>
6	<input type="text"/> : <input type="text"/>	<input type="text"/> : <input type="text"/>	<input type="checkbox"/>	0 <input type="text"/>
7	<input type="text"/> : <input type="text"/>	<input type="text"/> : <input type="text"/>	<input type="checkbox"/>	0 <input type="text"/>
8	<input type="text"/> : <input type="text"/>	<input type="text"/> : <input type="text"/>	<input type="checkbox"/>	0 <input type="text"/>

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

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

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

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

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

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

Each rule can be enabled or disabled individually.

Inbound Filter:

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

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

**Example 1:**

The screenshot displays the 'SECURITY SETTING' tab in a network configuration tool. The 'Outbound Packet Filter' section is active, showing a table of rules. The 'Enable' checkbox is checked. Below the table, there are radio buttons for 'Allow all to pass except those match the following rules.' and 'Deny all to pass except those match the following rules.', with the latter selected. A 'Schedule rule' dropdown is set to '(00)Always'. At the bottom, there are buttons for 'Save', 'Undo', 'Inbound Filter...', and 'MAC Level...'.

ID	Source IP : Ports	Destination IP : Ports	Enable	Schedule Rule#
1	1.2.3.100-1.2.3.149 : [ ]	[ ] : 25-100	<input checked="" type="checkbox"/>	0
2	1.2.3.10-1.2.3.20 : [ ]	[ ] : [ ]	<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
7	[ ] : [ ]	[ ] : [ ]	<input type="checkbox"/>	0
8	[ ] : [ ]	[ ] : [ ]	<input type="checkbox"/>	0

(1.2.3.100-1.2.3.149) They are allow to send mail (port 25), receive mail (port 110), and browse the Internet (port 80)

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

Others are all blocked.

**Example 2:**

ADMINISTRATOR's MAIN MENU   Status   Wizard   Logout

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

Packet Filters  
Domain Filters  
URL Blocking  
MAC Control  
Miscellaneous

**Outbound Packet Filter** [ HELP ]

Item	Setting			
▶ Outbound Filter	<input checked="" type="checkbox"/> Enable			
<input type="radio"/> Allow all to pass except those match the following rules. <input checked="" type="radio"/> Deny all to pass except those match the following rules.				
Schedule rule (00)Always <input type="button" value="Copy to"/> ID -- <input type="button" value="ID"/>				
ID	Source IP : Ports	Destination IP : Ports	Enable	Schedule Rule#
1	1.2.3.100-1.2.3.199 : <input type="text"/>	<input type="text"/> : 21	<input checked="" type="checkbox"/>	<input type="text" value="0"/>
2	1.2.3.100-1.2.3.199 : <input type="text"/>	<input type="text"/> : 119	<input checked="" type="checkbox"/>	<input type="text" value="0"/>
3	<input type="text"/> : <input type="text"/>	<input type="text"/> : <input type="text"/>	<input type="checkbox"/>	<input type="text" value="0"/>
4	<input type="text"/> : <input type="text"/>	<input type="text"/> : <input type="text"/>	<input type="checkbox"/>	<input type="text" value="0"/>
5	<input type="text"/> : <input type="text"/>	<input type="text"/> : <input type="text"/>	<input type="checkbox"/>	<input type="text" value="0"/>
6	<input type="text"/> : <input type="text"/>	<input type="text"/> : <input type="text"/>	<input type="checkbox"/>	<input type="text" value="0"/>
7	<input type="text"/> : <input type="text"/>	<input type="text"/> : <input type="text"/>	<input type="checkbox"/>	<input type="text" value="0"/>
8	<input type="text"/> : <input type="text"/>	<input type="text"/> : <input type="text"/>	<input type="checkbox"/>	<input type="text" value="0"/>

(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:**

<input type="checkbox"/> BASIC SETTING <input type="checkbox"/> FORWARDING RULES <input checked="" type="checkbox"/> SECURITY SETTING <input type="checkbox"/> ADVANCED SETTING <input type="checkbox"/> TOOLBOX																																																						
<ul style="list-style-type: none"> <li>• Packet Filters</li> <li>• Domain Filters</li> <li>• URL Blocking</li> <li>• MAC Control</li> <li>• Miscellaneous</li> </ul>	<div style="border: 1px solid gray; padding: 5px;"> <div style="border-bottom: 1px solid gray; padding-bottom: 5px;"> <span style="float: left;">Inbound Packet Filter</span> <span style="float: right;">[ HELP ]</span> </div> <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="width: 40%;">Item</th> <th style="width: 60%;">Setting</th> </tr> </thead> <tbody> <tr> <td>▶ Inbound Filter</td> <td><input checked="" type="checkbox"/> Enable</td> </tr> <tr> <td colspan="2"> <input checked="" type="radio"/> Allow all to pass except those match the following rules.  <input type="radio"/> Deny all to pass except those match the following rules.           </td> </tr> <tr> <td colspan="2" style="text-align: center;">             Schedule rule (00)Always <input type="button" value="Copy to ID"/> -- <input type="button" value="ID"/> </td> </tr> <tr> <th>ID</th> <th>Source IP : Ports</th> <th>Destination IP : Ports</th> <th>Enable</th> <th>Schedule Rule#</th> </tr> <tr> <td>1</td> <td>192.168.123.149 : <input type="text"/></td> <td><input type="text"/> : 25-100</td> <td><input checked="" type="checkbox"/></td> <td><input type="text" value="0"/></td> </tr> <tr> <td>2</td> <td>192.168.123.20 : <input type="text"/></td> <td><input type="text"/> : <input type="text"/></td> <td><input checked="" type="checkbox"/></td> <td><input type="text" value="0"/></td> </tr> <tr> <td>3</td> <td><input type="text"/> : <input type="text"/></td> <td><input type="text"/> : <input type="text"/></td> <td><input type="checkbox"/></td> <td><input type="text" value="0"/></td> </tr> <tr> <td>4</td> <td><input type="text"/> : <input type="text"/></td> <td><input type="text"/> : <input type="text"/></td> <td><input type="checkbox"/></td> <td><input type="text" value="0"/></td> </tr> <tr> <td>5</td> <td><input type="text"/> : <input type="text"/></td> <td><input type="text"/> : <input type="text"/></td> <td><input type="checkbox"/></td> <td><input type="text" value="0"/></td> </tr> <tr> <td>6</td> <td><input type="text"/> : <input type="text"/></td> <td><input type="text"/> : <input type="text"/></td> <td><input type="checkbox"/></td> <td><input type="text" value="0"/></td> </tr> <tr> <td>7</td> <td><input type="text"/> : <input type="text"/></td> <td><input type="text"/> : <input type="text"/></td> <td><input type="checkbox"/></td> <td><input type="text" value="0"/></td> </tr> <tr> <td>8</td> <td><input type="text"/> : <input type="text"/></td> <td><input type="text"/> : <input type="text"/></td> <td><input type="checkbox"/></td> <td><input type="text" value="0"/></td> </tr> </tbody> </table> <div style="text-align: center; margin-top: 5px;"> <input type="button" value="Save"/> <input type="button" value="Undo"/> <input type="button" value="Outbound Filter..."/> <input type="button" value="MAC Level..."/> </div> </div>	Item	Setting	▶ Inbound Filter	<input checked="" type="checkbox"/> Enable	<input checked="" type="radio"/> Allow all to pass except those match the following rules. <input type="radio"/> Deny all to pass except those match the following rules.		Schedule rule (00)Always <input type="button" value="Copy to ID"/> -- <input type="button" value="ID"/>		ID	Source IP : Ports	Destination IP : Ports	Enable	Schedule Rule#	1	192.168.123.149 : <input type="text"/>	<input type="text"/> : 25-100	<input checked="" type="checkbox"/>	<input type="text" value="0"/>	2	192.168.123.20 : <input type="text"/>	<input type="text"/> : <input type="text"/>	<input checked="" type="checkbox"/>	<input type="text" value="0"/>	3	<input type="text"/> : <input type="text"/>	<input type="text"/> : <input type="text"/>	<input type="checkbox"/>	<input type="text" value="0"/>	4	<input type="text"/> : <input type="text"/>	<input type="text"/> : <input type="text"/>	<input type="checkbox"/>	<input type="text" value="0"/>	5	<input type="text"/> : <input type="text"/>	<input type="text"/> : <input type="text"/>	<input type="checkbox"/>	<input type="text" value="0"/>	6	<input type="text"/> : <input type="text"/>	<input type="text"/> : <input type="text"/>	<input type="checkbox"/>	<input type="text" value="0"/>	7	<input type="text"/> : <input type="text"/>	<input type="text"/> : <input type="text"/>	<input type="checkbox"/>	<input type="text" value="0"/>	8	<input type="text"/> : <input type="text"/>	<input type="text"/> : <input type="text"/>	<input type="checkbox"/>	<input type="text" value="0"/>
Item	Setting																																																					
▶ Inbound Filter	<input checked="" type="checkbox"/> Enable																																																					
<input checked="" type="radio"/> Allow all to pass except those match the following rules. <input type="radio"/> Deny all to pass except those match the following rules.																																																						
Schedule rule (00)Always <input type="button" value="Copy to ID"/> -- <input type="button" value="ID"/>																																																						
ID	Source IP : Ports	Destination IP : Ports	Enable	Schedule Rule#																																																		
1	192.168.123.149 : <input type="text"/>	<input type="text"/> : 25-100	<input checked="" type="checkbox"/>	<input type="text" value="0"/>																																																		
2	192.168.123.20 : <input type="text"/>	<input type="text"/> : <input type="text"/>	<input checked="" type="checkbox"/>	<input type="text" value="0"/>																																																		
3	<input type="text"/> : <input type="text"/>	<input type="text"/> : <input type="text"/>	<input type="checkbox"/>	<input type="text" value="0"/>																																																		
4	<input type="text"/> : <input type="text"/>	<input type="text"/> : <input type="text"/>	<input type="checkbox"/>	<input type="text" value="0"/>																																																		
5	<input type="text"/> : <input type="text"/>	<input type="text"/> : <input type="text"/>	<input type="checkbox"/>	<input type="text" value="0"/>																																																		
6	<input type="text"/> : <input type="text"/>	<input type="text"/> : <input type="text"/>	<input type="checkbox"/>	<input type="text" value="0"/>																																																		
7	<input type="text"/> : <input type="text"/>	<input type="text"/> : <input type="text"/>	<input type="checkbox"/>	<input type="text" value="0"/>																																																		
8	<input type="text"/> : <input type="text"/>	<input type="text"/> : <input type="text"/>	<input type="checkbox"/>	<input type="text" value="0"/>																																																		

(192.168.123.100-192.168.123.149) They are allowed to send mail (port 25), receive mail (port 110), and browse Internet (port 80); port 53 (DNS) is necessary to resolve the domain name.

(192.168.123.10-192.168.123.20) They can do everything (block nothing)

Others are all blocked.

**Example 2:**

BASIC SETTING  
  FORWARDING RULES  
  SECURITY SETTING  
  ADVANCED SETTING  
  TOOLBOX

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.				
Schedule rule (00)Always <input type="button" value="Copy to ID"/> -- <input type="button" value=""/>				
ID	Source IP : Ports	Destination IP : Ports	Enable	Schedule Rule#
1	192.168.123.100 : <input type="text"/>	<input type="text"/> : 21	<input checked="" type="checkbox"/>	<input type="text" value="0"/>
2	192.168.123.119 : <input type="text"/>	<input type="text"/> : 119	<input checked="" type="checkbox"/>	<input type="text" value="0"/>
3	<input type="text"/> : <input type="text"/>	<input type="text"/> : <input type="text"/>	<input type="checkbox"/>	<input type="text" value="0"/>
4	<input type="text"/> : <input type="text"/>	<input type="text"/> : <input type="text"/>	<input type="checkbox"/>	<input type="text" value="0"/>
5	<input type="text"/> : <input type="text"/>	<input type="text"/> : <input type="text"/>	<input type="checkbox"/>	<input type="text" value="0"/>
6	<input type="text"/> : <input type="text"/>	<input type="text"/> : <input type="text"/>	<input type="checkbox"/>	<input type="text" value="0"/>
7	<input type="text"/> : <input type="text"/>	<input type="text"/> : <input type="text"/>	<input type="checkbox"/>	<input type="text" value="0"/>
8	<input type="text"/> : <input type="text"/>	<input type="text"/> : <input type="text"/>	<input type="checkbox"/>	<input type="text" value="0"/>

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

Others are allowed

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



## 4.6.2 Domain Filter

ADMINISTRATOR's MAIN MENU   Status   Wizard   Logout

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

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

**Domain Filter** [ HELP ]

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

ID	Domain Suffix	Action	Enable
1	<input type="text" value="www.msn.com"/>	<input type="checkbox"/> Drop <input type="checkbox"/> Log	<input type="checkbox"/>
2	<input type="text"/>	<input type="checkbox"/> Drop <input type="checkbox"/> Log	<input type="checkbox"/>
3	<input type="text"/>	<input type="checkbox"/> Drop <input type="checkbox"/> Log	<input type="checkbox"/>
4	<input type="text"/>	<input type="checkbox"/> Drop <input type="checkbox"/> Log	<input type="checkbox"/>
5	<input type="text"/>	<input type="checkbox"/> Drop <input type="checkbox"/> Log	<input type="checkbox"/>
6	<input type="text"/>	<input type="checkbox"/> Drop <input type="checkbox"/> Log	<input type="checkbox"/>
7	<input type="text"/>	<input type="checkbox"/> Drop <input type="checkbox"/> Log	<input type="checkbox"/>
8	<input type="text"/>	<input type="checkbox"/> Drop <input type="checkbox"/> Log	<input type="checkbox"/>
9	<input type="text"/>	<input type="checkbox"/> Drop <input type="checkbox"/> Log	<input type="checkbox"/>

### Domain Filter

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

#### Domain Filter Enable

Check if you want to enable Domain Filter.

#### Log DNS Query

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

#### Privilege IP Addresses Range

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

#### Domain Suffix

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

#### Action

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

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

#### Enable

Check to enable each rule.

**Example:**

BASIC SETTING  
  FORWARDING RULES  
  SECURITY SETTING  
  ADVANCED SETTING  
  TOOLBOX

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

**Domain Filter** [ HELP ]

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

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

In this example:

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

## 4.6.3 URL Blocking

The screenshot shows the 'URL Blocking' configuration page. At the top, there is a navigation bar with 'ADMINISTRATOR's MAIN MENU', 'Status', 'Wizard', and 'Logout'. Below this is a sub-menu with 'BASIC SETTING', 'FORWARDING RULES', 'SECURITY SETTING' (highlighted), 'ADVANCED SETTING', and 'TOOLBOX'. The left sidebar lists 'Packet Filters', 'Domain Filters', 'URL Blocking', 'MAC Control', and 'Miscellaneous'. The main content area is titled 'URL Blocking' and includes a '[ HELP ]' link. It features a table with the following structure:

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

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

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

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

### **URL Blocking Enable**

Checked if you want to enable URL Blocking.

### **URL**

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

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

### **Enable**

Checked to enable each rule.

ADMINISTRATOR'S MAIN MENU    > Status    > Wizard    > Logout

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

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

**URL Blocking** [ HELP ]

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

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

ADMINISTRATOR's MAIN MENU    Status    Wizard    Logout

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

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

**MAC Address Control** [HELP]

Item	Setting
MAC Address Control	<input checked="" type="checkbox"/> Enable
<input checked="" type="checkbox"/> Connection control	Wireless and wired clients with <b>C</b> checked can connect to this device; and <input type="text" value="deny"/> unspecified MAC addresses to connect.
<input type="checkbox"/> Association control	Wireless clients with <b>A</b> checked can associate to the wireless LAN; and <input type="text" value="deny"/> unspecified MAC addresses to associate.

DHCP clients --- Select one --- Copy to ID --

ID	MAC Address	IP Address	C	A
1	<input type="text" value="00-90-CC-1D-9D-40"/>	192.168.122. <input type="text" value="13"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
2	<input type="text" value="00-50-BA-24-05-E7"/>	192.168.122. <input type="text" value="18"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
3	<input type="text" value="00-90-CC-15-79-DC"/>	192.168.122. <input type="text" value="218"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
4	<input type="text" value="00-50-18-FF-12-34"/>	192.168.122. <input type="text" value="226"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

<< Previous    Next >>    Save    Undo

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

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

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

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

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

**Control table**

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

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

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

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



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

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

**Example:**

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

ADMINISTRATOR's MAIN MENU   Status   Wizard   Logout

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

Packet Filters  
Domain Filters  
URL Blocking  
MAC Control  
Miscellaneous

**MAC Address Control** [ HELP ]

Item	Setting
MAC Address Control	<input checked="" type="checkbox"/> Enable
<input checked="" type="checkbox"/> Connection control	Wireless and wired clients with <b>C</b> checked can connect to this device; and <input type="text" value="allow"/> unspecified MAC addresses to connect.
<input checked="" type="checkbox"/> Association control	Wireless clients with <b>A</b> checked can associate to the wireless LAN; and <input type="text" value="deny"/> unspecified MAC addresses to associate.

DHCP clients   ID

ID	MAC Address	IP Address	C	A
9	<input type="text" value="00-12-34-56-78-90"/>	192.168.122. <input type="text" value="100"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
10	<input type="text" value="00-12-34-56-78-92"/>	192.168.122. <input type="text"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
11	<input type="text" value="00-09-76-54-32-10"/>	192.168.122. <input type="text" value="101"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
12	<input type="text"/>	192.168.122. <input type="text"/>	<input type="checkbox"/>	<input type="checkbox"/>

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

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

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

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

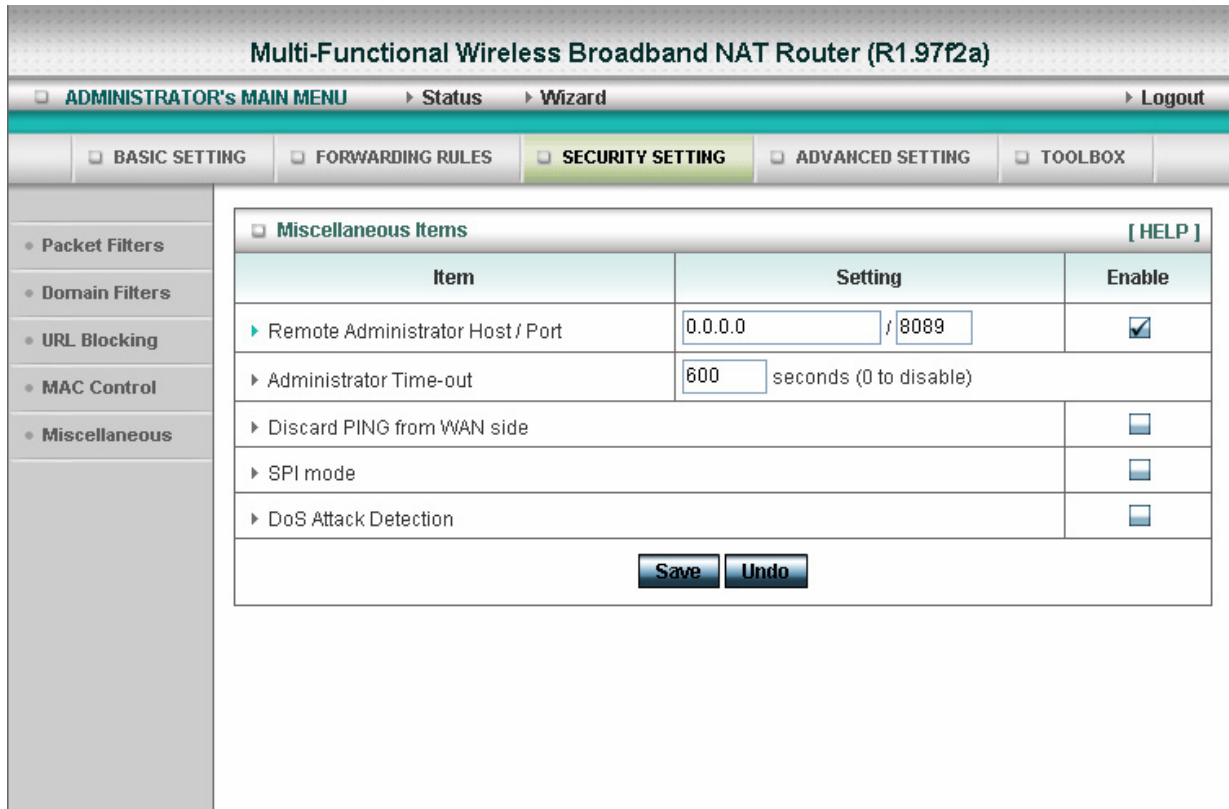
Client 2 will obtain its IP address from the IP Address pool specified in the "DHCP Server" page or can use a manually assigned static IP address.

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

5. Clients 2 and 3 and other wired clients with a MAC address unspecified in the Control table are all allowed to connect to this device. But client 1 is denied to connect to this device.

6. Clients 1 and 2 are allowed to associate to the wireless LAN, but a wireless client with a MAC address not specified in the Control table is denied to associate to the wireless LAN. Client 3 is a wired client and so is not affected by Association control.

#### 4.6.5 Miscellaneous Items



##### Remote Administrator Host/Port

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

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

##### Administrator Time-out

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

##### Discard PING from WAN side

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

##### SPI Mode

When this feature is enabled, the router will record the packet information pass through the router like



IP address, port address, ACK, SEQ number and so on. And the router will check every incoming packet to detect if this packet is valid.

### DoS Attack Detection

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

## 4.7 Advanced Settings

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

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