

User Manual

CDE530AM-002
WiFi Broadband Router

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 | 4 |
| 1.1 Packing List | 4 |
| 1.2 Spec Summary Table | 5 |
| 1.3 Hardware Configuration..... | 7 |
| 1.4 LED indicators | 8 |
| 1.5 Button Definition..... | 8 |
| 1.6 Procedure for Hardware Installation | 9 |
| Chapter 2 Getting Start..... | 11 |
| Chapter 3 Making Configuration | 17 |
| 3.1 Login to Configure from Wizard..... | 18 |
| 3.2 System Status | 22 |
| 3.3 Advanced | 22 |
| 3.3.1 Basic Setting | 22 |
| 3.3.2 Forwarding Rules | 37 |
| 3.3.3 Security Settings..... | 41 |
| 3.3.4 Advanced Settings | 55 |
| 3.3.5 Toolbox..... | 65 |
| Appendix A FAQ and Troubleshooting | 68 |
| What can I do when I have some trouble at the first time? | 68 |
| How do I connect router by using wireless? | 70 |

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.

1.1 Packing List

| items | Description | Contents | Quantity |
|-------|-----------------------|--|----------|
| 1 | WiFi Broadband Router |  | 1 |
| 3 | Power adapter 5V 1A |  | 1 |
| 4 | CD |  | 1 |

- Wireless broadband router unit
- Installation CD-ROM
- Power adapter

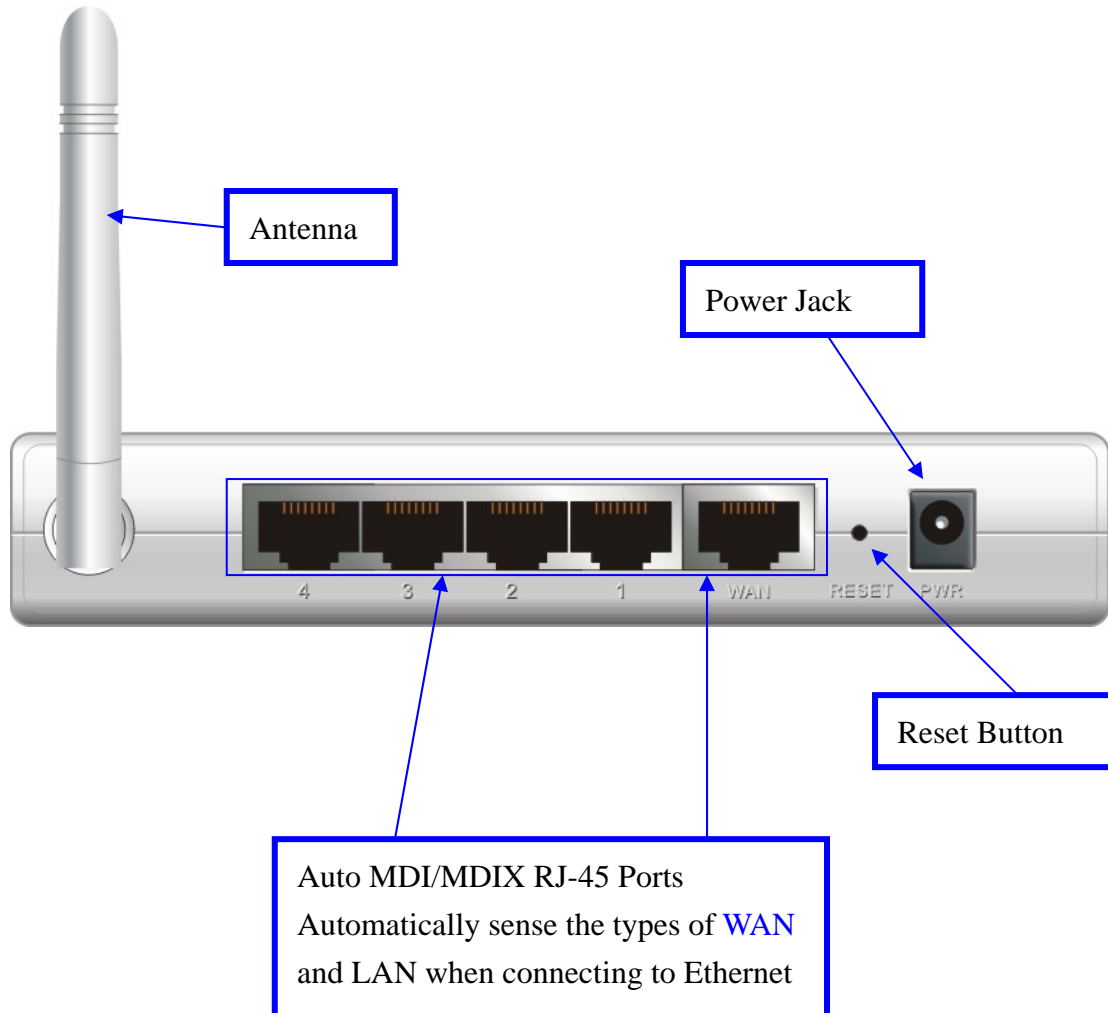
1.2 Spec Summary Table

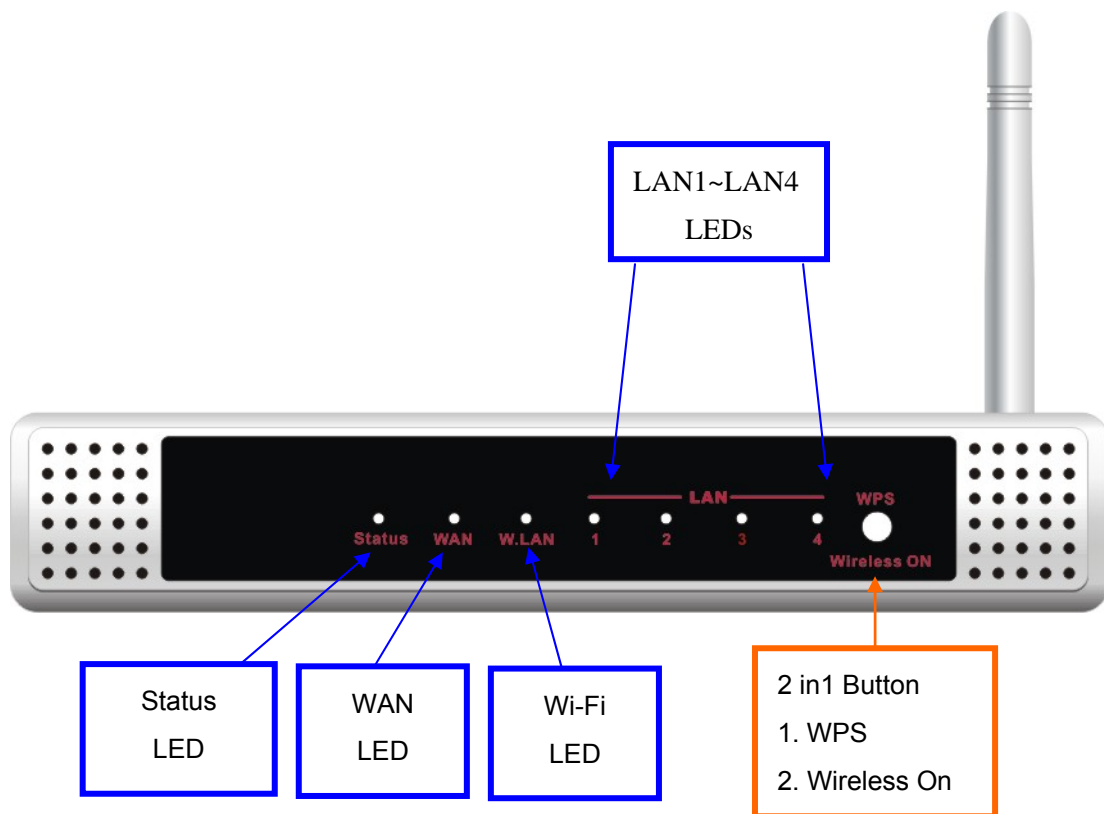
| Device Interface | | CDE530AM-002 |
|------------------------|--|--------------|
| Ethernet WAN | RJ-45 port, 10/100Mbps, auto-MDI/MDIX | 1 |
| Ethernet LAN | RJ-45 port, 10/100Mbps, auto-MDI/MDIX | 4 |
| Antenna | 2 dBi fixed antenna | 1 |
| WPS Button/Wireless On | For WPS connection and Enable “Wireless Function” | 1 |
| Reset Button | Reset to Factory Default setting | 1 |
| LED Indication | Status / WAN / LAN1 ~ LAN4/ WiFi | ● |
| Power Jack | DC Power Jack, powered via external DC 5V/1A switching power adapter | 1 |
| Wireless LAN (WiFi) | | |
| Standard | IEEE 802.11b/g/n-lite compliance | ● |
| SSID | SSID broadcast or in stealth mode | ● |
| Channel | Auto-selection, manually | ● |
| Security | WEP, WPA, WPA-PSK, WPA2, WPA2-PSK | ● |
| WPS | WPS (Wi-Fi Protected Setup) | ● |
| WMM | WMM (Wi-Fi Multimedia) | ● |
| Functionality | | |
| Ethernet WAN | PPPoE, DHCP client, Static IP | ● |
| WAN Connection | Auto-reconnect, dial-on-demand, manually | ● |
| One-to-Many NAT | Virtual server, special application, DMZ, Super DMZ(IP pass-through) | ● |
| NAT Session | Support NAT session | 10000 |
| SPI Firewall | IP/Service filter, URL blocking. | ● |
| DoS Protection | DoS (Deny of Service) detection and protection | ● |
| Routing Protocol | Static route, dynamic route (RIP v1/v2) | ● |
| Management | SNMP, UPnP IGD, syslog, DDNS | ● |
| Administration | Web-based UI, remote login, | ● |

| | | |
|--|--|------------|
| | backup/restore setting | |
| Performance | NAT up to 90Mbps and Wireless up to 70Mbps | |
| Environment & Certification | | |
| Package Information | CDE530AM-002, DC 5V/1A power adapter, Quick Installation Guide | |
| Package Information | Device dimension (mm) | |
| | Package dimension (246x210x62mm) SP/MP/ZP | 156x110x22 |
| | Package dimension (214x146x69mm) PP | ● |
| | Package dimension (290x234x100mm) AP | ○ |
| Operation Temp | Temp.: 0~40°C, Humidity 10%~90% non-condensing | ● |
| Storage Temp | Temp.: -10~70°C, Humidity: 0~95% non-condensing | ● |
| EMI Certification | CE/FCC compliance | ● |
| RoHS | RoHS compliance | ● |

***Specifications are subject to change without prior notice.**

1.3 Hardware Configuration





1.4 LED indicators

| | LED status | Description |
|----------|---------------------|---------------------------|
| Status | Green in flash | Device status is working. |
| WAN LED | Green | RJ45 cable is plugged |
| | Green in flash | Data access |
| LAN LED | Green | RJ45 cable is plugged |
| | Green in flash | Data access |
| WiFi LED | Green | WLAN is on |
| | Green in flash | Data access |
| | Green in fast flash | Device is in WPS PBC mode |
| | Green in dark | Wi-Fi Radio is disabled |

1.5 Button Definition

| | Description |
|---------------------------|--|
| Enable "Wireless" and WPS | 1. When Wireless is off, press this button (about 1 sec) to enable "Wireless Radio". 2. When Wireless is On, press this button (about 1 sec) to execute WPS function. |
| Reset | Press (6) sec to reset to default when the device works simultaneously. |

1.6 Procedure for Hardware Installation

Step 1 Insert the Ethernet cable into LAN

Port:

Insert the Ethernet patch cable into LAN port on the back panel of Router, and an available Ethernet port on the network adapter in the computer you will use to configure the unit.



Step 2 Insert the Ethernet patch cable into Wired WAN port:

Insert the Ethernet patch cable from DSL Modem into Wired WAN port on the back panel of Router.



Step 3 Power on Router:

Connect the power adapter to the receptor on the back panel of your Router.



Step 5. Complete the setup.

When complete, the Status LED will flash.



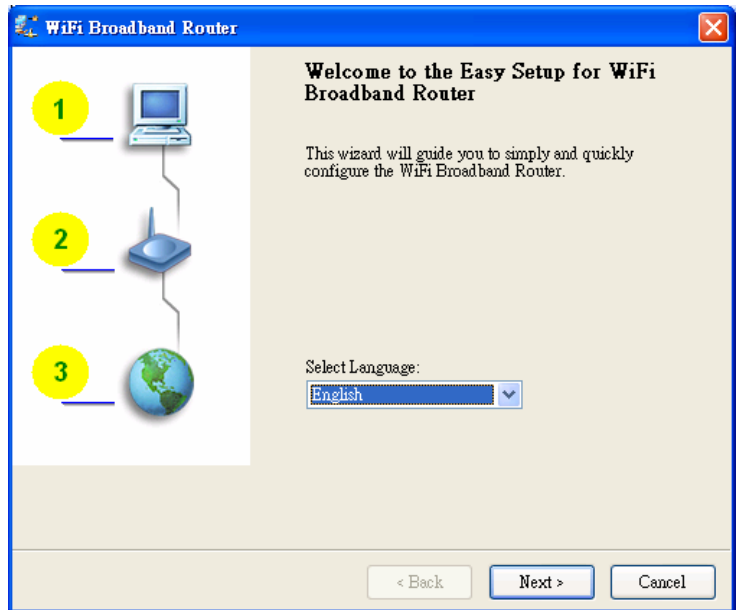
Chapter 2 Getting Start

Insert the CD into CD reader on your PC. The program, AutoRun, will be executed automatically.

And then you can click the Easy setup Icon for this utility.

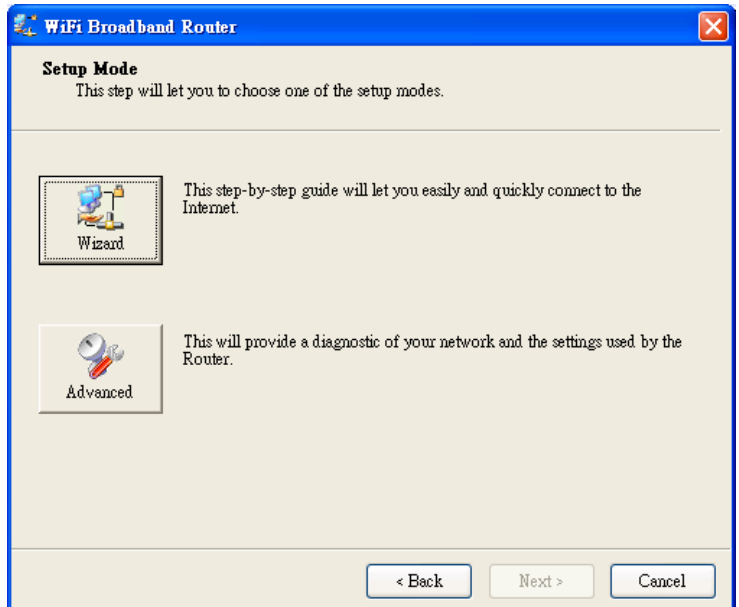
Configure the settings by the following steps.

2.1. Select Language then click “Next” for continues.



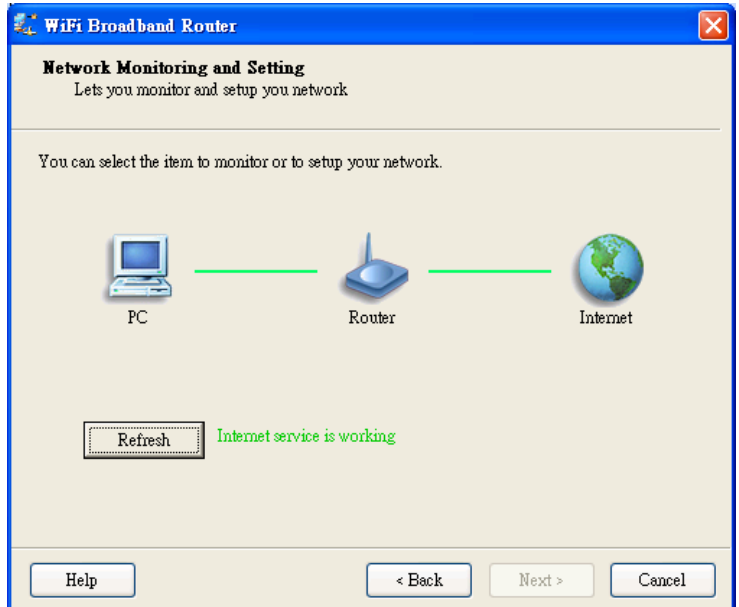
2.2 Setup mode

You can select Wizard mode to run the setup step-by-step or run advanced mode to diagnose the network settings of the router.



2.3 Advanced mode Setup.

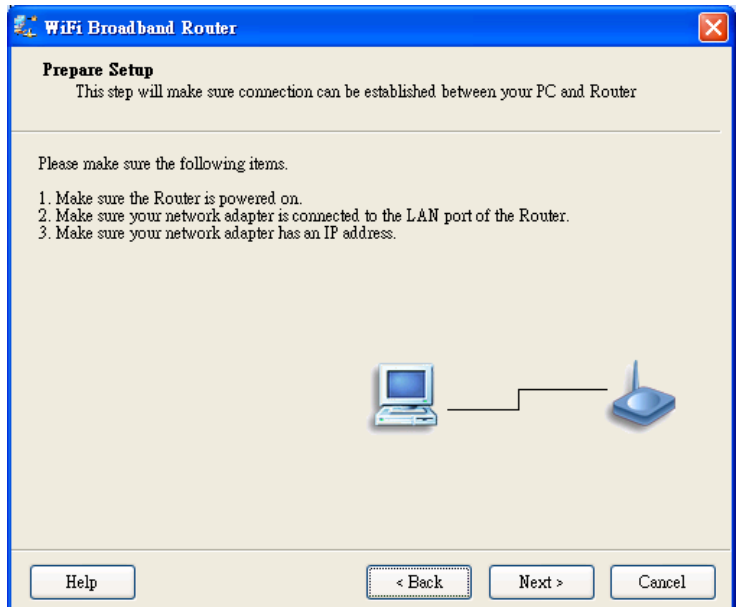
Check the PC, Router or Internet icons for the Status of PC, Router or Internet.



2.4 Quick Wizard Install mode Setup

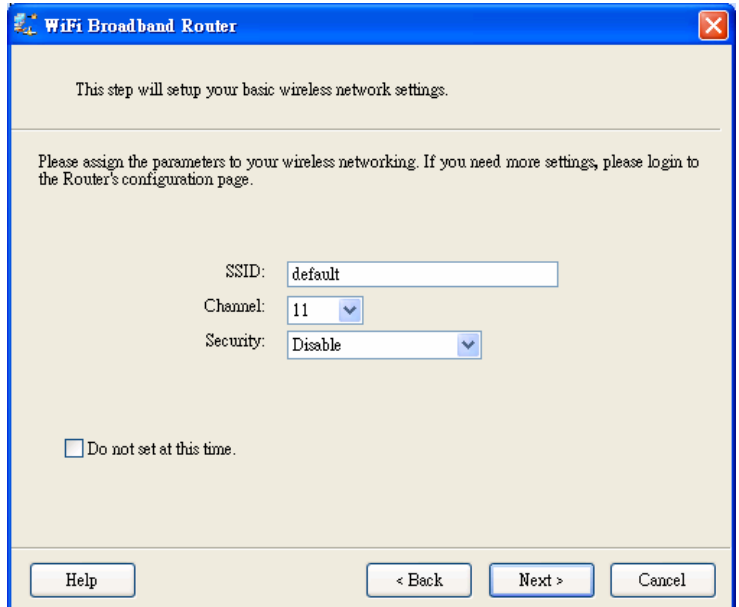
1. Make sure the router is powered on.
2. Make sure your network adapter is connected to the LAN port of the router
3. Make sure your network adapter has an IP address.

Click "Next" for continues



2.5. Wireless Setting.

Key in the SSID, Channel and Security options, and then click “Next” for continues.



The screenshot shows a window titled "WiFi Broadband Router" with a close button in the top right corner. The main content area contains the following text and controls:

This step will setup your basic wireless network settings.

Please assign the parameters to your wireless networking. If you need more settings, please login to the Router's configuration page.

SSID:

Channel:

Security:

Do not set at this time.

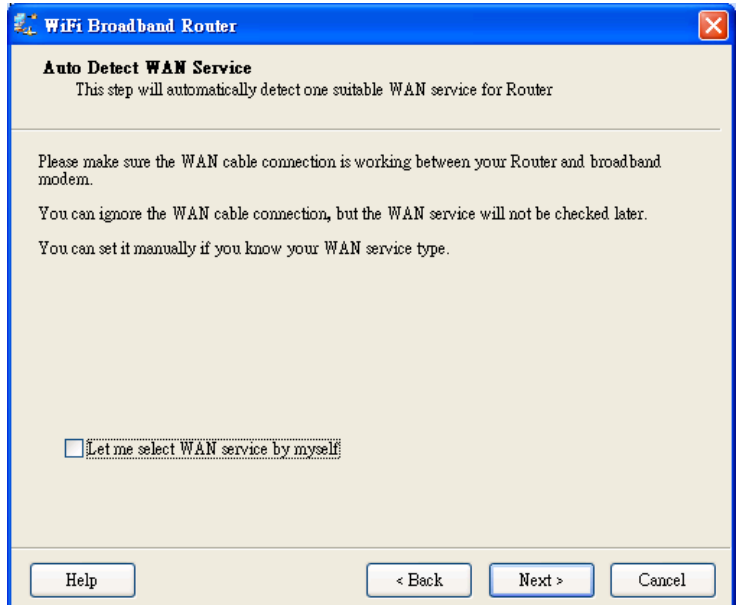
At the bottom of the window, there are four buttons: "Help", "< Back", "Next >", and "Cancel".

2.6 Auto Detect WAN Service.

Click “Next” for continue.

Click the button, “Let me select WAN service by myself”, to disable this function.

Note: The Item supports to detect the Dynamic and PPPoE WAN Services only



The screenshot shows a window titled "WiFi Broadband Router" with a close button in the top right corner. The main content area contains the following text and controls:

Auto Detect WAN Service

This step will automatically detect one suitable WAN service for Router

Please make sure the WAN cable connection is working between your Router and broadband modem.

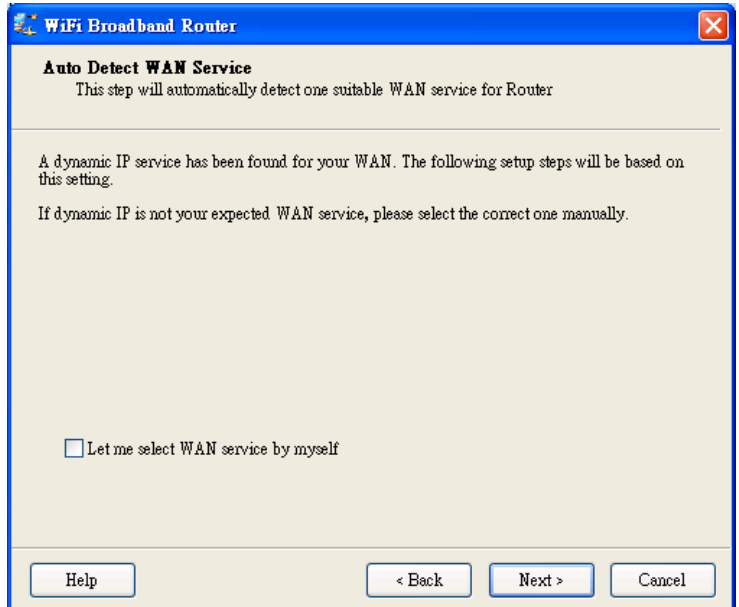
You can ignore the WAN cable connection, but the WAN service will not be checked later.

You can set it manually if you know your WAN service type.

Let me select WAN service by myself

At the bottom of the window, there are four buttons: "Help", "< Back", "Next >", and "Cancel".

Example, the Dynamic WAN type is detected.

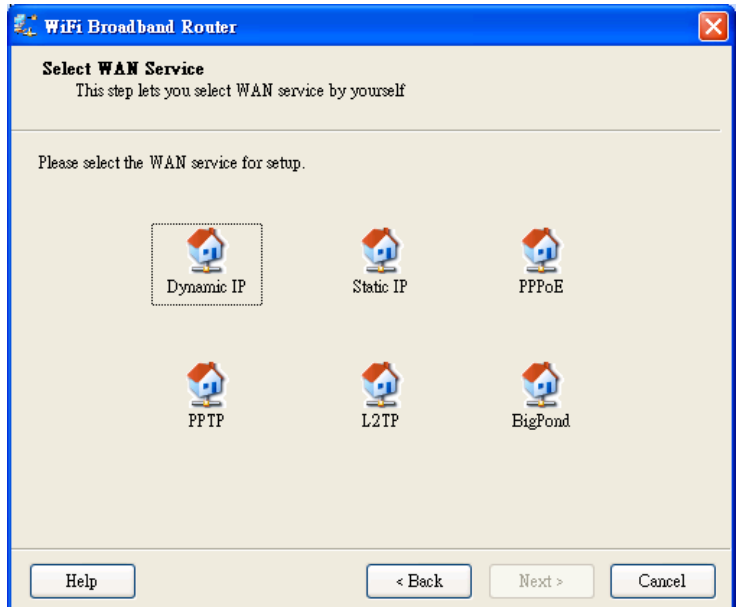


2.7. Manual select WAN Service

In the manual mode, Click the any icons for continues.

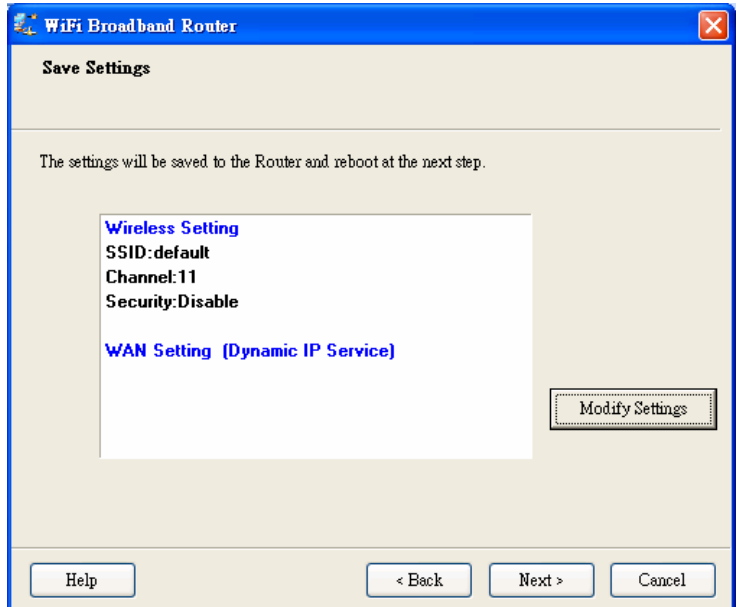
2.8 Summary of the settings and Next to "Reboot"

Click "Next" for continue.



2.9 Apply the Settings or Modify.

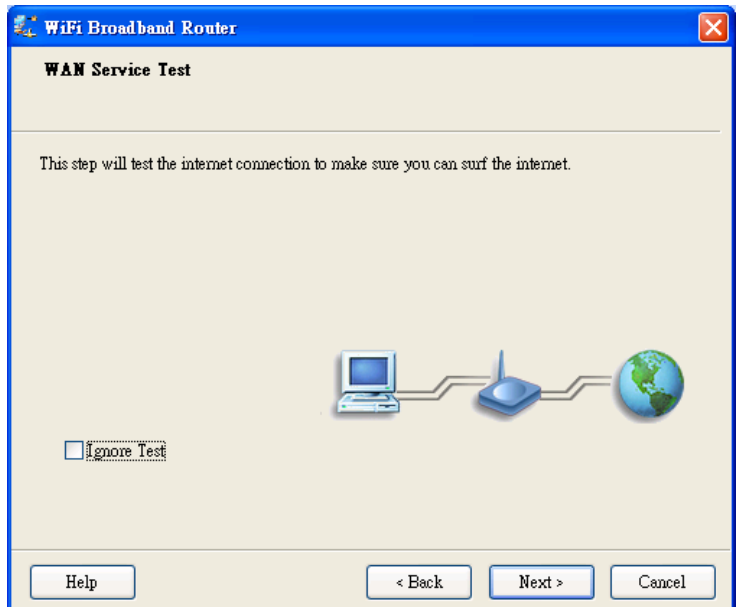
Click "Next" for continue.



2.10 Test the Internet connection.

Test WAN Networking service. Click "Next" for continue.

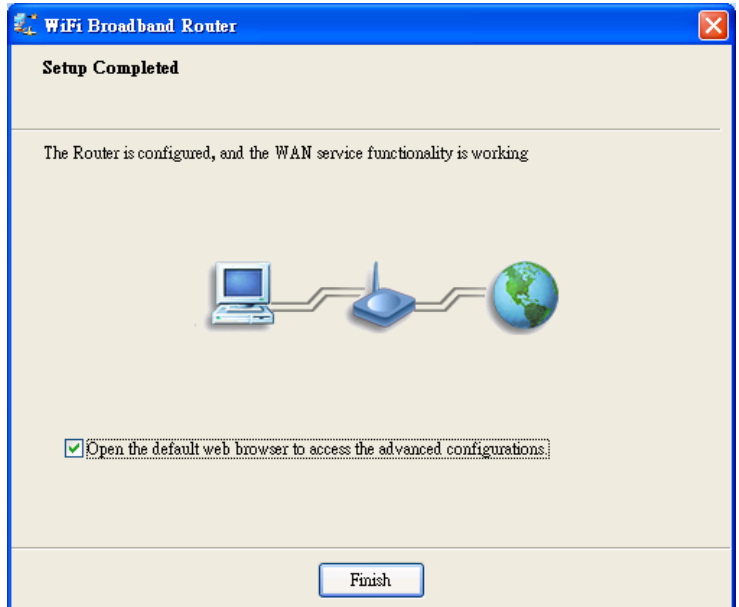
You can ignore the by select the "Ignore Test".



2.11 Setup Completed.

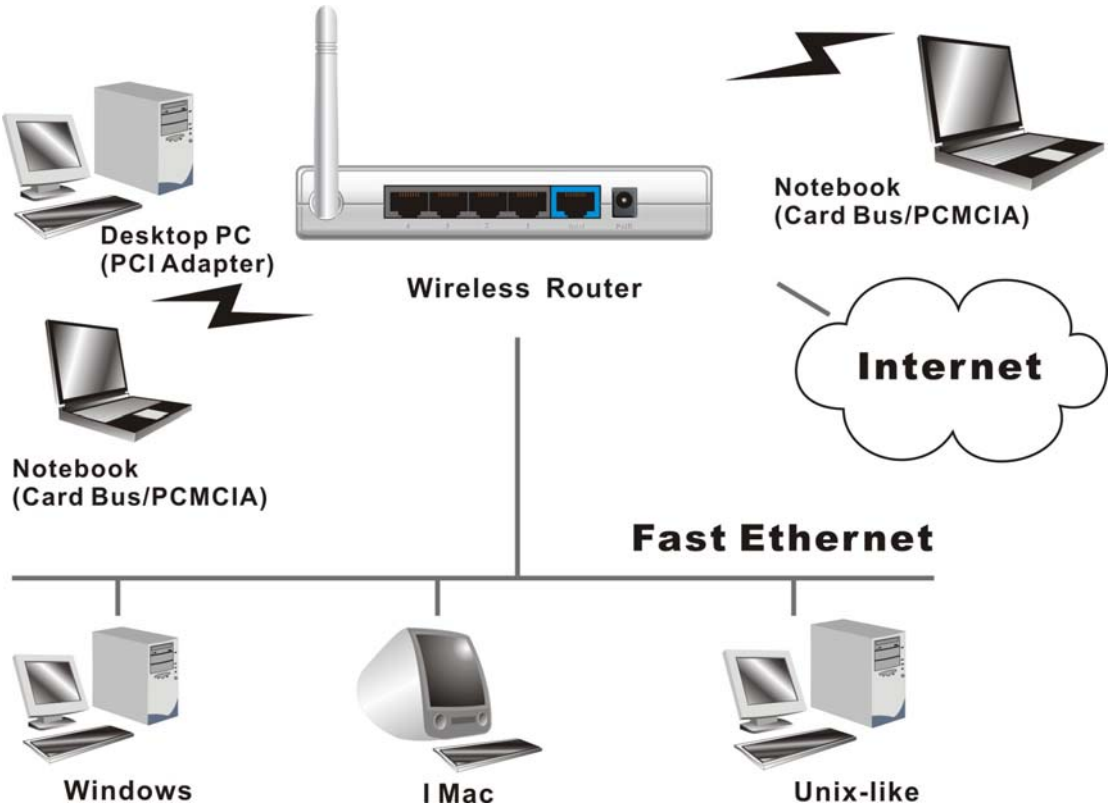
The EzSetup is finish, you can open the default web browser to configure advanced settings of the Router.

Click "Finish" to complete the installation.



Chapter 3 Making Configuration

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



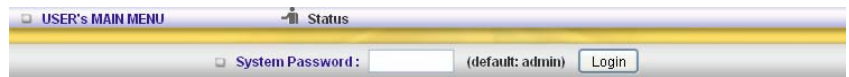
3.1 Login to Configure from Wizard

Type in the IP Address

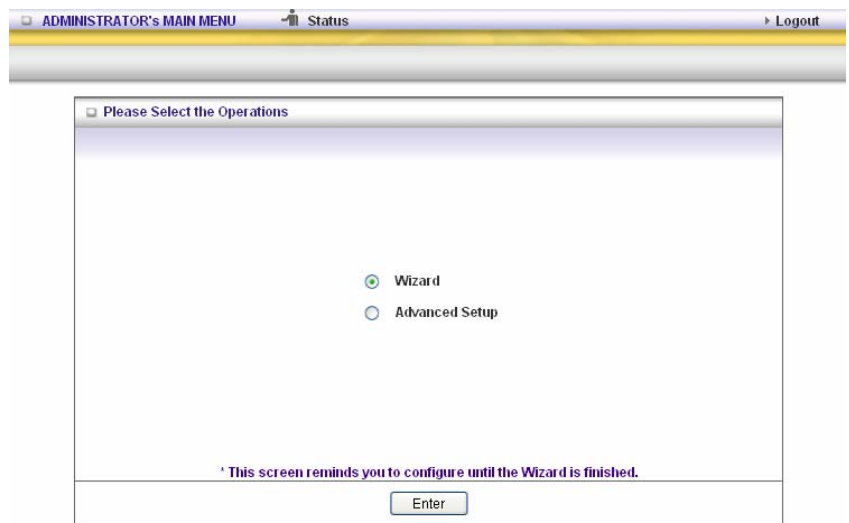
(<http://192.168.123.254>)



Type password, the default is "admin" and click 'login' button.



Press "Wizard" for basic settings with simple way.



Press "Next" to start wizard.



Step 1:
Set up your system password.

ADMINISTRATOR's MAIN MENU Status Wizard Advanced Logout

Setup Wizard - Setup Login Password [EXIT]

▶ Old Password

▶ New Password

▶ Reconfirm

< Back [Start > **Password** > WAN > Wireless > Summary > Finish!] Next >

Step 2:
Select Wan Type.

Auto Detecting or
Setup Manually.

ADMINISTRATOR's MAIN MENU Status Wizard Advanced Logout

Setup Wizard - WAN Type Setup [EXIT]

Auto Detecting WAN Type

Setup WAN Type Manually

< Back [Start > Password > **WAN** > Wireless > Summary > Finish!] Next >

ADMINISTRATOR's MAIN MENU Status Wizard Advanced Logout

Setup Wizard - Select WAN Type [EXIT]

ISP assigns you a static IP address. (Static IP Address)

Obtain an IP address from ISP automatically. (Dynamic IP Address)

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

Some ISPs require the use of PPPoE to connect to their services. (PPP over Ethernet)

Some ISPs require the use of PPTP to connect to their services. (PPTP)

Some ISPs require the use of L2TP to connect to their services. (L2TP)

< Back [Start > Password > Wireless > Summary > Finish!] Next >

Step 3:
Setup the LAN IP and WAN
Type.

ADMINISTRATOR'S MAIN MENU Status Wizard Advanced Logout

Setup Wizard - WAN Settings - Dynamic IP Address [EXIT]

▶ LAN IP Address: 192.168.122.224

▶ Host Name: (optional)

▶ WAN's MAC Address: 00-1A-72-12-A8-89 Restore MAC

< Back [Start > Password > **WAN** > Wireless > Summary > Finish!] Next >

Example:

Step 4:
Please fill in PPPoE service
information which is provided by
your ISP.

ADMINISTRATOR'S MAIN MENU Status Wizard Advanced Logout

Setup Wizard - WAN Settings - PPP over Ethernet [EXIT]

▶ LAN IP Address: 192.168.122.224

▶ Account:

▶ Password:

▶ Primary DNS: 0.0.0.0

▶ Secondary DNS: 0.0.0.0

▶ PPPoE Service Name: (optional)

▶ Assigned IP Address: 0.0.0.0 (optional)

< Back [Start > Password > Wireless > Summary > Finish!] Next >

Step 5:
Set up your Wireless.

ADMINISTRATOR'S MAIN MENU Status Wizard Advanced Logout

Setup Wizard - Wireless settings [EXIT]

▶ Wireless function: Enable Disable

▶ Network ID(SSID): default

▶ Channel: Auto

< Back [Start > Password > WAN > **Wireless** > Summary > Finish!] Next >

Set up your Authentication and Encryption.

The screenshot shows the 'Setup Wizard - Wireless Security' page. On the left, a tree view shows 'Security' expanded, with sub-items 'WEP', 'Key 1', 'Key 2', 'Key 3', and 'Key 4'. The 'WEP' section is active, showing a dropdown menu set to 'WEP', radio buttons for '64 bits' (selected) and '128 bits', and a text input field containing '1234567890'. Below the input fields, a note states: 'Please configure 26 for 128bits or 10 for 64 bits hexadecimal (0, 1, 2...8, 9, A, B...F) digits.' At the bottom, there are '< Back' and 'Next >' buttons, and a breadcrumb trail: '[Start > Password > WAN > **Wireless** > Summary > Finish!]'.

Step 6:
Then click Apply Setting.
And then the device will reboot.

The screenshot shows the 'Setup Wizard - Summary' page. It prompts the user to 'Please confirm the information below.' and displays a table with the following settings:

| | |
|-----------------------------|--------------------|
| [WAN Setting] | |
| WAN Type | Dynamic IP Address |
| Host Name | - |
| WAN's MAC Address | 00-1A-72-12-A8-89 |
| [Wireless Setting] | |
| Wireless | Enable |
| SSID | default |
| Channel | 11 |
| Security | 64-bit WEP Enabled |

Below the table, there is a checkbox labeled 'Do you want to proceed the network testing?'. At the bottom, there are '< Back' and 'Apply Settings' buttons, and a breadcrumb trail: '[Start > Password > WAN > Wireless > **Summary** > Finish!]'.

Step 7:
Click Finish to complete it.

The screenshot shows the 'Setup Wizard' completion screen. The main heading is 'Configuration is Completed.' Below this, it says: 'Please click "Finish" to back to Status page. Or you can click "Configure Again" to setup the wizard again.' At the bottom, there are 'Configure Again' and 'Finish' buttons, and a breadcrumb trail: '[Start > Password > WAN > Wireless > Summary > **Finish!**]'.

3.2 System Status

| ADMINISTRATOR's MAIN MENU Status Wizard Advanced Logout | | |
|---|----------------------------|--|
| System Status [HELP] | | |
| Item | WAN Status | Sidenote |
| Remaining Lease Time | 00:09:54 | <input type="button" value="Renew"/> |
| IP Address | 192.168.122.139 | <input type="button" value="Release"/> |
| Subnet Mask | 255.255.255.0 | |
| Gateway | 192.168.122.210 | |
| Domain Name Server | 192.168.123.10, 168.95.1.1 | |
| MAC Address | 00-1A-72-12-A8-89 | |
| Wireless Status | | |
| Item | WLAN Status | Sidenote |
| Wireless mode | Enable | |
| SSID | default | |
| Channel | Auto | |
| Security | WEP | 64-bit WEP |
| MAC Address | 00-50-18-00-0F-E0 | |

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

WAN Port Status.

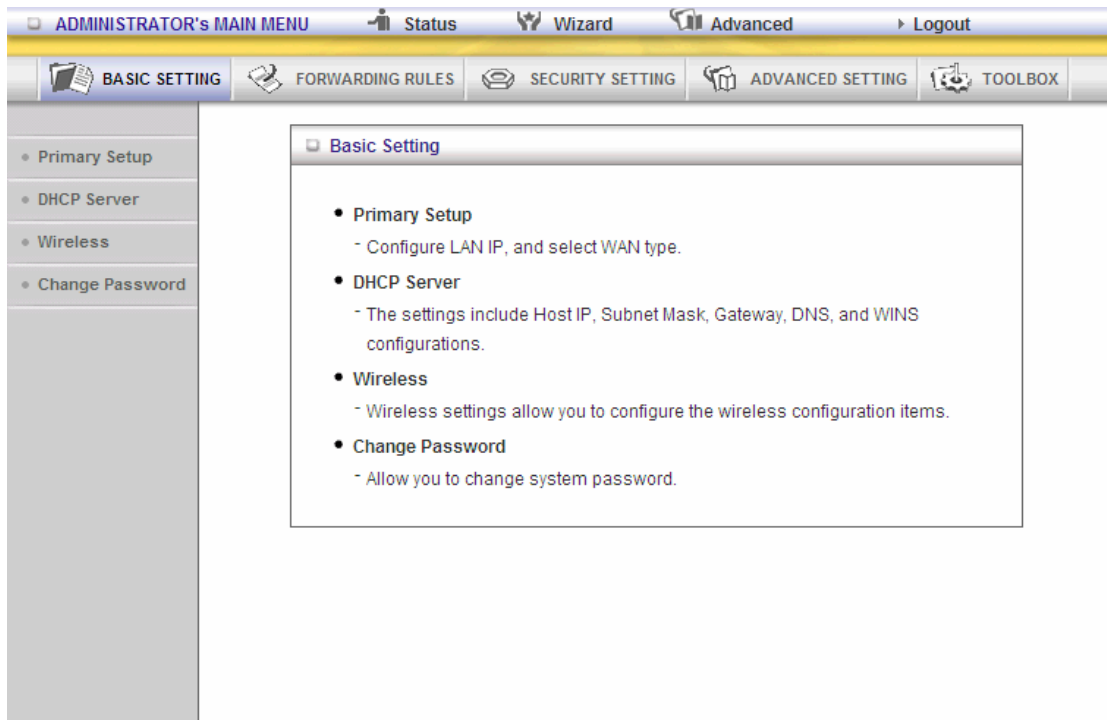
If the WAN port is assigned a dynamic IP, there may appear a "**Renew**" or "**Release**" button on the Sidenote column. You can click this button to renew or release IP manually.

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

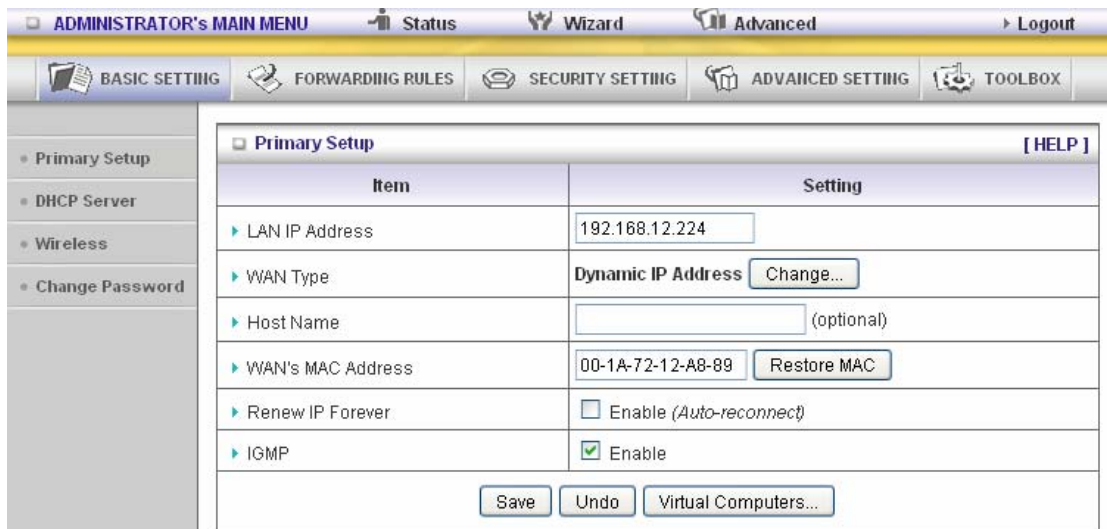
3.3 Advanced

3.3.1 Basic Setting

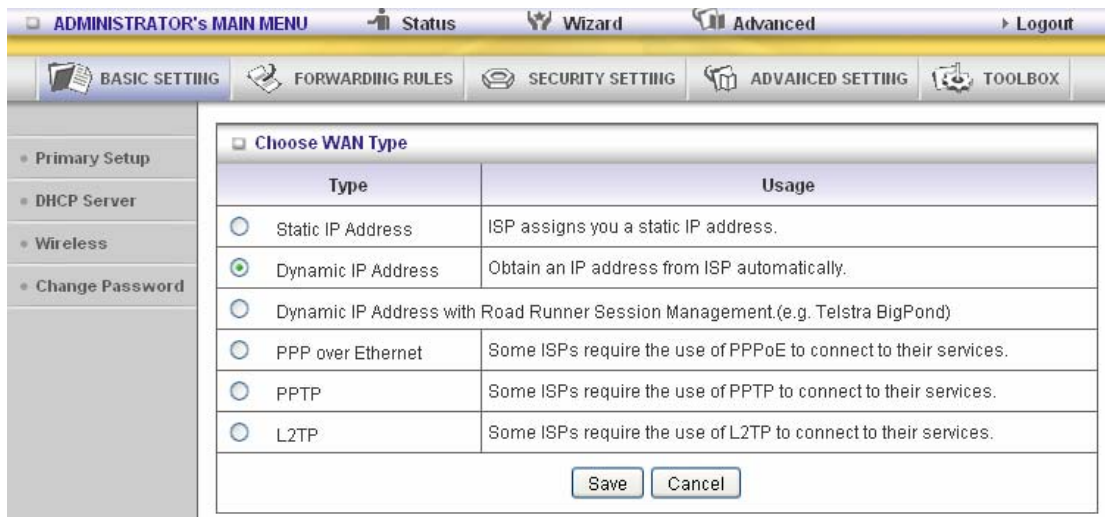
Please Select "Advanced Setup" to Setup



3.3.1.1 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. PPP over Ethernet: Some ISPs require the use of PPPoE to connect to their services.
 - D. 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

Static IP Address: ISP assigns you a static IP address:

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

ADMINISTRATOR's MAIN MENU Status Wizard Advanced Logout

BASIC SETTING FORWARDING RULES SECURITY SETTING ADVANCED SETTING TOOLBOX

- Primary Setup
- DHCP Server
- Wireless
- Change Password

| Primary Setup [HELP] | |
|------------------------|--|
| Item | Setting |
| ▶ LAN IP Address | 192.168.12.224 |
| ▶ WAN Type | Static IP Address <input type="button" value="Change..."/> |
| ▶ WAN IP Address | 0.0.0.0 |
| ▶ WAN Subnet Mask | 255.255.255.0 |
| ▶ WAN Gateway | 0.0.0.0 |
| ▶ Primary DNS | 0.0.0.0 |
| ▶ Secondary DNS | 0.0.0.0 |
| ▶ IGMP | <input checked="" type="checkbox"/> Enable |

Saved! The change doesn't take effect until router is rebooted.

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

Host Name: optional. Required by some ISPs, for example, @Home.

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.

ADMINISTRATOR's MAIN MENU Status Wizard Advanced Logout

BASIC SETTING FORWARDING RULES SECURITY SETTING ADVANCED SETTING TOOLBOX

- Primary Setup
- DHCP Server
- Wireless
- Change Password

| Primary Setup [HELP] | |
|------------------------|--|
| Item | Setting |
| ▶ LAN IP Address | 192.168.12.224 |
| ▶ WAN Type | Dynamic IP Address <input type="button" value="Change..."/> |
| ▶ Host Name | <input type="text"/> (optional) |
| ▶ WAN's MAC Address | 00-1A-72-12-A8-89 <input type="button" value="Restore MAC"/> |
| ▶ Renew IP Forever | <input type="checkbox"/> Enable (Auto-reconnect) |
| ▶ IGMP | <input checked="" type="checkbox"/> Enable |

Saved! The change doesn't take effect until router is rebooted.

PPP over Ethernet: Some ISPs require the use of PPPoE to connect to their services.

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.

PPPoE Service Name: optional. Input the service name if your ISP requires it. Otherwise, leave it blank.

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.

Maximum Transmission Unit (MTU): Most ISP offers MTU value to users. The most common MTU value is 1492.

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 Status-page.

The screenshot shows the 'Primary Setup' configuration page. The interface includes a top navigation bar with 'ADMINISTRATOR's MAIN MENU', 'Status', 'Wizard', 'Advanced', and 'Logout'. Below this is a secondary navigation bar with 'BASIC SETTING', 'FORWARDING RULES', 'SECURITY SETTING', 'ADVANCED SETTING', and 'TOOLBOX'. The main content area is titled 'Primary Setup' and contains a table of settings:

| Item | Setting |
|---------------------|--|
| LAN IP Address | 192.168.12.224 |
| WAN Type | PPP over Ethernet <input type="button" value="Change..."/> |
| PPPoE Account | <input type="text"/> |
| PPPoE Password | <input type="password" value="....."/> |
| Primary DNS | 0.0.0.0 |
| Secondary DNS | 0.0.0.0 |
| Maximum Idle Time | 300 seconds |
| Connection Control | Connect-on-demand <input type="button" value="v"/> |
| PPPoE Service Name | <input type="text"/> (optional) |
| Assigned IP Address | 0.0.0.0 (optional) |
| MTU | 1492 |
| IGMP | <input checked="" type="checkbox"/> Enable |

At the bottom of the table are three buttons: 'Save', 'Undo', and 'Reboot'.

PPTP: Some ISPs require the use of PPTP to connect to their services

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.

4. Connection ID: optional. Input the connection ID if your ISP requires it.

5. Maximum Idle Time: the time of no activity to disconnect your PPTP session. Set it to zero or

enable Auto-reconnect to disable this feature. If Auto-reconnect is enabled, this product will connect to ISP automatically, after system is restarted or connection is dropped.

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.

| Item | Setting |
|------------------------|--|
| LAN IP Address | 192.168.12.224 |
| WAN Type | PPTP <input type="button" value="Change..."/> |
| IP Mode | Static IP Address <input type="button" value="v"/> |
| My IP Address | 0.0.0.0 |
| My Subnet Mask | 255.255.255.0 |
| Gateway IP | 0.0.0.0 |
| Server IP Address/Name | <input type="text"/> |
| PPTP Account | <input type="text"/> |
| PPTP Password | ••••• |
| Connection ID | <input type="text"/> (optional) |
| Maximum Idle Time | 300 seconds |
| Connection Control | Connect-on-demand <input type="button" value="v"/> |
| MTU | 1460 |
| IGMP | <input checked="" type="checkbox"/> Enable |

L2TP: Some ISPs require the use of L2TP to connect to their services

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.

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.

| ADMINISTRATOR's MAIN MENU | | Status | Wizard | Advanced | Logout | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
|---|---|------------------|------------------|------------------|---------|------|---------|------------------|----------------|------------|---|-----------|--|--------------|---------|---------------|---------------|------------------|---------|--------------------------|----------------------|----------------|----------------------|-----------------|-------|---------------------|-------------|----------------------|--|-------|------|--------|--|
| BASIC SETTING | | FORWARDING RULES | SECURITY SETTING | ADVANCED SETTING | TOOLBOX | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| <ul style="list-style-type: none"> Primary Setup DHCP Server Wireless Change Password | <div style="text-align: right;">[HELP]</div> <table border="1"> <thead> <tr> <th>Item</th> <th>Setting</th> </tr> </thead> <tr> <td>▶ LAN IP Address</td> <td>192.168.12.224</td> </tr> <tr> <td>▶ WAN Type</td> <td>L2TP <input type="button" value="Change..."/></td> </tr> <tr> <td>▶ IP Mode</td> <td>Static IP Address <input type="button" value="v"/></td> </tr> <tr> <td>▶ IP Address</td> <td>0.0.0.0</td> </tr> <tr> <td>▶ Subnet Mask</td> <td>255.255.255.0</td> </tr> <tr> <td>▶ WAN Gateway IP</td> <td>0.0.0.0</td> </tr> <tr> <td>▶ Server IP Address/Name</td> <td><input type="text"/></td> </tr> <tr> <td>▶ L2TP Account</td> <td><input type="text"/></td> </tr> <tr> <td>▶ L2TP Password</td> <td>•••••</td> </tr> <tr> <td>▶ Maximum Idle Time</td> <td>300 seconds</td> </tr> <tr> <td>▶ Connection Control</td> <td>Connect-on-demand <input type="button" value="v"/></td> </tr> <tr> <td>▶ MTU</td> <td>1460</td> </tr> <tr> <td>▶ IGMP</td> <td><input checked="" type="checkbox"/> Enable</td> </tr> </table> | | | | | Item | Setting | ▶ LAN IP Address | 192.168.12.224 | ▶ WAN Type | L2TP <input type="button" value="Change..."/> | ▶ IP Mode | Static IP Address <input type="button" value="v"/> | ▶ IP Address | 0.0.0.0 | ▶ Subnet Mask | 255.255.255.0 | ▶ WAN Gateway IP | 0.0.0.0 | ▶ Server IP Address/Name | <input type="text"/> | ▶ L2TP Account | <input type="text"/> | ▶ L2TP Password | ••••• | ▶ Maximum Idle Time | 300 seconds | ▶ Connection Control | Connect-on-demand <input type="button" value="v"/> | ▶ MTU | 1460 | ▶ IGMP | <input checked="" type="checkbox"/> Enable |
| Item | Setting | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| ▶ LAN IP Address | 192.168.12.224 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| ▶ WAN Type | L2TP <input type="button" value="Change..."/> | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| ▶ IP Mode | Static IP Address <input type="button" value="v"/> | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| ▶ IP Address | 0.0.0.0 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| ▶ Subnet Mask | 255.255.255.0 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| ▶ WAN Gateway IP | 0.0.0.0 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| ▶ Server IP Address/Name | <input type="text"/> | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| ▶ L2TP Account | <input type="text"/> | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| ▶ L2TP Password | ••••• | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| ▶ Maximum Idle Time | 300 seconds | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| ▶ Connection Control | Connect-on-demand <input type="button" value="v"/> | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| ▶ MTU | 1460 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| ▶ IGMP | <input checked="" type="checkbox"/> Enable | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |

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

ADMINISTRATOR's MAIN MENU Status Wizard Advanced Logout

BASIC SETTING FORWARDING RULES SECURITY SETTING ADVANCED SETTING TOOLBOX

Primary Setup
DHCP Server
Wireless
Change Password

Allow you to setup the one-to-one mapping of multiple global IP address and local IP address.

Virtual Computers [HELP]

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

| ID | Global IP | Local IP | Enable |
|----|----------------------|----------------------------------|--------------------------|
| 1 | <input type="text"/> | 192.168.12. <input type="text"/> | <input type="checkbox"/> |
| 2 | <input type="text"/> | 192.168.12. <input type="text"/> | <input type="checkbox"/> |
| 3 | <input type="text"/> | 192.168.12. <input type="text"/> | <input type="checkbox"/> |
| 4 | <input type="text"/> | 192.168.12. <input type="text"/> | <input type="checkbox"/> |
| 5 | <input type="text"/> | 192.168.12. <input type="text"/> | <input type="checkbox"/> |

Save Undo

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

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

3.3.1.2 DHCP Server

ADMINISTRATOR's MAIN MENU Status Wizard Advanced Logout

BASIC SETTING FORWARDING RULES SECURITY SETTING ADVANCED SETTING TOOLBOX

Primary Setup
DHCP Server
Wireless
Change Password

DHCP Server [HELP]

| Item | Setting |
|----------------------------|---|
| ▶ DHCP Server | <input type="radio"/> Disable <input checked="" type="radio"/> Enable |
| ▶ Lease Time | <input type="text" value="5"/> Minutes |
| ▶ IP Pool Starting Address | <input type="text" value="100"/> |
| ▶ IP Pool Ending Address | <input type="text" value="199"/> |
| ▶ Domain Name | <input type="text"/> |
| ▶ Primary DNS | <input type="text" value="0.0.0.0"/> |
| ▶ Secondary DNS | <input type="text" value="0.0.0.0"/> |
| ▶ Primary WINS | <input type="text" value="0.0.0.0"/> |
| ▶ Secondary WINS | <input type="text" value="0.0.0.0"/> |
| ▶ Gateway | <input type="text" value="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.
8. **DHCP Client List:**



3.3.1.3 Wireless Setting

| Item | Setting |
|------------------|---|
| Wireless | <input checked="" type="radio"/> Enable <input type="radio"/> Disable |
| Network ID(SSID) | default |
| Wireless Mode | <input checked="" type="radio"/> Mixed mode <input type="radio"/> 11g only <input type="radio"/> 11b only |
| SSID Broadcast | <input checked="" type="radio"/> Enable <input type="radio"/> Disable |
| Channel | Auto |
| WDS | Enter... |
| WPS | Enter... |
| Security | WEP |
| Key Mode | HEX |
| WEP | <input checked="" type="radio"/> 64 bits <input type="radio"/> 128 bits |
| Key 1 | <input checked="" type="radio"/> 1234567890 |
| Key 2 | <input type="radio"/> [Empty] |
| Key 3 | <input type="radio"/> [Empty] |
| Key 4 | <input type="radio"/> [Empty] |

Buttons: 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,

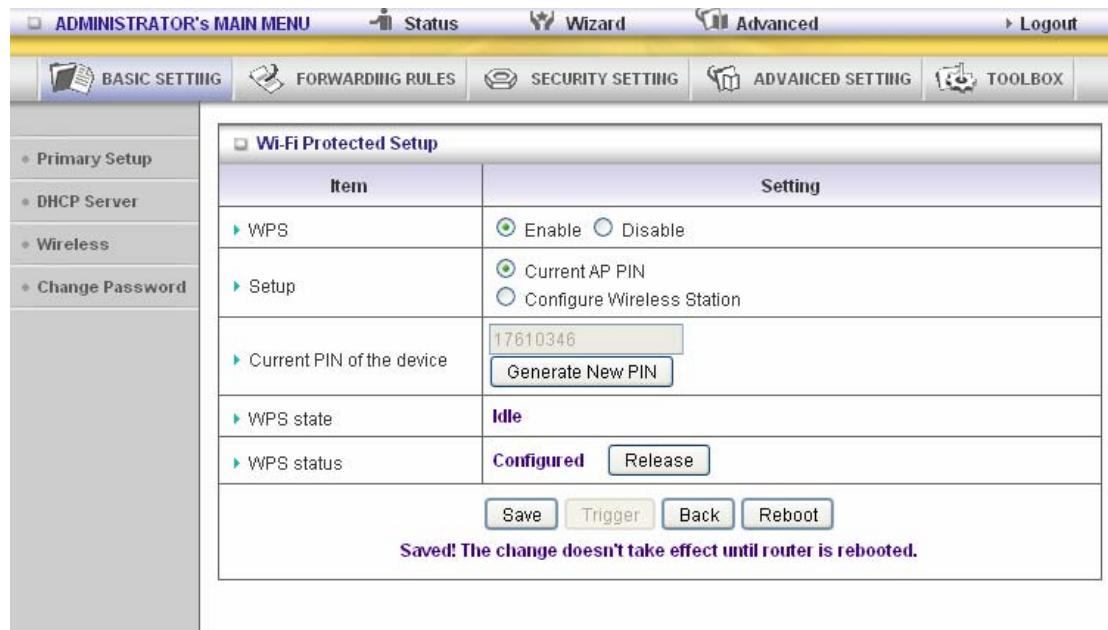
This function is disabled, the wireless clients can not find the device from beacons.

Channel: The radio channel number. The permissible channels depend on the Regulatory Domain.

WPS (WiFi Protection Setup)

WPS is WiFi Protection Setup which is similar to WCN-NET and offers safe and

easy way in Wireless Connection.



ADMINISTRATOR's MAIN MENU Status Wizard Advanced Logout

BASIC SETTING FORWARDING RULES SECURITY SETTING ADVANCED SETTING TOOLBOX

- Primary Setup
- DHCP Server
- Wireless
- Change Password

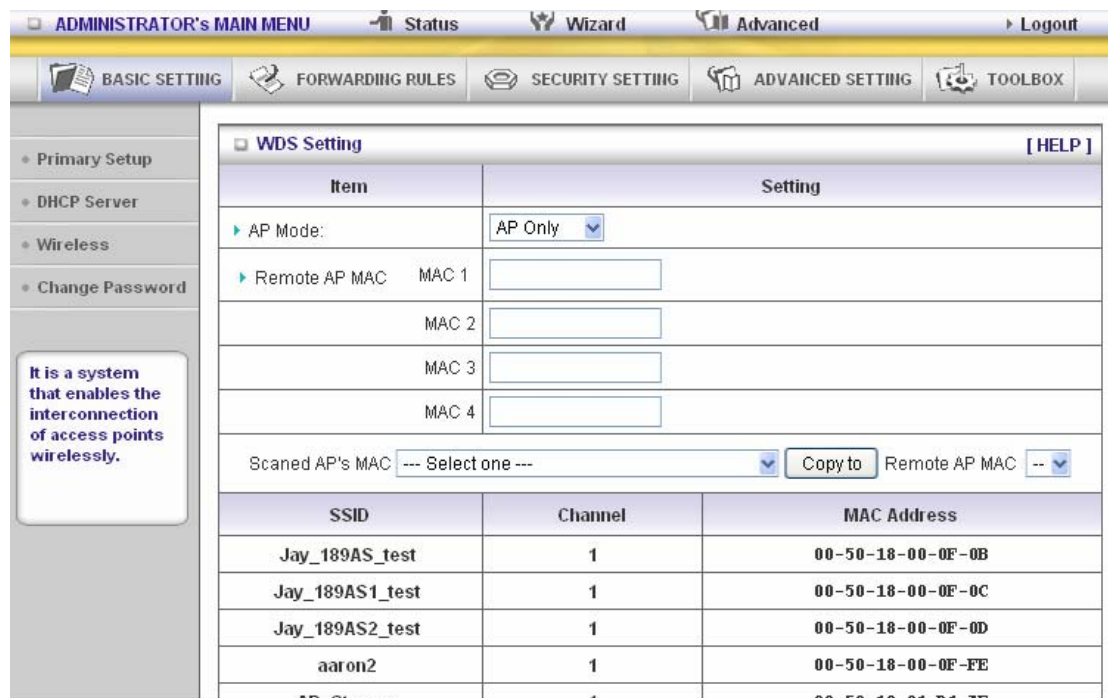
Wi-Fi Protected Setup

| Item | Setting |
|---------------------------|---|
| WPS | <input checked="" type="radio"/> Enable <input type="radio"/> Disable |
| Setup | <input checked="" type="radio"/> Current AP PIN <input type="radio"/> Configure Wireless Station |
| Current PIN of the device | 17610346 <input type="button" value="Generate New PIN"/> |
| WPS state | Idle |
| WPS status | Configured <input type="button" value="Release"/> |

Saved! The change doesn't take effect until router is rebooted.

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.



ADMINISTRATOR's MAIN MENU Status Wizard Advanced Logout

BASIC SETTING FORWARDING RULES SECURITY SETTING ADVANCED SETTING TOOLBOX

- Primary Setup
- DHCP Server
- Wireless
- Change Password

WDS Setting [HELP]

| Item | Setting |
|------------------|--|
| AP Mode: | AP Only |
| Remote AP MAC | MAC 1: <input type="text"/> MAC 2: <input type="text"/> MAC 3: <input type="text"/> MAC 4: <input type="text"/> |
| Scanned AP's MAC | --- Select one --- <input type="button" value="Copy to"/> Remote AP MAC -- |

| SSID | Channel | MAC Address |
|-----------------|---------|-------------------|
| Jay_189AS_test | 1 | 00-50-18-00-0E-0B |
| Jay_189AS1_test | 1 | 00-50-18-00-0E-0C |
| Jay_189AS2_test | 1 | 00-50-18-00-0E-0D |
| aaron2 | 1 | 00-50-18-00-0E-FE |
| AP Storage | 1 | 00-50-18-21-D1-7F |

It is a system that enables the interconnection of access points wirelessly.

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 'Wireless Setting' configuration page. 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', 'ADVANCED SETTING', and 'TOOLBOX'. The left sidebar contains a tree view with 'Primary Setup', 'DHCP Server', 'Wireless', and 'Change Password'. The main content area is titled 'Wireless Setting' and contains a table with the following items and settings:

| Item | Setting |
|-----------------------|---|
| Wireless | <input checked="" type="radio"/> Enable <input type="radio"/> Disable |
| Network ID(SSID) | default |
| Wireless Mode | <input checked="" type="radio"/> Mixed mode <input type="radio"/> 11g only <input type="radio"/> 11b only |
| SSID Broadcast | <input checked="" type="radio"/> Enable <input type="radio"/> Disable |
| Channel | Auto |
| WDS | Enter... |
| WPS | Enter... |
| 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 | |

At the bottom of the table are three buttons: 'Save', 'Undo', and 'Wireless Client List...'.

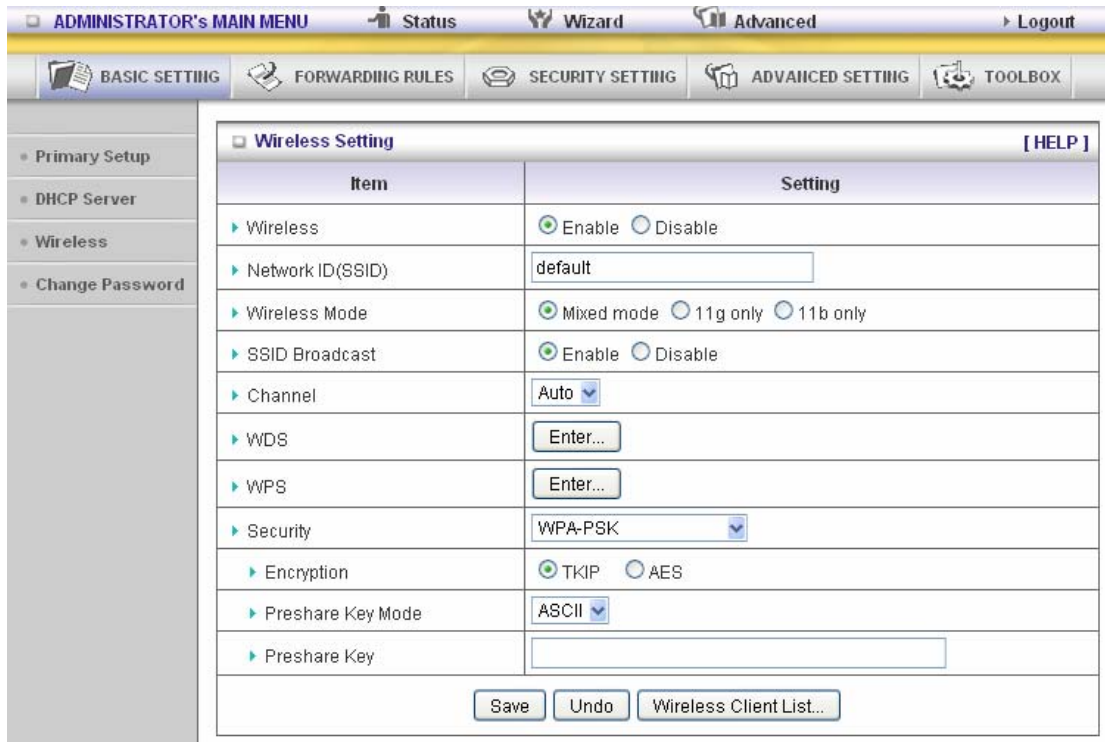
WPA-PSK

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



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

ADMINISTRATOR'S MAIN MENU Status Wizard Advanced Logout

BASIC SETTING FORWARDING RULES SECURITY SETTING ADVANCED SETTING TOOLBOX

- Primary Setup
- DHCP Server
- Wireless
- Change Password

Wireless Setting [HELP]

| Item | Setting |
|-------------------|---|
| Wireless | <input checked="" type="radio"/> Enable <input type="radio"/> Disable |
| Network ID(SSID) | default |
| Wireless Mode | <input checked="" type="radio"/> Mixed mode <input type="radio"/> 11g only <input type="radio"/> 11b only |
| SSID Broadcast | <input checked="" type="radio"/> Enable <input type="radio"/> Disable |
| Channel | Auto |
| WDS | Enter... |
| WPS | Enter... |
| Security | WPA-PSK / WPA2-PSK |
| Encryption | TKIP + AES |
| Preshare Key Mode | ASCII |
| Preshare Key | |

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.

Wireless Client List

ADMINISTRATOR's MAIN MENU Status Wizard Advanced Logout

BASIC SETTING FORWARDING RULES SECURITY SETTING ADVANCED SETTING TOOLBOX

- Primary Setup
- DHCP Server
- Wireless
- Change Password

Wireless Client List

| Connected Time | MAC Address |
|--------------------------|-------------------|
| Tue Jan 26 09:39:58 2010 | 00-1C-BF-00-C6-37 |

Back Refresh

3.3.1.4 Change Password

ADMINISTRATOR's MAIN MENU Status Wizard Advanced Logout

BASIC SETTING FORWARDING RULES SECURITY SETTING ADVANCED SETTING TOOLBOX

- Primary Setup
- DHCP Server
- Wireless
- Change Password

Change Password

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

Save Undo

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

3.3.2 Forwarding Rules

ADMINISTRATOR's MAIN MENU Status Wizard Advanced Logout

BASIC SETTING FORWARDING RULES SECURITY SETTING ADVANCED SETTING TOOLBOX

- Virtual Server
- Special AP
- Miscellaneous

Forwarding Rules

- Virtual Server**
 - Allows others to access WWW, FTP, and other services on your LAN.
- Special Application**
 - This configuration allows some applications to connect, and work with the NAT router.
- Miscellaneous**
 - IP Address of DMZ Host: Allows a computer to be exposed to unrestricted 2-way communication. Note that, this feature should be used only when needed.
 - 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.

3.3.2.1 Virtual Server

ADMINISTRATOR's MAIN MENU Status Wizard Advanced Logout

BASIC SETTING FORWARDING RULES SECURITY SETTING ADVANCED SETTING TOOLBOX

Virtual Server [HELP]

Well known services: POP3 (110)

Schedule rule: (00)Always Copy to ID: 3

| ID | Server IP | Service Ports | Protocol | Enable | Schedule Rule# |
|----|----------------|---------------|----------|-------------------------------------|----------------|
| 1 | 192.168.12.123 | 21 | Both | <input checked="" type="checkbox"/> | 0 |
| 2 | 192.168.12.1 | 25 | Both | <input checked="" type="checkbox"/> | 0 |
| 3 | 192.168.12.1 | 110 | Both | <input checked="" type="checkbox"/> | 0 |
| 4 | 192.168.12. | | Both | <input type="checkbox"/> | 0 |
| 5 | 192.168.12. | | Both | <input type="checkbox"/> | 0 |
| 6 | 192.168.12. | | Both | <input type="checkbox"/> | 0 |
| 7 | 192.168.12. | | Both | <input type="checkbox"/> | 0 |
| 8 | 192.168.12. | | Both | <input type="checkbox"/> | 0 |
| 9 | 192.168.12. | | Both | <input type="checkbox"/> | 0 |
| 10 | 192.168.12. | | 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**.

3.3.2.2 Special AP

ADMINISTRATOR's MAIN MENU Status Wizard Advanced Logout

BASIC SETTING FORWARDING RULES SECURITY SETTING ADVANCED SETTING TOOLBOX

Virtual Server
Special AP
Miscellaneous

Special Applications [HELP]

Popular applications: MSN Gaming Zone Copy to: ID 2

| ID | Trigger | Incoming Ports | Enable |
|----|---------|-----------------------|-------------------------------------|
| 1 | 7175 | 51200-51201,51210 | <input checked="" type="checkbox"/> |
| 2 | 47624 | 2300-2400,28800-29000 | <input checked="" type="checkbox"/> |
| 3 | | | <input type="checkbox"/> |
| 4 | | | <input type="checkbox"/> |
| 5 | | | <input type="checkbox"/> |
| 6 | | | <input type="checkbox"/> |
| 7 | | | <input type="checkbox"/> |
| 8 | | | <input type="checkbox"/> |

Save Undo

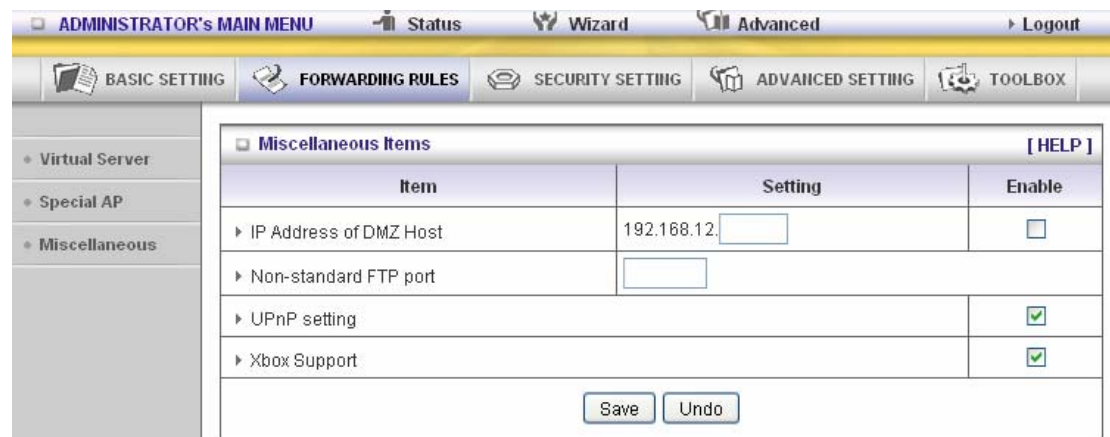
Some applications require multiple connections, like Internet games, Video conferencing, Internet telephony, etc. Because of the firewall function, these applications cannot work with a pure NAT router. The **Special Applications** feature allows some of these applications to work with this product.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

3.3.2.3 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.

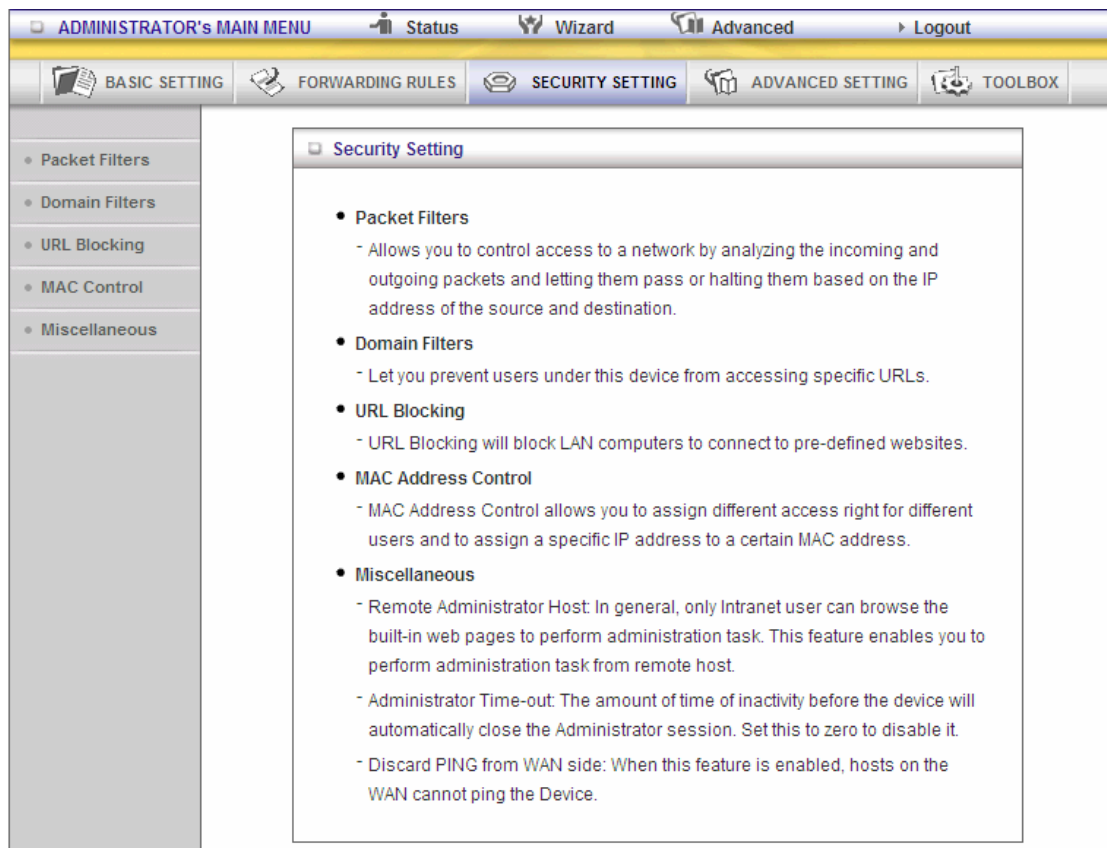
UpnP Setting

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





3.3.3 Security Settings



3.3.3.1 Packet Filters

| ID | Source IP | Destination IP : Ports | Enable | Schedule Rule# |
|----|-----------|------------------------|--------------------------|----------------|
| 1 | | : 20-21 | <input type="checkbox"/> | 0 |
| 2 | | : 80 | <input type="checkbox"/> | 0 |
| 3 | | : 443 | <input type="checkbox"/> | 0 |
| 4 | | : 53 | <input type="checkbox"/> | 0 |
| 5 | | : 25 | <input type="checkbox"/> | 0 |
| 6 | | : 110 | <input type="checkbox"/> | 0 |
| 7 | | : 23 | <input type="checkbox"/> | 0 |
| 8 | | : | <input type="checkbox"/> | 0 |

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**.

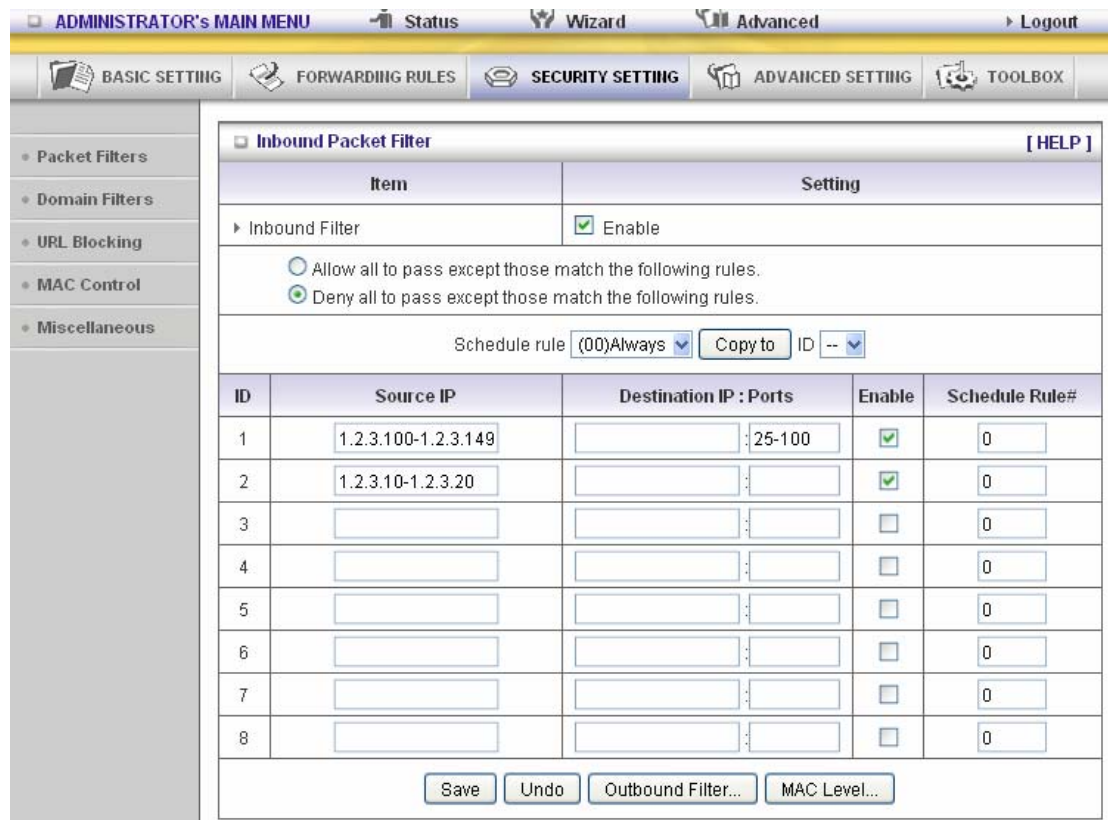
Each rule can be enabled or disabled individually.

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) Remote hosts are allow to send mail (port 25), and browse the Internet (port 80)

(1.2.3.10-1.2.3.20) Remote hosts can do everything (block nothing)

Others are all blocked.

Example 2:

ADMINISTRATOR's MAIN MENU Status Wizard Advanced Logout

BASIC SETTING FORWARDING RULES SECURITY SETTING ADVANCED SETTING TOOLBOX

- 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. | | | | |
| Schedule rule (00)Always Copy to ID -- | | | | |
| ID | Source IP | Destination IP : Ports | Enable | Schedule Rule# |
| 1 | 1.2.3.100-1.2.3.199 | : 21 | <input checked="" type="checkbox"/> | 0 |
| 2 | 1.2.3.100-1.2.3.199 | : 199 | <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 |

(1.2.3.100-1.2.3.119) Remote hosts can do everything except read net news (port 119) and transfer files via FTP (port 21) behind Router Server.

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:

Router LAN IP is 192.168.12.254

Inbound Packet Filter [HELP]

| Item | Setting | | | |
|--|--|------------------------|-------------------------------------|----------------|
| ▶ Inbound 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 Copy to ID -- | | | | |
| ID | Source IP | Destination IP : Ports | Enable | Schedule Rule# |
| 1 | 100-192.168.12.149 | : 21-100 | <input checked="" type="checkbox"/> | 0 |
| 2 | 2.10-192.168.12.20 | : | <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 |

Save Undo Outbound Filter... MAC Level...

(192.168.12.100-192.168.12.149) Located hosts are only 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.

(192.168.12.10-192.168.12.20) Located hosts can do everything (block nothing)
Others are all blocked.

Example 2:

Router LAN IP is 192.168.12.254

The screenshot shows the 'Inbound Packet Filter' configuration page. The interface includes a top 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 lists filter categories: 'Packet Filters', 'Domain Filters', 'URL Blocking', 'MAC Control', and 'Miscellaneous'. The main content area is titled 'Inbound Packet Filter' and includes a '[HELP]' link. It features a table with columns for 'Item' and 'Setting'. The 'Inbound Filter' is enabled. There are two radio buttons: 'Allow all to pass except those match the following rules.' (selected) and 'Deny all to pass except those match the following rules.'. Below this is a 'Schedule rule' dropdown set to '(00)Always' and a 'Copy to ID' dropdown. A table lists 8 rules with columns for 'ID', 'Source IP', 'Destination IP : Ports', 'Enable', and 'Schedule Rule#'. Rules 1 and 2 are enabled, while rules 3-8 are disabled. At the bottom are buttons for 'Save', 'Undo', 'Outbound Filter...', and 'MAC Level...'.

| Item | Setting | | | |
|--|--|------------------------|-------------------------------------|----------------|
| ▶ Inbound Filter | <input checked="" type="checkbox"/> Enable | | | |
| <input checked="" type="radio"/> Allow all to pass except those match the following rules. <input type="radio"/> Deny all to pass except those match the following rules. | | | | |
| Schedule rule (00)Always <input type="button" value="Copy to ID --"/> | | | | |
| ID | Source IP | Destination IP : Ports | Enable | Schedule Rule# |
| 1 | 192.168.12.100 | : 21 | <input checked="" type="checkbox"/> | 0 |
| 2 | 192.168.12.119 | : 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 |
| 7 | | : | <input type="checkbox"/> | 0 |
| 8 | | : | <input type="checkbox"/> | 0 |

(192.168.12.100 and 192.168.12.119) Located Hosts 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.

3.3.3.2 Domain filters

Domain Filter [HELP]

| Item | Setting |
|------------------------------|--|
| Domain Filter | <input checked="" type="checkbox"/> Enable |
| Log DNS Query | <input type="checkbox"/> Enable |
| Privilege IP Addresses Range | From <input type="text" value="1"/> To <input type="text" value="10"/> |

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

Domain Filter

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

Domain Filter Enable

Check if you want to enable Domain Filter.

Log DNS Query

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

Privilege IP Addresses Range

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

Domain Suffix

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

Action

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

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

Enable

Check to enable each rule.

Example:

ADMINISTRATOR's MAIN MENU Status Wizard Advanced 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="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.baidu.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.baidu.com” will be blocked, but the action will not be record in log-file.
4. IP address x.x.x.1~x.x.x.99 can access Internet without restriction.

3.3.3.3 URL Blocking

ADMINISTRATOR's MAIN MENU Status Wizard Advanced 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 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"/> |

Save Undo

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

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

URL Blocking Enable

Checked if you want to enable URL Blocking.

URL

If any part of the Website's URL matches the pre-defined word, the connection will be blocked. For example, you can use pre-defined word "sex" to block all websites if their URLs contain pre-defined word "sex".

Enable

Checked to enable each rule.

ADMINISTRATOR'S MAIN MENU Status Wizard Advanced Logout

BASIC SETTING FORWARDING RULES SECURITY SETTING ADVANCED SETTING TOOLBOX

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

URL Blocking [HELP]

| Item | Setting | |
|----------------|--|-------------------------------------|
| ▶ URL Blocking | <input checked="" type="checkbox"/> Enable | |
| ID | URL | Enable |
| 1 | <input type="text" value="msn"/> | <input checked="" type="checkbox"/> |
| 2 | <input type="text" value="sina"/> | <input checked="" 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"/> |

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

3.3.3.4 MAC control

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

The configuration options are as follows:

- MAC Address Control:** Enable
- Connection control:** Connection control. Description: Wireless and wired clients with **C** checked can connect to this device; and **allow** unspecified MAC addresses to connect.
- Association control:** Association control. Description: Wireless clients with **A** checked can associate to the wireless LAN; and **deny** unspecified MAC addresses to associate. **Note: Association control has no effect on wired clients.**

Below the settings is a 'DHCP clients' dropdown menu (set to '--- Select one ---') and a 'Copy to ID' dropdown menu (set to '--').

| 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"/> |

At the bottom of the table are navigation buttons: '<< Previous', 'Next >>', 'Save', and '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 |
|----|----------------------|----------------------------------|--------------------------|--------------------------|
| 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.

The image shows a user interface element consisting of a combobox labeled "DHCP clients" with the text "-- select one --" and a dropdown arrow. To its right is a button labeled "Copy to" followed by another combobox labeled "ID" with "--" and a dropdown arrow.

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:

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 C checked can connect to this device; and allow unspecified MAC addresses to connect. |
| <input checked="" type="checkbox"/> Association control | Wireless clients with A checked can associate to the wireless LAN; and deny unspecified MAC addresses to associate. Note: Association control has no effect on wired clients. |

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

| ID | MAC Address | IP Address | C | A |
|----|-------------------|----------------|-------------------------------------|-------------------------------------|
| 1 | 00-12-34-56-78-90 | 192.168.12.100 | <input type="checkbox"/> | <input checked="" type="checkbox"/> |
| 2 | 00-12-34-56-78-92 | 192.168.12. | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |
| 3 | 00-09-76-54-32-10 | 192.168.12.101 | <input checked="" type="checkbox"/> | <input type="checkbox"/> |
| 4 | | 192.168.12. | <input type="checkbox"/> | <input type="checkbox"/> |

<< Previous Next >> Save Undo

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

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

ID 1 - "00-12-34-56-78-90" --> 192.168.12.100

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

3.3.3.5 Miscellaneous Items

| Item | Setting | Enable |
|----------------------------------|----------------------------|-------------------------------------|
| Remote Administrator Host / Port | 0.0.0.0 / 88 | <input type="checkbox"/> |
| Administrator Time-out | 600 seconds (0 to disable) | |
| Discard PING from WAN side | | <input type="checkbox"/> |
| SPI mode | | <input type="checkbox"/> |
| DoS Attack Detection | | <input type="checkbox"/> |
| VPN PPTP Pass-Through | | <input checked="" type="checkbox"/> |
| VPN IPSec Pass-Through | | <input checked="" type="checkbox"/> |

Remote Administrator Host/Port

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

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

Administrator Time-out

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

Discard PING from WAN side

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

SPI Mode

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

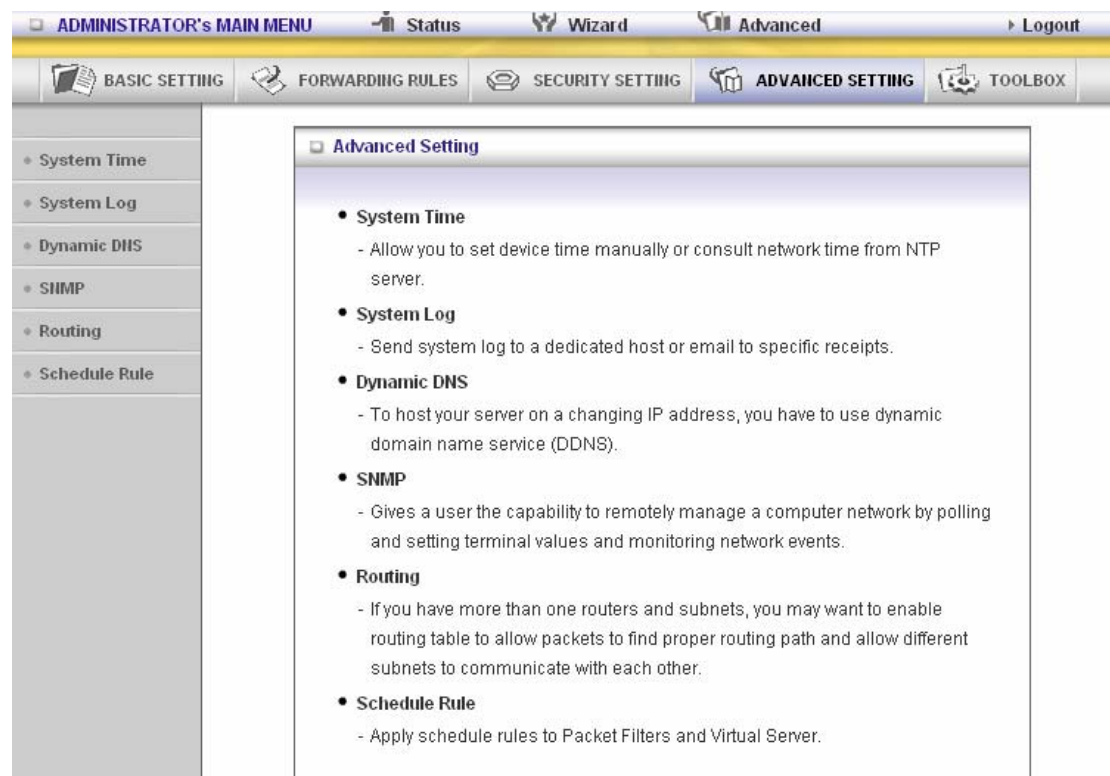
DoS Attack Detection

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

VPN PPTP and IPSec Pass-Through

Virtual Private Networking (VPN) is typically used for work-related networking. For VPN tunnels, the router supports IPSec Passthrough and PPTP Passthrough.

3.3.4 Advanced Settings



The screenshot displays the router's administrative interface. At the top, there is a navigation bar with the following items: ADMINISTRATOR'S MAIN MENU, Status, Wizard, Advanced, and Logout. Below this is a secondary menu with icons and labels for BASIC SETTING, FORWARDING RULES, SECURITY SETTING, ADVANCED SETTING (which is currently selected), and TOOLBOX. On the left side, a vertical sidebar lists several settings categories: System Time, System Log, Dynamic DNS, SNMP, Routing, and Schedule Rule. The main content area is titled "Advanced Setting" and contains a list of five items, each with a brief description:

- **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.

3.3.4.1 System Time

The screenshot shows the 'System Time' configuration page. The interface includes a top navigation bar with 'ADMINISTRATOR's MAIN MENU', 'Status', 'Wizard', 'Advanced', and 'Logout'. Below this is a secondary navigation bar with 'BASIC SETTING', 'FORWARDING RULES', 'SECURITY SETTING', 'ADVANCED SETTING', and 'TOOLBOX'. The main content area is titled 'System Time' and contains the following settings:

| Item | Setting |
|--|--|
| System Time | 2010年1月26日 下午 01:31:56 |
| Get Date and Time by NTP Protocol | <input checked="" type="radio"/> <input type="button" value="Sync Now !"/> |
| Time Server | time.nist.gov |
| Time Zone | (GMT+08:00) Beijing, Hong Kong, Singapore, Taipei |
| Set Date and Time using PC's Date and Time | <input type="radio"/> |
| PC Date and Time | 2010年1月26日 下午 01:31:55 |
| Set Date and Time manually | <input type="radio"/> |
| Date | Year: 2009 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 |
| End | Month: Jan Day: 01 Hour: 00 |

At the bottom of the configuration area are 'Save' and 'Undo' buttons.

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.

3.3.4.2 System Log

| Item | Setting | Enable |
|-------------------------------|--|--------------------------|
| ▶ IP Address of Syslog Server | 192.168.12. [input] | <input type="checkbox"/> |
| ▶ E-mail Alert | [Send Mail Now] | <input type="checkbox"/> |
| • SMTP Server IP/Port | [input] | |
| • E-mail addresses | [input] | |
| • E-mail Subject | [input] | |
| • User name | [input] | |
| • 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 | |

[View Log...] [Save] [Undo]

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.

3.3.4.3 Dynamic DNS

The screenshot shows a web-based administrator interface for configuring Dynamic DNS. 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 main content area is titled 'Dynamic DNS' and includes a '[HELP]' link. It features a table with two columns: 'Item' and 'Setting'. The 'DDNS' item has radio buttons for 'Disable' (selected) and 'Enable'. The 'Provider' item has a dropdown menu set to 'DynDNS.org(Dynamic)' and a 'Provider website' button. The 'Host Name', 'Username / E-mail', and 'Password / Key' items each have a corresponding text input field. The 'Password / Key' field is masked with dots. At the bottom of the form are 'Save' and 'Undo' buttons. On the left side of the interface, there is a sidebar menu with options: 'System Time', 'System Log', 'Dynamic DNS', 'SHMP', 'Routing', and 'Schedule Rule'.

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

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.

3.3.4.4 SNMP

| Item | Setting |
|-----------------|---|
| ▶ Enable SNMP | <input checked="" type="checkbox"/> Local <input type="checkbox"/> Remote |
| ▶ Get Community | <input type="text" value="public"/> |
| ▶ Set Community | <input type="text" value="private"/> |
| ▶ IP 1 | <input type="text"/> |
| ▶ IP 2 | <input type="text"/> |
| ▶ IP 3 | <input type="text"/> |
| ▶ IP 4 | <input type="text"/> |
| ▶ SNMP Version | <input type="radio"/> V1 <input checked="" type="radio"/> V2c |

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

Enable SNMP

You must check Local, 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.

IP 1, IP 2, IP 3, IP 4

Input your SNMP Management PC's IP here. User has to configure to where this device should send SNMP Trap message.

SNMP Version

Please select proper SNMP Version that your SNMP Management software supports.

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.

Click on “Save” to store your setting or “Undo” to give up.

3.3.4.5 Routing

The screenshot shows the 'Routing Table' 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 navigation bar with 'BASIC SETTING', 'FORWARDING RULES', 'SECURITY SETTING', 'ADVANCED SETTING', and 'TOOLBOX'. The left sidebar contains a tree view with items: System Time, System Log, Dynamic DNS, SNMP, Routing (selected), and Schedule Rule. The main content area is titled 'Routing Table' and includes a '[HELP]' link. It features a table with two main sections: 'Dynamic Routing' and 'Static Routing'. Under 'Dynamic Routing', there are radio buttons for 'Disable' (selected), 'RIPv1', and 'RIPv2'. Under 'Static Routing', there are radio buttons for 'Disable' (selected) and 'Enable'. Below these is a table with 8 rows and 6 columns: ID, Destination, Subnet Mask, Gateway, Hop, and Enable. Each cell in the table contains an empty text input field. At the bottom of the table, there are 'Save' and 'Undo' buttons.

| Dynamic Routing | | Setting | | | |
|-----------------|----------------------|--|----------------------|----------------------|--------------------------|
| Dynamic Routing | | <input checked="" type="radio"/> Disable <input type="radio"/> RIPv1 <input type="radio"/> RIPv2 | | | |
| Static Routing | | <input checked="" type="radio"/> Disable <input type="radio"/> Enable | | | |
| ID | Destination | Subnet Mask | Gateway | Hop | Enable |
| 1 | <input type="text"/> | <input type="text"/> | <input type="text"/> | <input type="text"/> | <input type="checkbox"/> |
| 2 | <input type="text"/> | <input type="text"/> | <input type="text"/> | <input type="text"/> | <input type="checkbox"/> |
| 3 | <input type="text"/> | <input type="text"/> | <input type="text"/> | <input type="text"/> | <input type="checkbox"/> |
| 4 | <input type="text"/> | <input type="text"/> | <input type="text"/> | <input type="text"/> | <input type="checkbox"/> |
| 5 | <input type="text"/> | <input type="text"/> | <input type="text"/> | <input type="text"/> | <input type="checkbox"/> |
| 6 | <input type="text"/> | <input type="text"/> | <input type="text"/> | <input type="text"/> | <input type="checkbox"/> |
| 7 | <input type="text"/> | <input type="text"/> | <input type="text"/> | <input type="text"/> | <input type="checkbox"/> |
| 8 | <input type="text"/> | <input type="text"/> | <input type="text"/> | <input type="text"/> | <input type="checkbox"/> |

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

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

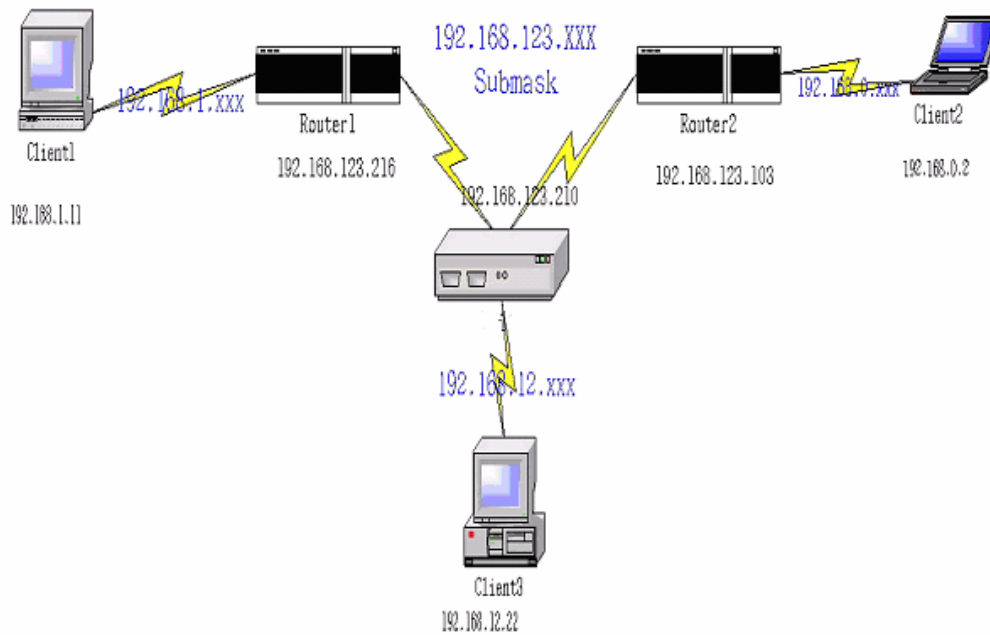
Dynamic Routing

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 | ✓ |

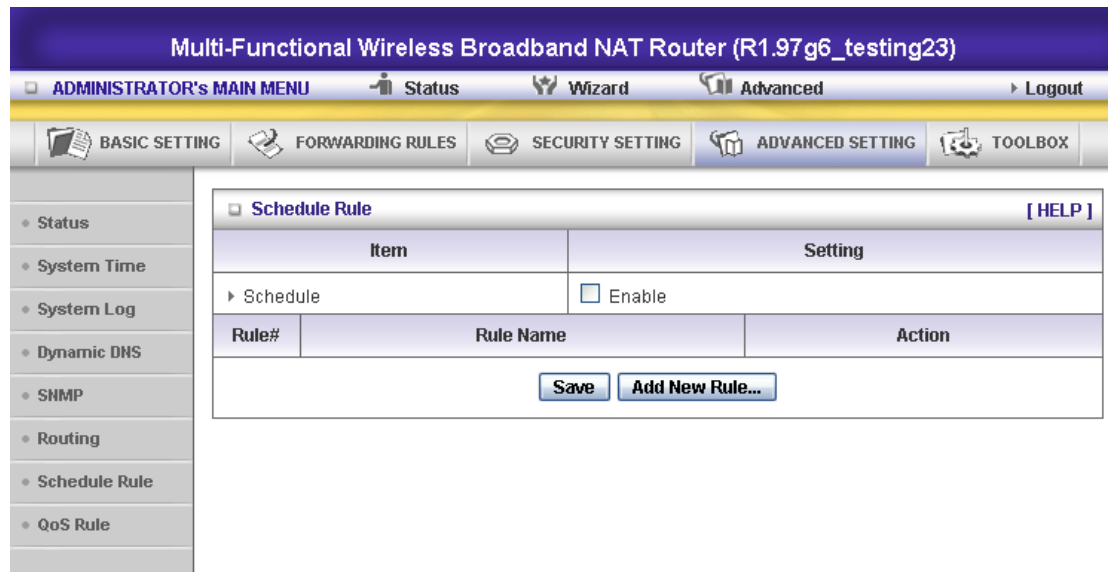
So if, for example, the client3 wanted to send an IP data gram to 192.168.0.2, it would use the above table to determine that it had to go via 192.168.123.103 (a gateway),

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.

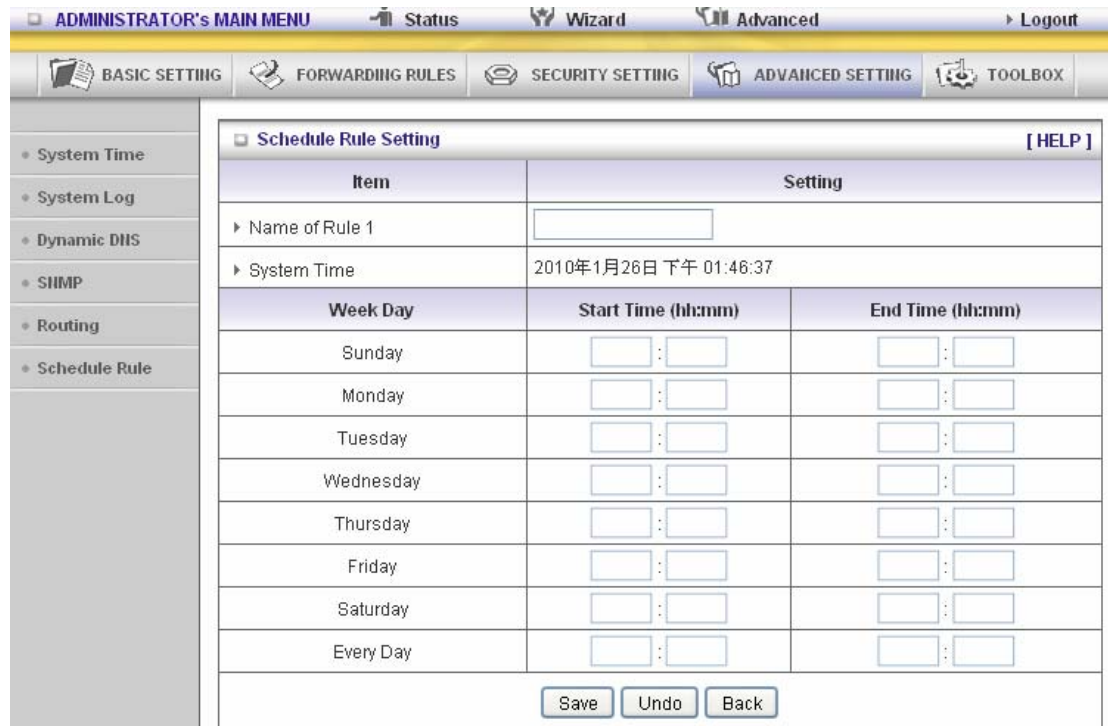
3.3.4.6 Schedule Rule



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)

| ID | Server IP | Service Ports | Protocol | Enable | Schedule Rule# |
|----|--------------|---------------|----------|-------------------------------------|----------------|
| 1 | 192.168.12.1 | 21 | Both | <input checked="" type="checkbox"/> | 1 |
| 2 | 192.168.12. | | Both | <input type="checkbox"/> | 0 |
| 3 | 192.168.12. | | Both | <input type="checkbox"/> | 0 |
| 4 | 192.168.12. | | Both | <input type="checkbox"/> | 0 |
| 5 | 192.168.12. | | Both | <input type="checkbox"/> | 0 |
| 6 | 192.168.12. | | Both | <input type="checkbox"/> | 0 |
| 7 | 192.168.12. | | Both | <input type="checkbox"/> | 0 |
| 8 | 192.168.12. | | Both | <input type="checkbox"/> | 0 |
| 9 | 192.168.12. | | Both | <input type="checkbox"/> | 0 |
| 10 | 192.168.12. | | Both | <input type="checkbox"/> | 0 |

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

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

Outbound Packet Filter [HELP]

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

3.3.5 Toolbox

The screenshot shows the administrator's main menu with the following navigation options: ADMINISTRATOR's MAIN MENU, Status, Wizard, Advanced, and Logout. The main menu is divided into sections: BASIC SETTING, FORWARDING RULES, SECURITY SETTING, ADVANCED SETTING, and TOOLBOX. The TOOLBOX section 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.

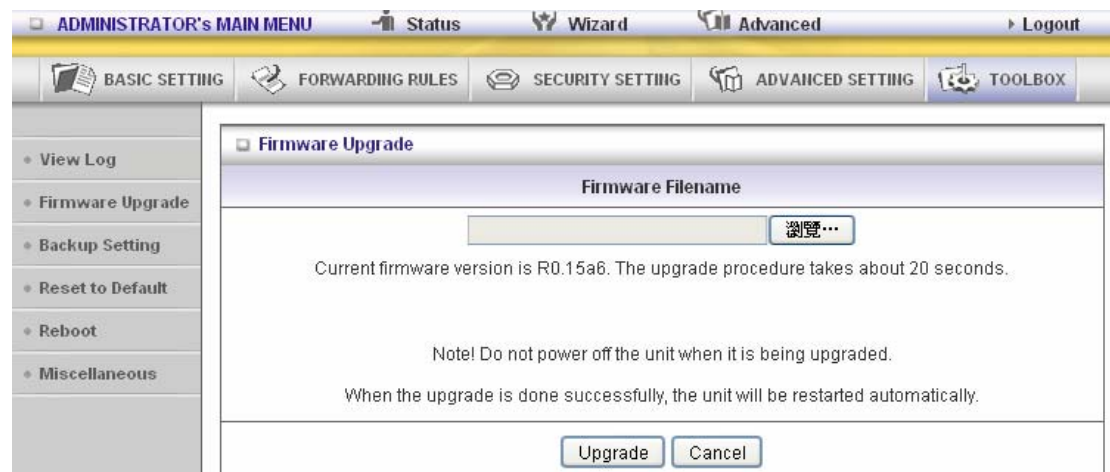
3.3.5.1 View Log

The screenshot shows the administrator's main menu with the following navigation options: ADMINISTRATOR's MAIN MENU, Status, Wizard, Advanced, and Logout. The main menu is divided into sections: BASIC SETTING, FORWARDING RULES, SECURITY SETTING, ADVANCED SETTING, and TOOLBOX. The TOOLBOX section is selected, displaying the System Log section:

| System Log | |
|------------------------|---|
| ITEM | Info |
| WAN Type | Dynamic IP Address (R0.15a6) |
| Display time | Tue Jan 26 14:00:40 2010 |
| Time | Log |
| 2010年1月26日 上午 09:53:29 | Blocked access attempt from 192.168.122.77:2717 to TCP port 27284 |
| 2010年1月26日 上午 09:53:36 | Blocked access attempt from 192.168.122.77:2717 to TCP port 27284 |
| 2010年1月26日 上午 09:55:25 | DHCP:release |
| 2010年1月26日 上午 09:40:03 | Restarted by 192.168.12.149 |
| 2010年1月26日 上午 09:40:04 | == USB OTG Init == |
| 2010年1月26日 上午 09:40:12 | DOD:triggered internally |
| 2010年1月26日 上午 09:40:12 | DHCP:discover(My Host) |
| 2010年1月26日 上午 09:40:12 | DHCP:offer(192.168.122.210) |
| 2010年1月26日 上午 09:40:12 | DHCP:request(192.168.122.191) |
| 2010年1月26日 上午 09:40:15 | DHCP:ack(DOL=600,T1=300,T2=525) |
| 2010年1月26日 上午 09:40:41 | Blocked access attempt from 192.168.122.77:1346 to UDP port 10696 |

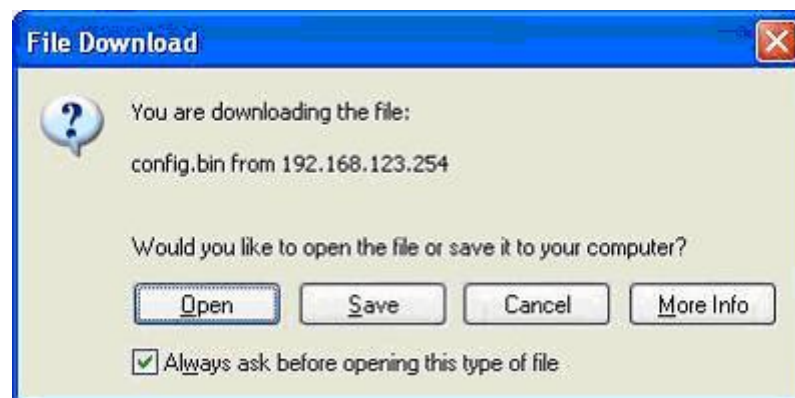
You can View system log by clicking the **View Log** button

3.3.5.2 Firmware Upgrade



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

3.3.5.3 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.

3.3.5.4 Reset to default



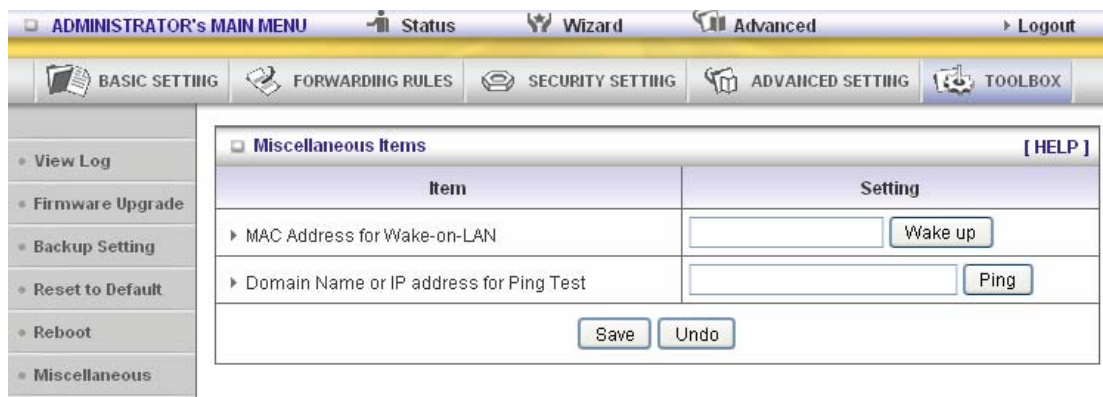
You can also reset this product to factory default by clicking the **Reset to default** button.

3.3.5.5 Reboot



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

3.3.5.6 Miscellaneous Items



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 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: Press Wireless on /off and WPS button simultaneously about 5 sec

Status will start flashing about 5 times, remove the finger. The RESTORE process is completed.

4. 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. |

5. When I use Static IP Address to roam Internet, I can access or ping

global IP 202.93.91.218, But I can not access the site that inputs domain name, for example <http://espn.com> ?

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

How do I connect router by using wireless?

1.How to start to use wireless?

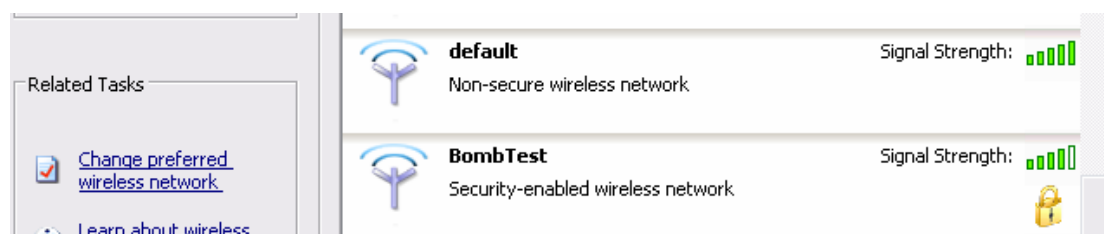
A: First, make sure that you already installed wireless client device in your computer. Then check the Configuration of wireless router. The default is as below:

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

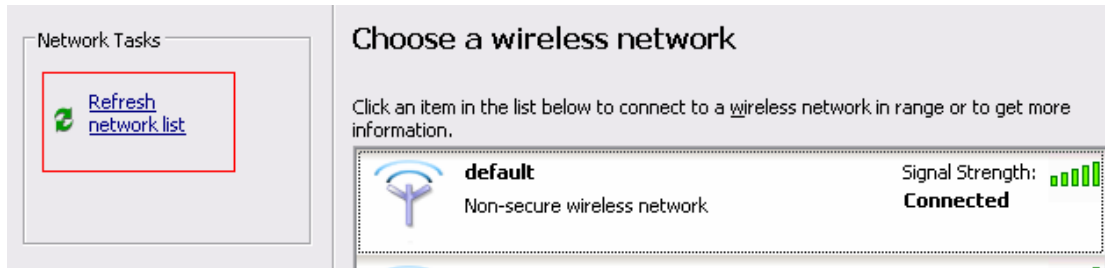
About wireless client, you will see wireless icon:



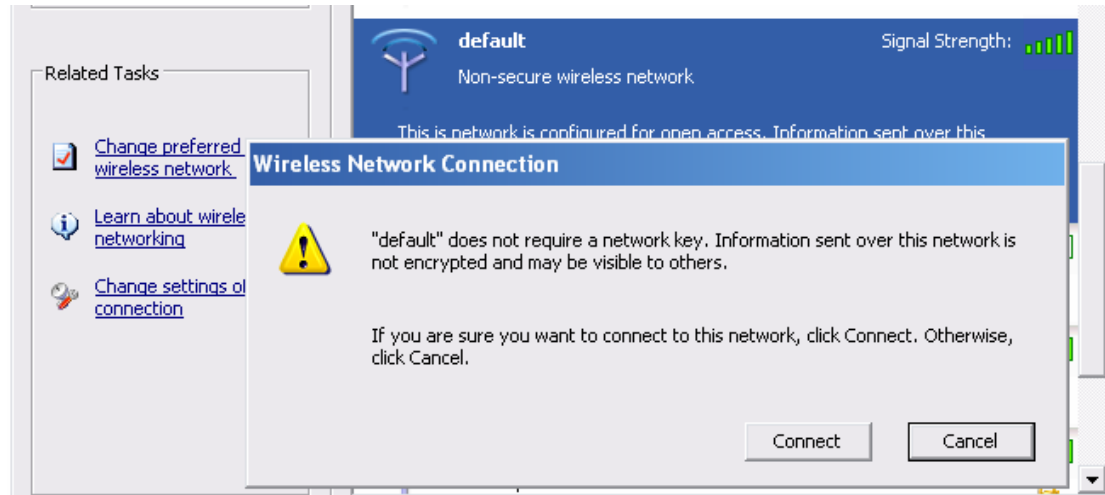
Then click and will see the ap list that wireless client can be accessed:



If the client can not access your wireless router, please refresh network list again. However, I still can not fine 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



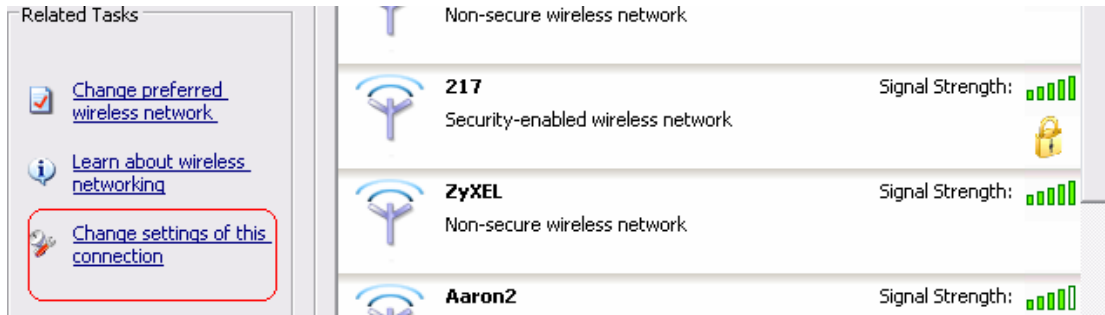
and get ip from router:

```
Ethernet adapter Wireless Network Connection 5:

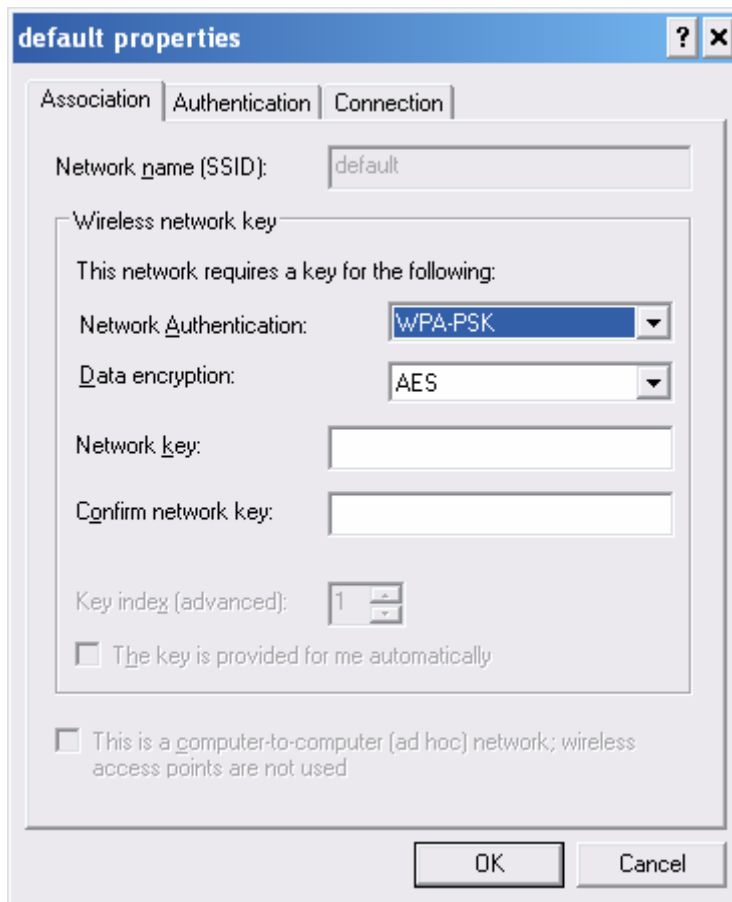
    Connection-specific DNS Suffix  . : 
    IP Address . . . . . : 192.168.123.165
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.123.254
```

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.

Federal Communication Commission 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 harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

FCC Caution: Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.

This 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, and (2) this device must accept any interference received, including interference that may cause undesired operation.

Country Code Statement

For product available in the USA/Canada market, only channel 1~11 can be operated. Selection of other channels is not possible.

Co-located

This device and its antenna(s) must not be co-located or operation in conjunction with any other antenna or transmitter.

IMPORTANT NOTE:

FCC Radiation Exposure Statement:

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment.

This equipment should be installed and operated with minimum distance 20cm between the radiator & your body.